## Configuring Security

**Lab Time**: 45 minutes

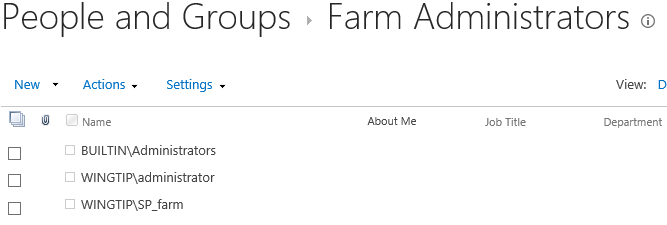
**Lab Folder**: C:\Student\Modules\Security\lab

**Lab Overview**: In the following lab, you will configure various security permission and authentication settings as well as create two new web applications. You will configure the first web application to use Kerberos authentication and you will configure the second web application to authenticate using Basic Authentication with SSL.

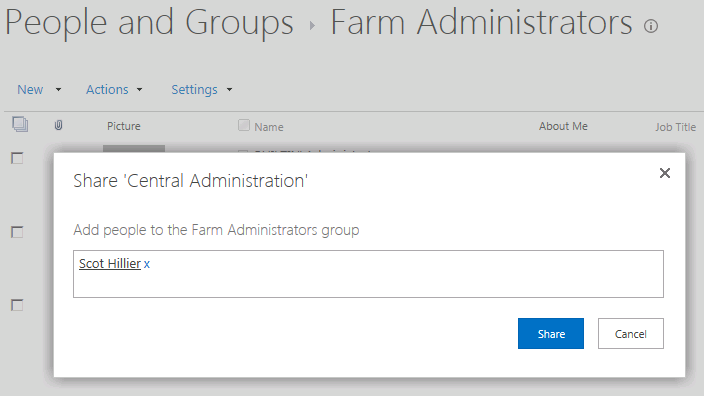
### Exercise 1: Add Active Directory Users as Farm Administrator

In this exercise you will learn how to add an Active Directory user account as a Farm Administrator.

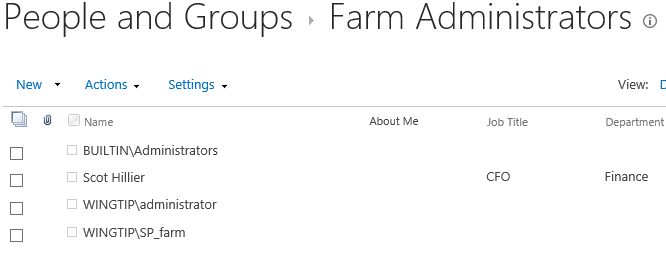
1. Navigate to Central Administration.
2. Click the **Manage the farm administrators group** hyperlink under the **Security** section.
3. You should now be at a page which lists all farm administrator accounts. Notice the accounts that are already there.



1. You can add another farm administrator by clicking the **New** button.
2. Add the user Scot Hillier (**WINGTIP\ScotH**) as a farm administrator.



1. Click the **Share** button to add this user. When the Farm Administrators page refreshes, you should now see this user displayed as a farm administrator.



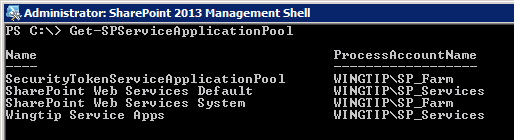
1. Return to the SharePoint Central Administration home page.

In this exercise you configured a user account to provide that user with farm-level administrative permissions.

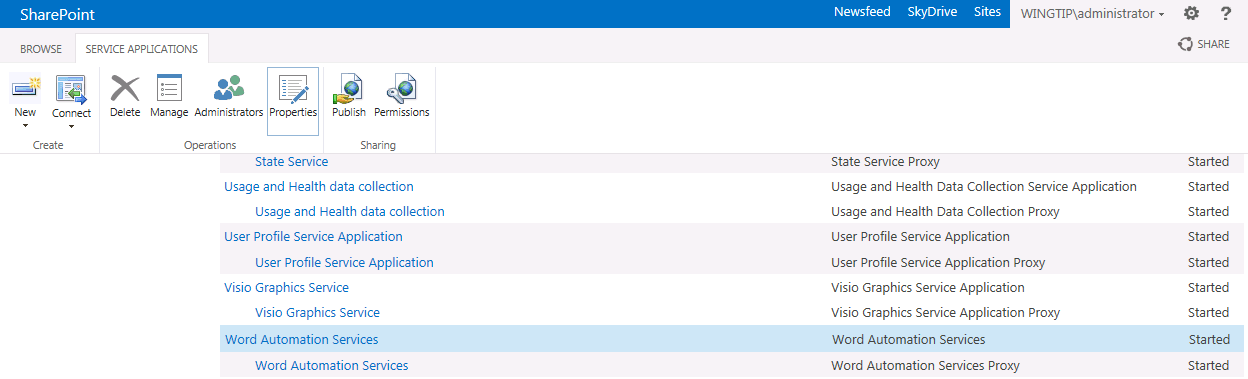
### Exercise 2: Configuring Application Pools and Service Accounts

In this lab you will configure the application pools for both a service application and a web application. As you will see configuring the application pool for a service application can often be accomplished using Central Administration. However, configuring the application pool for a web application often requires using PowerShell cmdlets.

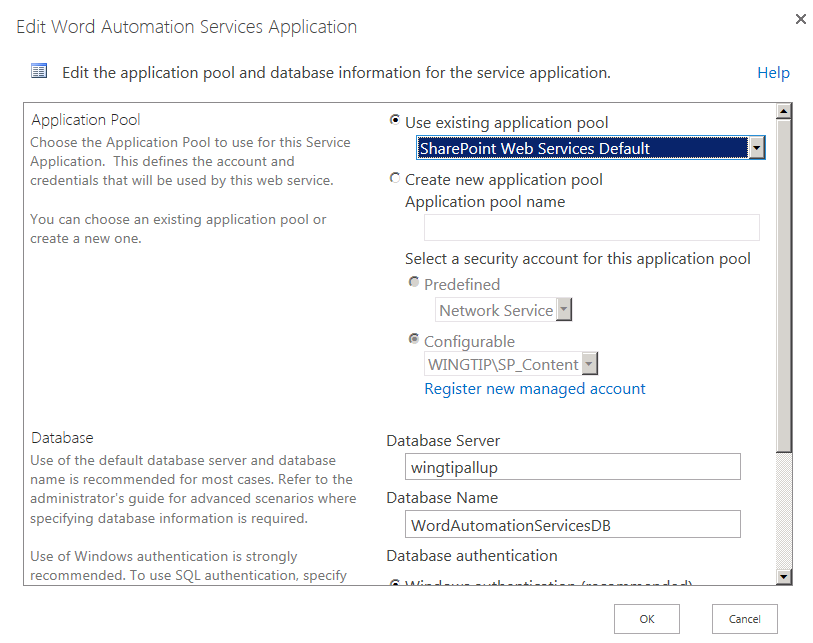
1. From the Windows **Start** menu, launch the **SharePoint 2013 Management Shell**.
2. Execute the **Get-SPServiceApplicationPool** cmdlet to see what service application pools are being used in the farm.



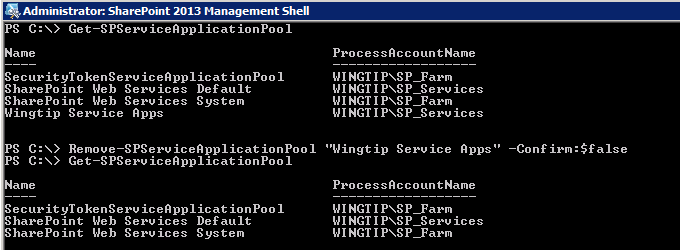
1. You should see that there are two service application pools that run under the **SP\_Farm** account that were created automatically when you created the farm. There are two other service application pools that run under the account **SP\_Services**. The service application pool named **Wingtip Service Apps** was created when you manually created the service application for **Word Automation Services** in the previous lab. The other service application pool named **SharePoint Web Services Default** was also created in the previous lab when you ran the Farm Configuration Wizard to create the other service applications.
2. Configure the **Word Automation Services** application to use the same service application pool as the other service applications.
   1. Navigate to **Central Administration** in the browser.
   2. Under the **Application Management** section click the **Manage service applications** link to navigate to the **Manage Service Applications** page.
   3. Scroll down the page and select **Word Automation Services** from the list of service applications.  
      (Note: Be sure to select the First one in the list; the one with the Type column set to **Word Automation Services** and not the second one with the Type column set to Word Automation Services Proxy. Additionally, do not click on the Word Automation Services hyperlink as this will open the Management page and not the properties page as shown in the next step.)



* 1. Click the **Properties** button in the ribbon to see the properties page for the **Word Automation Services** application.
  2. In the **Edit Word Automation Services Application** dialog, use the drop down list to change the application pool from **Wingtip Service Apps** to **SharePoint Web Services Default** and then click the **OK** button to save your configuration changes.

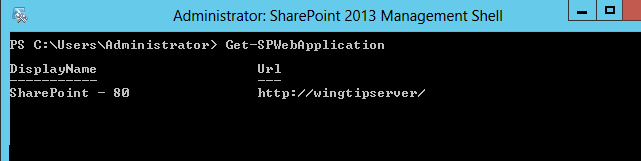


1. At this point, there are no longer any service applications that are currently using the service application pool named **Wingtip Service Apps**. Therefore, you should remove this service application pool since it is no longer needed.
   1. Return to the SharePoint 2013 Management Shell.
   2. Execute the Get-SPServiceApplicationPool cmdlet to list the existing set of service application pools. You should be able to verify that the service application pool named Wingtip Service Apps is still there.
   3. Execute the Remove-SPServiceApplicationPool cmdlet passing the name Wingtip Service Apps in quotes to remove the service application pool.
   4. Execute the Get-SPServiceApplicationPool cmdlet again to verify the service application pool has been removed.



You have just configured all the service applications in your farm to use a single service application pool. Now you will take on the task of changing the identity of the application pool used by the web application that was created by the Farm Configuration Wizard. The reason that this is important is that the Farm Configuration Wizard configured the identity of the web application it created using the **WINGTIP\SP\_Services** account. It is important to configure the application pools for web applications using a different user account than the user account used to configure the identity of service application pools to provide better security isolation. In this lab exercise and others that follow, you will configure all web applications with an application pool using the identity of the **WINGTIP\SP\_Content** account.

1. In the SharePoint 2013 Management Shell, execute the **Get-SPWebApplication** cmdlet. You should see this cmdlet returns a single web application with a display name of **SharePoint – 80** and an Url of **http://WingtipServer**.

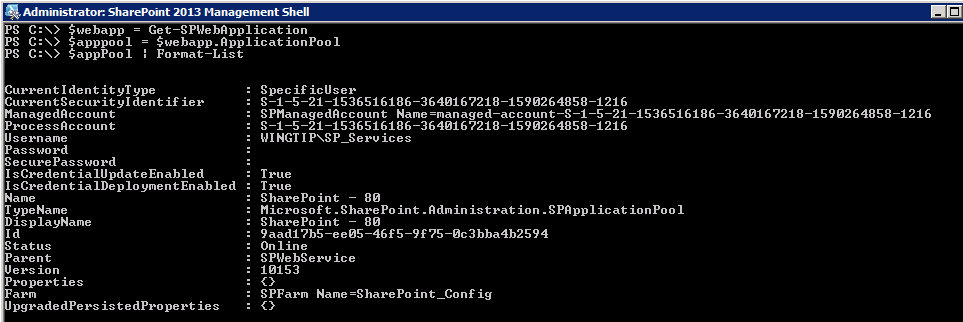


1. Now you will use PowerShell variables to get more information about the application pool used by this web application. Type the following commands into the PowerShell console windows and press ENTER after each one

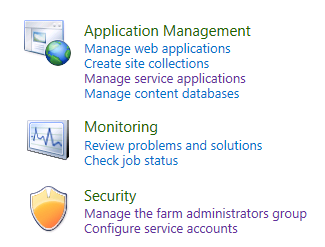
$webapp = Get-SPWebApplication

$apppool = $webapp.ApplicationPool

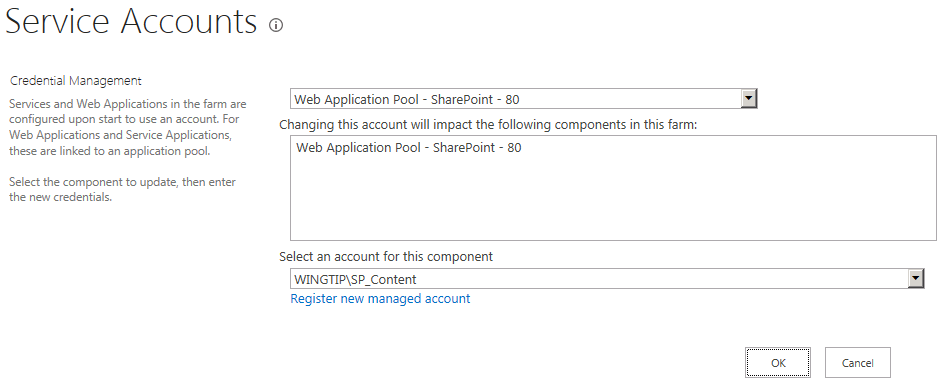
$appPool | Format-List



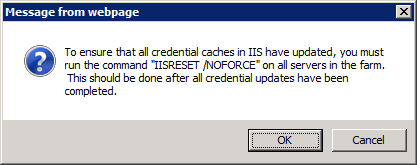
1. You should be able to see that the application pool has properties named **ManagedAccount** and **Username**. These properties track the Active Directory account which gives the web application pool its identity. There is a problem in that the Farm Configuration Wizard has configured this application pool with an identity of **WINGTIP\SP\_Services**. You do not want the application pools for web applications and service applications to run under the same account.
2. In this step you will reconfigure the application pool used by the web application to use the **SP\_Content** account instead of **SP\_Services**.
   1. Go to the home page of Central Administration.
   2. Click the Configure service accounts hyperlink under the Security category.



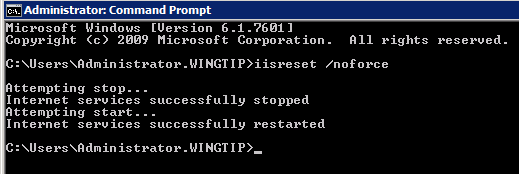
* 1. On the **Service Accounts** page, use the drop down menu to select the web application pool named **SharePoint – 80**. You should be able to see that the application pool is currently using the **WINGTIP\SP\_Services** account. In the drop down menu titled **Select an account for this component**, change the account from **WINGTIP\SP\_Services** to **WINGTIP\SP\_Content**. Once you have made the change, click **OK** to save your configuration changes.



* 1. You will be prompted by a message stating that an IISRESET must be run on the farm. Click **OK**.



* 1. From the Windows **Start** menu, click **Command Prompt**. Once the command prompt appears, type **iisreset /noforce** in the console and press Enter.

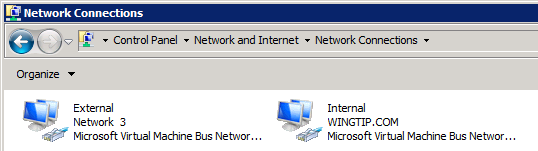


In this exercise you reconfigured the application pools for a service application and a web application. You have effectively reduced the number of application pools being used in your farm and you have reconfigured a web application pool to use a separate identity from that used by the farm's service application pools.

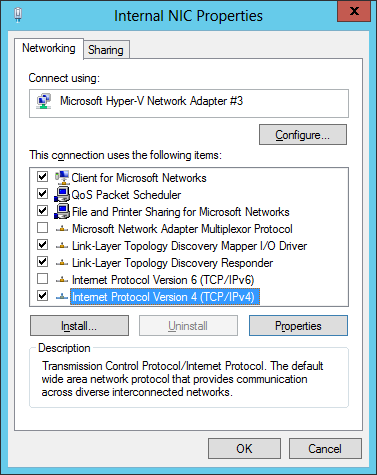
### Exercise 3: Configuring DNS Settings in DNS Manager

In this exercise you will add DNS A Records to redirect requests sent to the DNS names of **intranet.wingtip.com** and **extranet.wingtip.com** to IP addresses of the **WingtipServer** server. You will also configure the **WingtipServer** server to support two new IP addresses. More specifically, you will add a new IP address of **192.168.150.2** for the DNS name of **intranet.wingtip.com** and an IP address of **192.168.150.3** for the DNS name of **extranet.wingtip.com**. The IP addresses and DNS settings you configure in this exercise will be required to complete the remaining exercises in this lab.

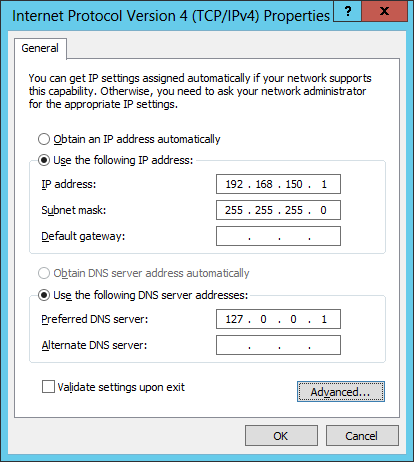
1. Add support to the **Internal** network adapter for the **WingtipServer** server to support two new IP addresses.
   1. Press the **Windows** key and type "Control Panel".
   2. Click the **Control Panel** tile.
   3. Click the link titled **Network and Internet**.
   4. Click the link **Network and Sharing Center**.
   5. Click the link **Change adapter settings**. At this point you should see the two network cards that are configured for the **WingtipServer** server.



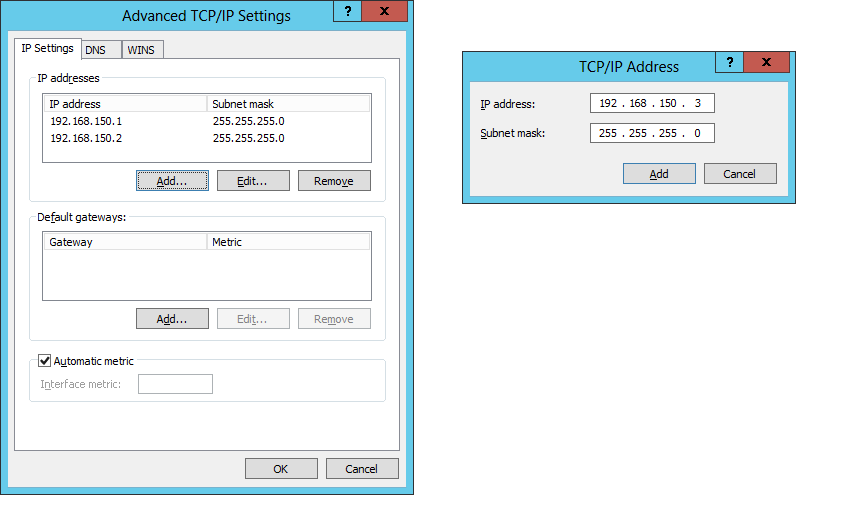
* 1. Right-click the **Internal** adapter and choose properties.



* 1. Select **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**. You should see that the IP address it set to **192.168.150.1**.



* 1. Click the **Advanced** button at the bottom of the dialog. This dialog has an Add button which allows you to add new IP addresses. Add two new IP addresses for **192.168.150.2** and **192.168.150.3**.



* 1. When you are done you should see the network card now displays support for the following three IP addresses.

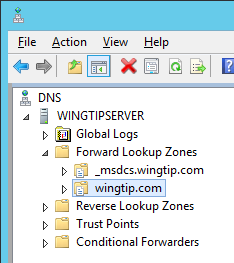
192.168.150.1

192.168.150.2

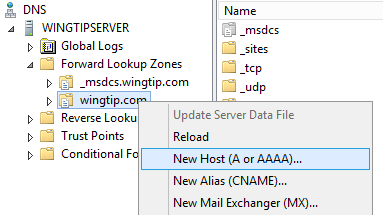
192.168.150.3

* 1. Chose **OK** to close all dialogs until you reach the **Properties** page for the network adapter. Click **Close** to close the Properties dialog for the network adapter.

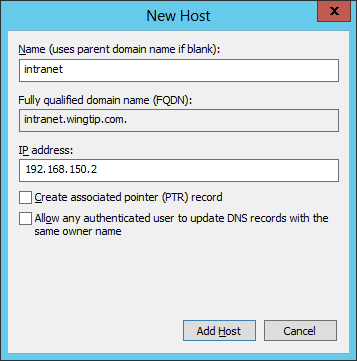
1. Configure DNS settings for **intranet.wingtip.com** and **extranet.wingtip.com**.
   1. Press the **Windows** key and type "DNS".
   2. Click the **DNS** tile to start the **DNS Manager**.
   3. In the DNS Manager, navigate down the hierarchy of nodes to **DNS » WINGTIPSERVER » Forward Lookup Zones » wingtip.com**.



* 1. Create an A Host DNS record for **intranet.wingtip.com** pointing to **192.168.150.2**. Right-click on the **wingtip.com** node and create a new A record by selecting the menu command **New Host (A or AAAA)**.



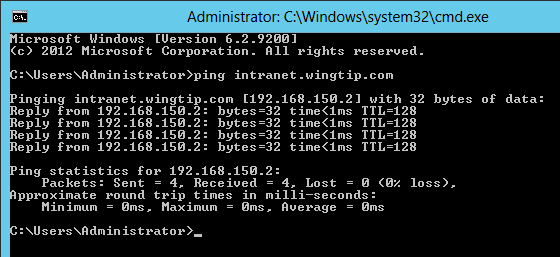
* 1. In the **New Host** dialog enter a **Name** of **intranet** and an **IP** address of **192.168.150.2**. When you are done click the **Add Host** button to create the new A Record.



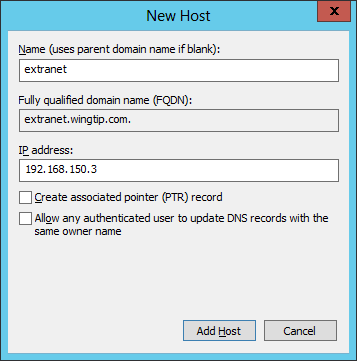
* 1. Click **OK** and **Done**. You should now be able to verify that the DNS A Record was created.



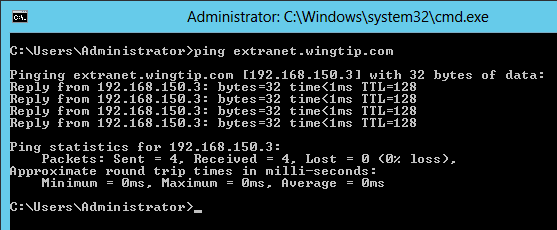
* 1. Now it is time to test your work. Verify you can resolve the DNS names of **intranet.wingtip.com** to the correct IP address. Bring up a standard Windows command prompt. Ensure you can **ping** the DNS name of **intranet.wingtip.com** and have it resolve to the IP address of **192.168.150.2**.



* 1. Create an A Host DNS record for **extranet.wingtip.com** pointing to **192.168.150.3**. Follow the exact same set of steps that you did when you created the A Host DNS record for **intranet.wingtip.com**.

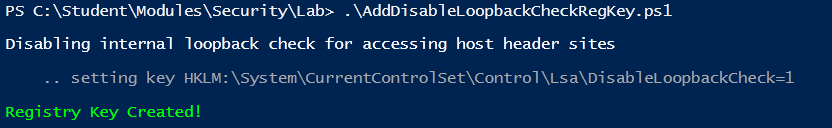


* 1. When you are done, ensure you can **ping** the domain **extranet.wingtip.com** just like you were able to ping **intranet.wingtip.com**.

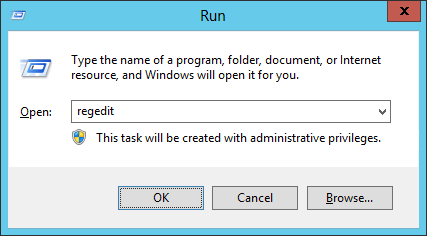


* 1. You are now done configuring the DNS setting for **intranet.wingtip.com** and **extranet.wingtip.com**.

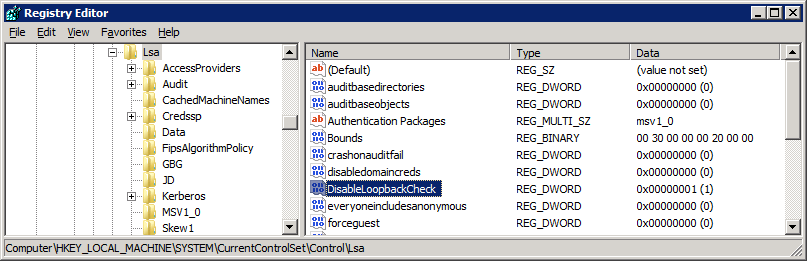
1. Run a PowerShell script to add the **DisableLookbackCheck** key to the registry.
   1. Look in folder for this lab at **c:\Student\Modules\Security\Lab**. Locate the script named **AddDisableLoopbackCheckRegKey.ps1** and execute it by right-clicking and selecting **Run PowerShell script**.



* 1. After running the script you will have added the **DisableLoopbackCheck** key to the registry which will allow browsers running on the **WingtipServer** server to resolve DNS names such as **intranet.wingtip.com** and **extranet.wingtip.com** to IP addresses on the local machine.
  2. Run the **Windows Registry Editor** by pressing **Windows** + **R** to display the Windows **Run** dialog. Type "RegEdit" and press **OK**.



* 1. Navigate to the registry key **[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]** and verify that the **DisableLoopbackCheck** key has been added.



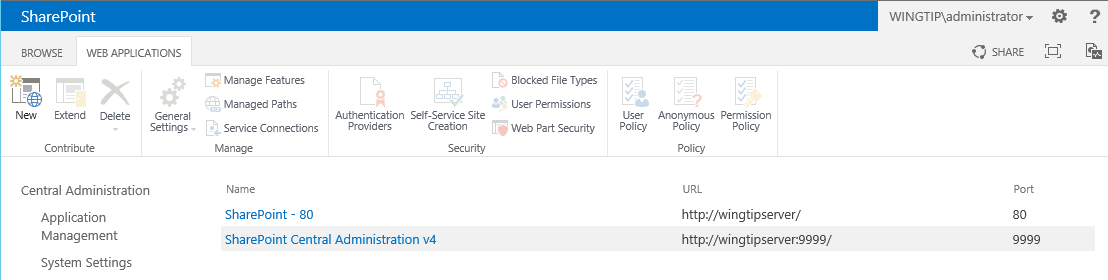
* 1. Close the Registry Editor.
  2. Since you are configuring a server inside a testing environment, it is acceptable to use the **DisableLoopbackCheck** key. However, remember that in a production environment that you should avoid configuring servers using the **DisableLoopbackCheck** key and use the **BackConnectionHostNames** key instead.

In this exercise you added A Host DNS records to resolve the domains of **intranet.wingtip.com** and **extranet.wingtip.com** to IP addresses of the **WingtipServer** server. You will put this work to use in the next exercise.

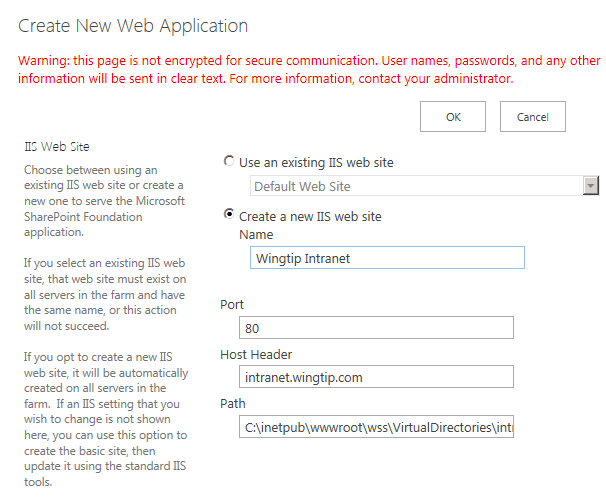
### Exercise 4: Create a new Web Application which uses Kerberos Authentication

In this exercise you will create a new Web Application at **http://intranet.wingtip.com** which authenticates users using Kerberos authentication.

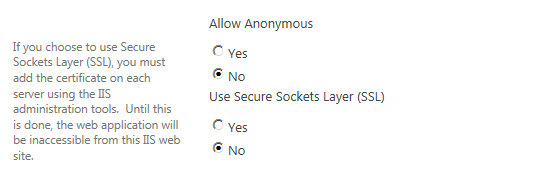
1. Launch **Central Administration** and click the **Manage web applications** link under **Application Management**.
2. On the **Web Applications Management** page, click the **New** button in the top left corner of the ribbon which will bring up the **Create New Web Application** dialog.



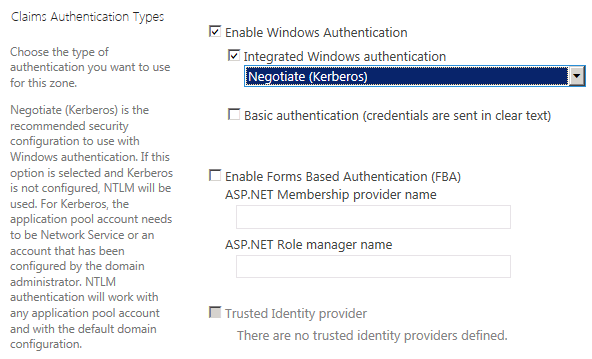
1. You should now be looking at the **Create New Web Application** dialog. At the top of this dialog you will see the **IIS Web Site** section. Enter a new IIS Web Site name of **Wingtip Intranet** and a **Port** setting to **80**. Enter a **Host Header** of **intranet.wingtip.com** and leave the **Path** setting with its default value. Your settings should mirror the following screenshot.



1. Move down to the **Security Configuration** section of the **Create New Web Application** dialog. You can leave the **Allow Anonymous** settings in this section with its default values. Leave the **Use Secure Sockets Layer (SSL)** set to **No**.



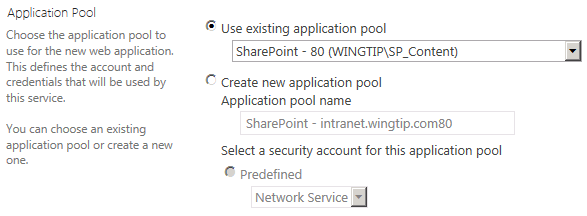
1. In the **Claim Authentication Type** section, leave the default selections of **Enable Windows Authentication** and **Integrated Windows authentication**. However, there is one change you need to make. In the drop down the menu under the Integrated Windows authentication checkbox, change the setting from the default value of **NTLM** to **Negotiate (Kerberos)** as shown in the following screenshot..



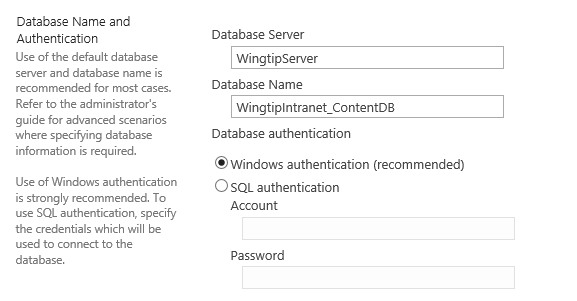
1. In the **Sign In Page URL** section, leave .the default selection of **Default Sign in Page**.
2. In the **Public URL** section, remove the port number from the end of the URL so it appears as **http://intranet.wingtip.com**.



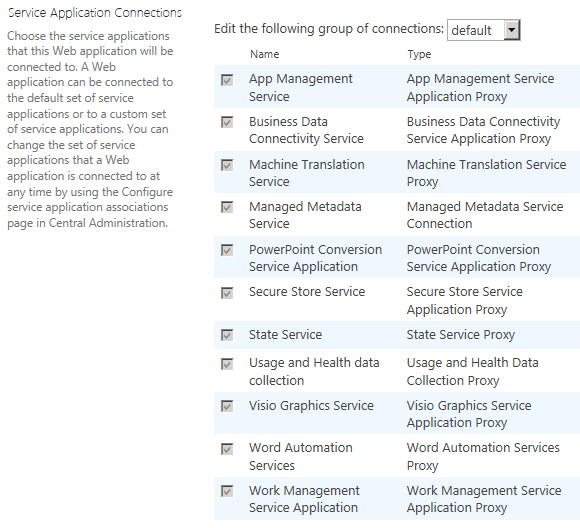
1. Move down to the **Application Pool** section and select the option for **Use existing application pool**. Select the application pool named **SharePoint - 80** that is being used by the other web application that was created by the Farm Configuration Wizard. As you can see, this web application pool is configured with an identity of **WINGTP\SP\_Content**.



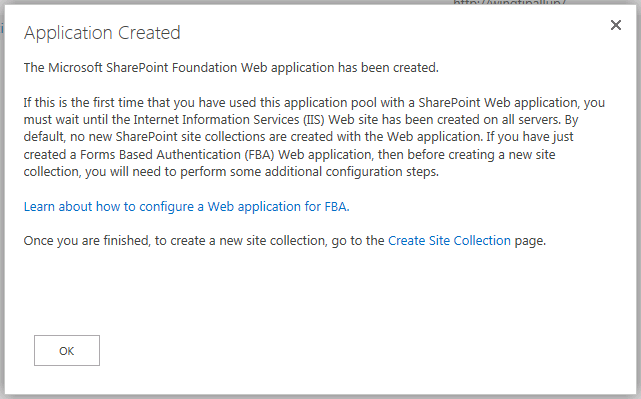
1. Move down to the Database Name and Authentication section of the Create New Web Application dialog. Make sure Database Server is set to **WingtipServer**. Change the Database Name to **WingtipIntranet\_ContentDB**. Leave the Database authentication setting set to Windows authentication.



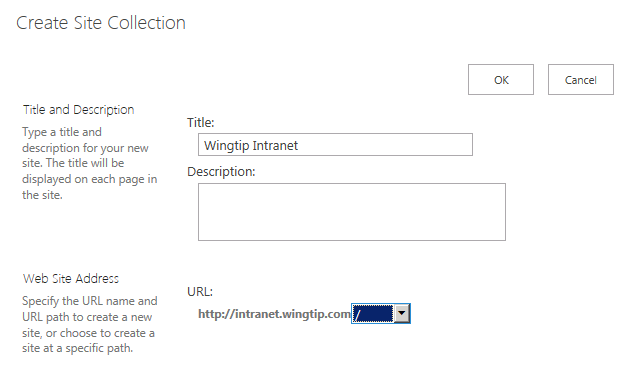
1. The next section is **Failover Server** which you can leave in its default state with a blank value.
2. The next section is the **Service Application Connections** section. Leave this in its default state where it is assigned to the **default** group of service application connections.



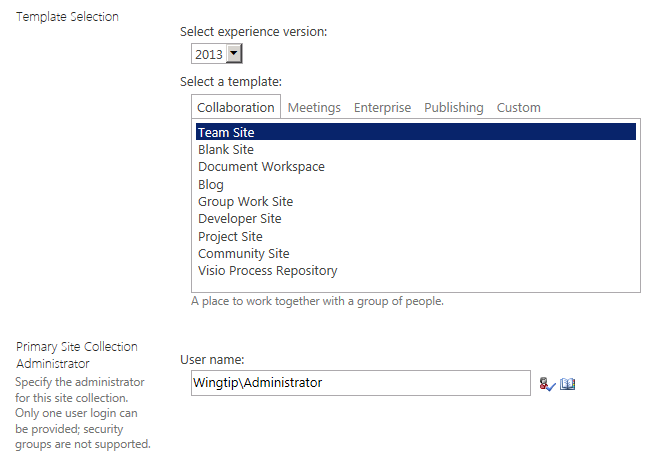
1. Ensure that the Customer Experience Improvement Program setting is set to **No**.
2. Now click the **OK** button to provision the new Web Application.
3. After the new Web application has been created, you will be prompted with the following dialog. Click the link at the bottom with the caption **Create Site Collection**.



1. In the **Create Site Collection** dialog, you must fill in the information to create a new team site
   1. Enter a **Title** of **Wingtip Intranet** and leave the **URL** setting with the default value.



* 1. In the **Template** Selection section, make sure **Team Site** is selected as the site template for the top-level site. Also assign the **WINGTIP\Administrator** account as the **Primary Site Collection Administrator**.



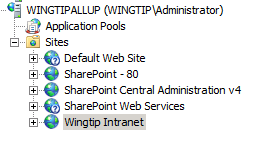
* 1. Leave all other settings with their default values and Click the OK button to create the new site collection.
  2. When the site collection has been created, you will be prompted with a dialog with a link to the new site. Do not click the link to navigate to the new site yet. Instead close the Internet Explorer. If you have multiple windows of the Internet Explorer open, close all of them.

Now you have created the web application using Central Administration. However you still need to make a few changes outside of SharePoint to properly configure the new web application. The first change you will make will be inside IIS to configure the IIS Web site used by the new application to only accept requests which target the IP address of 192.168.150.2. The second change you will make will be to add a service provider name to ensure Kerberos authentication works correctly.

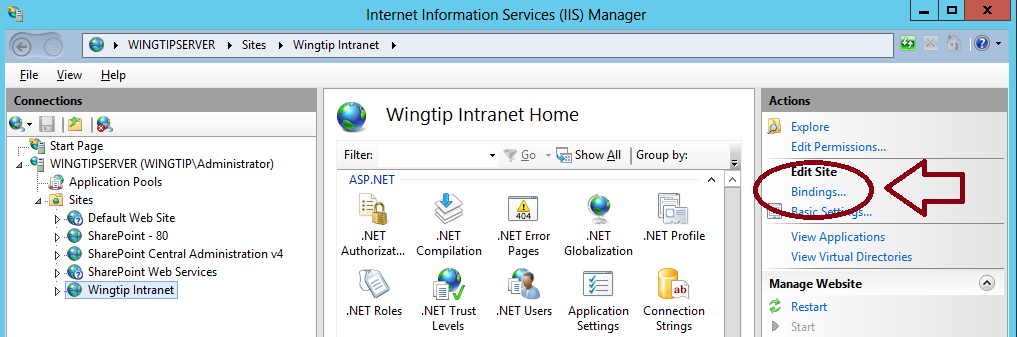
1. Configure the IIS Web site for intranet.wingtip.com to use the IP address of **192.168.150.2**.
   1. Launch the **IIS Manager** by pressing the **Windows** key to display the Widows **Start** page and clicking the tile with the caption **Internet Information services (IIS)**.



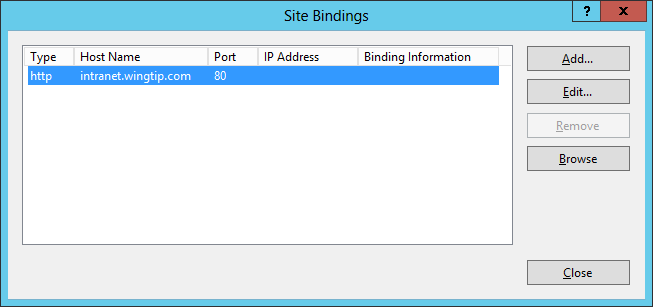
* 1. Locate the IIS Web Site named **Wingtip Intranet**. This is the IIS web site that SharePoint created when you created the **Wingtip Intranet** web application.



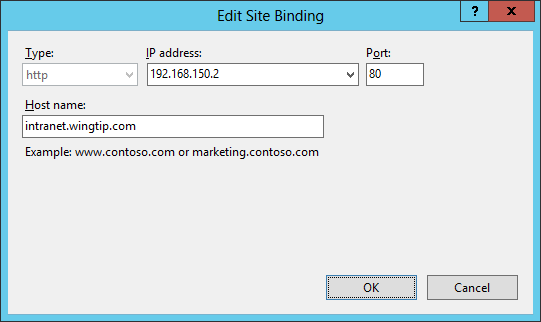
* 1. With **Wingtip Intranet** selected, click on the Bindings link on the right-side task pane of the IIS Manager.



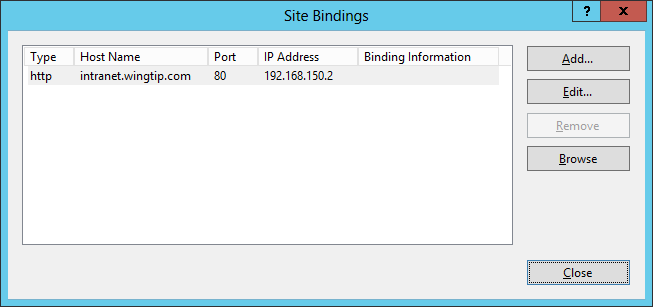
* 1. When you click the **Bindings** link, the IIS Manager will display the **Site Bindings** dialog. You should be able to see that there is a single binding for the **Host Name** of **intranet.wingtip.com** which shows a blank **IP Address** setting which means this binding will accept incoming requests from any IP addresses that are unassigned.



* 1. Select the **Edit** button to edit the **IP Address** setting for this binding. Change the **IP Address** setting to **192.168.150.2** and the click **OK** to save your changes and close the **Edit Site Bindings** dialog.



* 1. Next, click the **Close** button to close the **Site Bindings** dialog.

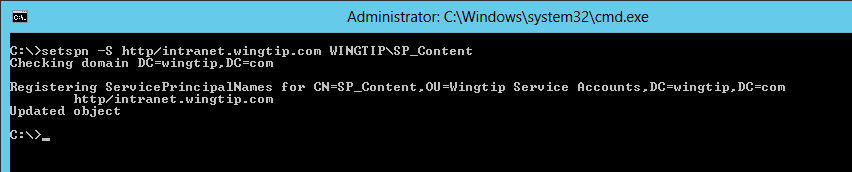


* 1. You have now finished configuring the binding for the IIS Web site for the **Wingtip Intranet**.

1. In the final configuration step you use the **setspn.exe** utility to configure a service provider name which is need to make Kerberos authentication work properly.
   1. Open up a standard command prompt.
   2. Execute the following command using the **setspn.exe** utility.

setspn –S http/intranet.wingtip.com WINGTIP\SP\_Content

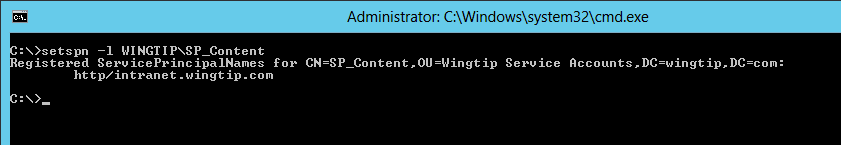
* 1. You should see the following output after running this command.



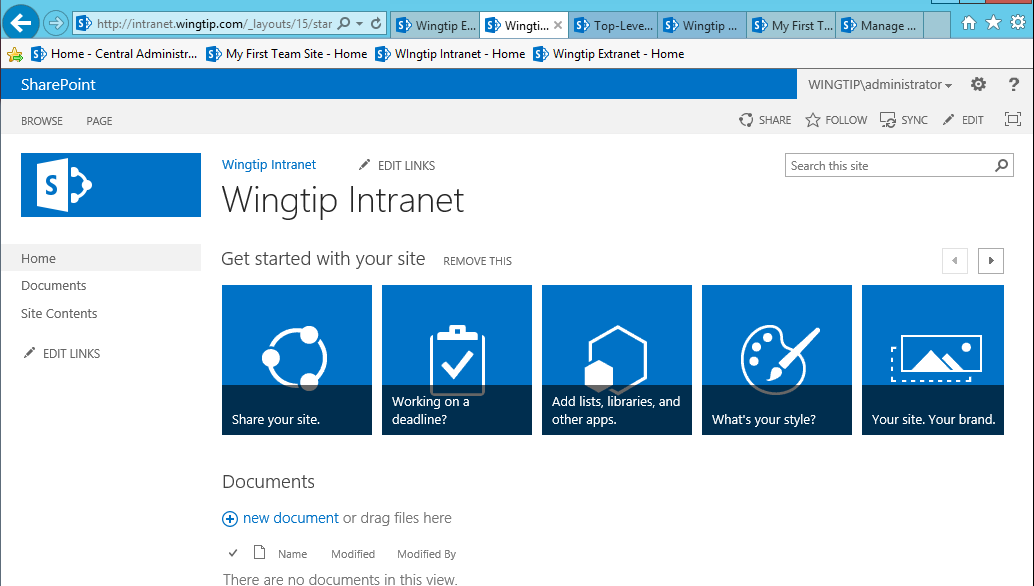
* 1. Verify that the service provider name was correctly registered by executing the following command to list the service provider names that have been registered for the account **WINGTIP\SP\_Content**.

Setspn.exe –l WINGTIP\SP\_Content

* 1. You should see the following output which lists the service provider names registered for the **SP\_Content** service account.



1. You are now finally finished with the configuration of the new web application and you should be able to launch the Internet Explorer and navigate to the new team site that has been create at **http://intranet.wingtip.com**. When you launch the Internet Explorer and attempt to access the site, you might be prompted for security credentials. Use a user name of **WINGTIP\Administrator** and a password of **Password1**. After a minute or two, you should see that the new team site that has been created at the root of the new web application which has an URL of **http://intranet.wingtip.com**.

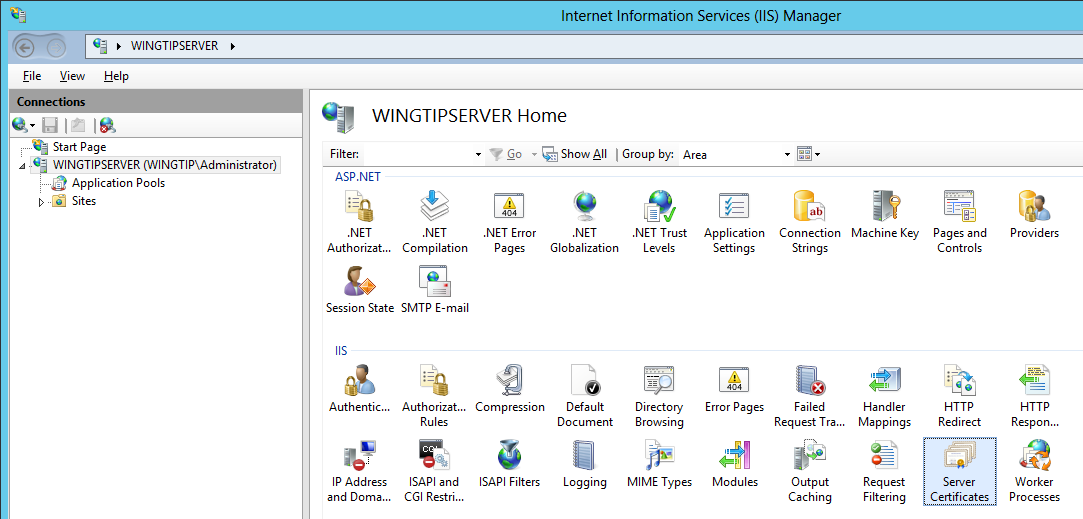


In this exercise you learned how to configure a web application to use a specific IP address and Kerberos authentication.

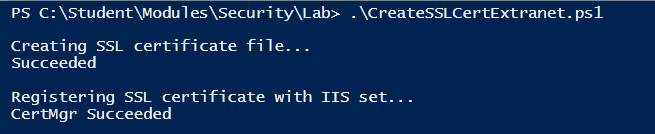
### Exercise 5: Add Test SSL Certificates to the WingtipServer VM

In this exercise you will create and install a test SSL certificate into IIS so that you can use SSL to encrypt data as it is sent back and forth between the browser and the Web server. In a real world scenario you would obtain a SSL certificate by making a certificate request to a Certificate Authority such a VeriSign, Thawte or GoDaddy. In this lab exercise, you will use utilities that are installed along with SharePoint 2013 to create certificates that can be used in testing scenarios such as the lab exercises in this training course.

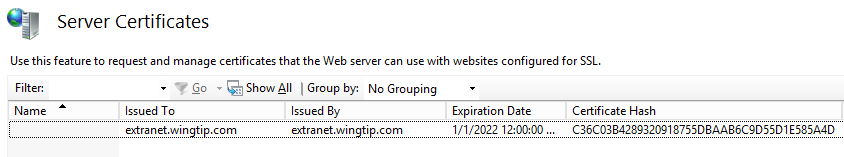
1. Launch or return to the **IIS Manager**.
2. In the IIS Manager, select the top node for the computer named **WINGTIPSERVER**. Once you have selected the **WINGTIPSERVER** node, look in the middle of the screen and find and double click on the **Server Certificates** icon.



1. Currently there isn't any certificates that you can use when testing a SharePoint farm. Therefore, you must create a new SSL certificate for testing.
2. Using the Windows Explorer, locate the student lab folder at **c:\Student\Modules\Security\Lab**. You should see inside this folder that there is a Windows PowerShell script named **CreateSSLCertExtranet.ps1**. If you are curious how to create a test SSL certificate using PowerShell, open the script in the Windows PowerShell ISE and review the code inside.
3. Execute the PowerShell script named **CreateSSLCertExtranet.ps1**. When you execute the script, you should see the following output.



1. Return to the IIS Manager and refresh the page (e.g. with the **Server Certificates** page open press the **F5** key) which shows the SSL certificates. You should be able to verify that the test SSL certificate issued to **extranet.wingtip.com** has been added.



In this exercise you created an SSL test certificate and installed it into IIS so that you can use it within a SharePoint web application that you will create in the following exercise.

### Exercise 6: Creating a new Web Application that uses SSL

In this exercise you will create a new Web Application at **https://extranet.wingtip.com**. One key difference between this lab and the previous lab where you create the Wingtip Intranet web application is that you will create the new web application using a PowerShell script instead of creating it manually through Central Administration.

1. Make sure you are logged on as **WINGTIP\Administrator** on the **WingtipServer** server.
2. Look in the folder for this lab at **C:\Student\Modules\Security\Lab** and locate the PowerShell script named **CreateWingtipExtranet.ps1**. Open this script using **Windows Powershell ISE.** Note there are a set of variables used to create a new web application. These variables are used to pass values to the following parameters in the call to **New-SPWebApplication**.

Name = "Wingtip Extranet"

Port = 443

HostHeader = "extranet.wingtip.com"

SecureSocketsLayer = $true

AuthenticationProvider = New-SPAuthenticationProvider -UseBasicAuthentication

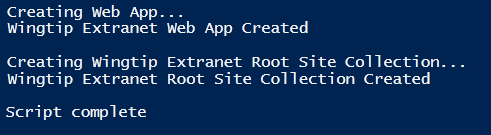
URL = "https://extranet.wingtip.com"

ApplicationPool = "SharePoint - 80"

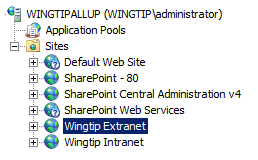
DatabaseServer = "WingtipServer"

DatabaseName = "WingtipExtranet\_ContentDB"

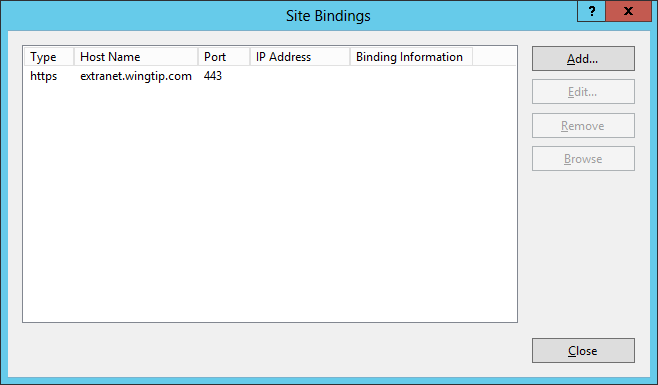
1. At the bottom of the script you will notice a call to **New-SPSite** which creates a new site collection at the root of the new web application.
2. Execute the script **CreateWingtipExtranet.ps1**. Since this script is creating a new web application and then a new site collection, it could take between 5-10 minutes to complete its execution. When the script finishes, you should see the following output.

.

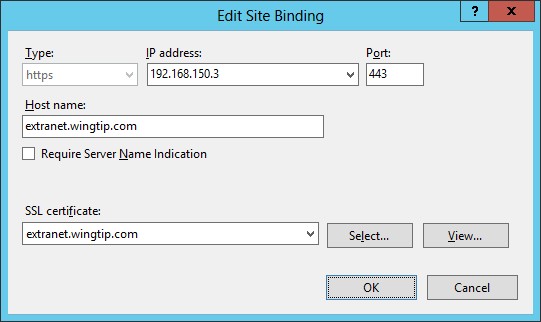
1. After the script completes, you must further configure the binding in the IIS site used by the new web application.
   1. Return to the IIS manager.
   2. Refresh the IIS website so you can see the new IIS website that was created for the **Wingtip Extranet** web application.



* 1. Inspect the bindings for **Wingtip Extranet** IIS Web site by clicking the **Bindings** link as you did for **Wingtip Intranet** earlier in this lab. You should be able to see that the IIS web site has a single binding **Type** of **https** with a **Host Name** of **extranet.wingtip.com** and a **Port** setting of **443**. However, this binding has not been correctly configured to only use the IP address for this domain which is **192.168.150.3**.

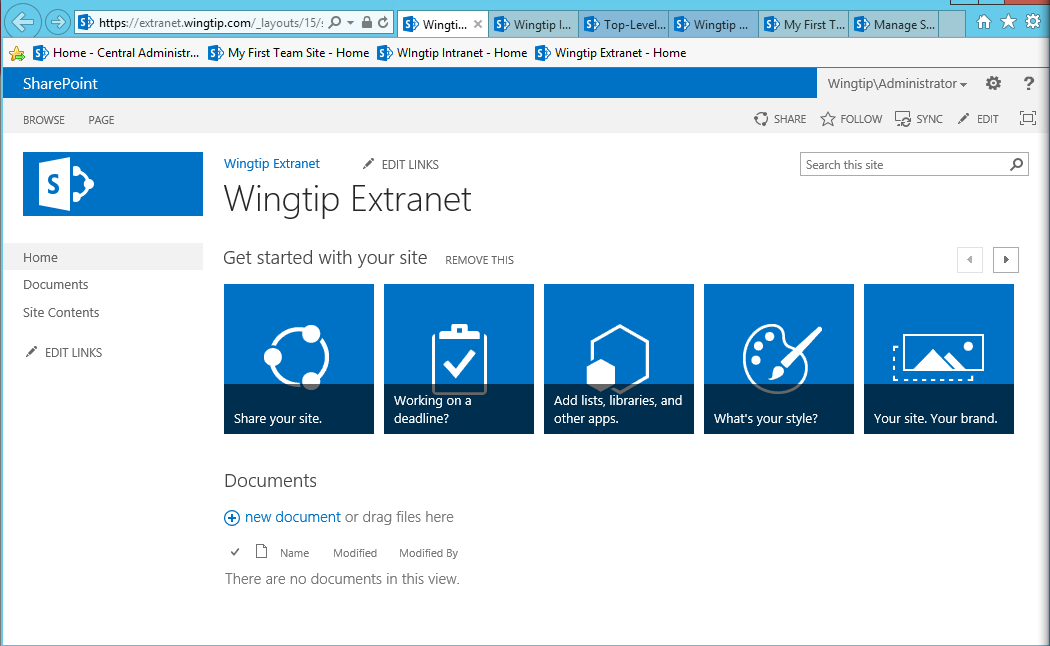


* 1. Click the **Edit** button to display the **Edit Site Binding** dialog. First, use the drop down menu for the **IP address** to select **192.168.150.3**. Next, use the drop down menu for **SSL certificate** to select **extranet.wingtip.com**. When you are done, click the **OK** button.



* 1. Click the **Close** button to close the **Site Bindings** dialog.

1. Launch the browser and navigate to **https://extranet.wingtip.com**. When you are prompted to log on, use a user name of **WINGTIP\Administrator** and a password of **Password1**. The web application should take a minute or two to initialize. After that the browser should display the home page of the new site collection that was created at the root of the new web application.

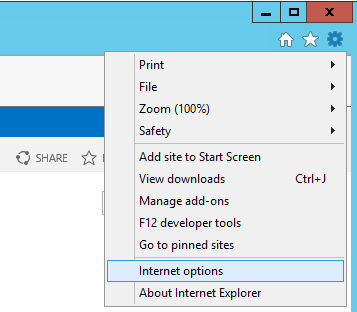


In this exercise you used a PowerShell script to create a web application which uses Basic Authentication and SSL.

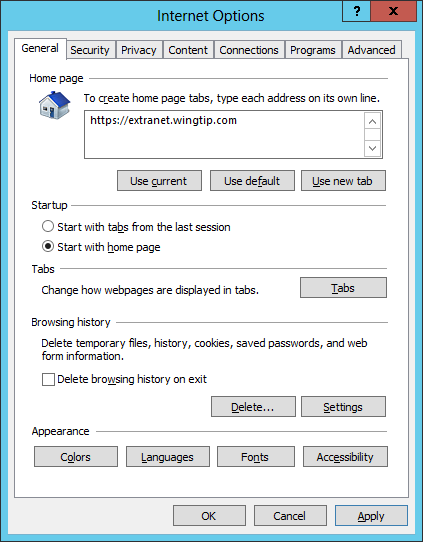
### Exercise 7: Configure Internet Explorer to Login Automatically

To make your life easier while going through these lab exercises, there are a few things you can do to configure Internet Explorer when browsing SharePoint 2013 sites. Given the number of times you will be required to authenticate against SharePoint sites in these lab exercises, it will make things far more convenient if you configure Internet Explorer to log in automatically with the current user's Windows account credentials.

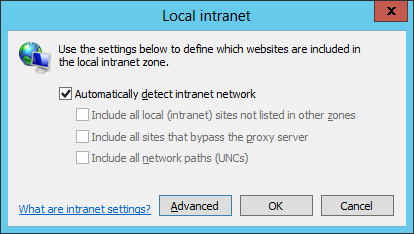
1. Close all instances of the Internet Explorer.
2. Launch a new Instance of Internet Explorer and navigate to **https://extranet.wingtip.com**.
3. You should observe that you are prompted to log in.
4. Log in using the credentials of **WINGTIP\Administrator** account.
5. Inside the Internet Explorer, drop down the Settings menu and select **Internet Options**.



1. In the **General** tab, enter a Home page address of **https://extranet.wingtip.com**. Click the **Apply** button to save your setting.



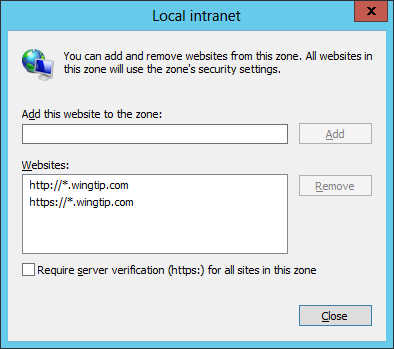
1. Click to the **Security** tab and select the zone named **Local Intranet**. Click the **Sites** button to configure the Local Intranet zone. The Internet Explorer will display the **Local Intranet** dialog. Click on the **Advanced** button.



1. The next dialog allows you to add one or more URLs to the Local Intranet zone. Add the following URLs to the list of Websites for the Local Intranet zone.

http://\*.wingtip.com

https://\*.wingtip.com



1. Click **Close** to dismiss the first dialog. Next click **OK** to dismiss the next dialog which should bring you back to the original Internet Options dialog. Click **OK** to save all your changes.
2. Now close and restart Internet Explorer. You should be able to navigate to **https://extranet.wingtip.com** without having to explicitly log in. You should also be able to navigate to **http://intranet.wingtip.com** without logging in as well.

In this exercise you configured Internet Explorer to pass the credentials of the currently logged in user to the site so you won’t have to login each time.