## Configuring Security in SharePoint 2010

**Lab Time**: 45 minutes

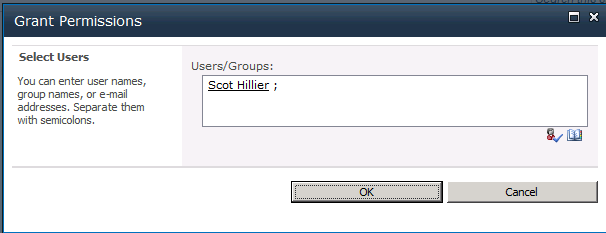
**Lab Folder**: C:\Student\Labs\04.Security

**Lab Overview**: In the following lab, you will configure various security permission and authorization settings. You will also configure alternate access mapping for Central Administration and make this Web application accessible through SSL.

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

In this exercise you will learn how to add Active Directory Users as Farm Administrator.

1. You can promote **Active Directory** users as **Farm Administrator**. In **SharePoint 2010 Central Administration**, click the **Manage the farm administrators group** hyperlink under the **Security** section.
2. This brings you to a page where all farm administrator accounts are listed. Notice the accounts that are already there.
3. You can add another farm administrator by clicking the **New** button and choose **New User**.
4. Add the user **Scot Hillier (WINGTIP\ScotH)** as a farm administrator.

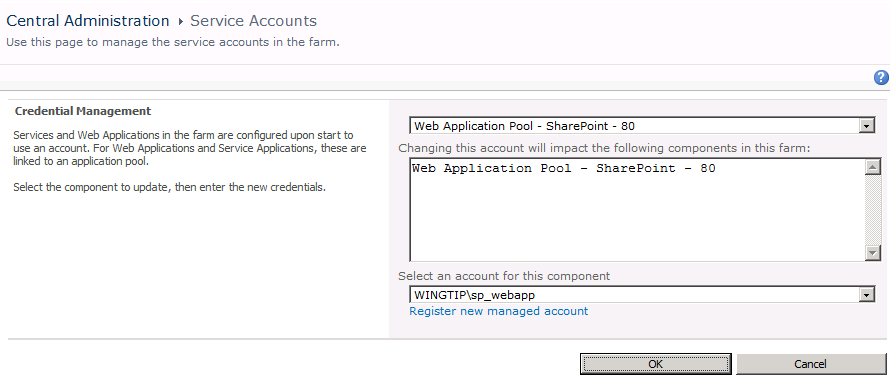


1. Click the **OK** button.
2. Return to the **SharePoint Central Administration** home page.

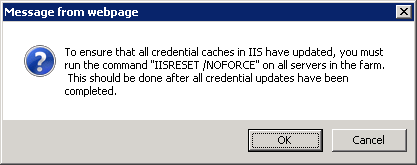
### Exercise 2: Managing Service Accounts

In this exercise you will learn how to configure service accounts. Services and Web Applications in the farm are configured upon start to use an account. For web applications and service applications, these are linked to an application pool.

1. In SharePoint **Central Administration**, you can also configure additional service accounts. The page where you can do this is also accessible from the home page. Click the **Configure service accounts** hyperlink under the **Security** category.
2. If you drop down the top combo box in **Service Accounts** page, you can see a large list of application pools that have been created and are currently being managed by SharePoint Foundation. The list contains all application pools for configured service applications. You should be able to locate an application pool for the Web application that was created by the Farm Wizard at [http://wingtipserver](http://webserver) and by the caption of **Web Application Pool – SharePoint - 80**. There is a problem because this application pool was configured to use the service account for Wingtip service applications instead of the proper service account for Web applications. Time to fix that.
   1. Select the application pool with the caption of **Web Application Pool – SharePoint 80**.
   2. Change the account for this component from **WINGIP\sp\_serviceapp** to **WINGTIP\sp\_webapp**.



* 1. Click **OK** to change the application pool identity.
  2. You will be prompted by a message stating that an IISRESET must be run on the farm. Click **OK**.



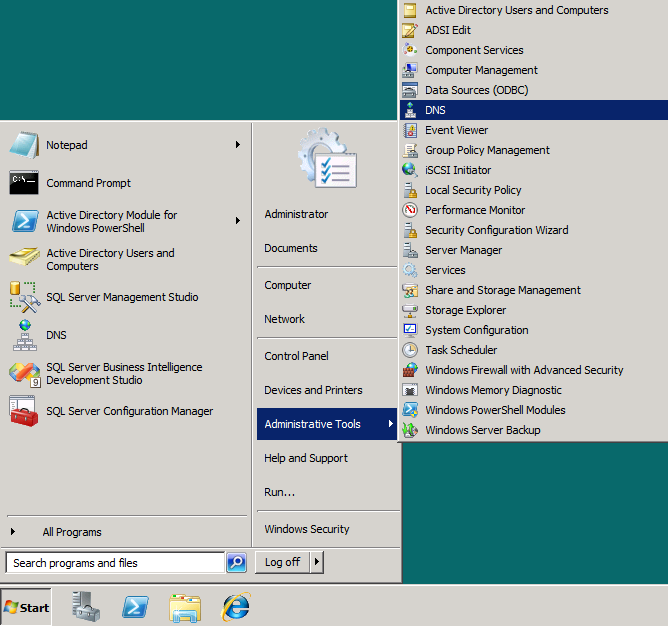
* 1. Click **Start » Command Prompt** type **iisreset** in the console and hit **Enter**.

1. You are now done with this exercise and you should know what to do if you need to inspect or modify which application pools to run using a specific service account.

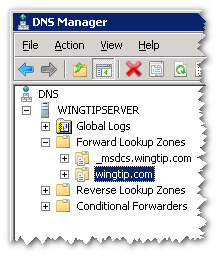
### Exercise 3: Configuring DNS A Host Records in DNS Manager

In this exercise you will add two DNS A Records to redirect requests sent to the DNS name of **testing.wingtip.com** to the IP address of **192.168.150.1**.

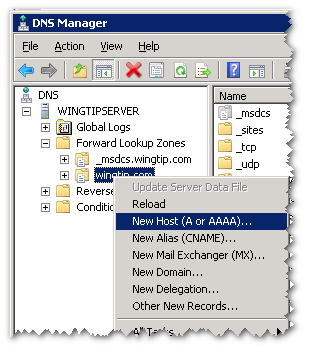
1. Start DNS Manager from **Start » Administrative Tools » DNS**.



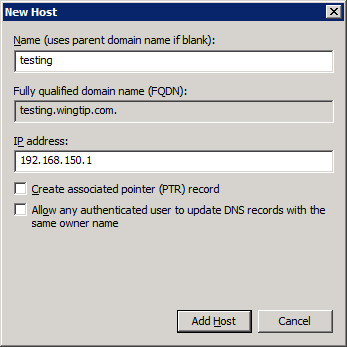
1. Create an A Host for **testing.wingtip.com** pointing to **192.168.150.1**
2. In the DNS Manager, navigate down the hierarchy of node to **DNS » WINGTIPSERVER » Forward Lookup Zones » wingtip.com**.



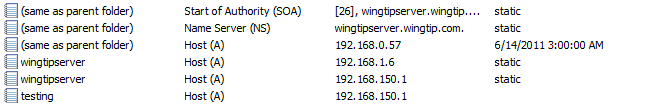
* 1. Right-click on the **wingtip.com** node and create a new A Record by selecting the menu command **New Host (A or AAAA)**.



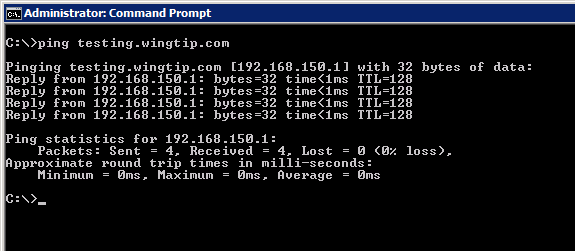
* 1. In the **New Host** dialog enter a **Name** of **testing** and an **IP address** of **192.168.150.1**. When you are done click the **Add Host** button to create the new A Record



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



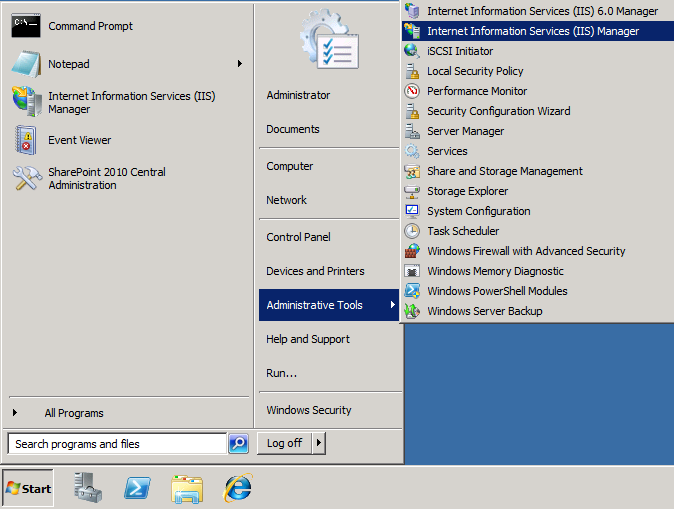
1. Now it is time to test your work. Verify you can resolve the DNS names of **testing.wingtip.com** to the correct IP address.
   1. Bring up a standard Windows command prompt.
   2. Ensure you can ping the DNS name of **testing.wingtip.com** and have it resolve to the IP address of **192.168.150.1**.



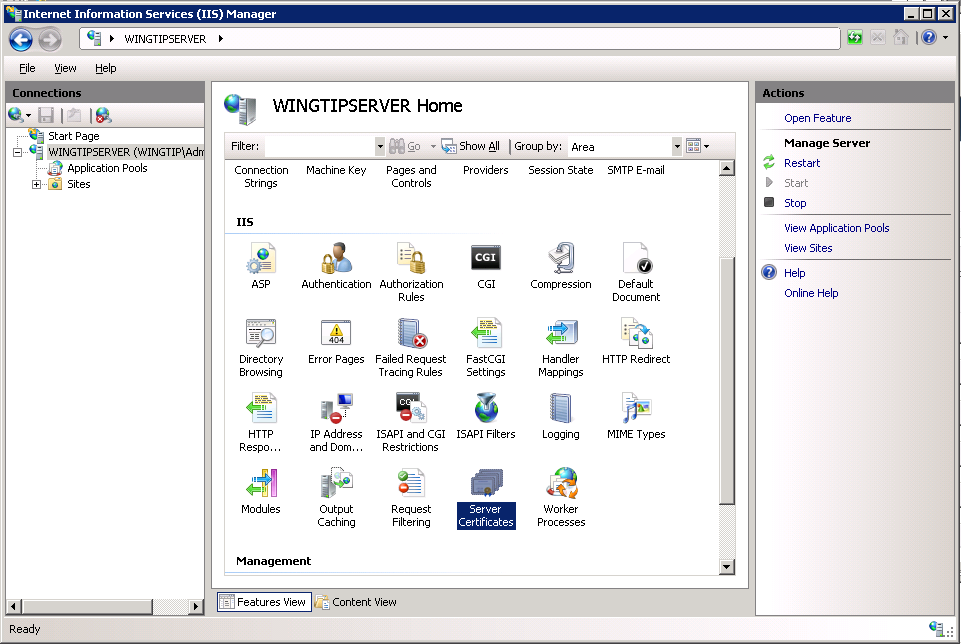
### Exercise 4: Configuring an SSL Certificate for Testing Purposes

In this exercise you will configure an SSL certificate so that in the next exercise you can configure the extended Web Application to 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 a utility that is part of the IIS Resource Kit named SELFSSL.EXE that will allow you to create a certificate on the WingtipServer VM for testing purposes.

1. Launch the IIS Manager from **Start » Administrative Tools » Internet Information Services (IIS) Manager**.



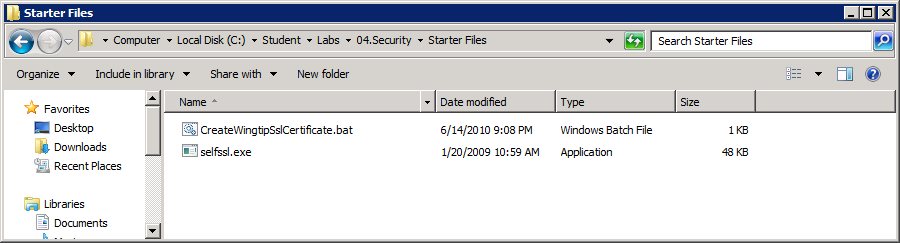
1. In the IIS Manager, select the top node for the computer named **WINGTIPSERVER**. Once you have selected the **WINGTIPSERVER** node, look in the middle of the screen and find and double click on the **Server Certificates** icon.



1. Currently there should be a single certificate based on the machine name. However, you will not be able to use this certificate with a DNS name such as **testing.wingtip.com**.



1. Using the Windows Explorer, locate and look inside the folder at **[[Lab Files]]\Starter Files**. You should see the selfssl.exe utility and a bath file named CreateWingtipCertificate.bat.

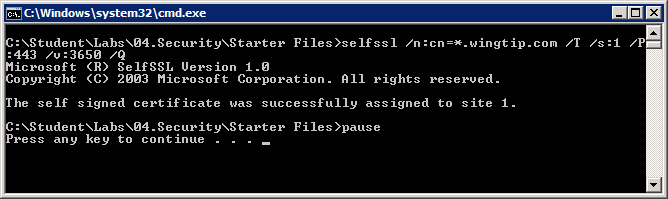


1. If you take a look at the batch file you will see it contains the instruction shown below to call selfssl.exe. This creates a test certificate that can be used with any DNS name that ends with **wingtip.com**.

selfssl /n:cn=\*.wingtip.com /T /s:1 /P:443 /v:3650 /Q

pause

1. Double click on **CreateWingtipCertificate.bat** to create the new certificate.



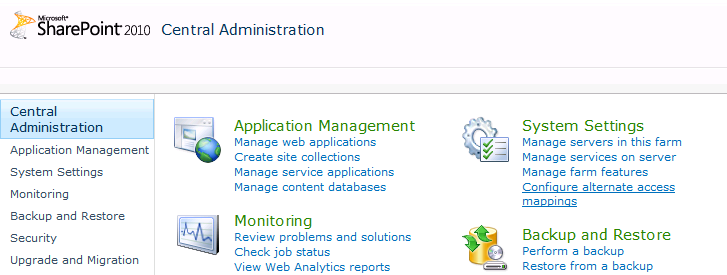
1. Return to the IIS Manager and refresh the view of Server Certificates. You should be able to see the new certificate issued to **\*.wingtip.com**.



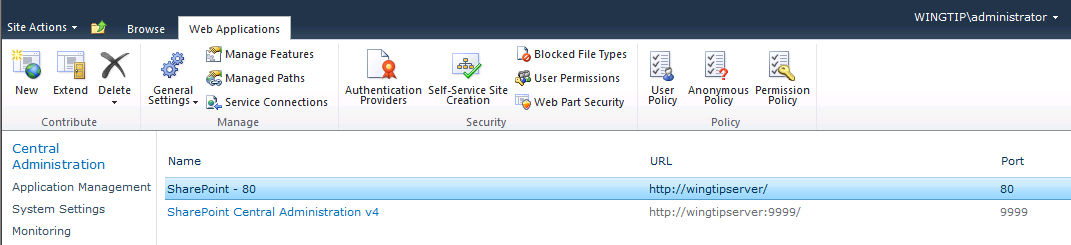
### Exercise 5: Extending a Web Application

In this exercise you will extend the Web Application which has been created at **http://wingtipserver** with a new zone. This will make it possible for the Web Application to support a second URL of **https://testing.wingtip.com**.

1. Launch the **SharePoint 2010 Central Administration** application by navigating the http://wingtipserver:9999/default.aspx in the browser.
2. In the **Application Management** section click **Manage web application** link.



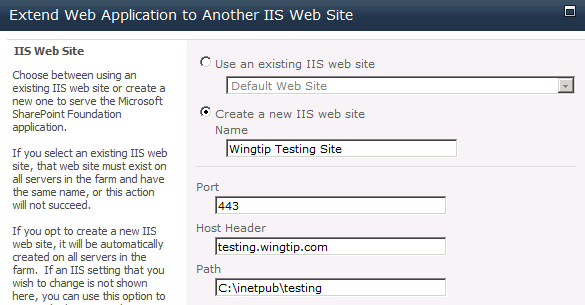
1. On the **Web Applications Management** page, inspect the set of existing Web Applications. You should see the Web Application for Central Administration as well as the Web Application which was created by the Farm Wizard at the URL of **http://wingtipserver**. Select the Web Application at the URL of **http://wingtipserver** so it becomes highlighted within the browser.



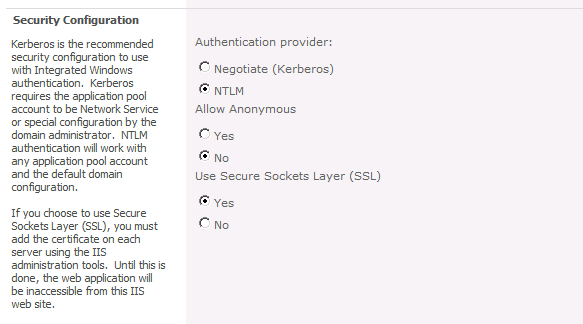
1. Once you have selected the Web Application at the URL of **http://wingtipserver**, click the **Extend** button in the **Contribute** group in the ribbon.



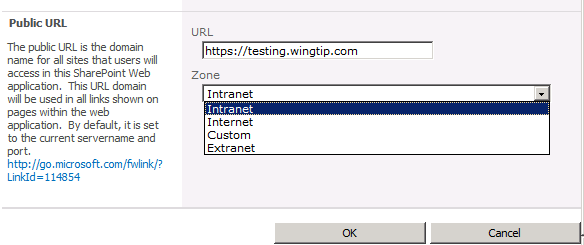
1. A modal dialog should appear with a long form which allows you to enter in data for creating a new zone which requires creating a new IIS Web Site. Enter the data in the **IIS Web Site** section as shown in the following screenshot. Note that you will be using a **Port** setting of **443** instead of **80** because this new zone will be configured to use SSL.



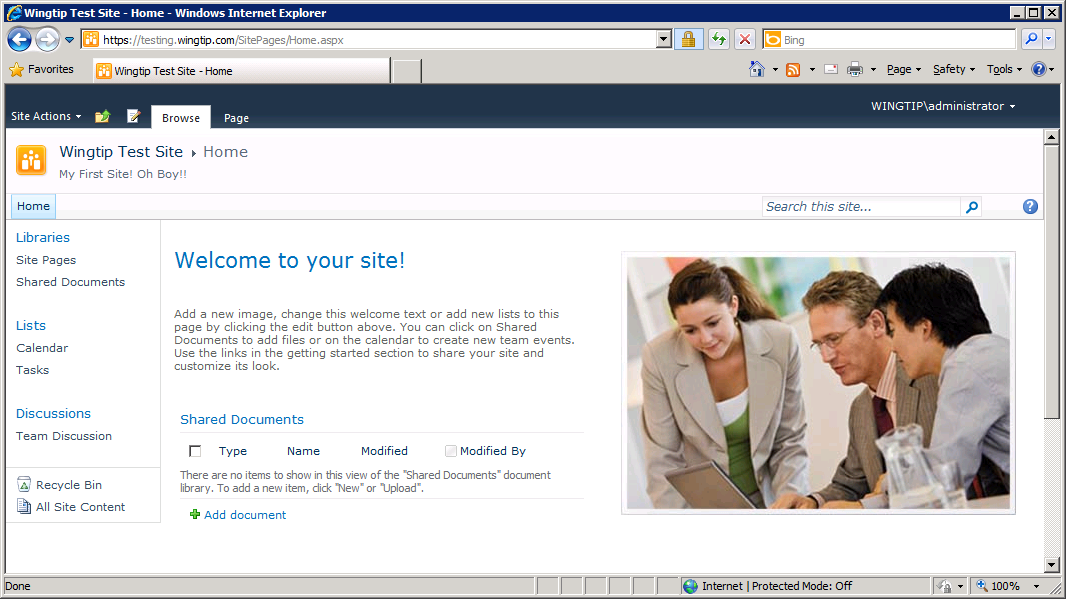
1. Enter the data in the **Security Configuration Section** section as shown in the following screenshot. Note that you must change the **Use Secure Sockets Layer (SSL)** setting from the default value of **No** to the required value of **Yes**.



1. At the bottom of the form, you will see the final section named **Public URL**. For the **URL** setting, remove the port number so that the URL is configured **https://testing.wingtip.com**. You will notice that the drop down box for the **Zone** setting provides four choices which are **Intranet**, **Internet**, **Custom** and **Extranet**. Note that your selection here will not actually change any behavior within the zone. It simply allows you to add a descriptive label. Leave the **Zone** setting with its default value of **Intranet** and click the **OK** button to create the new zone.

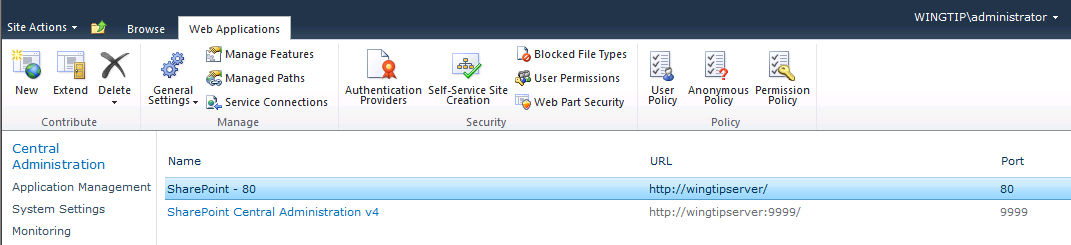


1. Once the Web Application has been extended and you have created the new zone, it is now time to test it out to make sure it is accessible.
   1. Shut down all instances of the Internet Explorer.
   2. Launch a new Instance of Internet Explorer.
   3. Navigate to **https://testing.wingtip.com.**
   4. When prompted to log in, you the credentials of the **WINGTIP\Administrator** account.
   5. You should see same site you created earlier through **https://testing.wingtip.com.**

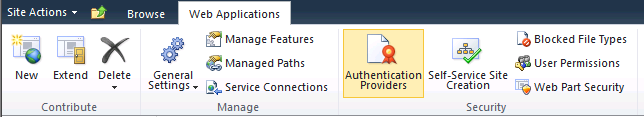


Now you will return to **Central Administration** in the browser so you can see where you can view and modify the security settings for this new zone.

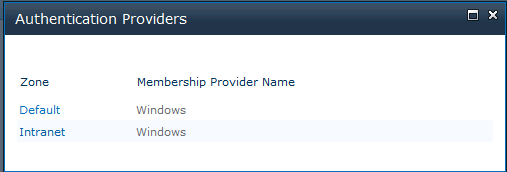
1. Navigate to **Central Administration**.
2. In the **Application Management** section click **Manage web application** link.
3. On the **Web Applications Management** page, select the Web Application at the URL of **http://wingtipserver** so it becomes highlighted within the browser.



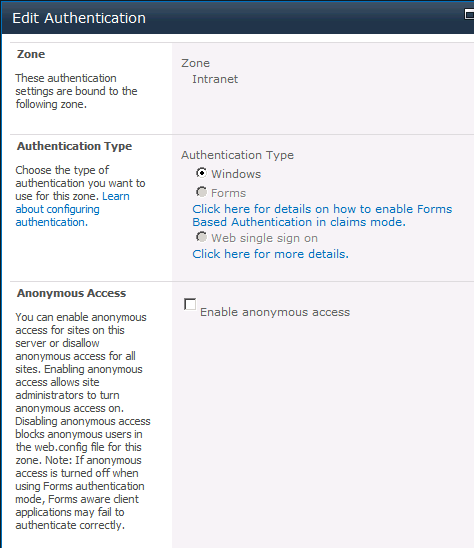
1. Once you have selected the Web Application at the URL of **http://wingtipserver**, click the **Authentication Providers** button in the **Security** group in the ribbon.



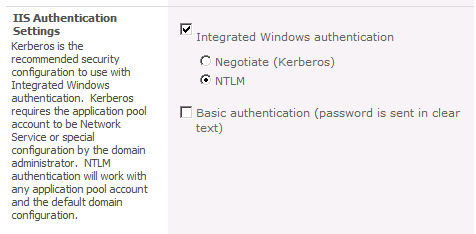
1. When you click the **Authentication Providers** button, a dialog appears showing you the zones for the selected Web Application. Click the **Intranet** link at the bottom left of the dialog.



1. When you click the **Intranet** link, a long modal form appears which allows you to view and edit the various security setting for the new zone you have just created. Note that there is an option for you to enable anonymous access.



1. If you scroll down to the **IIS Authentication Settings** section, you can see that you have the ability to configure support for **Integrated Windows Authentication** with a setting of either **Negotiate (Kerberos)** or **NTLM**. You can also configure the zone to support authentication using **Basic Authentication** instead of or in addition to **Integrated Windows Authentication**.



At this point, you are not required to change any of the security settings for the new zone. These last few steps have just been included to show you where you need to go to change the security settings for a zone when it is required.

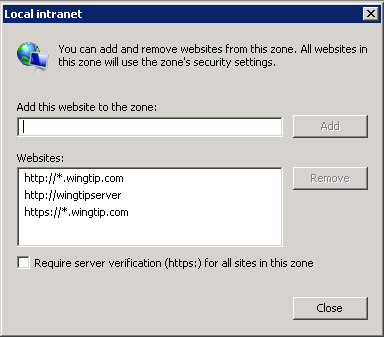
### Exercise 6: Configure Internet Explorer 8 to Login Automatically

To make life easier, there are a few things you can do to configure Internet Explorer when browsing SharePoint 2010 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 8 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://testing.wingtip.com**.
3. You should observe that you are prompted to log in.
4. Log in using the credentials of **WINGTIP\Administrator** account.

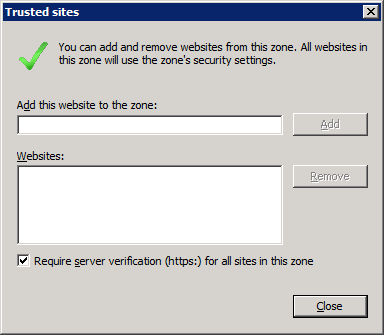
Now you will configure Internet Explorer to eliminate the need for you to explicitly log in.

1. Inside the Internet Explorer, drop down the **Tools** menu and select **Internet Options**.
2. In the **General** tab, enter a **Home page** address of [https://testing.wingtip.com](https://admin.wingtip.com). Click the **Apply** button to save your setting.
3. Click to the **Security** tab and select the zone named **Local Intranet**. Click the **Sites** button to configure the **Local Intranet** zone. Internet Explorer will display the Local Intranet dialog. Click on the **Advanced** button
4. 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**.
5. [https://\*.wingtip.com](https://*.wingtip.com)
   1. [http://\*.wingtip.com](http://*.wingtip.com)
   2. http://wingtipserver



* 1. Upon adding http://wingtipserverto the Local Intranet zone, you will be prompted asking if you wish to move the URL that exists in Trusted sites zone to Local Intranet zone. Click **Yes** to move it to Local Intranet zone.
  2. 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.

1. On the **Security** tab of the **Internet Options** dialog, select the zone named **Trusted Sites**. Click the **Sites** button to configure the **Trusted Sites** zone.
2. If there are any sites listed, remove all of them from the Trusted Sites zone. You are removing them because you do not want these URLs to conflict with the Website URLs and wildcards characters you added to the Local Intranet zone.



* 1. Click **Close** to save your work.

1. Now restart Internet Explorer. You should be able to navigate to **https://testing.wingtip.com** without having to explicitly log in.

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.