Securing Central Administration in SharePoint 2007

Craig Carpenter *MCT. MCSE, MCSA*

Partner

Combined Knowledge

SharePoint training and courseware providers.

http://www.combined-knowledge.com

Introduction

You will probably have noticed that on certain pages within Central Administration – especially those where you are configuring account settings, you receive a warning at the top of the page, stating that you are about to send username and password information across the network as plain text. This is because by default, Central Administration is configured to accept connections over HTTP only.

Now, this may not be an obvious concern since we only ever connect to Central Administration across the local LAN right? Well, consider that the majority of security breaches come from inside the network, and even if we only ever access Central Administration on the SharePoint server itself this will still send information over the wire, and we can see that connecting to Central Administration over HTTPS would be very beneficial.

If we are going to secure the connection to Central Administration using SSL, then it makes sense to also secure the connection the Shared Service Provider(s) admin site(s) in the same way as we will also need to provide potentially sensitive information when configuring the SSP.

Another problem with the way that SharePoint 2007 implements Central Administration is the fact that by default, we have a single sever in the farm hosting it. Should this server fail, we would be left with no access to Central Administration, and this is where the backup / restore tool is! Sure, we could run the configuration wizard on a different server and create a new Central Administration web site, but it would be better to have that additional site present to begin with.

In this paper, we'll look at solutions to the issues discussed above, namely:

- Securing the connection to Central Administration using SSL
- Securing the connection to the SSP Admin Site using SSL
- Providing additional Central Administration Web Applications for fault tolerance.

Terminology

You will notice in this document that I use the phrases web site and Web Application to refer to the same thing. The term web site will be used when discussing settings performed in IIS, in this case we are dealing with an IIS web site. I will use the term Web Application to refer to the site when discussing specifics to do with SharePoint, as now we are dealing with a SharePoint Web Application.

Securing the Connection to Central Administration Using SSL

When we create a Web Application in either Windows SharePoint Services (WSS) 3.0 or Microsoft Office SharePoint Server (MOSS) 2007, we have the option of configuring, amongst other things, the requirement for a connection using SSL. This will not configure the server certificate, which still needs to be done through the IIS console but it will define the default access mapping to the Web Application as https://<Web Application name>.

Since the Central Administration site is created by the SharePoint Products and Technologies Configuration Wizard, we do not get the option of configuring SSL for this particular Web Application, and therefore must configure everything through the IIS console.

In order to configure the Central Administration Web Application to accept SSL connections, we need to perform the following steps:

> Note that these steps assume that you have already completed the setup of the Windows Server 2003 Certificate Services component. If you have not yet completed the setup of Certificate Services, see the appendix *¨Configuring Certificate Services¨* at the end of this paper.

1. Using the IIS Management Console, open up the Properties page for the **SharePoint Central Administration v3** web site.

2. Select the **Directory Security** tab.

3. In the Secure communications section, click the **Server Certificate** button.

4. This will start the wizard to obtain and install a server certificate. Click **Next** on the welcome page.

5. Select the radio button to **Create a new certificate** and click **Next**.

6. Select the radio button to **Send the request immediately to an online certificate authority** and click **Next**.

7. Enter a certificate name, this does not have to match the server name, but should include enough information to easily identify the certificate in the Certificate authority console. Also select the bit length from the default length, however, 1024 bits should be sufficient for securing the Central Administration web site across the LAN. Unless your environment requires it, you should not need to select the check box to select a different cryptographic provider.

8. Specify values for the **Organization** and **Organizational Unit** fields. If fields have been used for previous certificate requests, you may be able to select values from the drop down menu. If no values are present, enter your own values. The company name would seem appropriate for the **Organization** field, where-as *SharePoint Central Admin* could be used for the **Organization Unit** field.

9. Define the **Common name** for the certificate. This should match the host header used to access the web site minus the protocol. For Central Administration, this will normally match the host name of the hosting web front end server.

10. Select the appropriate **Country** from the drop down menu (*GB*) and enter and appropriate value for **State/province** and **City/locality**.

11. Define the SSL port you wish to use. It is still a good idea to use a non standard (not 443) port number for this to provide basic security. If you configured the Central Administration to use a specific port number during the Configuration Wizard, you may wish to re-use this value if it is easy to remember. To do so, you will first need to change the port used for HTTP connections to the web site, as HTTP and HTTPS must be on different ports. Another reason for not using 443, is that IIS does not use Host Headers with HTTPS connections, and so there can only be on Web Application using SSL per IP address. Click **Next**.

12. Select the **Certificate authority** from which you wish to obtain the certificate in the drop down list and click **Next**.

13. Review the information in the certificate request and click **Next** if it is correct.

14. Click **Finish** and the certificate will be issued and installed on the server.

Now, you may think that the next step is to configure the Central Administration web site to require a secure connection, by selecting this option on the **Secure Communications** page for the web site in the IIS Management Console. However, if you enable this now, you will find that you will then not be able to open Central Administration using the shortcuts on the Start menu, or indeed with the URL **https://MOSS SERVER:port**. The URL that the Central Administration Web Application will respond to is defined by the default Access Mapping, which is, of course, configured in Central Administration. So before we configure the web site in IIS to only accept secure connections, we must fist change the Access Mapping for the Web Application.

1. Open up the Central Administration site. If you find that the shortcuts no longer work, then use the full URL **https://MOSS SERVER:port/default.aspx**.

2. Select the **Operations** tab.

3. Click the **Alternate access mappings** link in the **Global Configuration** section.

4. Click the **Edit Public URLs** link on the toolbar at the top of the list.

5. In the **Alternate Access Mapping Collection** section, use the drop down box to select **Central Administration**.

6. Now change the **Default** field to match the URL of the HTTPS connection for Central Administration (**https://MOSS SERVER:port**).

7. If you want to also be able to use an un-secured HTTP connection to Central Administration, enter the original URL into one of the other fields, such as Intranet or custom.

If you want to always use HTTPS when connecting to Central Administration then you should now return to the IIS Management Console and configure the web site to require SSL. You can do this by:

1. On the **Properties** page of the Central Administration web site, select the **Directory Security** tab.

2. In the Secure communications section, click the **Edit** button.

3. Select the **Require secure channel (SSL)** check box and, if required, select the **Require 128-bit encryption** check box.

4. Click **OK** twice.

5. Now test the Central Administration short cut from the **Start** menu to ensure that it connects to the HTTPS connection correctly.

Securing the Shared Service Provider Administration Site using SSL

Now that we have secured the communications to the Central Administration web site by using SSL, it makes sense to apply the same security to the SSP Administration sites(s). We will deal with this in two sections, configuring SSL when creating the SSP Administration site, and configuring SSL for an existing SSP.

Configuring SSL During SSP Administration Site Creation.

This is quite straight forward as, we have the option of configuring SSL during Web Application creation.

1. When creating the Web Application for the Shared Service Provider's Administration site, select the **Yes** radio button for the **Use Secure Sockets Layer (SSL)** option under the **Security Configuration** section. This will change the protocol used in the load balanced URL to HTTPS. Again, ensure you use a port other than 443, to provide basic security and also allow you to secure a user Web Application with SSL if required.

2. Complete the remainder of the **Create Web Application** screen as normal and click **OK**.

3. Complete the creation of the Shared Service Provider as normal.

4. Open the IIS Management Console and bring up the properties of the SSP Administration Site.

5. Select the **Directory Security** tab.

6. In the Secure communications section, click the **Server Certificate** button.

7. This will start the wizard to obtain and install a server certificate. Click **Next** on the welcome page.

8. Select the radio button to **Create a new certificate** and click **Next**.

9. Select the radio button to **Send the request immediately to an online certificate authority** and click **Next**.

10. Enter a certificate name, again, this does not have to match the server name, but should include enough information to easily identify the certificate in the Certificate authority console. Also select the bit length and cryptographic provider option as before.

11. Specify values for the **Organization** and **Organizational Unit** fields.

12. Define the **Common name** for the certificate. Again, this needs to match the host header used to access the web site and again will probably match the host name of the server.

15. Select the appropriate **Country** from the drop down menu and enter and appropriate value for **State/province** and **City/locality**.

16. Define the SSL port you wish to use. Again, you will ideally want to use a port other than 443. Click **Next**.

17. Select the **Certificate authority** from which you wish to obtain the certificate in the drop down list and click **Next**.

18. Review the information in the certificate request and click **Next** if it is correct.

19. Click **Finish** and the certificate will be issued and installed on the server.

20. You may want to configure the site to require an SSL connection as described above.

Configuring SSL for an Existing Shared Service Provider

The process of securing the connection to an existing Shared Service Providers administration site is the same as that for securing the connection to Central Administration. Since we have already discussed this, I won't duplicate the individual steps here. The general steps are:

1. Install a certificate to the SSPs administration site using the IIS Management Console. See individual steps detailed above for this process.

2. Change the default Access Mapping for the SSP administration site from the **Operations** tab of Central Administration. Again, see the section above for detailed steps of this task.

3. Set the SSP administration site to require an SSL connection using the IIS Management Console.

Providing Redundancy by Hosting a Second Central Administration Web Application.

By default both MOSS and WSS v3 provide a single Central Administration Web Application. Even though all Web Applications (including Central Administration) are replicated to all Web Front End (WFE) servers, should the original SharePoint server become unavailable, you will lose access to Central Administration. Therefore, it is recommended that in a multi server farm, you have at least two Central Administration web applications for fault tolerance.

To create an additional Central Administration Web Application, we need to run the configuration wizard on a WFE server and then define an Access Mapping to allow us to connect to the Web Application on that server. The Central Administration Web Application can be created either the first time the configuration wizard is run, when joining the server to the farm, or subsequently to add Central Administration to an existing Web Front End server.

The following instructions cover running the configuration wizard on an existing WFE server. For new WFE servers, you should follow the wizard as normal, to add the server to the farm and use the **Advanced** button on the final page, to create the Central Administration Web Application.

1. On the WFE server where you wish to host the Central Administration Web Application, start the **SharePoint Products and Technologies Configuration Wizard** from the **Start** menu. The wizard can be found in either the SharePoint program group or in Administrative Tools.

2. Click **Next** on the first page, to start the wizard proper.

3. Click **Yes** in the pop up dialogue box stating that services will be restarted.

4. Ensure you have the option **Do not disconnect from this server farm** selected, and click **Next**.

5. Click the **Advanced Settings** button.

6. Select the option to **Use this machine to host the web site** and then click **OK**

7. Verify the information, note that the Central Administration URL will still be that of the original server.

8. Click **Next** to start the wizard processing the changes. This can take several minutes, so feel free to amuse yourself while it runs...

9. On the **Configuration Successful** page, click **Finish**.

The reason that the URL displayed at the end of the wizard still maps to the original server, and indeed the fact that if you attempt to connect to Central Administration on the new server, you will be redirected to the original one, is down to access mappings. What is needed, to allow both Central Administration Web Applications to be accessible, is to add the URL of the second server as an alternate access mapping for Central Administration.

1. Open up the Central Administration site. You can connect to the site on the second server by using the full URL **http(s)://MOSS SERVER 2:port/default.aspx**.

2. Select the **Operations** tab.

3. Click the **Alternate access mappings** link in the **Global Configuration** section.

4. Click the **Edit Public URLs** link on the toolbar at the top of the list.

5. In the **Alternate Access Mapping Collection** section, use the drop down box to select **Central Administration**.

6. Now add an additional path for the URL of the additional Central Administration server into one of the other fields, such as Intranet or Custom.