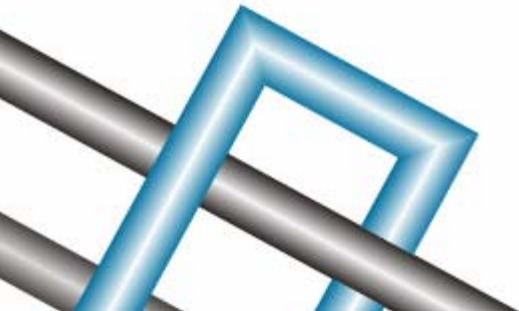


design and
implementation
of strategic
technology
solutions



34736 Moffat Ave., Mission, BC V2V 6R6
Tel: 604.820.1619 Cel: 604.996.6331
gower.mike@shaw.ca www.itblueprint.ca

Publishing Multiple Websites and OWA FBA using SSL Basic Authentication and Wildcard Certificates v1.0.1



Publishing multiple websites and OWA using SSL

Foreword

The OWA implementation builds on testing that was already completed using a non-SSL connection. These steps setup full SSL connectivity from the client to the ISA Server as well as from the ISA server to the Exchange server. Most of these steps were obtained from various tutorials and papers already provided on ISAServer.org, however, this scenario is slightly different than any of the tutorials provided. Please see the end of the document for references to these tutorials and documents.

The following information is provided as-is and is meant to be a solution for the following scenario.

Scenario

In this scenario, the requirements are:

1. Use of an ISA 2004 standard server that has 1 internal and 1 dmz facing nic
2. Publishing more than 1 other web server in addition to the OWA using basic authentication and SSL certificates
3. Publishing OWA using Forms Based Authentication and SSL certificates
4. Use of a stand-alone Microsoft Certificate Authority
5. Externally facing firewall (such as a Cisco PIX) with 1 public (Internet) facing IP address (Note - these instructions will also work if the ISA server is externally facing)
6. Testing has been done with both ISA 2004 and ISA 2004 with SP1 installed

Pre-Installation Comments:

1. You cannot use forms based authentication on the Exchange server if you want to use it on ISA. In this scenario I configure OWA forms based authentication on the SSL listener.
2. There are several generalized names used in this document. You will need to replace instances of these names with your specific local information.
 - a. Replace **fqdn.com** with your company's published domain name. (Example: company.com)
 - b. Replace **CAServer** with the name of your internal stand-alone Certificate Authority Server.
3. The requirements dictate that a wildcard certificate will be used on the ISA server in order to publish multiple web servers/sites.
4. It is assumed that the required ports and configurations have been made on the externally facing firewall to forward port 443 traffic to the ISA Server.

Installation Steps

1. Ensure that your hosted External DNS has an entry for owa.fqdn.com that points to your firewall.
2. Preparing to use certificates - For use with your own Certificate Authority
 - a. Add the Certificate Authority Services to a server. (In the steps below, I used the Exchange 2003 server, although any member domain server will do. These instructions would need to be modified if the CA were added to a domain controller.

- b. Select Stand-alone root CA
 - c. Provide the common name to be used. Recommendation: **fqdn.com**
 - d. Accept the remaining defaults
 - e. Change the default time period validity for issued certificates by going to the following registry key: (The default is 1 year).
 - i. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\fqdn.com [Validity period] changed from 1 to 5
 - ii. For more information, see KB Q239539
3. To publish multiple sites after we publish OWA, we are going to have to use a **wildcard** certificate on the Web listener on the ISA server due to the limitation that you can have only one certificate per IP address per listener. For more information, refer to the following link: [Publishing Multiple Web Sites using a Wildcard Certificate](http://www.isaserver.org/tutorials/2004wildcardcert.html) by Thomas Shinder. (<http://www.isaserver.org/tutorials/2004wildcardcert.html>)
 - a. From the Exchange Server's IIS snapin (can be launched from Start | Administrative Tools) - click on Default Web Site | Properties | Directory Security tab and then click on Server Certificate
 - b. Select **Create a new certificate**
 - c. Select **"prepare the request now, but send it later"**
 - i. Name: Wildcard certificate
 - ii. Organization: <Enter your company/organization name>
 - iii. Organizational Unit: <Enter your department or unit>
 - iv. For common name, use **"*.fqdn.com"** (without the quotes).
 - v. Country: <Enter info>
 - vi. State/Province: <Enter info>
 - vii. City: <Enter info>
 - d. Save to **c:\wildcertreq.txt**
4. Browse to your CA (ie. <http://CAServer/certsrv>)
 - a. Request a certificate
 - b. Advanced certificate request
 - c. Submit a base 64...
 - d. Paste the contents of the **c:\wildcertreq.txt** from the Exchange server into the Saved Request field and submit the request (leaving the attributes field blank)
 - e. Go to the console of the Certificate Authority server and Issue the certificate request (Administrative Tools | Certificate Authority | Select **fqdn.com** | Pending requests and right click on the ID | All tasks | Issue

Note: You can also have the stand-alone CA issue the certificates automatically during this process and then change the process back so that requests must be approved. This may save you a bit of time for other certificates.

 - f. Go back to the OWA Exchange server, browse to the CA (ie. <http://CAServer/certsrv>) and click on View Status of a Pending Certificate
 - g. Click on the saved request, click download certificate, and save the certificate to the local drive (ie. **c:\wildcertnew.cer**)
5. Browse again to the CA (ie. <http://CAServer/certsrv>)
 - a. Click Download a Certificate, change or CRL
 - b. Click **Install this CA certificate chain**
 - c. Click Yes and Yes to accept the certificate
6. From your OWA hosted Exchange servers' IIS Manager, go to the Default Web Site, Directory Security, click on Server Certificate and select Process Certificate, pointing to the saved **c:\wildcertnew.cer** file. Select port 443 and complete the process using defaults.

7. Export the certificate to a file by accessing the IIS default web server on the Exchange Server,
 - a. go to the **Directory Security** tab of the **Default Web Site** and click **View Certificate**
 - b. On the certificate window, select the **details** tab, and click **Copy to file**. In the wizard, select **Yes**, to **export the private key, uncheck strong protection**, and check **“include all certificates”**, **set a password**, and select to save the certificate to a file named **c:\wildcertnew.pfx**. Copy the file to the ISA firewall’s local hard drive.

8. From the ISA Server
 - a. Ensure that the wildcard certificate just created (**c:\wildcertnew.pfx**) has been copied locally.
 - b. On the ISA firewall, click **Start -> Run**, type **mmc** and click **OK**. In the new console either click **CRTL+M**, or select **Add/Remove Snap-in** from the file menu. On the **Standalone** tab, select **Certificates** and click **Add**. Select **Computer Account**, and click **Next**. Select **Local Computer** and click **Finish**. Click **Close** and **OK**.
 - c. Expand **“Certificates”** In the console, right click the **Personal** node, **All Tasks** and click **Import**
 - d. Select the **c:\wildcardnew.pfx** file and supply the password. Ensure that you **Do Not** mark the key as exportable. Use the remaining default values.

At this point, the ISA server has the wildcard certificate installed. We’ll now re-do some steps on the OWA Exchange server.

9. Prepare the new OWA Exchange 2003 certificate
 - a. Log on to the OWA Exchange 2003 server you intend to publish to the web.
 - b. Open the **Internet Information Services (IIS) Manager** tool from the **Administrative Tools** menu, and expand the web sites tree. Locate and click **Properties** on the **Default Web Site**, which holds the OWA virtual directories. Select to the **Directory Security** tab, and click **Server Certificate.... remove current certificate**
 - c. Again, from the Exchange server, go to **IIS Manager, Default Web Site, Directory Security**, and click on **Server Certificate** and **create a new certificate**
 - d. Select to **Prepare the request now, but send it later**, and click **Next**. Leave the certificate name as **Default Web Site**, and the Bit Length: **1024** and click **Next**. Type the name of your organization and an OU, and click **Next**. In the **Common Name** window, make sure to enter the **exact FQDN** that will be used by external users to access the OWA web site. (Example: **owa.fqdn.com**)
 - e. Complete the remaining information and save the file to **c:\owacertreq.txt**.

10. Form a request to create a certificate
 - a. To approve the certificate request, open a web browser on the Exchange server and enter the URL to the CA server. For example: **http://CAserver/CertSrv**.
 - b. On the Certificate Services Welcome screen, click **Request a certificate**. Select advanced certificate request, and click **“Submit a certificate request by using a base 64 encoded...”**
 - c. On the Submit a Certificate Request or Renewal Request page focus on the Saved Request window.
 - d. Open the request file generated earlier, (**c:\owacertreq.txt**), with notepad, and copy the content code between the Begin and End sections, and paste into the Saved Request window.
 - e. When done click **Submit**. Wait for the **Certificate Pending**, and close the web browser.
 - f. Log on to the console of the certificate server, open the **Certification Authority** console from the **Administrative tools** menu. Expand the CA, and navigate to the **Pending Requests** tree. On the right pane you will see the certificate request waiting to be approved. Right click the certificate and select **All Tasks** and then **Issue**. The issued certificate will be moved to the **Issued Certificates** container.

- g. Go back to the OWA Exchange server. Open the web browser and point to **http://CAServer/CertSrv**, and click **View the status of a pending certificate request**. Click the certificate link, and select **Download certificate** using the **DER Encoded**. Save the file to **c:\owacertnew.cer**.
 - h. Open the IIS console on the Exchange server, and again navigate to the **Directory Security** tab of the **Default Web Site**. Click **Server Certificate...** and use the wizard to process the pending request. Provide with the **owacertnew.cer** file, verify port 443 as the SSL port, click Next, Finish, and OK to close the properties page.
 - i. **Restart the Default web site.**
 - j. Ensure that the local Exchange 2003 server has a hosts file entry pointing to the name used. Edit the C:\Windows\System32\Drivers\Hosts file by adding a line pointing to the local exchange server. (Example: **X.X.X.X owa.fqdn.com**), where **X.X.X.X** is the *internal* IP address of the OWA exchange server.
 - k. Open the web browser and point to **http://CAServer/CertSrv**, click on **Download a CA certificate chain...** and then click on **Install this CA**. This step ensures that the Exchange server trusts the root domain (ie. **fqdn.com**)
11. Export the certificate to a file by accessing the IIS default web server on the OWA Exchange Server,
- a. Go to the **Directory Security** tab of the **Default Web Site** and click **View Certificate**
 - b. On the certificate window, select the **details** tab, and click **Copy to file**. In the wizard, select **Yes**, to **export the private key, uncheck strong protection**, and check **“include all certificates”**, **set a password**, and select to save the certificate to a file named **c:\owacertnew.pfx**. Copy the file to the ISA firewall’s local hard drive.
12. From the ISA Server
- a. Ensure that the owa certificate just created (**c:\owacertnew.pfx**) has been copied locally.
 - b. On the ISA firewall, click **Start -> Run**, type **mmc** and click OK. In the new console either click **CRTL+M**, or select **Add/Remove Snap-in** from the file menu. On the **Standalone** tab, select **Certificates** and click **Add**. Select **Computer Account**, and click Next. Select **Local Computer** and click Finish. Click **Close** and **OK**.
 - c. Expand “Certificates” In the console, right click the **Personal** node, **All Tasks** and click **Import**
 - d. Select the **c:\owacardnew.pfx** file and supply the password. Ensure that you **Do Not** mark the key as exportable. Use the remaining default values.
 - e. Ensure that the local ISA server has a hosts file entry pointing to the name used. Edit the C:\Windows\System32\Drivers\Hosts file by adding a line pointing to the local exchange server. (Example: **X.X.X.X owa.fqdn.com**), where **X.X.X.X** is the *internal* IP address of the OWA exchange server.

At this point, the Default web site is SSL enabled, which means you can access it using either HTTP or HTTPS. Test to make sure. Temporarily add any required localhost firewall access rules to do the test from the ISA server.

13. OWA Site configuration
- a. From the IIS manager, expand **Default Web Site**. You will be making modifications to the following site directories:
 - i. **/Exchange**
 - ii. **/ExchWeb**
 - iii. **/Public**
 - b. Start by going to the properties of **/Exchange**
 - c. Click **Directory Security**, click **Edit** and in the Authentication Methods box, remove the checkmark from **all** boxes. Select **Basic** authentication.
 - d. Enter your internal domain name (ie. **fqdn.com**)
 - e. Apply the changes and then repeat these steps for **/ExchWeb** and **/Public**

14. Force SSL on directories
 - a. From the IIS manager, expand **Default Web Site**. You will be making modifications to the following site directories:
 - i. **/Exchange**
 - ii. **/ExchWeb**
 - iii. **/Public**
 - b. Start by going to the properties of **/Exchange**
 - c. Click Directory Security, click **Edit** and in the **secure communications** box and put a checkmark in the **Require 128-bit encryption** checkbox.
 - d. Apply the changes and then repeat these steps for **/ExchWeb** and **/Public**
15. Check Browser Connectivity
 - a. On the ISA server, we need to be able to resolve the common name (**owa.fqdn.com**) to the internal Exchange IP address using DNS
 - b. Open a web browser on the ISA firewall, and enter the URL for test. The URL should be in the form of: **https://owa.fqdn.com/exchange**

From the ISA Server:

16. **Backup the existing ISA configuration** and remove any existing web publishing rules and web listeners (use the Toolbox to remove the web listener) dealing with port 443.

Note: This is where we have to get a little tricky if we want to have OWA use Forms based authentication **AND** be able to publish other websites and use basic authentication. For more information, please see the following link: [Supporting Both Basic and Forms-based Authentication with a Single External IP Address and Web Listener](http://www.isaserver.org/tutorials/2004pubowamobile.html)
(<http://www.isaserver.org/tutorials/2004pubowamobile.html>)

17. Request a certificate from the CA Web enrollment site
 - a. Browse to the CA (ie. <http://CAServer/certsrv>)
 - b. On the Welcome page, click **Request a certificate**
 - c. On the Request Certificate page, Click **advanced certificate request**
 - d. On the Advanced certificate request page, click **Create and submit a request to this CA**
 - i. In the **name** field, for the common name, enter **localhost** into the text box
 - ii. Select **Server Authentication Certificate** from the template list
 - iii. Put a checkmark in the **Store certificate in the local computer certificate store**
 - iv. Click Submit
 - e. Click Yes in the **Potential Scripting violation** dialog box
18. From the CA Server, launch the Certificate Authority and issue the certificate for the new pending request.
19. Return to the ISA server, browse to the CA (ie. <http://CAServer/certsrv>) and click on **View the status of a pending certificate request**
 - a. Click on the certificate in question, and then click on the **Install this certificate** link, clicking YES to install the certificate. Close the browser.
20. Create a Web Publishing Rule that forwards Incoming OWA Requests to the localhost Web Listener (or edit the Wildcard SSL listener previously created by changing the name and the authentication type from Integrated to Basic). If creating new, use the following steps:
 - a. Task pane | Publish a Mail Server
 - b. Name: **Main OWA FBA (External to Localhost)**
 - c. Select **Web client Access** for Access type
 - d. Select **Outlook Web Access** for Services
 - e. Select **Secure connection to clients and mail server** for the Bridging mode
 - f. On the **Specify the Web Mail server page**, enter **localhost** in the **Web mail server** text box
 - g. On the public Name details page, enter **owa.fqdn.com**
 - h. Create a new web listener

- i. Name: **OWA SSL External (basic)**
- ii. Network: **External**
- iii. Port Specification: remove HTTP, Enable SSL
- iv. Click on **Select** and provide the wildcard certificate (***.fqdn.com**)
- v. Finish the Listener setup
- vi. Click Edit on the Listener, and under Preferences | Authentication, remove the checkmark on Integrated and select Basic and YES to the warning.
- vii. Finish the rule and then right click on **Properties** for the rule just created.
- viii. Click on the **Paths** tab.

- 1. Click **Add**
- 2. Enter the value **/cookieauth.dll**

Note: If you wish to redirect requests for **https://owa.fqdn.com** to **https://owa.fqdn.com/exchange** you must also enter the following value in the **Paths** tab.

- 3. Enter the value **/exchange** pointing to \

- ix. Note: The paths should look like the following:

| | |
|--------------------|-----------------|
| <same as internal> | /cookieauth.dll |
| <same as internal> | /exchange/* |
| <same as internal> | /exchweb/* |
| <same as internal> | /public/* |
| / | /exchange\ |

- x. Select the same as published folder and click Apply and OK
- xi. Ensure that **“Requests appear to come from ISA server and require 128 bit encryption is selected”**

- 21. Create a Web Publishing Rule that forwards Incoming requests to the LocalHost Listener to the OWA Web Site

- a. Task pane | Publish a Mail Server
- b. Name: **Secondary OWA FBA (Localhost to Exchange)**
- c. Select **Web client Access** for Access type
- d. Select **Outlook Web Access** for Services
- e. Select **Secure connection to clients and mail server** for the Bridging mode
- f. On the **Specify the Web Mail server page**, enter **owa.fqdn.com** in the **Web mail server** text box
- g. On the public name details page, select **Any domain name** in the **Accept requests for** list
- h. Create a new web listener
 - i. Name: **OWA SSL LocalHost (basic)**
 - ii. Network: **Localhost**
 - iii. Port Specification: remove HTTP, Enable SSL checkbox
 - iv. Click on **Select** and provide the **localhost** certificate
 - v. Finish the Listener setup
 - vi. Click Edit on the Listener, and under Authentication, remove the checkmark on Integrated and select **OWA Forms-based**
 - vii. Finish the rule and then right click on **Properties** for the rule.
 - viii. **Paths** tab: remove all existing paths. Click **Add**, and enter **/*** in the Specify the folder on the Web Site that you wish to publish. Select the **Same as published folder** option.
 - ix. Ensure that **“Requests appear to come from ISA server and require 128 bit encryption is selected”**

Let us now say that you need to publish another web site on a different internal IIS server. For the purpose of this example, we will access a training server.

22. Create a Web Publishing Rule that forwards all training traffic to the appropriate web site connections. (Example: training.fqdn.com)
 - a. Task pane | Publish a Mail Server
 - b. Name: **NON-OWA WebServer Rules - Training**
 - c. Select **Web client Access** for Access type
 - d. Remove checkmarks for OWA and add OMA
 - e. Select **Secure connection to clients and mail server** for the Bridging mode
 - f. On the **Specify the Web Mail server page**, enter **training.fqdn.com** in the **Web mail server** text box
 - g. On the public Name details page, enter **training.fqdn.com**
 - h. For the web listener, select the **OWA SSL External Wildcard Listener**
 - i. Accept all Users
 - j. Finish the rule and then right click on **Properties** for the rule.
 - k. **Paths** tab: Remove the existing OMA path and add any paths required for the training server. (Example: Click **Add**, and enter **/training/*** in the Specify the folder on the Web Site that you wish to publish. Select the **Same as published folder** option.)

Let us now say that you need to publish a third web site on a different internal IIS server. For the purpose of this example, we will access a sharepoint server.

23. Create another Web Publishing Rule that forwards all sharepoint (portal) non-OWA traffic to the appropriate web site connections. (Example: **portal.fqdn.com**)
 - a. Task pane | Publish a Mail Server
 - b. Name: **NON-OWA WebServer Rules - Portal**
 - c. Select **Web client Access** for Access type
 - d. Remove checkmarks for OWA and add OMA
 - e. Select **Secure connection to clients and mail server** for the Bridging mode
 - f. On the **Specify the Web Mail server page**, enter **portal.fqdn.com** in the **Web mail server** text box
 - g. On the public Name details page, enter **portal.fqdn.com**
 - h. For the web listener, select the **OWA SSL External Wildcard Listener**
 - i. Accept all Users
 - j. Finish the rule and then right click on **Properties** for the rule.
 - k. **Paths** tab: Click **Add**, and enter the directory to be published in the form of **/sharepointdir/*** in the Specify the folder on the Web Site that you wish to publish. Select the **Same as published folder** option.
24. Ensure that the host files on the sharepoint, training, exchange and ISA servers have been changed to reflect the required entries. Specifically, entries for **portal.fqdn.com** and **training.fqdn.com** and **owa.fqdn.com** should exist; pointing to the internal IP address of each server.
25. Cleanup - remember all those certificates that were saved to the local hard drives of the servers - you should go back and delete them now!

References:

1. [Publishing Multiple Web Sites using a Wildcard Certificate](http://www.isaserver.org/tutorials/2004pubowamobile.html), (http://www.isaserver.org/tutorials/2004pubowamobile.html) by Thomas Shinder
2. [Supporting Both Basic and Forms-based Authentication with a Single External IP Address and Web Listener](http://www.isaserver.org/tutorials/2004pubowamobile.html), (http://www.isaserver.org/tutorials/2004pubowamobile.html) by Thomas Shinder and Kai Wilkes