

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

PART I

Lately we have seen more interest in certificate based authentication with Exchange 2007 Outlook Web Access. Using certificates for authentication can be considered more secure because a user cannot gain access to the mailbox simply by knowing the user name and password. The certificate option prevents key loggers or other malware on a client machine capturing keystrokes to identify user account and passwords.

With a combination of a Certificate Authority, Exchange Server 2007 and ISA Server 2006 you can provide a certificate based authentication configuration with minimum changes to your current environment. A Windows 2003 Certificate Server, or your own trusted third party certificate provider can be used to provide user certificates. The advantage of the Windows certificate server is it allows for the auto-enrollment and publishing of certificates to Active Directory.

This post will not cover more advanced topics on how to properly set up a PKI infrastructure, or install and configure ISA server. It assumes these prerequisites are already in place and functioning. This document covers configuring Exchange 2007 client access server to Exchange 2007 mailbox servers. The steps for configuring Exchange 2003 configuration can be found at <http://technet.microsoft.com/en-us/magazine/cc137993.aspx>. I will post a follow up to outline the steps needed for Exchange Server 2007 on Windows 2008 with IIS 7.

Requirements

PKI environment

- The user certificate must be issued for Client Authentication. The default User template from a Windows certificate server will work in this scenario.
- The certificate can be on a Smart Card or in the in the personal certificate store of the client operating system.
- All Certificate Authorities must be included in the NTAAuthCertificates Container. Knowledge base article KB 295663 describes the process. <http://support.microsoft.com/kb/295663> .
- The User Principle Name (UPN) value for each user account must match the Subject Name field on the user's certificate.
- All servers must trust the entire Certificate Authority chain. This includes the ISA, CAS, and client workstation. The Certificate Authority Root certificate must be in the Trusted Root Certification Authorities store on all of these systems.

Active Directory

- The domain must be set to the Windows Server 2003 Domain Functional Level.
- Kerberos Constrained Delegation will be configured between the ISA and CAS computer accounts.

Exchange Configuration

- The Exchange CAS role server must require SSL at 128 bit strength on the Default Web Site.
- Forms Based Authentication cannot be used with certificate based authentication.
- Integrated authentication must be set on the OWA virtual directory.

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

ISA 2006 Server

- All ISA Servers and Exchange Servers must be members of the same Active Directory domain. Kerberos Constrained Delegation only works within the same domain.
- The ISA Server must be able to perform Certificate Revocation Checking. This is commonly called the CRL (pronounced Krill) list.
- OWA publishing rule must have the correct service principal name for the internet facing CAS servers. You can verify service principal names with the SetSPN utility. This utility is included with the Windows 2003 support tools.

Configure ISA Server 2006

Configure Kerberos Constrained Delegation

1. Open Active Directory Users and Computers
2. Go to the properties of the ISA computer account and click the delegation tab.
3. Select the **Trust this computer for delegation to specified services only** option and then select the **Use any authentication protocol** option. Click the **Add** button.
4. This will open the Add Services window. Click the Users or Computers button.
5. Enter the name of your internet facing CAS server and click **OK**.
6. After clicking **OK** a list of Service Principal Names (SPN) will be displayed for your server.

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

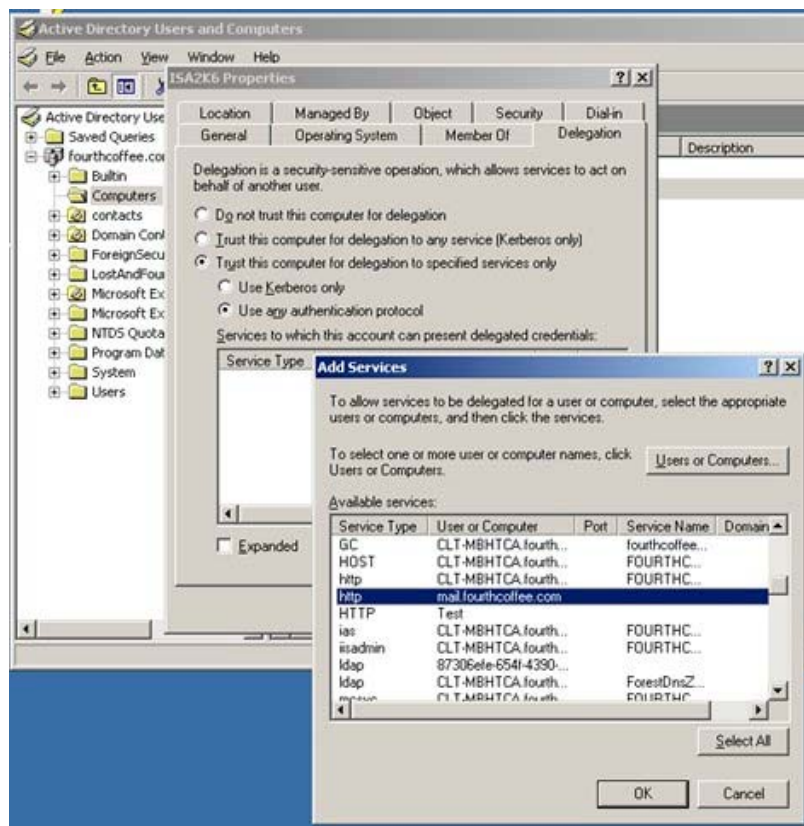
7. Select the appropriate HTTP SPN for your internet facing CAS server. You will need to add your Internet facing CAS role servers to this list. By default you will only see the HTTP/FQDN SPNs.

In my example I created a custom SPN record `http/mail.fourthcoffee.com` with the SetSPN.exe utility. This utility is included with the Windows Server 2003 support tools. Here is the TechNet document that covers the creation of SPN records and how they are used for constrained delegation:

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/df979570-81f6-4586-83c6-676bb005b13e.mspx?mfr=true>

Modifying the OWA Web Publishing Rule

1. This section assumes you already have an OWA publishing rule in place. We will only make the necessary changes to allow for certificate based authentication.
2. Open the ISA server management console
3. In the left pane expand Arrays/Server Name and highlight the Firewall Policy.
4. Open the properties of your Exchange 2007 Web Publishing rule.
5. Click on the Authentication Delegation tab.
6. Set the **Method used by ISA Server to authenticate to the published web server** to Kerberos Constrained Delegation.
7. Enter the correct SPN value for Kerberos Constrained Delegation. This needs to match the SPN you



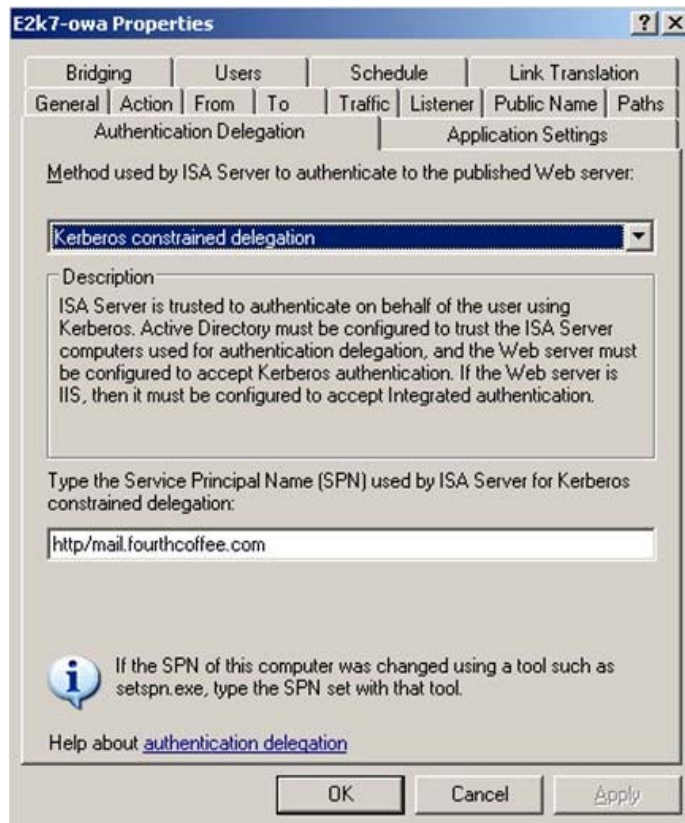
How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

selected for the computer account delegation.

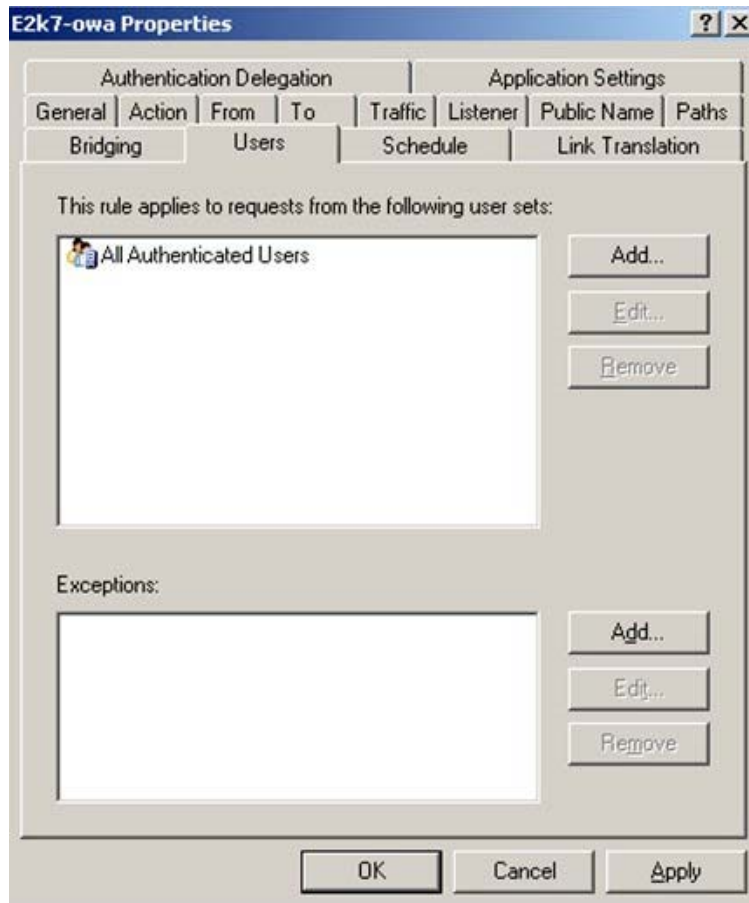
8. Click on the Users Tab. **All Authenticated** users should be listed.



How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog



Configure the Web Listener for the OWA publishing rule

You need to know what ISA rules are using the OWA listener before making this change. Setting the authentication as I do below could impact other websites or services that are published with this listener.

1. Go to the Listener tab of the OWA publishing rule.
2. Click the properties button.
3. Go to the Authentication tab.
4. Set **Method client uses to authenticate to ISA server** to **SSL Client Certificate Authentication**.

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog



6. Click the **Advanced** button on the Web Listener button

7. Check the box for **Require all users to authenticate**.



8. Click **OK** for all of the Web listener property pages.

9. Click **OK** the web publishing rule property page.

10. Click the Apply button to update the ISA configuration.



How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

Exchange Server 2007 CAS Configuration

You must enable integrated authentication on /OWA virtual directory. When you do this it will disable Forms Based Authentication. This can be done either through the management console or the management shell.

Configure Integrated Windows Server Authentication

Just to remind you these steps are for a CAS to Exchange 2007 mailbox servers. Setting integrated authentication on the /Exchange virtual directory requires configuring additional Kerberos constrained delegation. This means mailboxes Exchange 2003 server will not work until KCD is configured correctly.

1. Open the Exchange management Console.
2. Expand Server configuration in the left pane, and highlight Client Access.
3. In the middle pane highlight the internet facing CAS name.
4. Open the properties of the **OWA (Default Web Site)**.
5. Select the **User one or more standard authentication methods**: radio check box.
6. Select the **Integrated Windows Authentication** check box.
7. Click **OK**.
8. You will then be shown a dialog box that states IISReset /noforce must be run before changes become effective. Click OK to this box.
9. From a command prompt, run **iisreset /noforce**. This will restart the IIS services.

User Configuration in Active Directory

The user accounts that will use certificate based authentication must have the user certificate published to the Active Directory account. If you are using a Windows 2003 PKI Root Certificate Authority this is done by default.

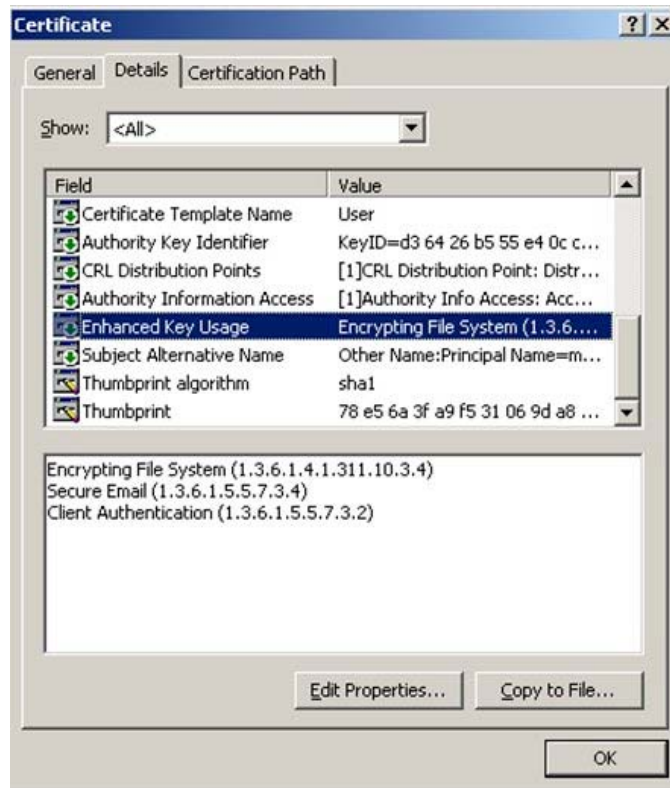
Verify the published User certificate in Active Directory

1. Open Active Directory Users and Computers.
2. Open the properties of the user account in question and click on the Published Certificate tab.
3. Double click the certificate to open it. Verify the following:
 - **General tab**: The valid from data must not be expired.
 - **Details Tab**
 1. Subject field must have the UPN matching the user account.
 2. Enhanced key Usage field must have Client Authentication.
 3. CRL Distribution Points must be accessible by the ISA server (either LDAP or HTTP)
 - **Certification Path tab**: The icons for the certificate chain must be green. If they are yellow or red then there is a problem with that certificate. You can double click the individual certificates to view them.

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog



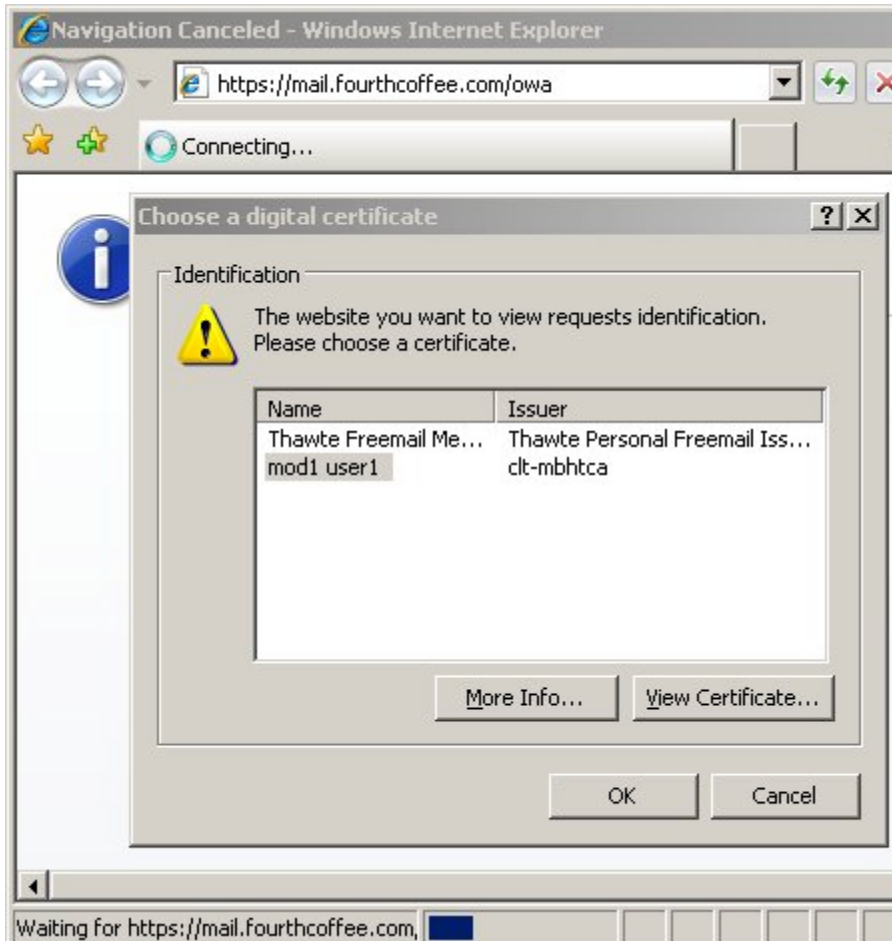
How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

What the clients see after these changes

When the user browses to the OWA URL, they will be prompted to supply their certificate. If the certificate is in the Personal certificate store, they can choose it from the list. Or they can have the certificate stored on a smartcard. At this point they would insert it into the smartcard reader.



After clicking OK, the user will be taken to the OWA page just as if they had entered the user name and password. If they do not have a certificate, or supplied a wrong or invalid certificate, the client would receive a 401 Unauthorized page with an ISA 12209 error code.

Windows Server 2003

- Public Key Infrastructure for Windows Server 2003
<http://www.microsoft.com/windowsserver2003/technologies/pki/default.aspx>
- Managing a Windows Server 2003 Public Key Infrastructure
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.aspx>
- Service principal names with Windows 2003
<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/df979570-81f6-4586-83c6-676bb005b13e.mspx?mfr=true>

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

Microsoft ISA Server 2006

- Microsoft ISA Server 2006: Enterprise Edition Installation Guide
http://www.microsoft.com/technet/isa/2006/deploy/ee_install_guide.mspx
- Publishing Exchange Server 2007 with ISA Server 2006
<http://www.microsoft.com/technet/isa/2006/deployment/exchange.mspx>
- Using ISA Server 2006 with Exchange 2007
<http://technet.microsoft.com/en-us/library/aa998036.aspx>
- Configuring ISA Server 2006 for Exchange Client Access
<http://technet.microsoft.com/en-us/library/aa997148.aspx>

PART II

In my last [post](#) I showed how to set up OWA certificate based authentication on a Windows 2003 CAS with ISA 2006. In this post, I will cover how to set this up when your Client Access server is running on Windows 2008 server *without* being published with ISA server.

Note: These steps are only for Exchange 2007 mailboxes, and will not work for the /Exchange virtual directory. Your PKI infrastructure should already be in place as well. This can be a Windows 2003 or Windows 2008 certificate server, or your favorite third party vendor.

First up is to see if the Client Certificate Mapping Authentication [Web-Client-Auth] component of IIS is installed. This component is not required to install Exchange 2007 so will most likely need to be installed. You can add this via Server Manager or with the ServerManagerCMD like below. A reboot of the server is required after the install.

ServermanagerCMD -query will give you a list of components installed. Look at the Web Server/Security section and see if Web-Client-Auth is installed. If not, install it.

ServerManagerCMD -install Web-Client-Auth

After the reboot you can begin configuring IIS.

1. Open IIS Manager and highlight the server name in the left hand pane.
2. Double click the Authentication icon in the middle pane.
3. Right click on Active Directory Client Certificate Authentication and select Enable.
4. Select the OWA virtual directory in the left pane under the Default Web Site.
5. Double click on the SSL Settings icon.
6. Set the Client Certificates radio button to Require.
7. Click Apply.

The next settings for IIS need to be done using the appcmd.exe command line utility. This is located in the `windows\system32\inetsrv` directory. This command allows you to unlock the XML configuration file to allow Client Certificate Mapping Authentication to be enabled.

```
appcmd unlock config /section:clientCertificateMappingAuthentication
appcmd set config "Default Web Site/OWA" -section:clientCertificateMappingAuthentication /enabled:true
```

How To Configure Certificate Based Authentication For OWA

DJ Ball

Microsoft Exchange Team Blog

Now just configure the OWA virtual directory from the Exchange Management shell. This will turn off forms based authentication, set Windows Authentication and Basic Authentication to false. Users will be required to present a certificate to access OWA after this step.

```
set-owavirtualdirectory -identity "server-name\OWA (Default Web Site)" -WindowsAuthentication:$false -  
BasicAuthentication:$false FormsAuthentication:$False  
IISreset /noforce
```

More information:

There is a new IIS 7 Administration Pack that has been released. This tool adds a configuration editor to the feature view in IIS manager. This will allow you to make the certificate mapping changes in IIS manager instead of using the AppCmd.exe utility. This tool is still a technical preview tool so I did not cover the steps. If you are interested you can get more details over on the [iis.net](#) page here, and download the tool here.