Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

How to publish Microsoft Exchange Active Sync (EAS) with ISA Server 2006 – Part one

Abstract

In this article series, I will show you how to publish Microsoft Exchange Server Active Sync (EAS) with ISA Server 2006 to provide secure e-mail access for you Windows Mobile 5 and 6.x clients.

Let's begin

In part one of this article series, I will give you some basic information how Exchange Direct push works and what steps have to be completed on Exchange and IIS site to publish Microsoft Exchange Active Sync.

Exchange Server 2003 provides secure access to your Exchange Server mailbox for mobile devices with Windows Mobile 5 and higher. With every Exchange Server version Microsoft extends and simplifies the mobile experience but it is always the same question how to provide secure mobile access from the Mobile clients to your internal network. The most extended Windows Mobile experience for Exchange Server 2003 comes with Service Pack 2. Exchange Server 2007 offers many more enhanced and new Windows mobile features as its predecessor Exchange Server 2003. One of the solutions is to use ISA Server 2006 which offers a wide range of security options, from HTTPS-Bridging for prae authentication of clients and access to only one URL.
For this article we will extend the security of our mobile client access with the help of client certificates on the mobile devices. Only a mobile client with a valid client certificate from our internal trusted CA is allowed to access the Exchange Server. It is also possible to extend the security, if ISA would only trust certificates from the issuing certificate security. I will tell you how later in this document.

On Exchange site

There are only a few steps to be done on the Exchange Server. Start the Exchange System Manager and navigate to the mobile service properties.

You must e*nable Direct Push over HTTP(s)* to allow access for Windows Mobile clients. Your Windows Mobile device must be version 5 or higher with MSFP (Messaging Security and Feature Pack).

Please note:

If you want to extend the security of your Exchange environment in the way to prevent some mobile clients from accessing the Exchange Server, read the following article:
http://msexchangeteam.com/archive/2008/09/05/449757.aspx

As an optional but recommended step you should also enable Device Security to enhance the security of your mobile devices.

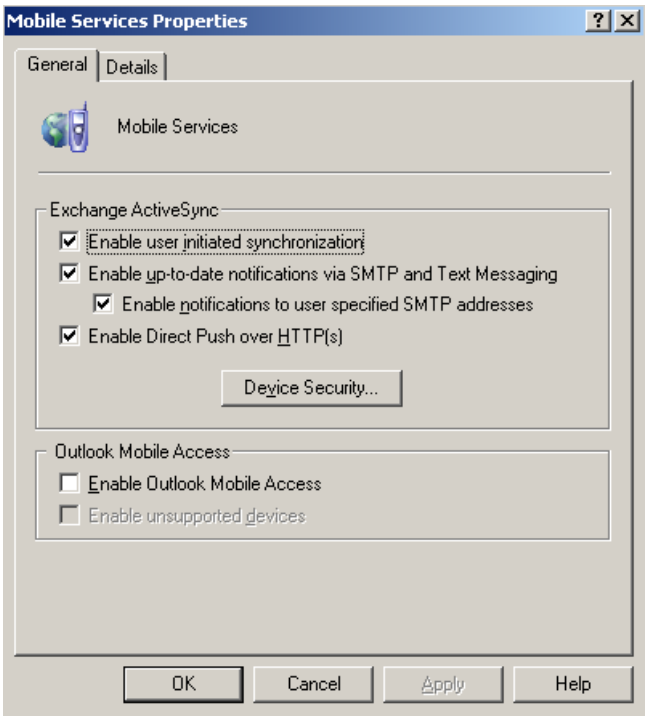

Figure 1: Enable Direct Push over HTTP(s)

There are several options which can be activated and enforced. You must decide which of these options are helpful for your Exchange organization and your mobile users.

As a recommended minimum password length you should enforce a minimum of 8 characters for passwords and passwords should require numbers and letters.

Figure 2: Device security settings

In my opinion it is always a good idea to wipe a device after a number x of failed logon attempts. A wipe after eight attempts is a good starting point.

For advanced Windows Mobile Device Administration, you should have a look at the upcoming Microsoft System Center Mobile Device Manager 2008. With the help of

the Microsoft System Center Mobile Device Manager (SYMDM), it is possible to centrally manage all parts of your Windows Mobile devices. You can find more information about WMDC on the following website: http://www.microsoft.com/windowsmobile/en-us/business/solutions/enterprise/mobile-device-manager.mspx. Microsoft System Center Mobile Device Manager requires Windows Mobile 6.1 clients or higher.

On IIS site

Because we want to secure the traffic between the Exchange Server and the Windows Mobile device, we must issue a webserver certificate which will be used to secure the communication. IIS needs a certificate for the default website. Because we are using an internal Enterprise CA in this article, it is possible to request the certificate from this CA.
If you don't have an internal CA, it is also possible to use tools which generate self signed certificates. One example of such a tool is SELFSSL from the IIS6 resource kit. If you use a self signed certificate it is necessary to import the self signed certificate also into the trusted Root CA certificate store on the Exchange and ISA Server.

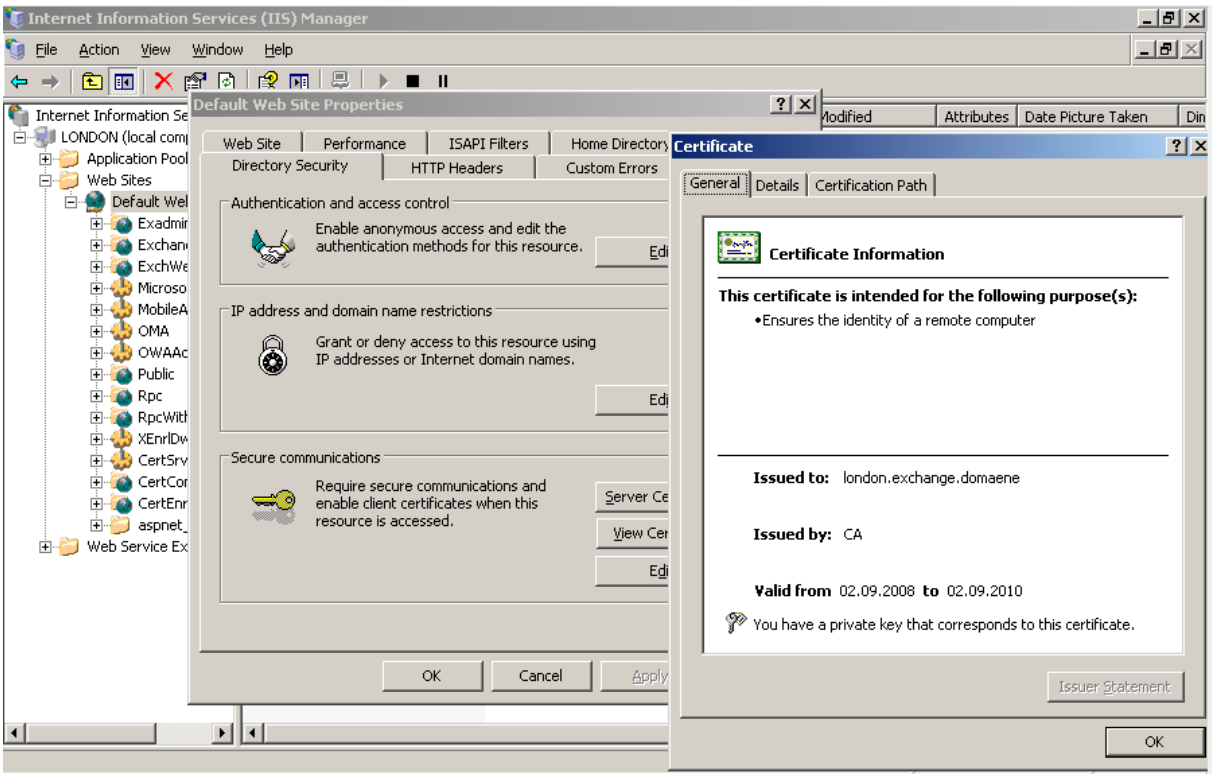

Figure 3: SSL certificate for the default IIS website

Please note:

The name that you use here is also part of the Common Name (CN) in the certificate. Please keep in mind that you have to use this name in the ISA publishing rule in the "to" field.

The dilemma

Microsoft Exchange Active Sync requires that for the Exchange virtual directory SSL is not enforced. That means if you not require SSL, users can access OWA with or without SSL. This should be no problem when you keep sure that ISA Server doesn't allow HTTP access to the OWA website.
If you are not lucky with this setting, it is possible to enforce SSL on the Exchange default website and to use Microsoft Exchange Active sync with a little bit more work. Read here how to do this. As a short note, the trick is to create an additional virtual directory for Exchange Active Sync. You have to copy the default /Exchange virtual directory to the new directory and after that you must point Exchange Active Sync to the new virtual directory. This is done via a registry key change.

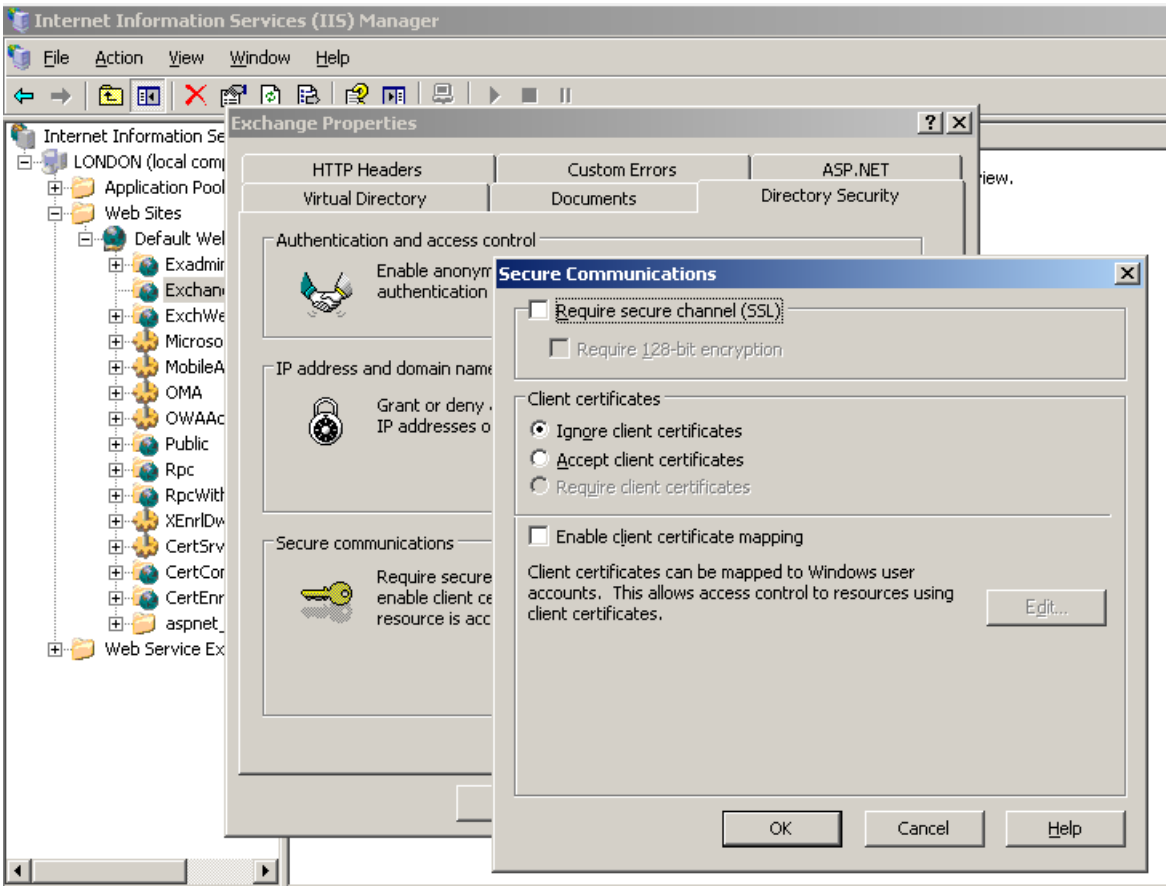

Figure 4: Do not require SSL on the Exchange virtual website

You also have to enable the use of client certificates. Enable *Require client certificates* and *Enable client certificate mapping.* Klick *Edit* and OK (you doesn't have to change something here; you must only klick *Edit* and *OK*, to enable the feature).

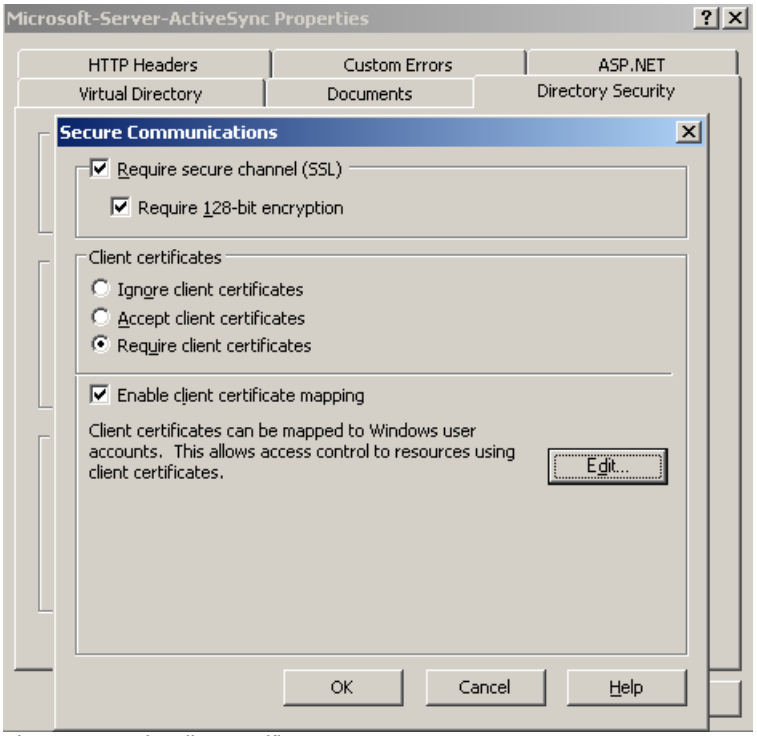

Figure 5: Require client certificates

As a last step we have to enable the Windows directory service mapper in the properties of the Websites section under the IIS computer object in IIS manager.

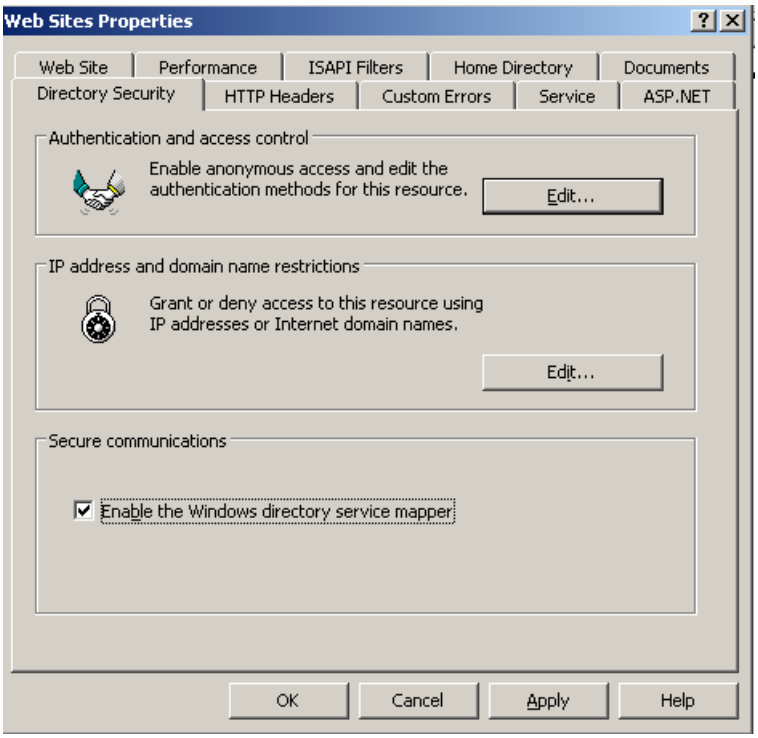

Figure 6: Enable the Windows directory service mapper

Kerberos constrained delegation

Because we are using client certificates, ISA must impersonate the authentication process and authenticate the user, so we have to use KCD (Kerberos constrained delegation). This is also one reason why ISA Server must be a member of the Active

Directory domain. Start the Active Directory Users and computers SnapIn (DSA.MSC), navigate to the ISA Server object – Delegation and activate the trusted for Delegation process for the HTTP and W3SVC process of the Exchange Server.

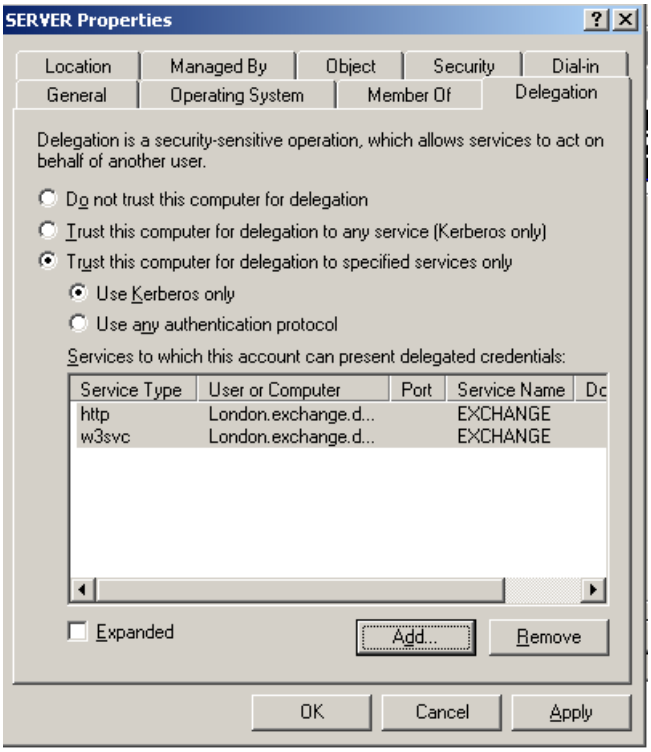

Figure 7: KCD

If you can't see the delegation tab you have to enable the *Advanced view* in DSA.MSC.

Requesting a certificate for the ISA publishing rule

As a next step we have to request on ISA Server for the public name of the publishing rule. You must request a certificate with the CN=Public name which is used as the external Server name in the mobile device configuration for EAS.

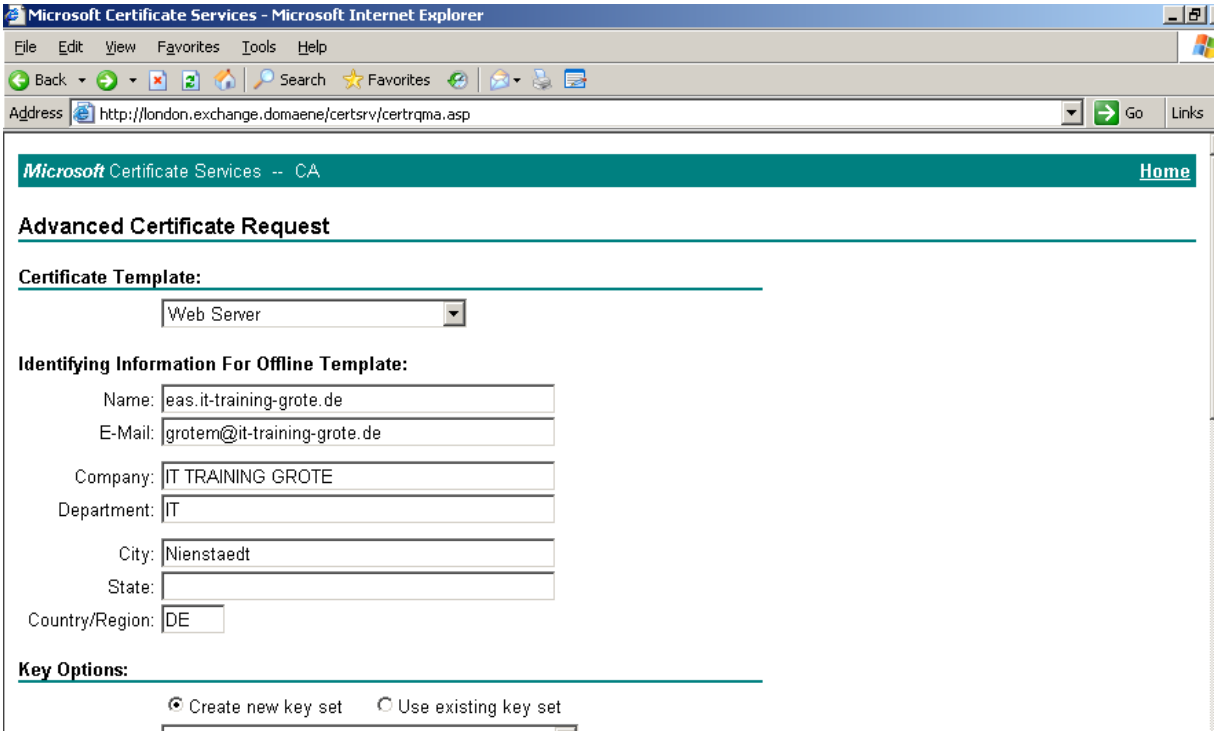

Figure 8: Request a certificate on ISA Server

If you cannot open the certsrv website on ISA Server you have to create a Firewall rule that allows HTTPS from LOCALHOST to the CA server.

Conclusion

In this article, I tried to show you how to use Exchange Active Sync with ISA Server 2006 and Exchange Server 2003 SP2 and client certificates. The combination of ISA Server 2006 and client certificates gives you a maximum of Security for Exchange Active Sync. As you have seen, multiple steps are required to enable Exchange Active Sync in this configuration and there are some pitfalls like wrong certificates and not correctly configured Kerberos Constrained Delegation, but I hope that this article will give you a good understanding how to implement a scenario like this in your environment.

Related links

Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2
http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx
How to use Microsoft Exchange Active Sync with SSL
http://support.microsoft.com/kb/817379/en-us
Microsoft Device Emulator 3.0 -- Standalone Release
http://www.microsoft.com/downloads/details.aspx?familyid=a6f6adaf-12e3-4b2f-a394-356e2c2fb114&displaylang=en
Securing Exchange Data from Unapproved Mobile Devices (or how to block a phone or service from taking data out of your Exchange Server)
http://msexchangeteam.com/archive/2008/09/05/449757.aspx
Microsoft System Center Mobile Device Manager 2008

http://www.microsoft.com/windowsmobile/en-us/business/solutions/enterprise/mobile-device-manager.mspx