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

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

This is part two of the article series how to publish Microsoft Exchange Active Sync with ISA Server 2006. I will show you how to create the ISA Server Web publishing rule and the Windows mobile device configuration.

The ISA publishing rule

After everything is configured on the internal network, we can now start by creating a new Exchange publishing rule. You should give the rule a name like *EAS publishing* or something else which is easy to remember.

The Exchange version is Exchange Server 2003 and we would only publish Exchange Active Sync.

Please note:

If you want to publish Exchange Active Sync with Exchange Server 2007, the publishing process on ISA Server is quite similar, but the configuration steps on Exchange Server site are more different. You can read <u>here</u> more about these steps.

New Exchange Publishing Rule Wiz	zard	X
Select Services Select the services that you ar	e publishing on this mail server.	
Exchange <u>v</u> ersion:	Exchange Server 2003	•
Web client mail services:		
Outlook Web Access		
Outlook <u>R</u> PC/HTTP(s)		
🔲 <u>P</u> ublish additional folde	rs on the Exchange Server for Outlook 2007 clients	
☐ Outlook Mobile Access ✓ Exchange ActiveSync		
	< <u>B</u> ack <u>N</u> ext > Car	ncel

Figure 1: Publishing EAS

Click Publish a single Website or Load Balancer

We will use SSL to connect to the published Web server or server farm, because we also enabled the use of SSL on the Microsoft-Server-ActiveSync directory.

Enter the internal site name. Please remember that the internal site name must match the Common Name of the certificate issued to the Exchange Server and the name must be resolvable from ISA Server. Before you click next, try to ping the Exchange Server by the name you enter in the following picture.

New Exchange Publishing Rule Wizard	×		
Internal Publishing Details Specify the internal name of the Exchange site or server you are publishing.			
Internal site name: Iondon.exchange.domaene The internal site name is the name of the Web site you are publishing as it appears internally. Typically, this is the name internal users type into their browsers to reach the Web site.			
The internal site name must match the common or subject alternative name (SAN) on the certificate bound on the Web site that you are publishing. If ISA Server cannot resolve the internal site name, ISA Server can connect using the computer name or IP address of the server hosting the site.			
Use a computer name or IP address to connect to the published server			
Computer name or IP address:			
< <u>B</u> ack <u>N</u> ext > Cancel			

Figure 2: Specify the internal Server name

Enter the public name which you will use in the mobile device configuration (remember that you have issued a certificate on ISA which Common Name (CN) must match with the public name).

New Exchange Publishing Rule Wizard	ł	×
Public Name Details Specify the public domain name (Fi published site.	QDN) or IP address users will type to reach the	
<u>A</u> ccept requests for: Only requests for this public name or IP	This domain name (type below): address will be forwarded to the published site.	•
P <u>u</u> blic name:	EAS.IT-TRAINING-GROTE.DE Example: www.contoso.com	
	< Back Next > C	ancel
	< <u>B</u> ack <u>N</u> ext > C	ancel

Figure 3: Public name details

Create a new Weblistener and name it EAS or something like that.

Require SSL secured connections with clients

In the Weblistener properties specify the external network as the source for the listener. If you plan to use more than on listener, specify the IP address which will be used to publish EAS.

Select the certificate for the EAS publishing rule. If the certificate doesn't show in the console, check that the certificate is in the local computer certificate store, that the certificate has a corresponding private key, that the certificate is valid and can be verified to the certificate chain path.

New Web Listener Definition Wizard					
Listener SSL Certificates Select a certificate for each IP address, or specify a single certificate for this Web listener.					
¢	Use a <u>single certificate for this Web Listener</u> eas.it-training-grote.de Select Certificate				
С	Assign a certificate for				
	IP Address	Network	Server	Certificate	
				Selec <u>t</u> Certificate	B
			< <u>B</u> ack	<u>N</u> ext >	Cancel

Figure 4: Select the certificate for the EAS publishing rule

As the authentication method you must select SSL Client Certificate Authentication.

New Web Listener Definition Wizard		×
Authentication Settings Select how clients will authenticate to ISA their credentials.	Server, and how ISA Server will validate	
Select how clients will provide credentials to	ISA Server:	
SSL Client Certificate Authentication		
Select how ISA Server will validate client cre	dentials:	
Mindows (Active Directory)	C RADIUS <u>O</u> TP	
C LDAP (Active Directory)	C RSA SecuriD	
O RADIUS		
Help about authentication settings		
	< <u>B</u> ack <u>N</u> ext> 0	Cancel

Figure 5: Select the authentication method

If you use client certificate authentication, ISA Server must be able to access the internal CA Server to access the CRL (Certificate Revocation List). If you click Yes, ISA Server will enable a system policy rule to get access to the internal network for CRL download.

Microsoft	Internet Security and Acceleration Server 2006	×
?	For SSL client certificate authentication, the system policy rule "Allow all HTTP traffic from ISA Serv to all networks (for CRL downloads)" must be enabled. This rule allows the latest Certificate Revocation List (CRL) to be downloaded to ISA Server for certificate validation. Certificates that cannot be validated will be considered revoked, and traffic will be denied. For more information, clie the Help button.	
	Do you want this system policy rule to be enabled?	
	<u>[Yes</u>] <u>N</u> o Help	

Figure 6: Enable a system policy rule for HTTP access

In a client certificate scenario with ISA Server we must use Kerberos Constrained Delegation (KCD), so ISA Server can impersonate the user to authenticate them against the authentication provider which is Active Directory.

New Exchange Publishing Rule Wizard			
Authentication Delegation Authentication delegation is the method ISA Server uses to authenticate the session it opens with the published site.			
Select the method used by ISA Server to authenticate to the published Web server:			
Kerberos constrained delegation			
Description ISA Server is trusted to authenticate on behalf of the user using Kerberos. Active Directory must be configured to trust the ISA Server computers used for authentication delegation, and the Web server must be configured to accept Kerberos authentication. If the Web server is IIS, then it must be configured to accept Integrated authentication.			
Type the Service Principal Name (SPN) used by ISA Server for Kerberos constrained delegation:			
http/london.exchange.domaene			
You may need to add this SPN to Active Directory.			
Help about <u>authentication delegation</u>			
< <u>B</u> ack <u>N</u> ext > Cancel			

Figure 7: KCD

The SPN (Service Principal Name) is based on the internal site name. Under some circumstances you have to manually add the SPN to ISA Server with the help of the command line tool SETSPN. You will find the SETSPN tool in the Windows Server 2003 support tools which can be found on the Windows Server 2003 CD or better as an updated version on the Microsoft <u>website</u>.

Specify the user group which is allowed to get access through the ISA publishing rule to the published Exchange Server.

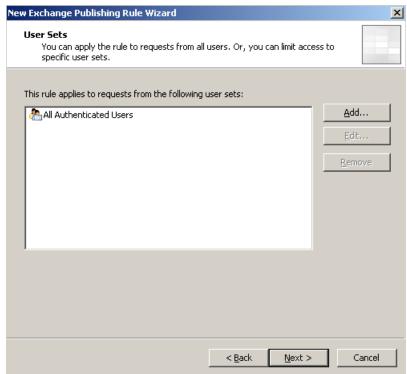
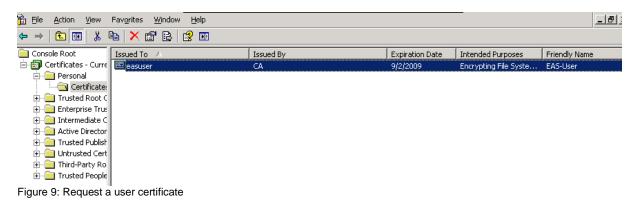


Figure 8: Select the user group which is allowed to access the internal network

The user also needs a certificate published to Active Directory. You must logon with the user credentials and request a user certificate. You can do this with the local MMC SnapIn.



Please note:

In this example we use this not user friendly and a little bit complicated process. If you must enable EAS with client certificates for a bunch of users you can use tools like <u>CertAuthTool</u> to automate this process, but this is out of the scope of this article.

In the next picture you can see the public key certificate mapped to the user account which would like to use Exchange Active Sync from his mobile device.

easuser Properties			? ×
Environment Sess Exchange Exchange F General Addres Published Certifical	General eatures s Account tes Member D)f Dial-in Object	es
Issued To	Issued By	Intended Purposes	Expiration
easuser	CA	Encrypting File Syste	02.09.20
.▲	Add from File	<u>V</u> iew Cer ∑iew Cer	▶ tificate py to File
		1	
0	IK Can	cel <u>A</u> pply	Help

Figure 10: Public key published in the user properties

Mobile device configuration

If you don't want to use a physical mobile device to test EAS with client certificates, you can use a Windows Mobile Device emulator like the Microsoft Device Emulator 3.0. You can find the link for the Emulator at the end of this article.

After downloading the Emulator, follow the installation instructions.

🚜 Microsoft Device Emulator version 3.0 Setup	_	
Welcome to Microsoft Device Emulator version 3.0 Setup		
This wizard will guide you through the installation process.		
	Next > Cancel	

Figure 11: Installing the device Emulator

After the mobile device is correctly installed and configured you must import the user certificate for the mobile user into the certificate store of the mobile device. To do that, the first part is to export the issued user certificate from the local user certificate store to a memory card and insert this memory card into the mobile device. You can also use the Windows Mobile Device Center in Windows Vista or Active Sync if you use Windows XP.

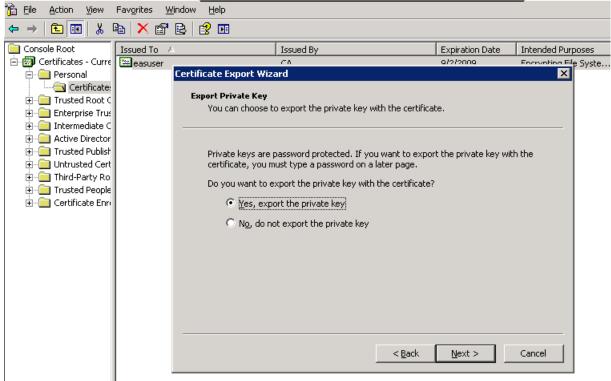


Figure 12:Export the certificate with the private key

On the Mobile device

After importing the certificate, start Microsoft Active Sync on the mobile device and follow the instructions to establish a connection to the Exchange Server.



Figure 13:Active Sync on the mobile device

If you are using a mobile device emulator, you must first cradle the device. To cradle the device you must use the Device Emulator Manager. This function allows the

mobile device to connect the Exchange Server over the TCP/IP connection of the client computer where the mobile device is connected to.

The client device must also have Exchange Active Sync (Windows XP) or the Windows Mobile Device Center (Windows Vista) installed.

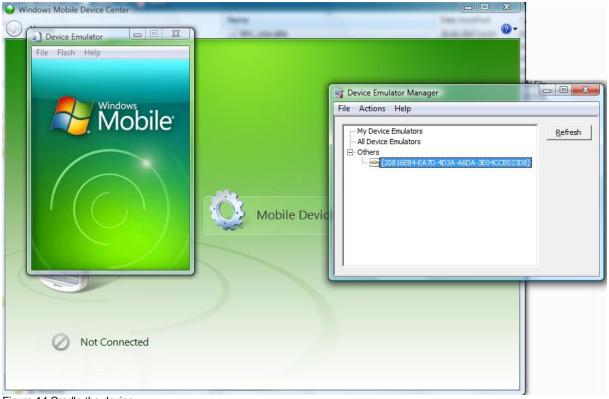


Figure 14:Cradle the device

If you cradled the device to the client PC, you can use DMA to connect the mobile device to the Client PC:

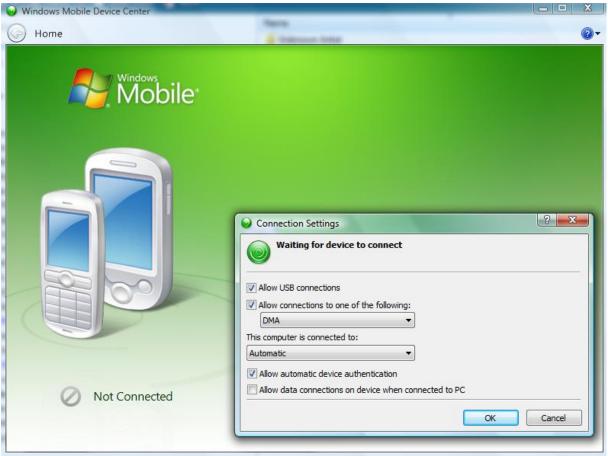


Figure 15:Use DMA to connect to the Mobile device

Synchronize the mobile device

To synchronize the mobile device click *Menu* on your mobile device. In the context menu click *Add Server Source*.

Add the Server name. The server name is the name which clients will use from the Internet. Do not enter the name of the internal Exchange Server! – Activate The Server name requires an encrypted connection.

Enter the username, password and Windows domain name of the user. After that you must select the items to sync. For some items it is possible to specify the sync time range (calendar) and the size of synced messages (e-mail).

If everything is correctly configured, click *Sync* and the mobile device should sync with your Exchange 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/mobiledevice-manager.mspx

Overview of Exchange ActiveSync in Exchange Server 2007

http://technet.microsoft.com/en-us/library/aa998357(EXCHG.80).aspx

Microsoft Exchange Server ActiveSync Certificate-Based Authentication Tool <u>http://www.microsoft.com/downloads/details.aspx?FamilyId=82510E18-7965-4883-A8C3-F73F1F4733AC&displaylang=en</u>