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

Microsoft Forefront UAG – Publishing Microsoft Exchange Server 2010 Outlook Anywhere and Exchange Active Sync

Abstract

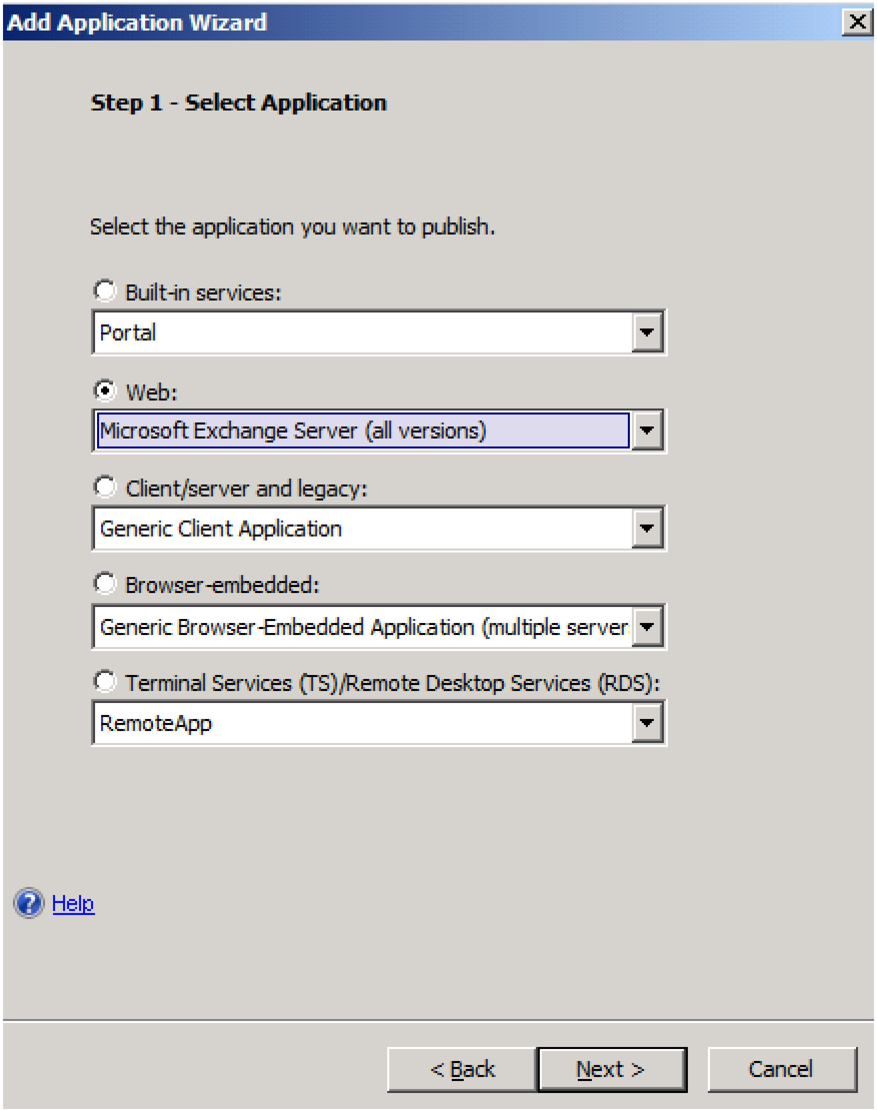
In this article I will show you how to publish Microsoft Exchange Server 2010 Outlook Anywhere and Exchange Active Sync with Forefront UAG.

Let's begin

In a previous article published at www.isaserver.org I showed you how to create a portal trunk in Forefront UAG to publish internal applications like Microsoft SharePoint. In this article I will demonstrate how to publish Outlook Web App from Microsoft Exchange Server 2010 through Forefront UAG.

To publish a Microsoft Exchange Server 2010 Outlook Web App start the Microsoft Forefront UAG Management console go to the HTTPS portal trunk created earlier and click add under in the applications window to start a wizard which will help you to publish different applications in the Forefront UAG portal.

Select Web – Microsoft Exchange Server (all versions) to publish the internal Microsoft Exchange Server 2010 or a Client Access Server (CAS) array of Exchange servers.



Step 1 - Select Application

Select the application you want to publish.

○ Built-in services:
Portal

● Web:
Microsoft Exchange Server (all versions)

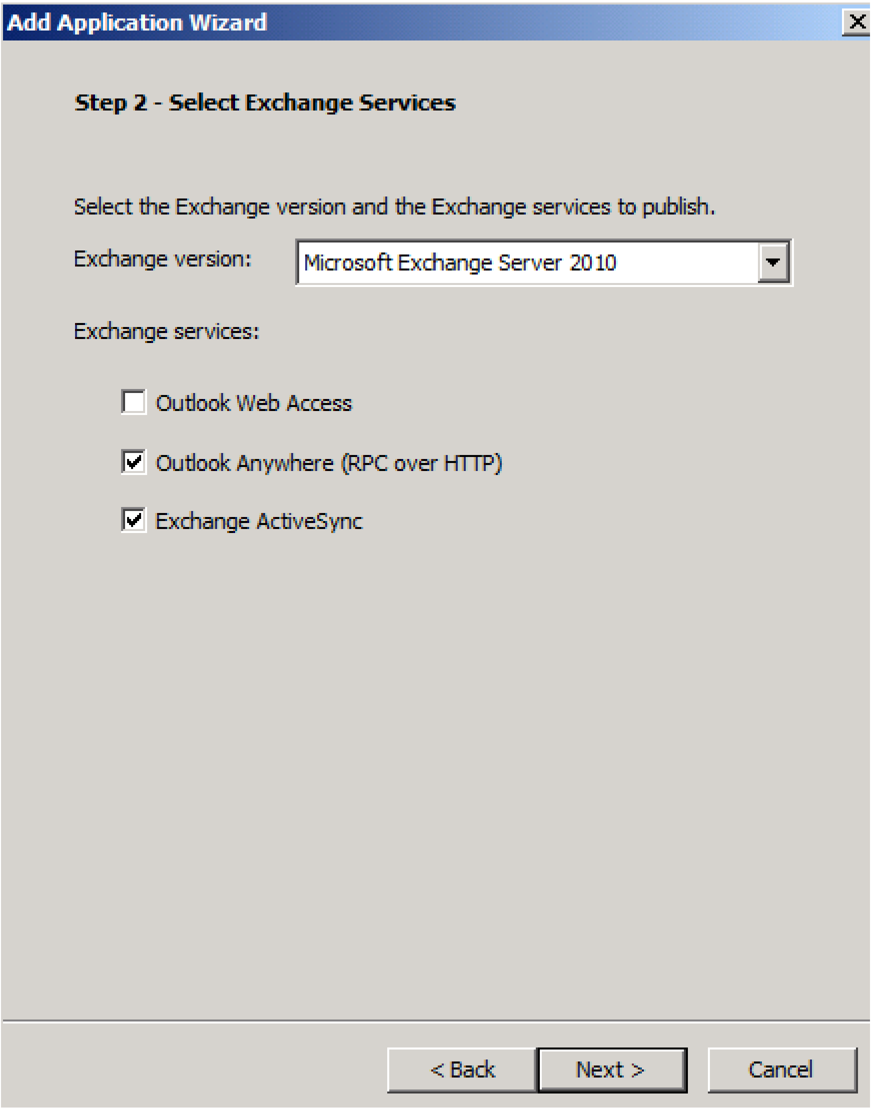
○ Client/server and legacy:
Generic Client Application

○ Browser-embedded:
Generic Browser-Embedded Application (multiple server

○ Terminal Services (TS)/Remote Desktop Services (RDS):
RemoteApp

Figure 1: Publish OA/EAS with Forefront UAG

Because we want to publish Exchange Server 2010 Outlook Anywhere and Exchange Active Sync, select Exchange Server 2010 as the version.



Step 2 - Select Exchange Services

Select the Exchange version and the Exchange services to publish.

Exchange version: Microsoft Exchange Server 2010

Exchange services:

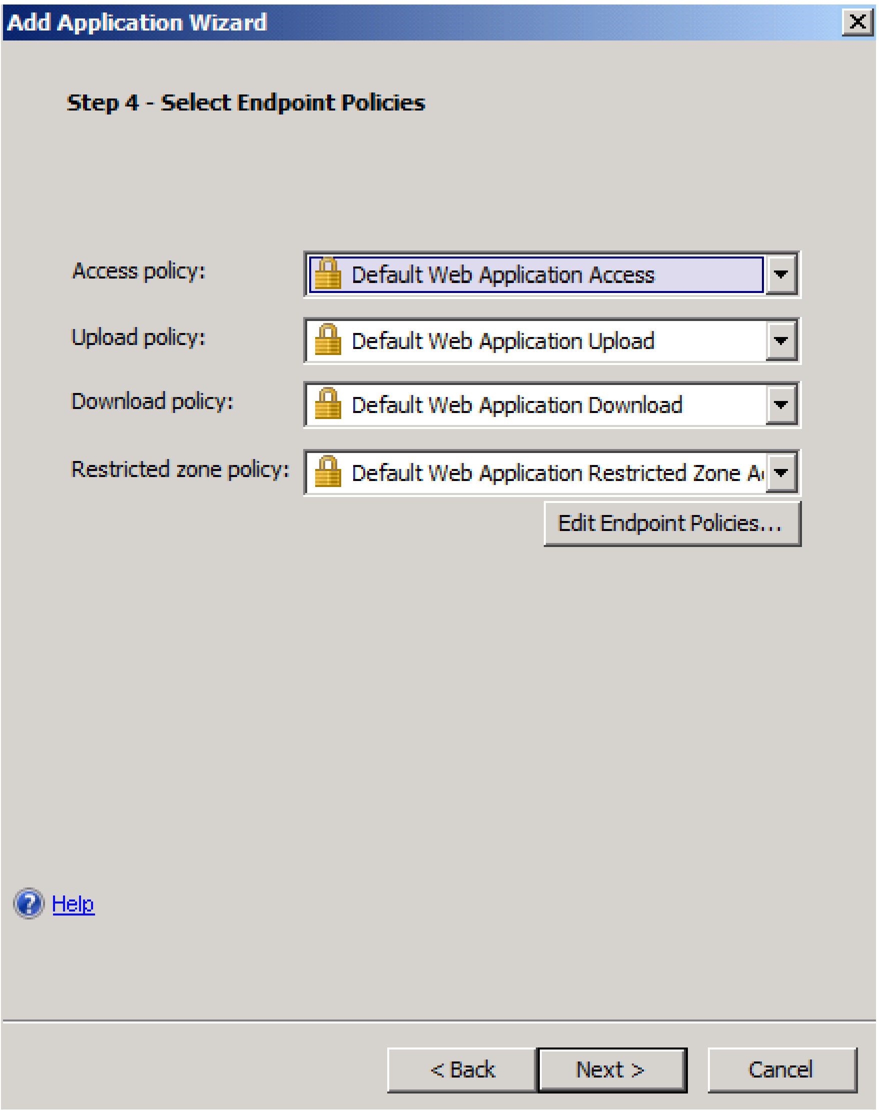
□ Outlook Web Access

☑ Outlook Anywhere (RPC over HTTP)

☑ Exchange ActiveSync

Figure 2: Select the Outlook Anywhere and Exchange Active Sync option

Next, we must specify a name for the new application. We will name the application Exchange. In Step 3 it is possible to configure endpoint policies for the application. Forefront UAG allows you to create endpoint policies at the port trunk level and at the application level to control access to the portal and the application from external clients. If you are unfamiliar with UAG Endpoint policies leave the settings unchanged.



Step 4 - Select Endpoint Policies

Access policy: Default Web Application Access

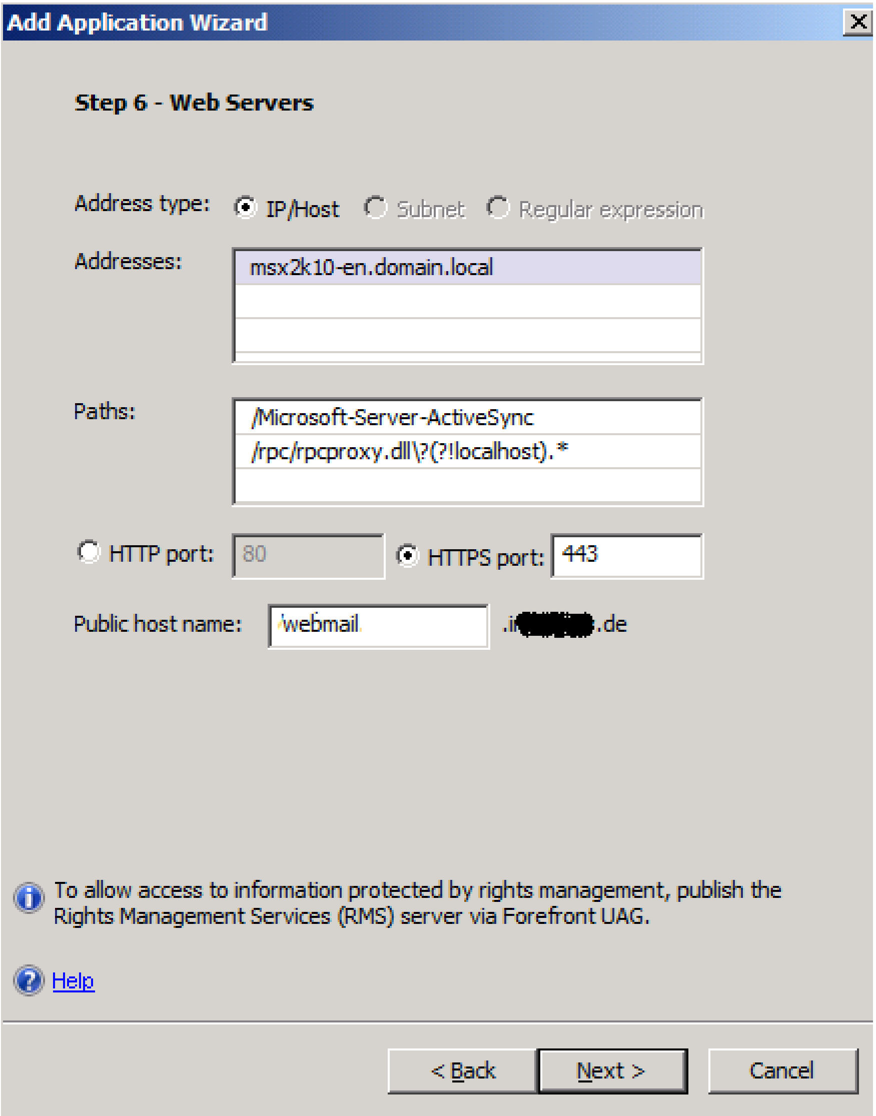
Upload policy: Default Web Application Upload

Download policy: Default Web Application Download

Restricted zone policy: Default Web Application Restricted Zone A

Figure 3: OA/EAS endpoint policies

Next click configure an application server. In Step 5 enter the FQDN of the internal Microsoft Exchange Server 2010 and the port you would like to use when Forefront UAG should access the internal Exchange Server. If you want to restrict access to a specific path you are able to do this in the UAG configuration wizard. The wizard allows access to all required paths like /Microsoft-Server-ActiveSync and for Outlook Anywhere to the /RPC directory but especially only to the RPCPROXY.DLL.



Step 6 - Web Servers

Address type: ● IP/Host ○ Subnet ○ Regular expression

Addresses:

```
msx2k10-en.domain.local
```

Paths:

```
/Microsoft-Server-ActiveSync
/rpc/rpcproxy.dll\?(?!localhost).*
```

○ HTTP port: 80 ● HTTPS port: 443

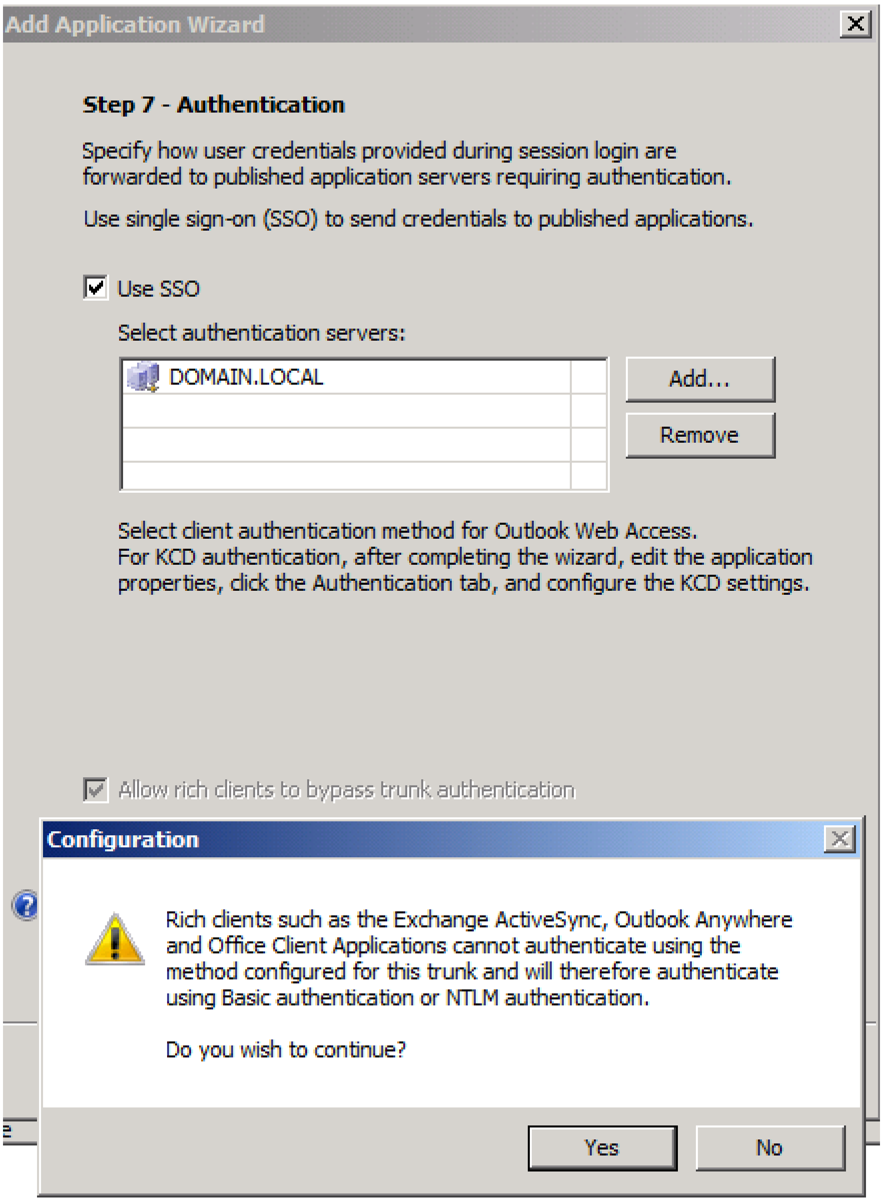
Public host name: webmail [redacted].de

To allow access to information protected by rights management, publish the Rights Management Services (RMS) server via Forefront UAG.

Figure 4: Specify the name of the internal Exchange Server

In Step 7 we can use different authentication mechanisms. Because we want to enable SSO (Single Sign On) for users which access the Forefront UAG portal to use the internal Exchange Server 2010.

Because rich clients as Microsoft Outlook and mobile phones which supports Exchange Active Sync cannot be authenticated through the portal directly, we must enable basic authentication or NTLM authentication which depends on the configuration of the Exchange Server and the Outlook clients for Outlook Anywhere.



Add Application Wizard

Step 7 - Authentication

Specify how user credentials provided during session login are forwarded to published application servers requiring authentication.

Use single sign-on (SSO) to send credentials to published applications.

☑ Use SSO

Select authentication servers:

DOMAIN.LOCAL

Select client authentication method for Outlook Web Access.
For KCD authentication, after completing the wizard, edit the application properties, click the Authentication tab, and configure the KCD settings.

☑ Allow rich clients to bypass trunk authentication

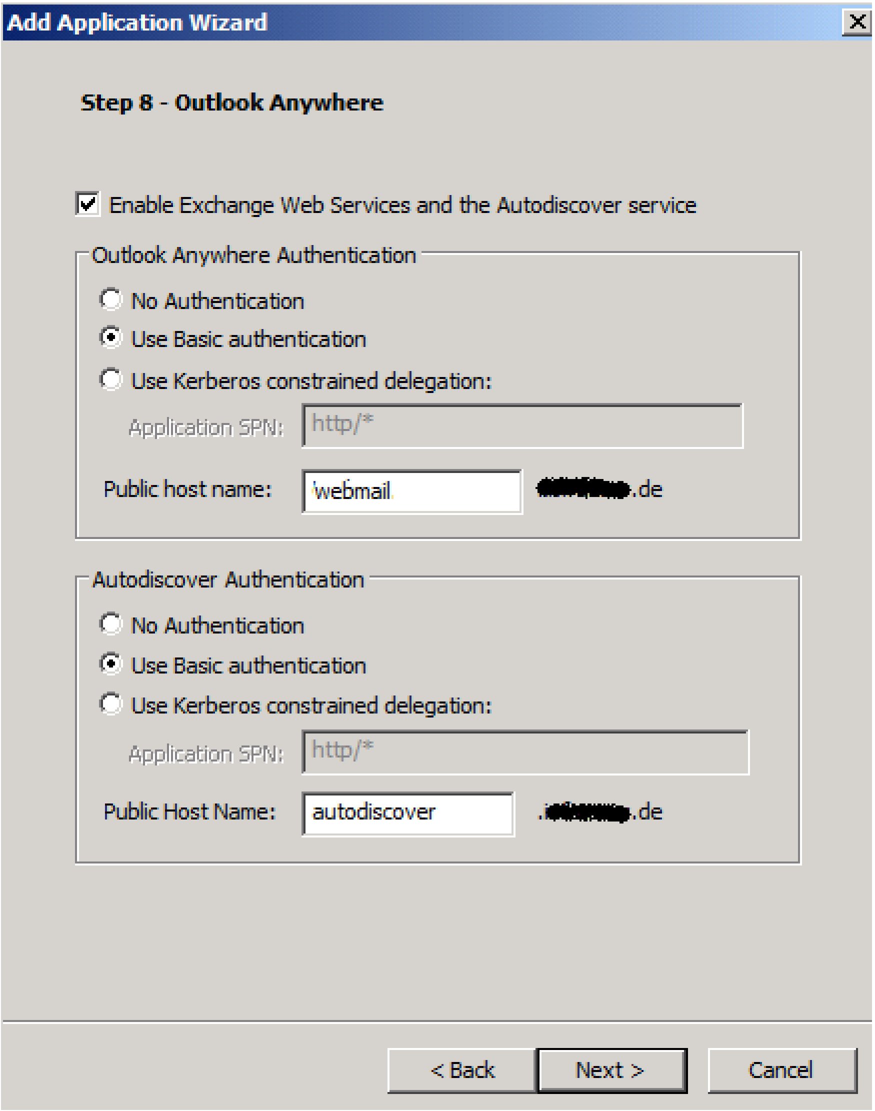
Configuration

Rich clients such as the Exchange ActiveSync, Outlook Anywhere and Office Client Applications cannot authenticate using the method configured for this trunk and will therefore authenticate using Basic authentication or NTLM authentication.

Do you wish to continue?

Figure 5: Enable SSO

By default Outlook Anywhere authentication uses basic authentication, but it is possible to change this to Windows authentication with KCD (Kerberos Constrained Delegation) but this requires additional configuration steps on the Exchange Server and in the Active Directory configuration. If you want to enable Autodiscover for Outlook Anywhere you must use an additonal public DNS name for Autodiscover and you must make sure that the certificate on the Forefront UAG Server contins the Autodiscover name as the common name (CN) or the SAN (Subject Alternate Name) must contain the name Autodiscover.



Add Application Wizard

Step 8 - Outlook Anywhere

☑ Enable Exchange Web Services and the Autodiscover service

Outlook Anywhere Authentication

○ No Authentication
● Use Basic authentication
○ Use Kerberos constrained delegation:

Application SPN: http/*

Public host name: webmail [redacted].de

Autodiscover Authentication

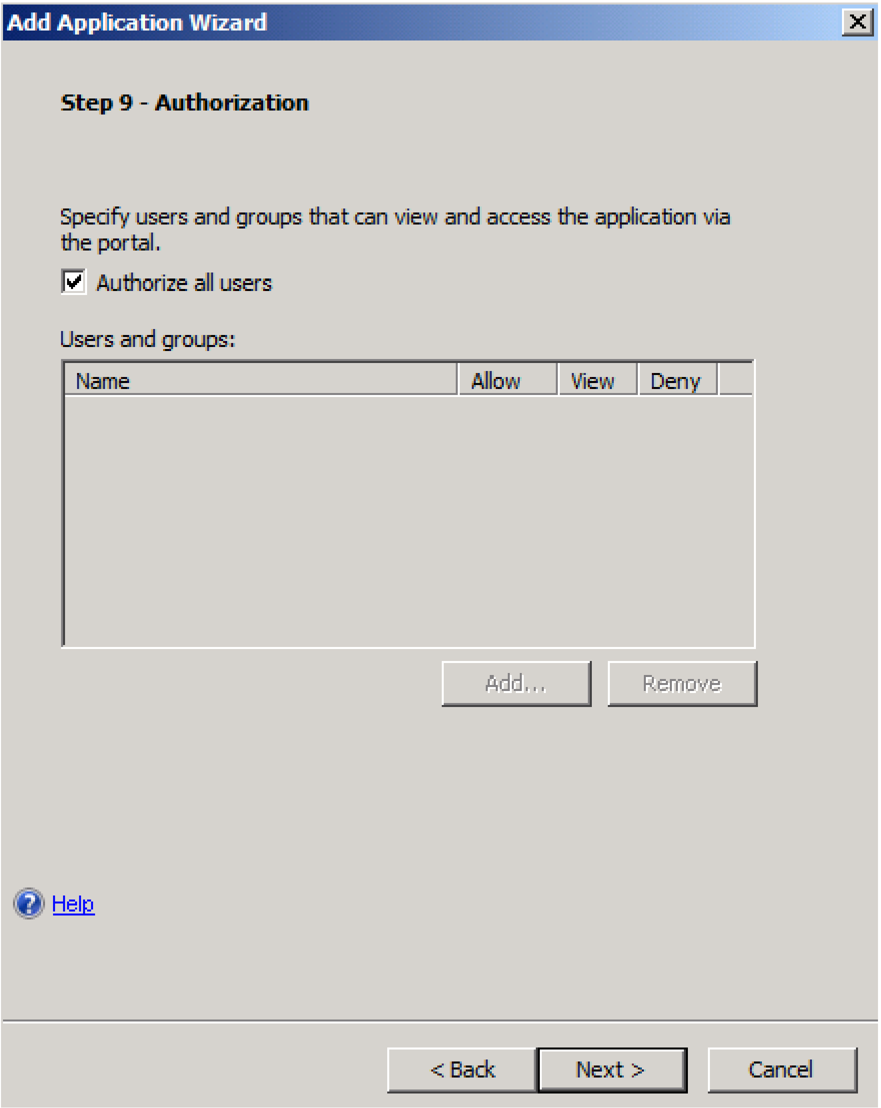
○ No Authentication
● Use Basic authentication
○ Use Kerberos constrained delegation:

Application SPN: http/*

Public Host Name: autodiscover .[redacted].de

Figure 6: Authentication options for Outlook Anywhere

In Step 9 it is possible to configure the authorization settings to access the application in the portal. If you would like to grant all authenticated users access to Outlook Anywhere or EAS leave the default setting unchanged. If you want to only grant specific users and user groups access OA and EAS uncheck the checkbox and select the users and usergroups from the previous created repository to grant or deny them access.



Add Application Wizard

Step 9 - Authorization

Specify users and groups that can view and access the application via the portal.

☑ Authorize all users

Users and groups:

Name	Allow	View	Deny

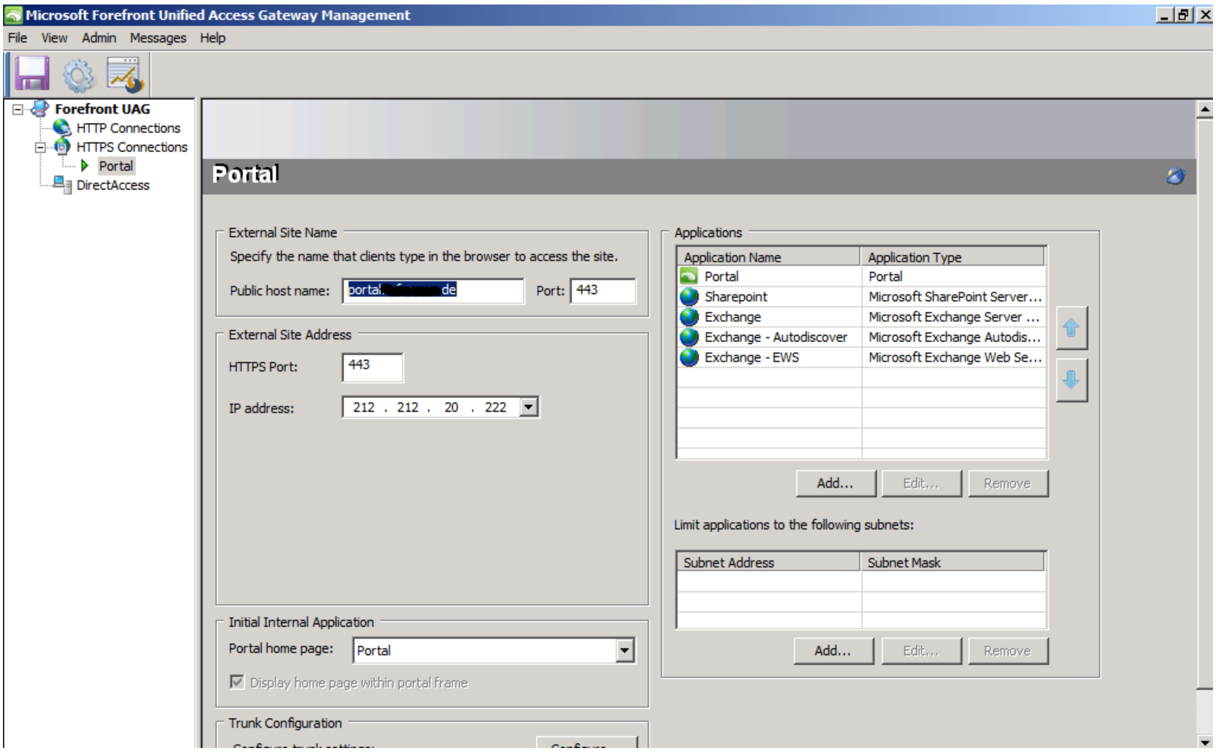
Figure 7: Allow all authenticated users access to Outlook Anywhere and Exchange Active Sync

Click Finish.

We must now save the configuration to store the changes to the Forefront UAG configuration. Click the floppy symbol to save the configuration. After that we can activate the configuration so that all changes will be effective after a short amount of time. To activate the configuration click the button right from the floppy symbol.

The UAG Exchange application wizard creates three applications:

- Exchange – For Outlook Anywhere and Exchange Active Sync access
- Exchange Autodiscover – For automatic Outlook mailbox configuration
- Exchange EWS – For Exchange Web Services



External Site Name

Specify the name that clients type in the browser to access the site.

Public host name: portal.[redacted]de Port: 443

External Site Address

HTTPS Port: 443

IP address: 212 . 212 . 20 . 222

Initial Internal Application

Portal home page: Portal

☑ Display home page within portal frame

Trunk Configuration

Applications

Application Name	Application Type
Portal	Portal
Sharepoint	Microsoft SharePoint Server...
Exchange	Microsoft Exchange Server ...
Exchange - Autodiscover	Microsoft Exchange Autodis...
Exchange - EWS	Microsoft Exchange Web Se...

Limit applications to the following subnets:

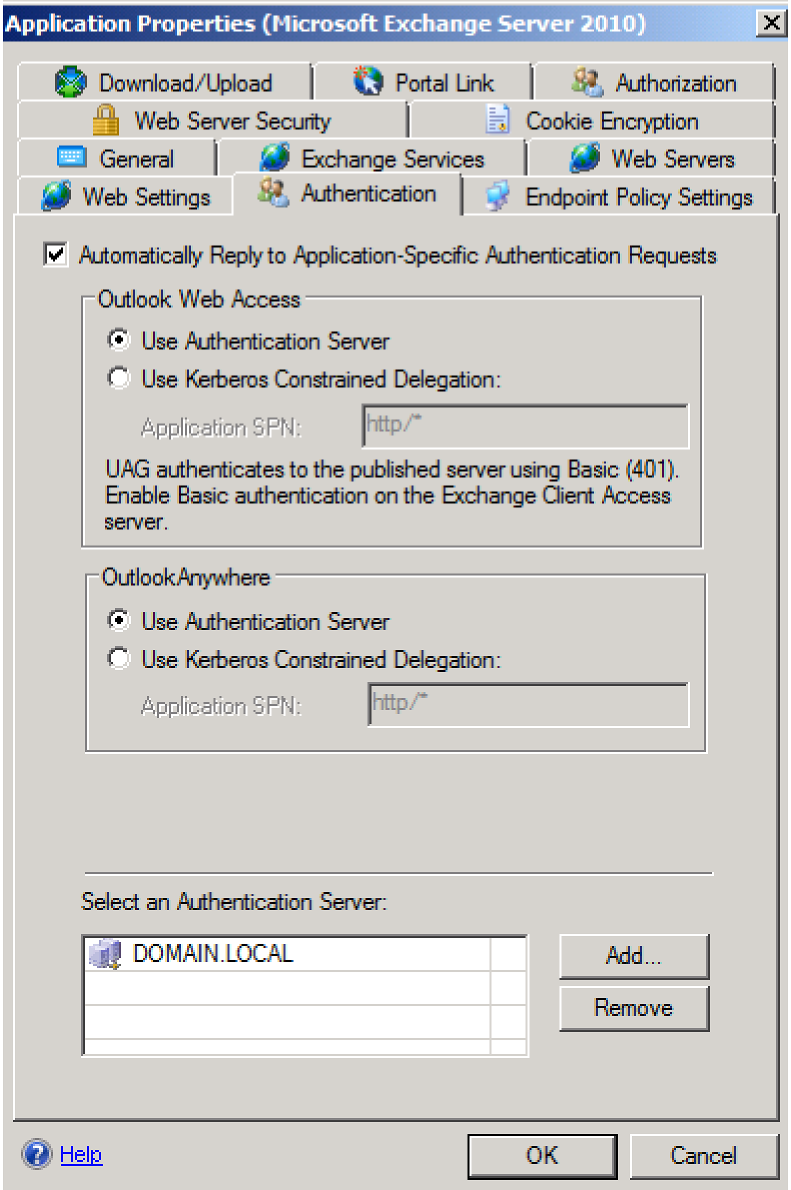
Subnet Address	Subnet Mask

Figure 8: The UAG application wizard creates different applications in the portal

After the wizard has finished publishing Outlook Anywhere and Exchange Active Sync it is possible to customize the settings created by the wizard.

Application Exchange

Forefront UAG uses basic authentication to authenticate against the Exchange Client Access (CAS) Server. The authentication settings must match the settings on the Exchange Server.



Application Properties (Microsoft Exchange Server 2010)

☑ Automatically Reply to Application-Specific Authentication Requests

Outlook Web Access

● Use Authentication Server

○ Use Kerberos Constrained Delegation:

Application SPN: http/*

UAG authenticates to the published server using Basic (401). Enable Basic authentication on the Exchange Client Access server.

OutlookAnywhere

● Use Authentication Server

○ Use Kerberos Constrained Delegation:

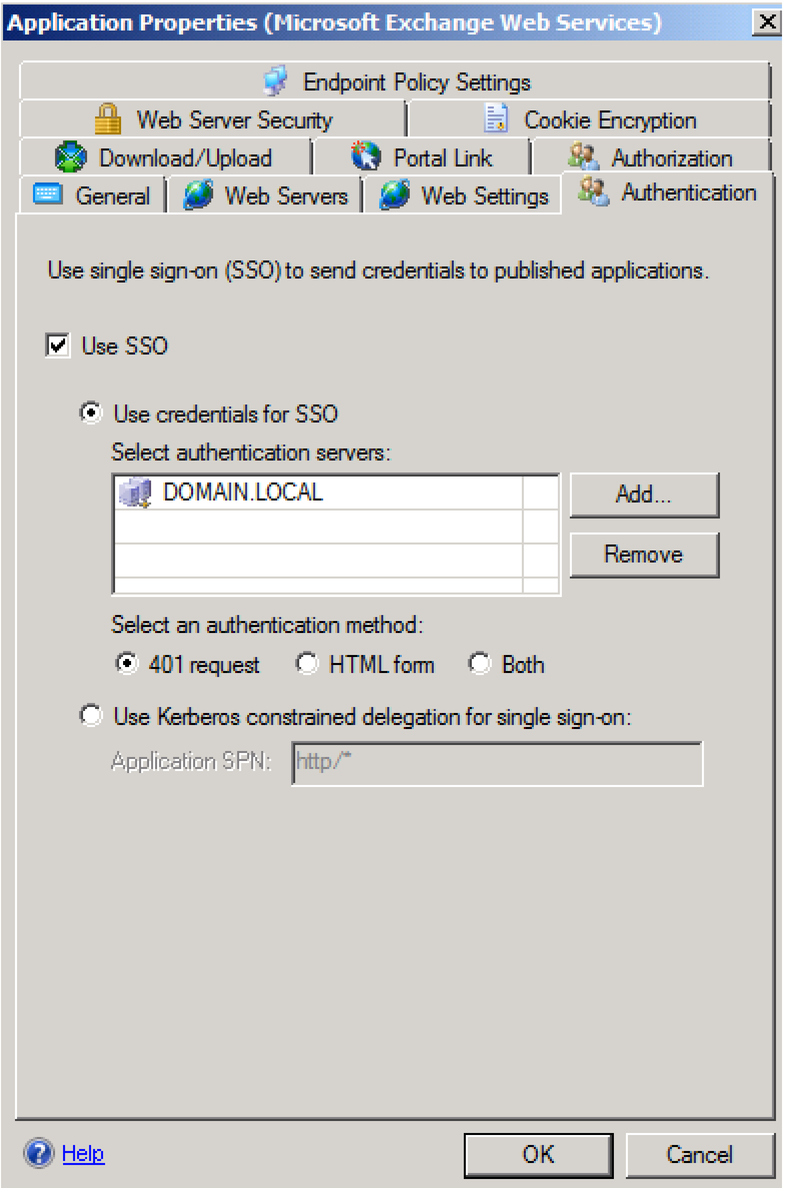
Application SPN: http/*

Select an Authentication Server:

DOMAIN.LOCAL

Figure 9: Application specific requests for OA and EAS

The Authentication option uses SSO for the published application and sends a 401 rquest to the Client Access Server



Use single sign-on (SSO) to send credentials to published applications.

☑ Use SSO

● Use credentials for SSO

Select authentication servers:

DOMAIN.LOCAL

Select an authentication method:

● 401 request ○ HTML form ○ Both

○ Use Kerberos constrained delegation for single sign-on:

Application SPN: http/*

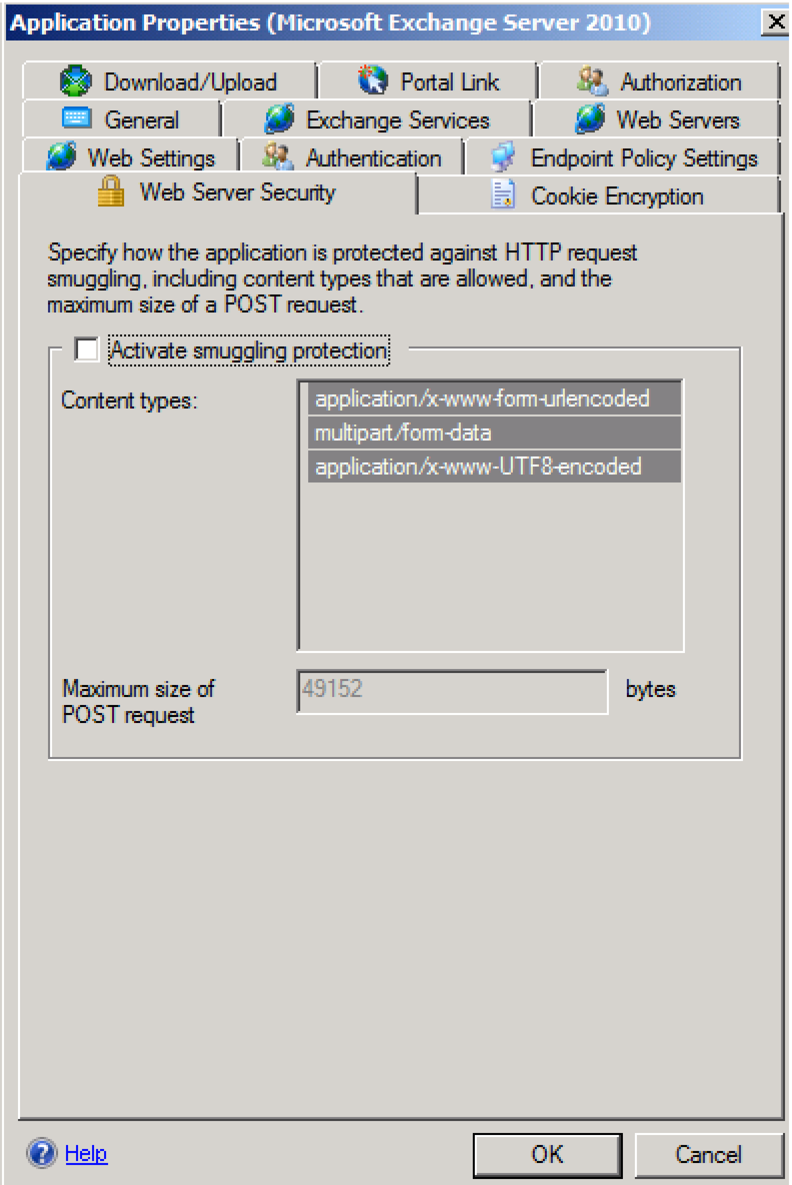
Figure 10: 401 request for Exchange EWS

Web Server Security

The Web Server Security tab allows you to activate the smuggling protection feature and the maximum size of the POST request. HRS can be used to block requests if the following conditions apply:

- The method is POST
- The content-type is not listed in the content-type list
- The length is greater than the specified maximum length

This option should be enabled only for servers that are vulnerable to HRS attacks. If this option is enabled when it is not required, applications may not behave as expected.



Specify how the application is protected against HTTP request smuggling, including content types that are allowed, and the maximum size of a POST request.

□ Activate smuggling protection

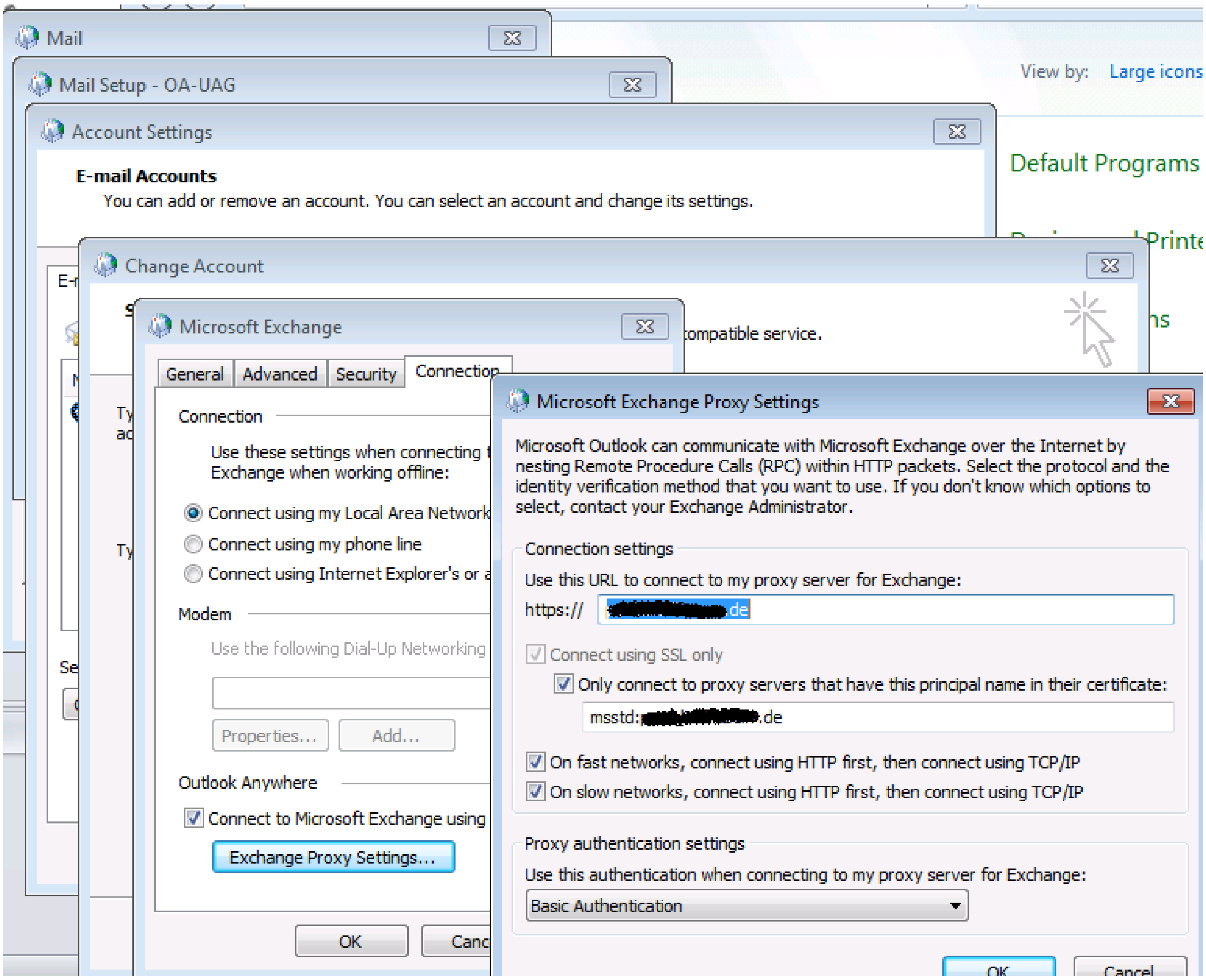
Content types:
application/x-www-form-urlencoded
multipart/form-data
application/x-www-UTF8-encoded

Maximum size of POST request 49152 bytes

Figure 11: Web Server Security

At client side – Outlook Anywhere

After all settings has been done at tehe Forefront UAG Server it is now time to configure the Outlook 2010 clients which should access the Exchange Server 2010 through Forefront UAG with Outlook Anywhere. Configure the e-mail settings in the control panel on the client to use Outlook Anywhere. Enter the public DNS name which points to the Forefront UAG Server and specify Basic Authentication as the authentication methods. The authentication settings must match the authentication options in Forefront UAG and the Exchange Client Access Server.



Mail

Mail Setup - OA-UAG

Account Settings

E-mail Accounts

You can add or remove an account. You can select an account and change its settings.

Change Account

Microsoft Exchange

General | Advanced | Security | Connection

Connection

Use these settings when connecting t
Exchange when working offline:

● Connect using my Local Area Network

○ Connect using my phone line

○ Connect using Internet Explorer's or a

Modem

Use the following Dial-Up Networking

Outlook Anywhere

☑ Connect to Microsoft Exchange using

Microsoft Exchange Proxy Settings

Microsoft Outlook can communicate with Microsoft Exchange over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Administrator.

Connection settings

Use this URL to connect to my proxy server for Exchange:

https:// [redacted].de

☑ Connect using SSL only

☑ Only connect to proxy servers that have this principal name in their certificate:

msstd:[redacted].de

☑ On fast networks, connect using HTTP first, then connect using TCP/IP

☑ On slow networks, connect using HTTP first, then connect using TCP/IP

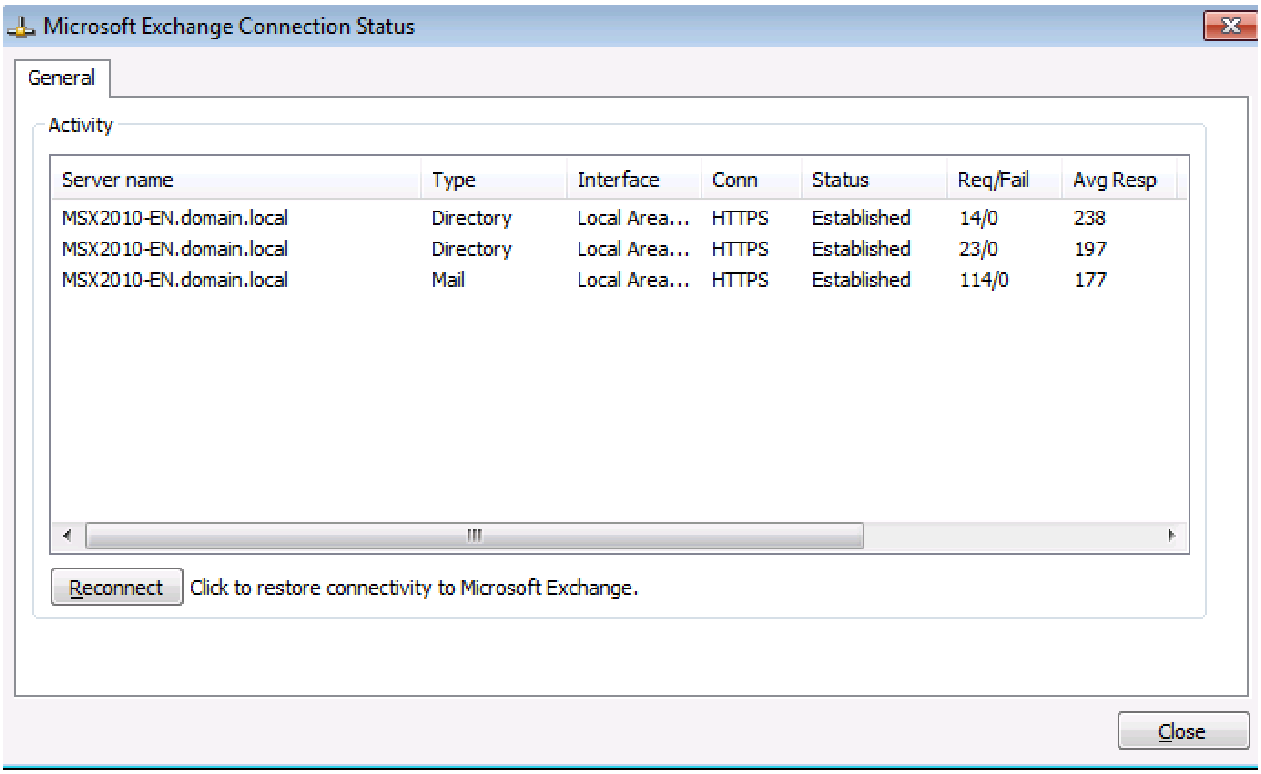
Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange:

Basic Authentication

Figure 12: Outlook Anywhere configuration in Outlook 2010

Start the Outlook application and right click the Outlook icon in the task pane and from the context menu select the Outlook connection settings option. As you can see in the following screenshot the Outlook client connects via HTTPS to the internal Exchange Server.



Server name	Type	Interface	Conn	Status	Req/Fail	Avg Resp
MSX2010-EN.domain.local	Directory	Local Area...	HTTPS	Established	14/0	238
MSX2010-EN.domain.local	Directory	Local Area...	HTTPS	Established	23/0	197
MSX2010-EN.domain.local	Mail	Local Area...	HTTPS	Established	114/0	177

Click to restore connectivity to Microsoft Exchange.

Figure 13: Succesful Outlook Anywhere connection

At client side – Exchange Active Sync

Depending on the mobile phone used, the configuration steps for connecting the mobile phone to the Exchange Server are different. As a high level step you must provide the following informations:

- Public DNS name which points to the Forefront UAG Server
- Active Directory Domain Name for users which wants to access the UAG Server
- User name and password
- Enable the checkbox that SSL should be used to connect to the Forefront UAG Server

Conclusion

In this article we published Microsoft Exchange Server 2010 Outlook Anywhere and Exchange Active Sync with Microsoft Forefront UAG. As you have seen, publishing a Microsoft Exchange Server 2010 with Forefront UAG provides much more capabilities and customization as to publish an Exchange Server 2010 with Microsoft Forefront TMG.

Related links

Publishing Outlook Anywhere on a Forefront UAG portal
http://technet.microsoft.com/en-us/library/ee921429.aspx
Exchange services publishing deployment options
http://technet.microsoft.com/en-us/library/dd861446.aspx
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG

http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Forefront UAG technical overview
http://technet.microsoft.com/en-us/library/ee690443.aspx