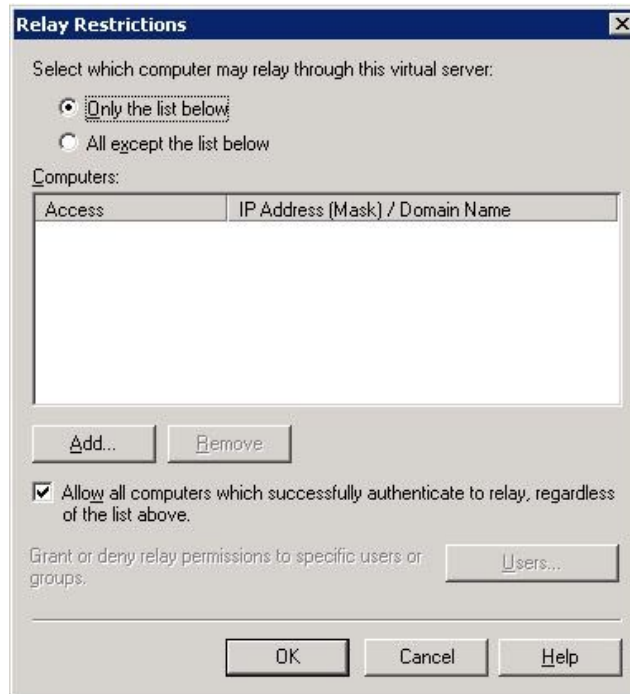

Allowing application servers to relay off Exchange Server 2007

From time to time, you need to allow an application server to relay off of your Exchange server. You might need to do this if you have a SharePoint, a CRM application like Dynamics, or a web site that sends emails to your employees or customers.

You might need to do this if you are getting the SMTP error message “550 5.7.1 Unable to relay”

The top rule is that you want to keep relay restricted as tightly as possible, even on servers that are not connected to the Internet. Usually this is done with authentication and/or restricting by IP address. Exchange 2003 provides the following relay restrictions on the SMTP VS:



Here are the equivalent options for how to configure this in Exchange 2007.

Allow all computers which successfully authenticate to relay, regardless of the list above

Like its predecessor, Exchange 2007 is configured to accept and relay email from hosts that authenticate by default. Both the “Default” and “Client” receive connectors are configured this way out of the box. Authenticating is the simplest method to submit messages, and preferred in many cases.

The Permissions Group that allows authenticated users to submit and relay is the “ExchangeUsers” group. The permissions that are granted with this permissions group are:

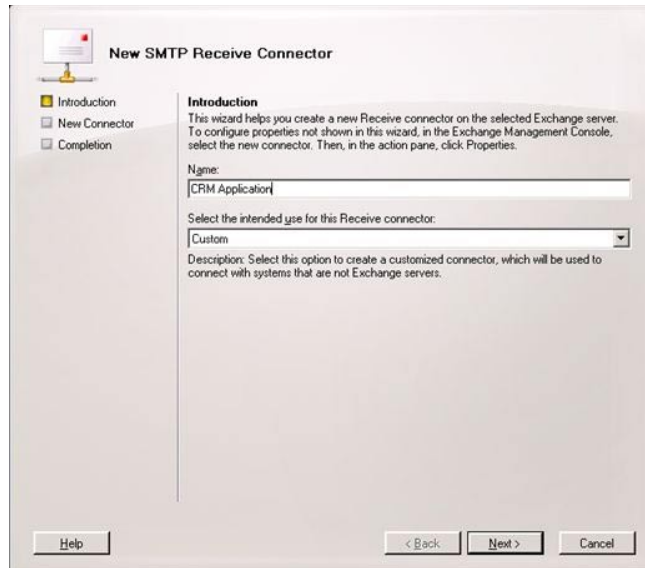
```
NT AUTHORITY\Authenticated Users {ms-Exch-SMTP-Submit}
NT AUTHORITY\Authenticated Users {ms-Exch-Accept-Headers-Routing}
NT AUTHORITY\Authenticated Users {ms-Exch-Bypass-Anti-Spam}
NT AUTHORITY\Authenticated Users {ms-Exch-SMTP-Accept-Any-Recipient}
```

The specific ACL that controls relay is the ms-Exch-SMTP-Accept-Any-Recipient.

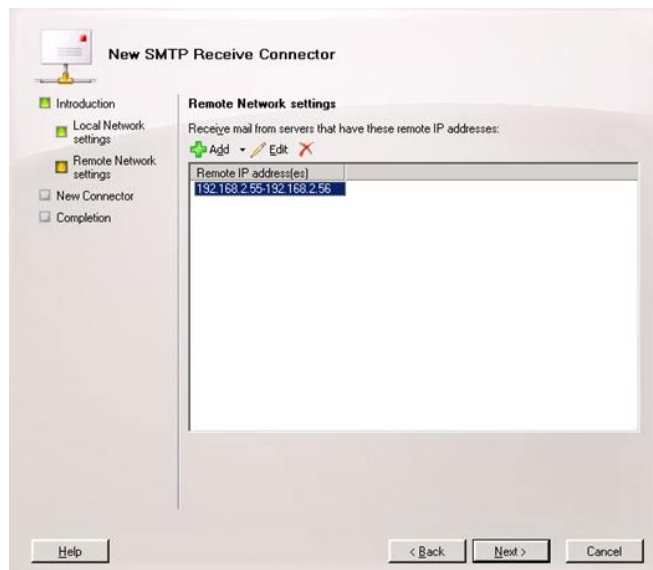
Only the list below (specify IP address)

This option is for those who cannot authenticate with Exchange. The most common example of this is an application server that needs to be able to relay messages through Exchange.

First, start with a new custom receive connector. You can think of receive connectors as protocol listeners. The closest equivalent to Exchange 2003 is an SMTP Virtual Server. You must create a new one because you will want to scope the remote IP Address(es) that you will allow.



The next screen you must pay particular attention to is the “Remote Network settings”. This is where you will specify the IP ranges of servers that will be allowed to submit mail. You definitely want to restrict this range down as much as you can. In this case, I want my two web servers, 192.168.2.55 & 192.168.2.56 to be allowed to relay.

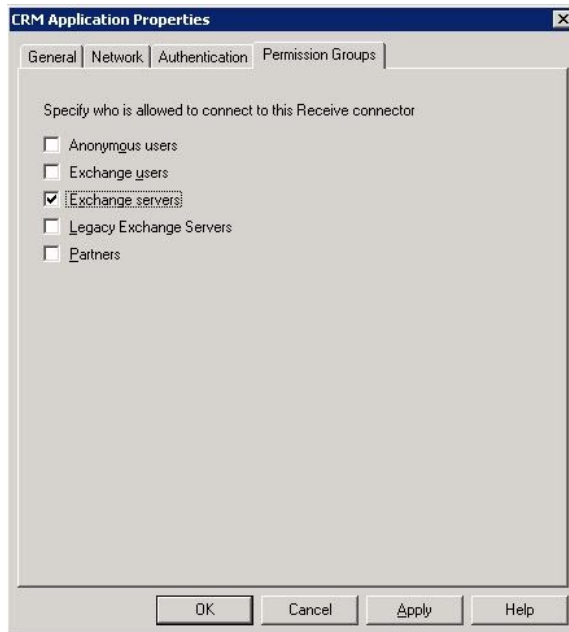


The next step is to create the connector, and open the properties. Now you have two options, which I will present. The first option will probably be the most common.

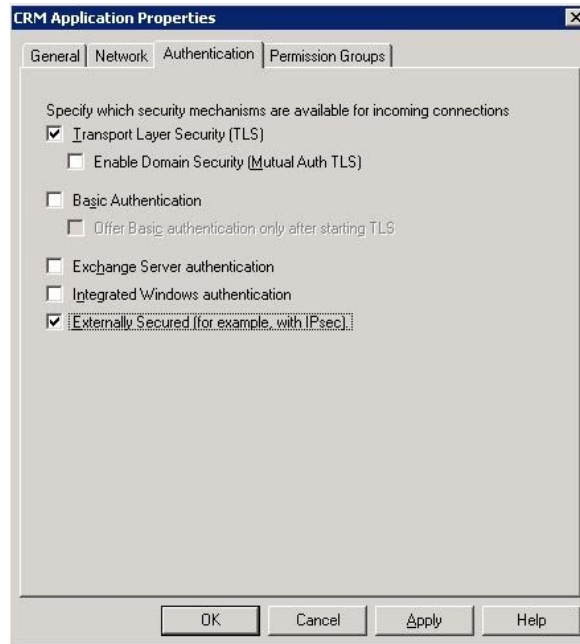
Option 1: Make your new scoped connector an Externally Secured connector

This option is the most common option, and preferred in most situations where the application that is submitting will be submitting email to your internal users as well as relaying to the outside world.

Before you can perform this step, it is required that you enable the Exchange Servers permission group. Once in the properties, go to the Permissions Groups tab and select Exchange servers.



Next, continue to the authentication mechanisms page and add the “Externally secured” mechanism. What this means is that you have complete trust that the previously designated IP addresses will be trusted by your organization.



Caveat: If you do not perform these two steps in order, the GUI blocks you from continuing.

Do not use this setting lightly. You will be granting several rights including the ability to send on behalf of users in your organization, the ability to ResolveP2 (that is, make it so that the messages appear to be sent from within the organization rather than anonymously), bypass anti-spam, and bypass size limits. The default “Externally Secured” permissions are as follows:

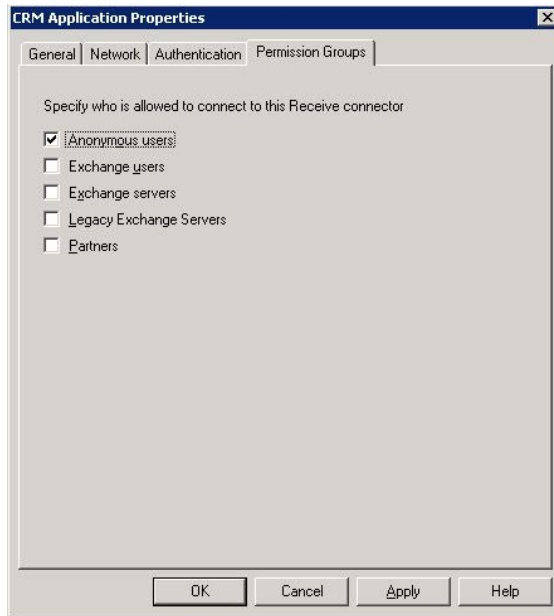
```
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Accept-Authoritative-Domain}
MS Exchange\Externally Secured Servers {ms-Exch-Bypass-Anti-Spam}
MS Exchange\Externally Secured Servers {ms-Exch-Bypass-Message-Size-Limit}
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Accept-Exch50}
MS Exchange\Externally Secured Servers {ms-Exch-Accept-Headers-Routing}
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Submit}
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Accept-Any-Recipient}
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Accept-Authentication-Flag}
MS Exchange\Externally Secured Servers {ms-Exch-SMTP-Accept-Any-Sender}
```

Basically you are telling Exchange to ignore internal security checks because you trust these servers. The nice thing about this option is that it is simple and grants the common rights that most people probably want.

Option 2: Grant the relay permission to Anonymous on your new scoped connector

This option grants the minimum amount of required privileges to the submitting application.

Taking the new scoped connector that you created, you have another option. You can simply grant the ms-Exch-SMTP-Accept-Any-Recipient permission to the anonymous account. Do this by first adding the Anonymous Permissions Group to the connector.



This grants the most common permissions to the anonymous account, but it does not grant the relay permission. This step must be done through the Exchange shell:

```
Get-ReceiveConnector "CRM Application" | Add-ADPermission -User "NT AUTHORITY\ANONYMOUS LOGON" -ExtendedRights "ms-Exch-SMTP-Accept-Any-Recipient"
```

In addition to being more difficult to complete, this step does not allow the anonymous account to bypass anti-spam, or ResolveP2.

Although it is completely different from the Exchange 2003 way of doing things, hopefully you find the new SMTP permissions model to be sensible.