Introduction

The purpose of this guide is to familiarize you with ExchangeDefender and walk you through the configuration, management and deployment of the service. ExchangeDefender is a transparent, cloud-based security solution that protects users from *email SPAM, viruses and even dangerous content on the web*. In addition to the security, ExchangeDefender also includes **LiveArchive**, a business continuity solution as well as a long term archiving solution for ***HIPAA / SOX / SEC* compliance** and ***eDiscovery***. Furthermore, ExchangeDefender also has transparent *SMTP encryption, web file sharing, desktop tools and more* to protect all corporate communication and collaboration activities on the Internet.

You can find more information about the service at http://www.exchangedefender.com.

Table of Contents

Checklist

In order to deploy ExchangeDefender and safely secure the mail server and individual users you need to have access to the following:

- **Domain Name (DNS) control** - Because ExchangeDefender is activated by pointing the domain's mail exchanger (MX) record to *inbound30.exchangedefender.com* you must have the ability to change the DNS.

- **Mail Server Administrative access** - Hackers and spammers can bypass ExchangeDefender if the mail server remains exposed to anonymous SMTP traffic. Furthermore, some data such as Active Directory (LDAP) access can only be accessed from the mail server. Finally, you will have to disable some built in antispam software that will interfere with the delivery of SPAM reports.

- **Firewall access** - You will need to make certain changes to the network access, such as blocking anonymous SMTP connections from the Internet unless they come from the ExchangeDefender IP ranges, and blocking internal SMTP connections to the external servers in case your network is compromised.

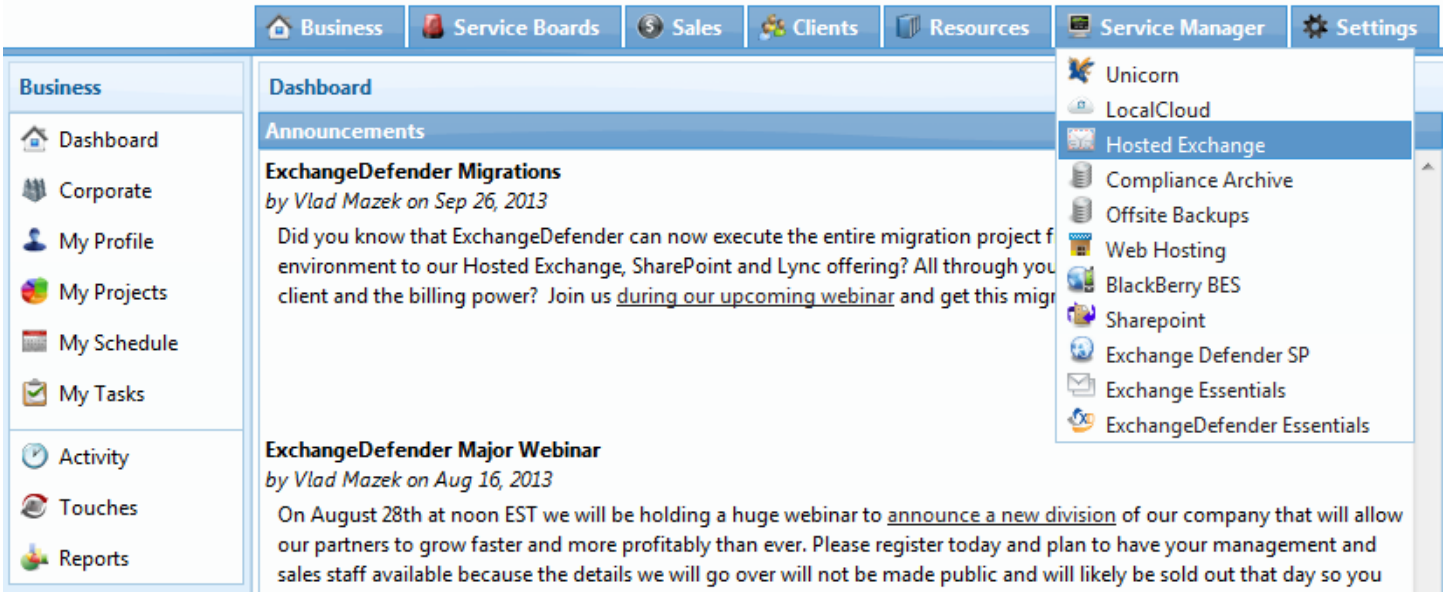
- **Desktop (Administrative User) access** - If you wish to deploy ExchangeDefender *SMTP Security, Desktop Agent,* you will need to have *administrative access* to the desktop in order to install software on the local system. We also recommend creation of several shortcuts on the users' Desktop so they can quickly locate resources when they need them.

- **Network Configuration** - You will need to know the IP address that the clients mail server is currently using and you must be able to accept mail on port 25 (while ExchangeDefender can deliver mail to ports other than 25, advanced configurations are beyond the scope of this guide).

- **Business Requirements** - You will need to make business related decisions about which features of ExchangeDefender will be enabled or disabled, when you would like to receive daily or intraday SPAM reports, whether or not you wish to enable LiveArchive business continuity, which passwords to assign to the new users and the contact information for the IT or contact person in the organization.

Setting Up Your Service Provider Portal

1. First, you will need to create your Service Provider Portal. To create your portal, click on the Service Manager tab.

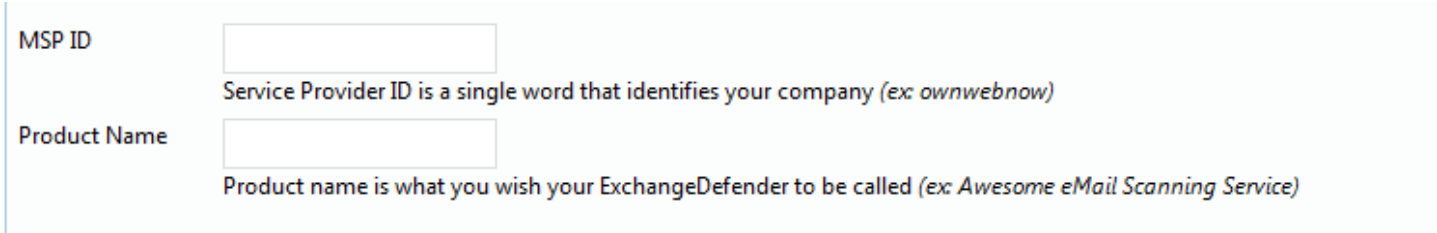


2. Next, click on **ExchangeDefender SP**. If you are creating an **ExchangeDefender Essentials Service Provider Portal**, scroll down and click subscribe the ExchangeDefender Essentials menu item.

3. Next, you will need to come up with a unique name for your Service Provider portal. We suggest using your company name. If you are planning to use both **ExchangeDefender** and **ExchangeDefender Essentials** you will need to have a variation on MSP ID, it will not accept the same ID twice.

   For Example: Try using *Ownwebnow Inc, Ownwebnow LLC, etc.*

The Product Name is what you would like your clients to see. For example, *Ownwebnow Cloud Filtration*, or *Ownwebnow Scanning Services, etc*. You will need to put your information as the Admin contact.



Service Provisioning

Service enrollment is a four step process through which you will be adding and configuring a new domain and it's users to the service. In the first step, you will be choosing how you wish to provide the user lists to ExchangeDefender. In the second step, you will be approving the domains that are about to be protected by ExchangeDefender. In the third step you will be reviewing email addresses and display names. Finally, you will be providing the service configuration and site specific policies for the new organization.

Creating Users: How to pick the right method

We currently offer three ways to create user accounts and import email addresses that will be protected by ExchangeDefender. Please review the following information carefully before selecting one.

- **XML Import** - This method is recommended for smaller sites running Microsoft Exchange mail servers. If you choose this method you will be downloading a *Visual Basic Script (.vbs)* that will export *Active Directory* mail-enabled user objects in an XML file that you can upload to ExchangeDefender. All users and associated display names and email addresses will be imported.

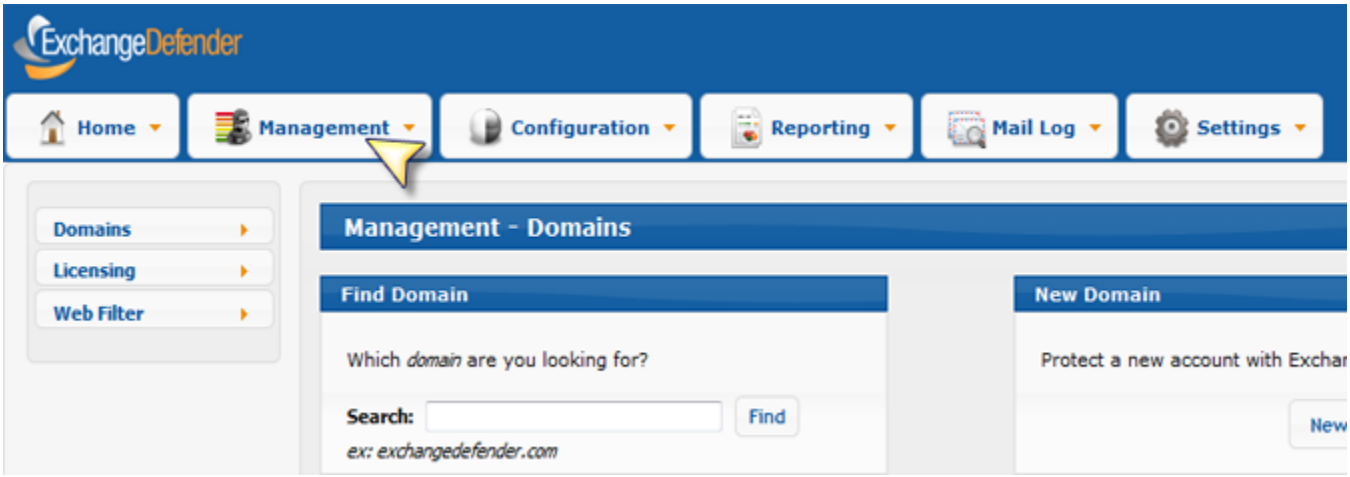
- **Manual Configuration** - This method is recommended for smaller sites and servers that are not running Microsoft Exchange and do not have an LDAP directory. Manual Configuration allows you to use a wizard import tool to type in user names and email addresses directly into ExchangeDefender.

- **XDSYNC LDAP tool for ExchangeDefender** - This method is recommended for larger deployments of Microsoft Exchange, or environments with high user turnover. By installing *XDSYNC LDAP tool* on your Microsoft Exchange server you will be assured that all changes to your mail-enabled Active Directory users will be applied to ExchangeDefender, removing any maintenance and user management of ExchangeDefender or double data entry.

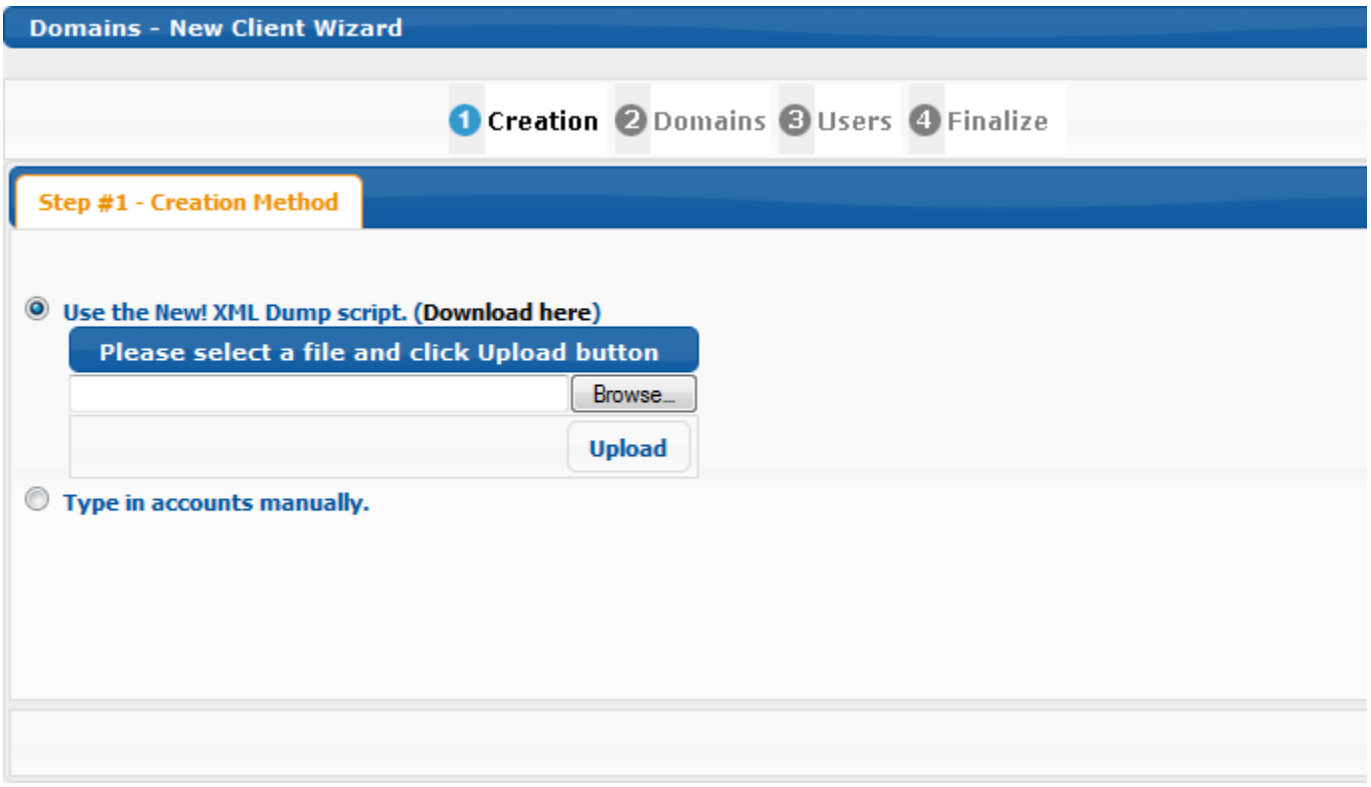
Service Enrollment

Protecting a domain with ExchangeDefender is quick and simple. First, let's get the list of users to add to ExchangeDefender.

1. To start the process please login as the *Service Provider* at https://admin.exchangedefender.com. Click on the **Management tab** and then on the **New User Wizard:**



2. Select how you wish to create your users:



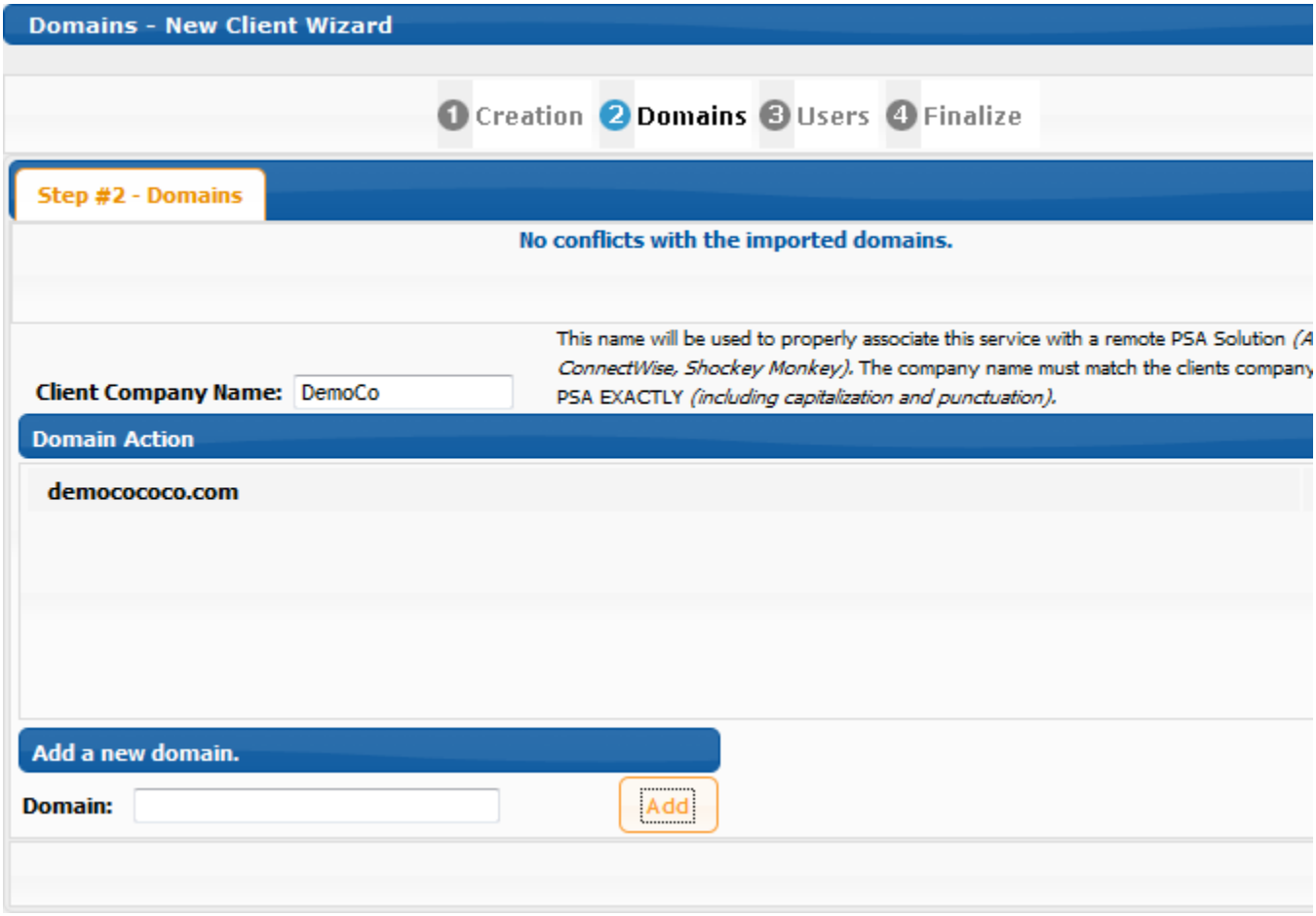
- If you wish to *type in the accounts manually*, or if you wish to *use the XDSYNC LDAP tool for ExchangeDefender*, select **"Type in accounts manually."** and **skip to step #4**.

- If you wish to use *the XML Dump script*, which we recommend, please **download the script from the screen above** and proceed to **step #3**.

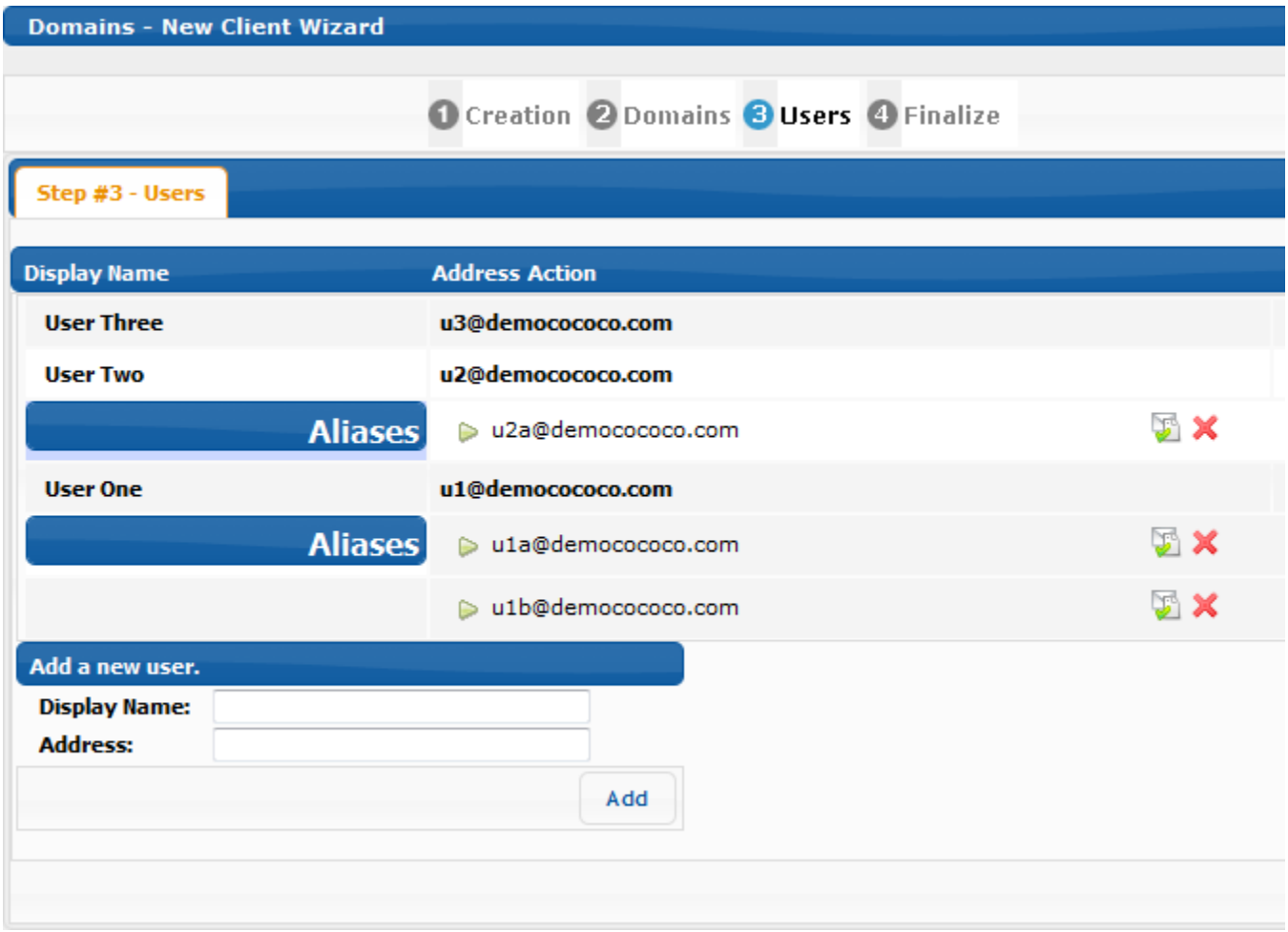
3. If you have chosen to use the *XML Dump script* (Visual Basic) please download it to your Microsoft Exchange server and execute it at the command prompt as follows:

    - *cscript ExportAddresses.vbs*
    - This script will create an XML file that you will have to upload to the screen above. The file is **C:\EmailAddresses.xml**
    - Click on **Upload** and when the file is confirmed, click on **Next**. Proceed to **step #4**.

4. In this step you will be asked to provide the domain names that will be protected on this server. You must type in the domain names and click on Add to validate the domains. If you import an XML file, the system will already list the domain names it has identified in the XML file. If there are any problems with the domains (such as invalid domain or a domain that is already protected by ExchangeDefender) they will show in the *"Conflict"* section at the top.



5. In this step we will confirm that our users are listed correctly.



You can add users to this list manually by typing in the users name and email address in the form on the bottom and clicking **Add**. Each user and alias will show up and you can *add, remove or delete aliases or users* from this list in realtime.

Note: *If you are using XDSYNC LDAP tool, you should only add the Administrator account here. The rest of the users will be uploaded automatically by XDSYNC.*

6. Finally, let's configure the domain policies.

Step #4 - Options

Users Password:

- (•) Random Passwords
- ( ) Custom Password

Administrator:

Please provide the name and e-mail address of the domain administrator. This person will be sent the welcome letter indicating the authentication information and instructions on how to deploy Exchange Defender 7 (MX records, IP restrictions, etc):

Admin Name:	Demo Admin
Admin E-mail:	nin@democococo.com
Admin Company:	Democococo
Admin Phone:	1231231231
Admin Password:	••••••••

[x] Send Administrator a welcome email.

Inbound IP Address:

Please provide an IP address where the mail server **receives** e-mail. This is where Exchange Defender 7 will deliver clean mail (Advanced Settings):

111.111.111.111

Outbound IP Address:

Please provide an IP address which the mail server uses to **send outgoing** email. Exchange Defender 7 will accept mail from this address and relay to the Internet (Advanced Settings):

111.111.111.111

SPAM Action:

Default action when Exchange Defender 7 encounters SPAM:

- ( ) Tag & Deliver
- (•) Quarantine
- ( ) Delete

SureSPAM Action:

Default action when Exchange Defender 7 encounters SureSPAM:

- ( ) Tag & Deliver
- (•) Quarantine
- ( ) Delete

SPAM Life:

Number of days spam is to remain active in the quarantine.

- (•) 7 Days
- ( ) 14 Days
- ( ) 24 Days
- ( ) 30 Days

Report Options:

When Exchange Defender 7 is set to quarantine SPAM or SureSPAM messages you can send the user daily and/or intraday SPAM quarantine reports to show them what Exchange Defender 7 intercepted.

- ( ) Disable e-mail reports
- ( ) Enable daily e-mail report
- (•) Enable daily and intraday e-mail reports

Report Schedule:

Generate **Daily** report at: 08:00

Generate **Intraday** report at: 14:00

Report Contents:

Should we report e-mail quarantines even when they do not contain any SPAM messages?

- (•) Report quarantines for all e-mail addresses
- ( ) Report quarantines only for e-mail addresses that have SPAM in them

- **Users Password** - Please select the default password that will be assigned to the accounts you are about to create. Users can change this password at any time.

- **Administrator** - Administrator is typically the IT contact person at the organization and the users on whose behalf all welcome messages are sent to the users.

  Note: *The password assigned here is the domain password that the site administrator can use to login to admin.exchangedefender.com and manage all the user and domain configurations.*

- **Inbound IP Address** - This is the IP address to which we will deliver all inbound mail. If you have a complex inbound network and wish to load balance the delivery across multiple servers or create a failover scenario, click on **Advanced Settings**.

- **Outbound IP Address** - This is the IP address from which we will accept outbound mail. If you have more than one IP address please provide it under Advanced Settings. Note: Typically the inbound and outbound IP address are the same.

- **SPAM Action** - What should we do with SPAM messages? We recommend to quarantine them.

- **SureSPAM Action** - What should we do with SureSPAM messages? We recommend to delete them.

- **SPAM Life** - How long should we keep the SPAM messages in the quarantine? By default we only keep 7 days meaning the user can release any quarantined SPAM messages received over the past seven days. Around holidays it makes sense to extend this period if staff takes longer vacations.

  Note: *We do not recommend changing this interval. Doing so causes exponential performance degradation because the database is larger and queries run exponentially slower.*

- **Report Options** - Choose if you want to enable Daily or Intraday SPAM digest reports. We recommend disabling these reports and relying on the portal, Outlook Add-in or Desktop agent.

- **Report Schedule** - If you have enabled the SPAM digest reports, pick the time at which you would like to have them generated. It takes up to 30 minutes for the report to be generated so please keep in mind that this setting only controls when the report is scheduled to be processed, not when it will be delivered.

- **Report Contents** - Report Contents allow users that have a lot of email addresses to not report email addresses that have no SPAM in the quarantine. Enabling this removes pages of *"No SPAM Quarantined"* in the report and reduces the report size.

- **Time Zone** - Time zone in which the client's server is located.

- **LiveArchive** - Select to enable or disable *LiveArchive Business Continuity*. If you choose to enable this solution, each user must login to their account when the domain is created in order to initialize the mailbox.

Congratulations, you have enabled **ExchangeDefender** protection on your domain. Please allow for up to an hour for the new configuration to propagate to all of ExchangeDefender servers and proceed to the next section on configuring your infrastructure.

Network Configuration

In order to properly deploy ExchangeDefender, you need to make several changes on your network. First, you have to change your MX record to point all of your inbound mail to ExchangeDefender. This way ExchangeDefender will stand in front of your mail server and bounce all the dangerous content that is sent to your network. Then, you should change your outbound smarthost to allow us to scan all of your outbound mail*. Finally, enforce IP restrictions so that you can only exchange mail through a trusted connection with ExchangeDefender.

**For users that rely on email for correspondence, outbound network will automatically archive all outbound emails. If you have a business requirement that includes sending out notifications, automated responses, marketing, large distribution lists or other non-correspondance items, we offer outbound-jr high speed relay designed for that specific need.*

MX Record

Please modify your MX record and change it to: **inbound30.exchangedefender.com**
You should not have any other MX records for your domain name (subdomain MX records are OK).

Outbound SmartHost

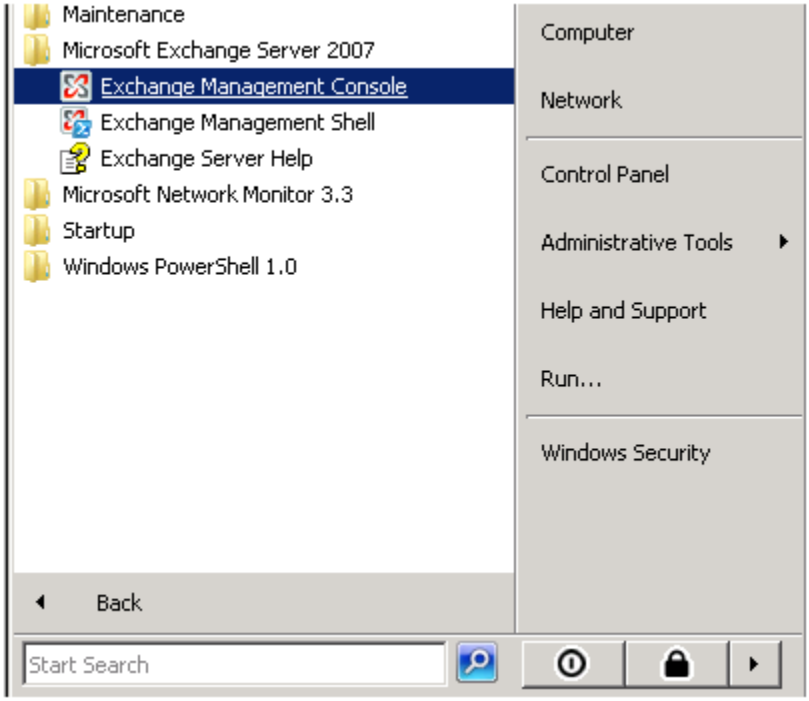
Please modify your SMTP server to route all outbound mail through the following smarthost:
outbound.exchangedefender.com

Outlook Configuration

Please follow these instructions to modify the smart host on **Exchange 2003 and 2007**:

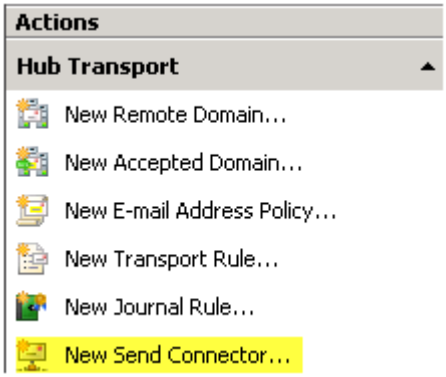
Exchange 2007/2010

1. Login as the Administrative user to your Exchange 2007/2010 server and open **Exchange Management Console**.

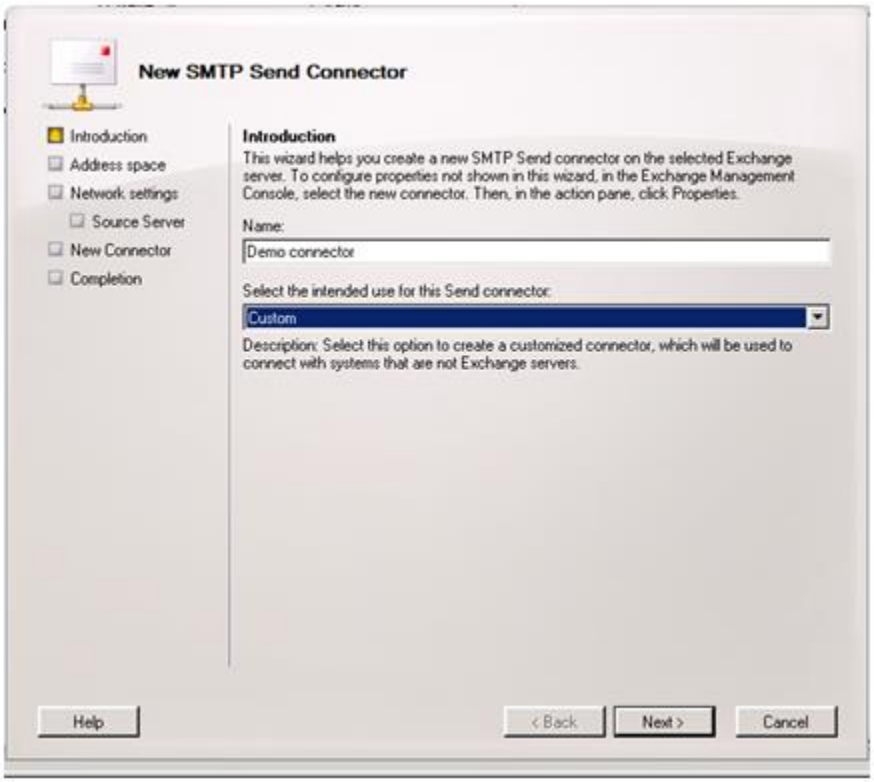


2. Expand *Organizational Configuration*, click **Hub Transport**.

3. On the right hand side under **Actions** click **New Send Connector**.

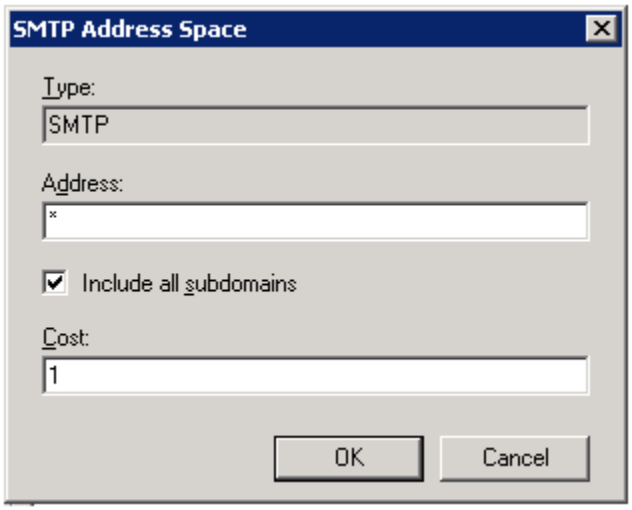


4. Give the Send Connector a name and select the intended use as *Custom.*

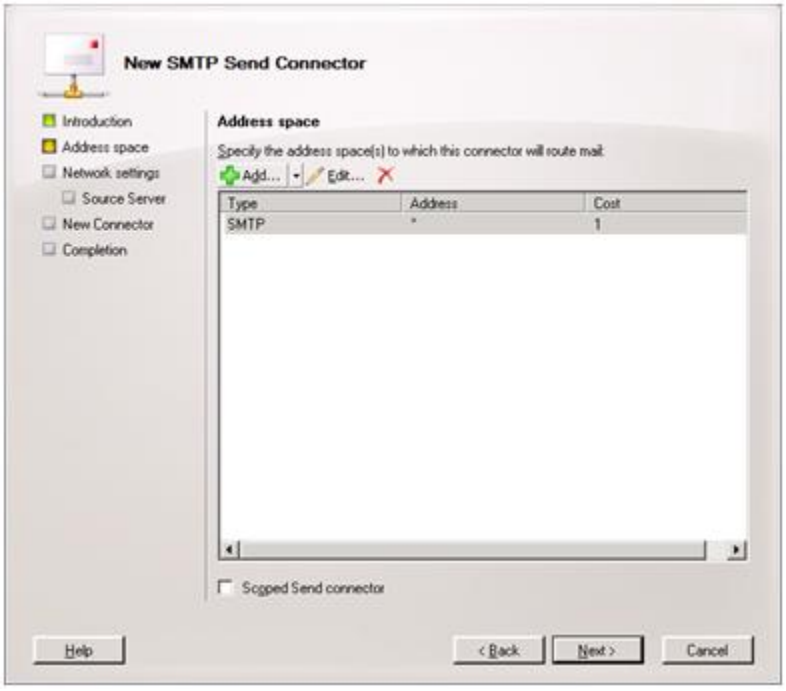


5. Click the **Add** button on the Address Space screen.

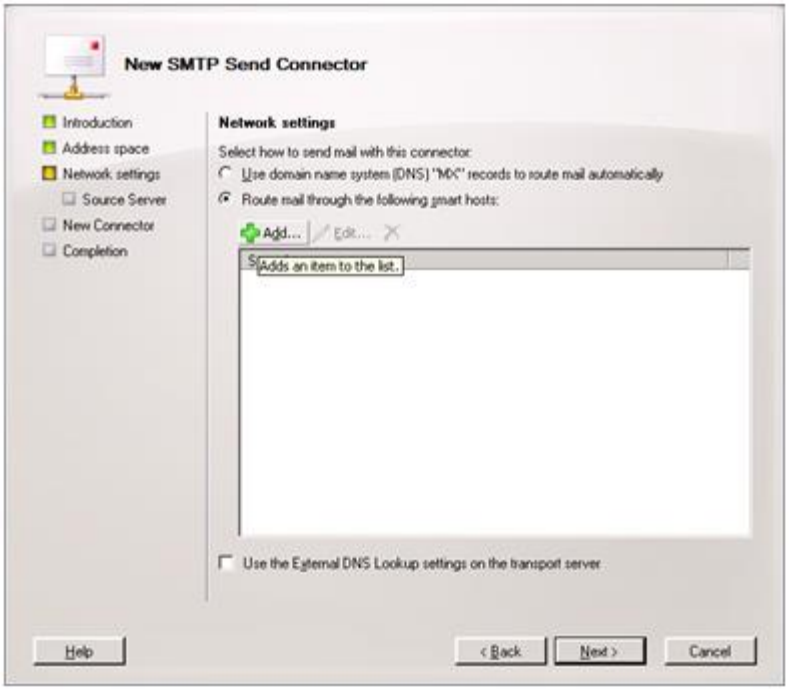
6. Under Address put the recipient domain name, check include all sub-domains and leave the cost as low as possible, click **OK**.



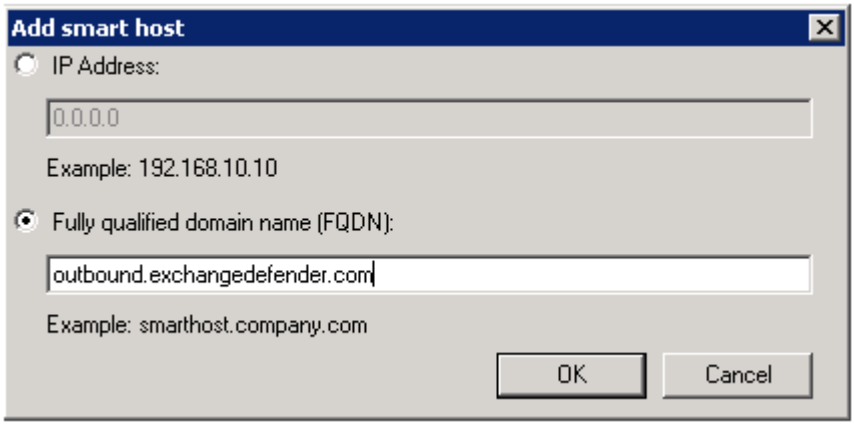
7. Click **Next**.



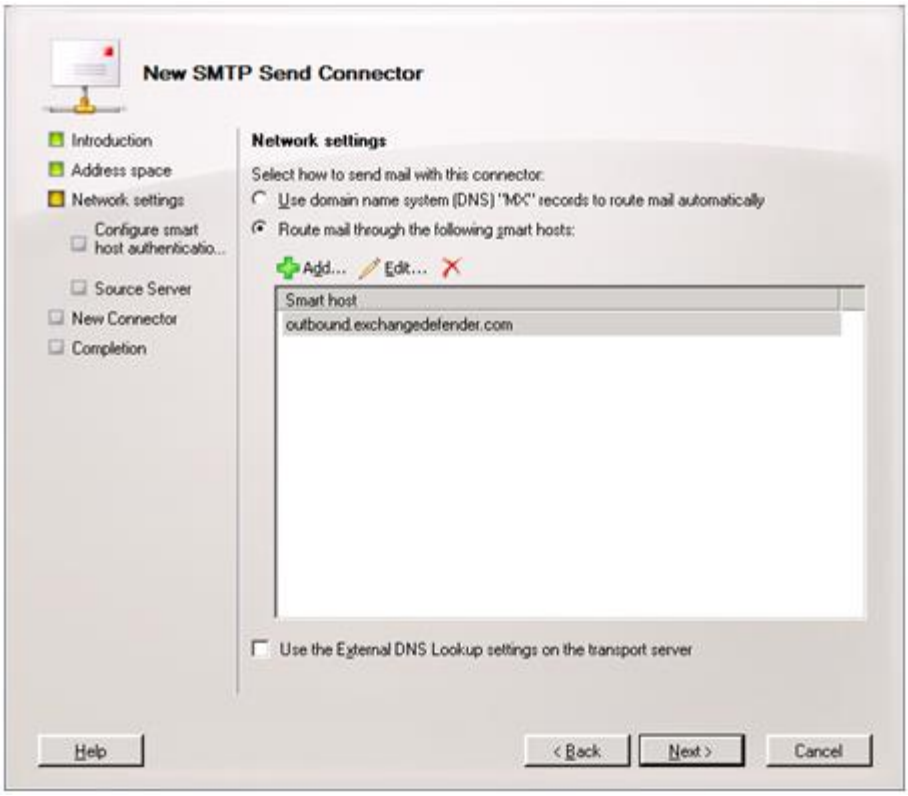
8. Select the radio button to "*Route mail through the follow smart hosts:*" and click **Add**.



9. Select the radio button to "*Fully qualified domain name (FQDN):*" and enter "*outbound.exchangedefender.com*" and click **OK**.

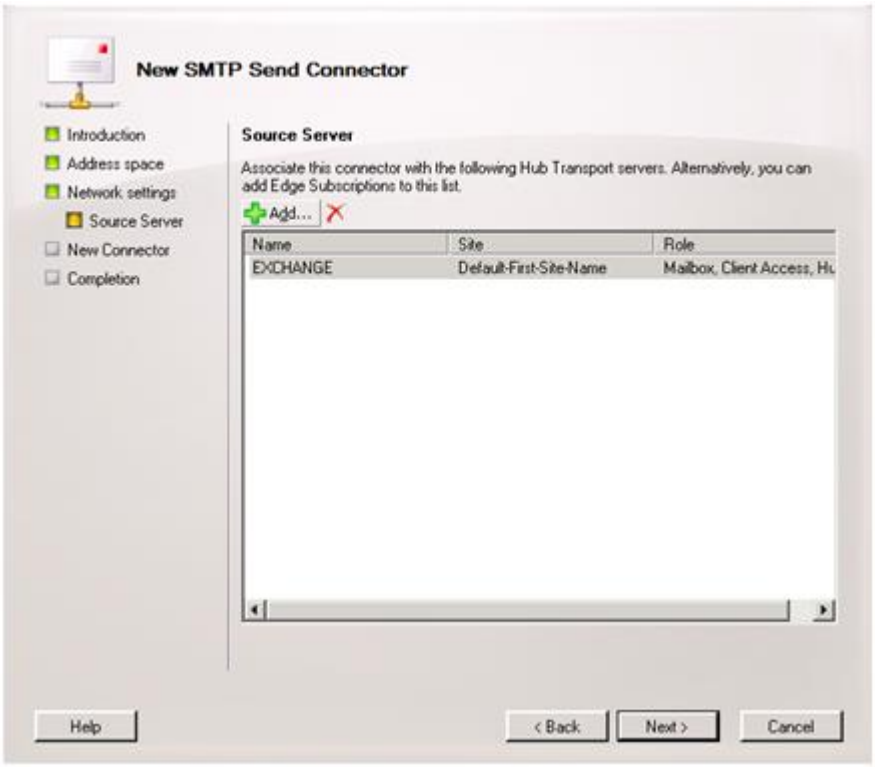


10. At this point, you should be able to see the server you specified listed then click **Next.**



11. Since ExchangeDefender uses your server's IP Address to authenticate access, leave the radio button set to Authentication Settings "*None*" and click **Next**.

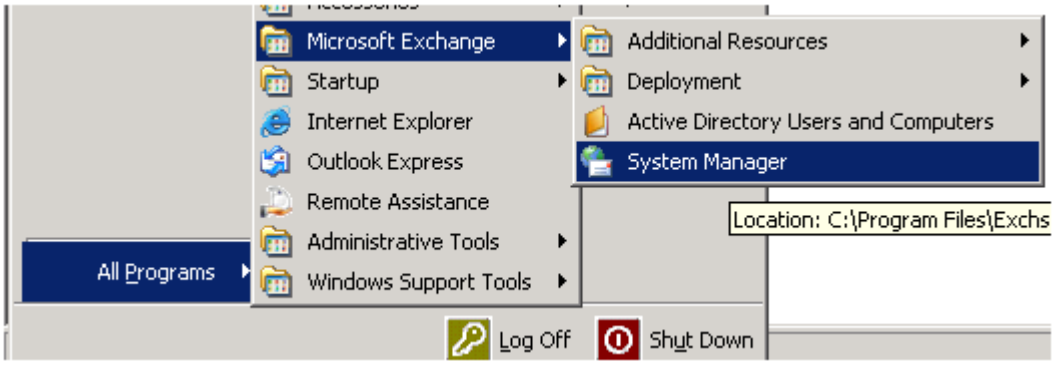
12. On the source server screen verify that the exchange server is listed (If not, click Add and find the server) and then click **Next**



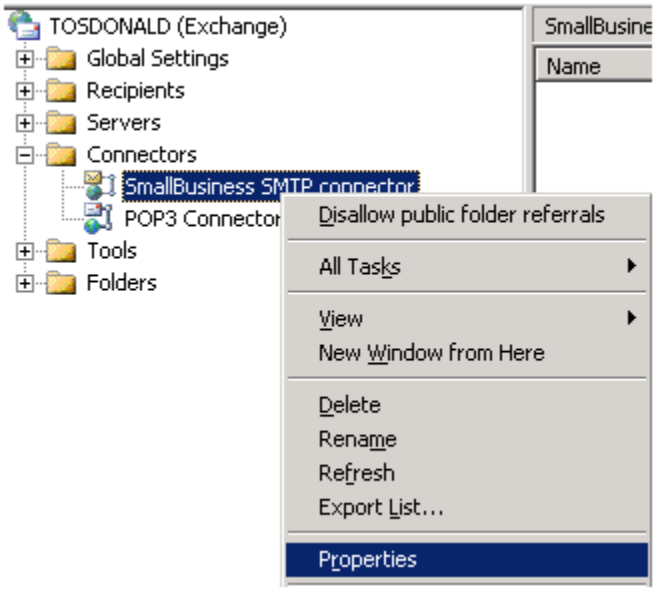
13. On the final screen you will see the commands that will be run to create the send connector. Click **New** and on then **Finish**

Exchange 2003

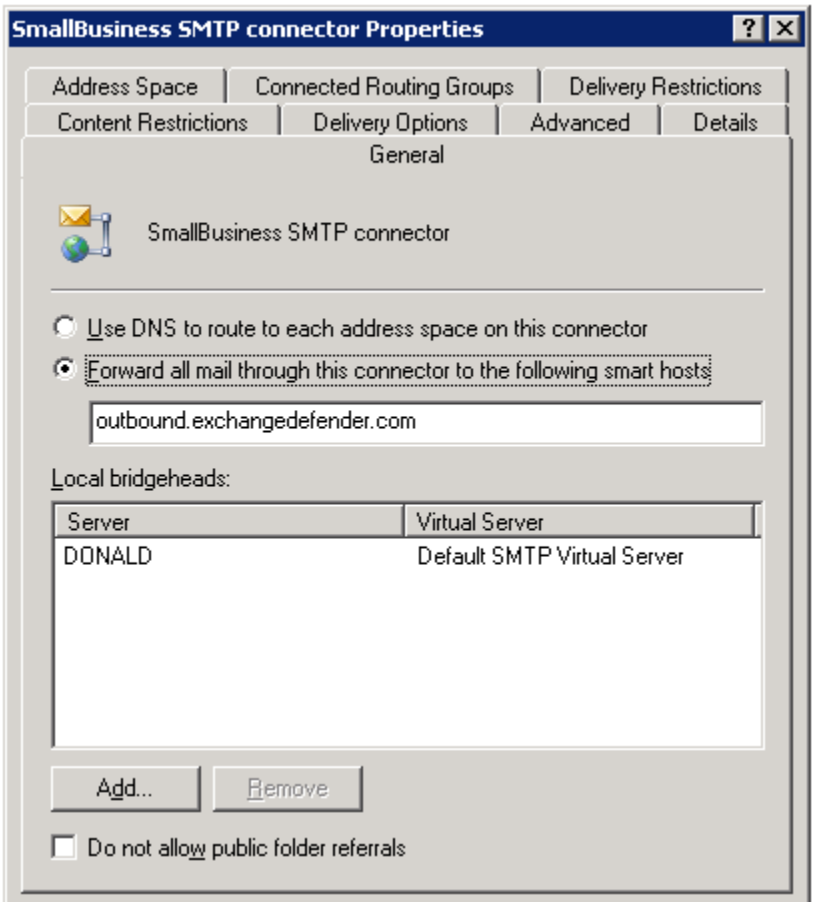
1. Login to your Exchange 2003 server and open *System Manager*.



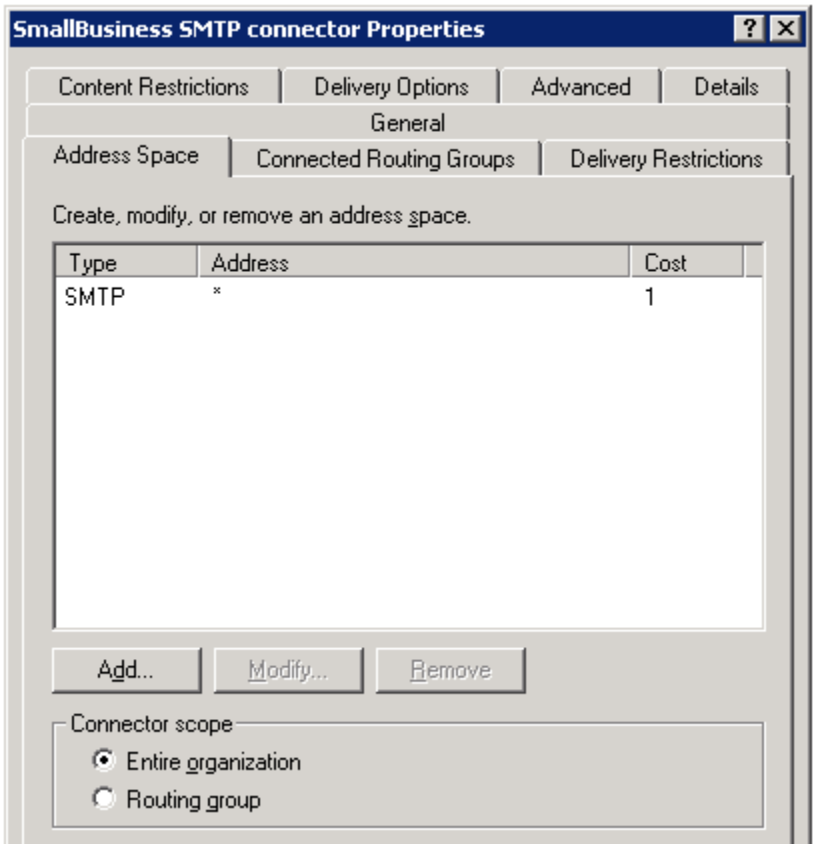
2. Expand Connectors , right click **SmallBusiness SMTP Connector** (or your active outgoing SMTP connector) and select properties.



3. In the general tab, set the radio option to *Forward all mail through this connector to the following smart hosts* and input *outbound.exchangedefender.com*



4. Navigate to the *Address Space* tab and ensure there is one entry with the address specified as * and the Cost as 1.



IP Restrictions

Enforcing IP restrictions is absolutely critical to complete protection of your mail server. Because hackers and spammers can easily bypass cloud services and target your server directly, mail servers protected by ExchangeDefender should accept anonymous SMTP connections only from the ExchangeDefender networks listed below:

65.99.255.0/24
206.125.40.0/24

You should allow inbound SMTP traffic from the above IP ranges only and deny all other traffic. You should only allow outbound SMTP traffic from your mail server to the ExchangeDefender outbound servers.

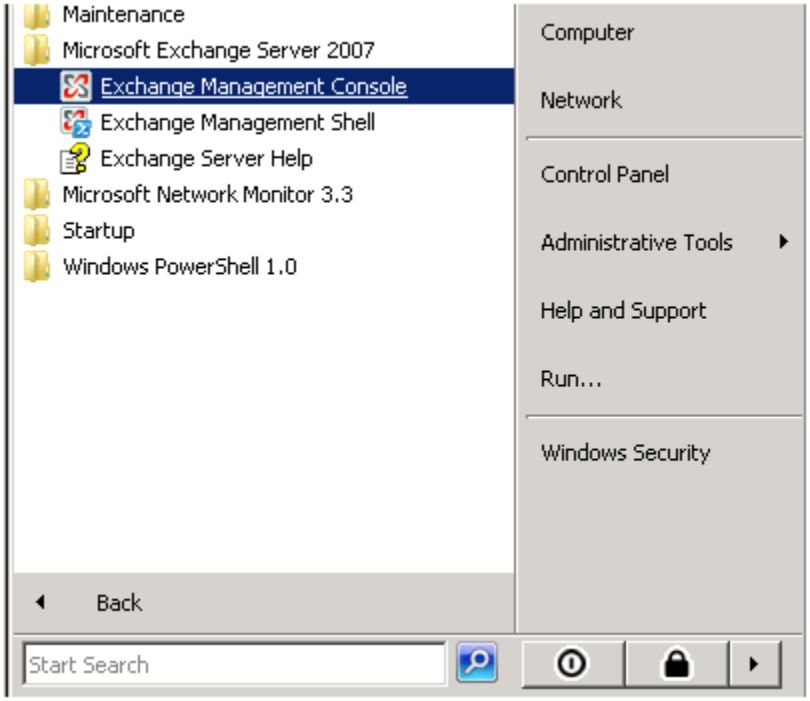
Please follow these instructions to enforce IP restrictions on Exchange 2003 and 2007:

Exchange 2007/2010

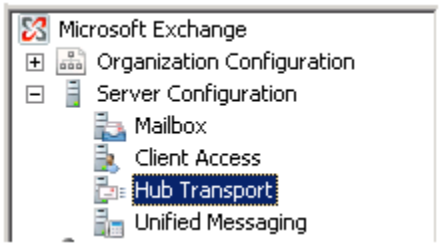
To program the IP address restrictions on the receive connector in Exchange 2007:

1. Obtain the latest list of ExchangeDefender IPs from the ExchangeDefender Deployment Guide under *'Configuring IP Restrictions'*

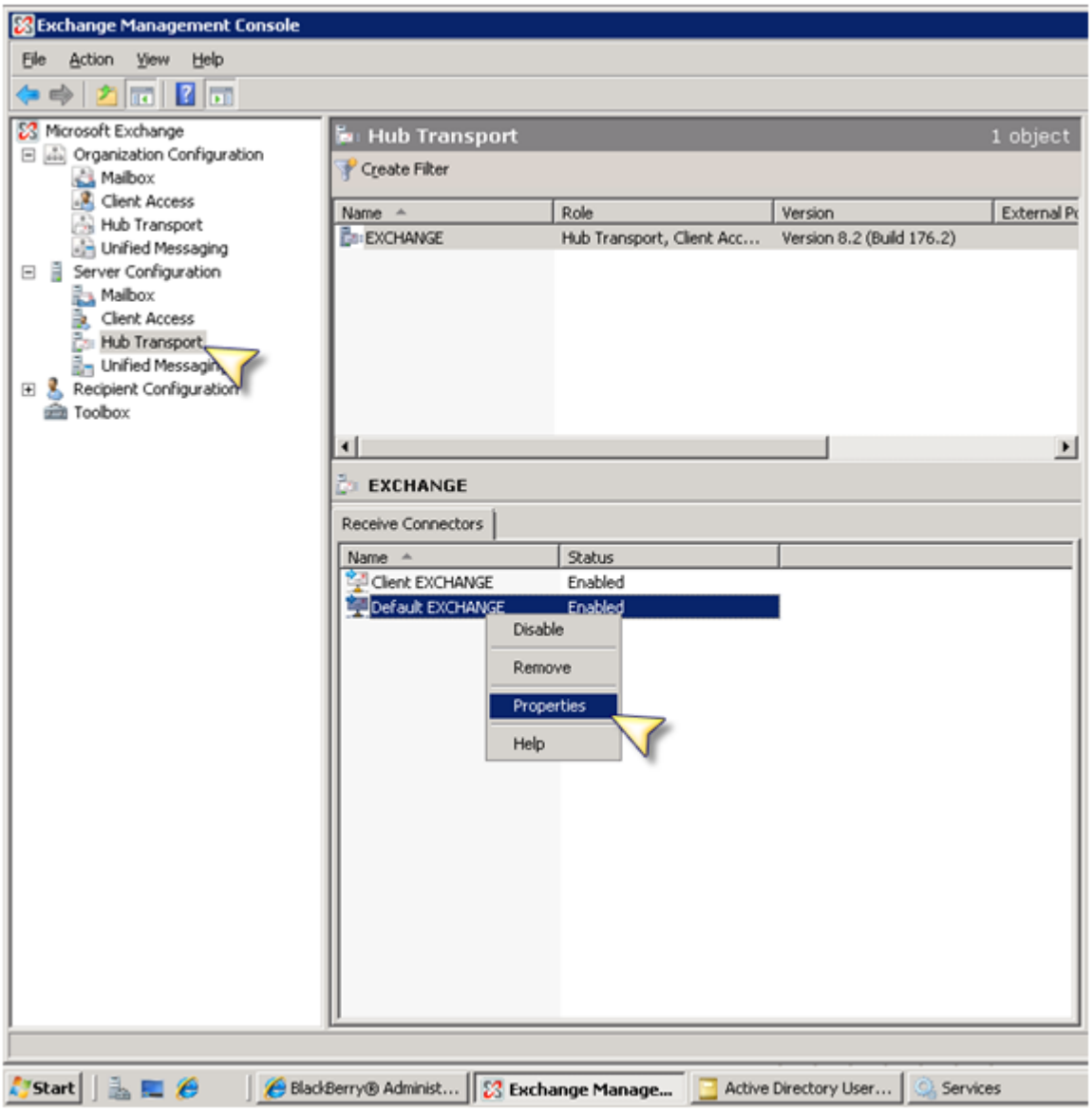
2. Open Exchange Management Console



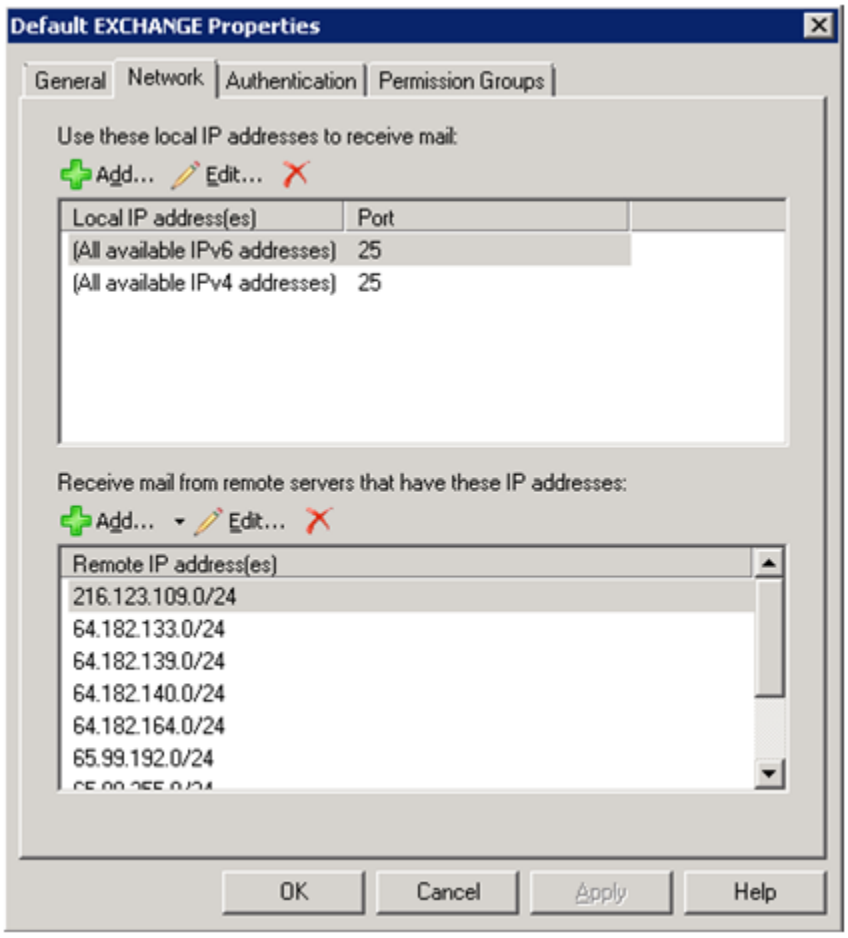
3. Expand Server Configuration, click **Hub Transport**



4. SBS Users: Right click on the *"SBS Internet Mail Connector"* and select Properties
NON-SBS Users: Right click on *"Default SERVERNAME"* and select *"Properties"*.

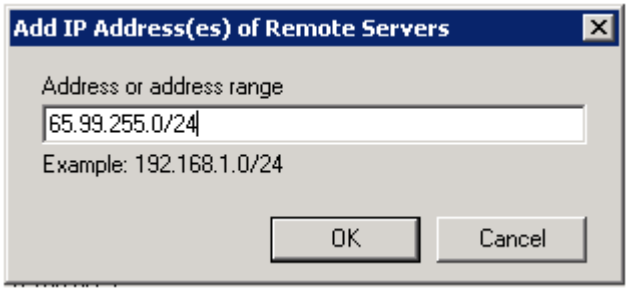


5. Once the dialog box pops up select the *"Network"* tab:

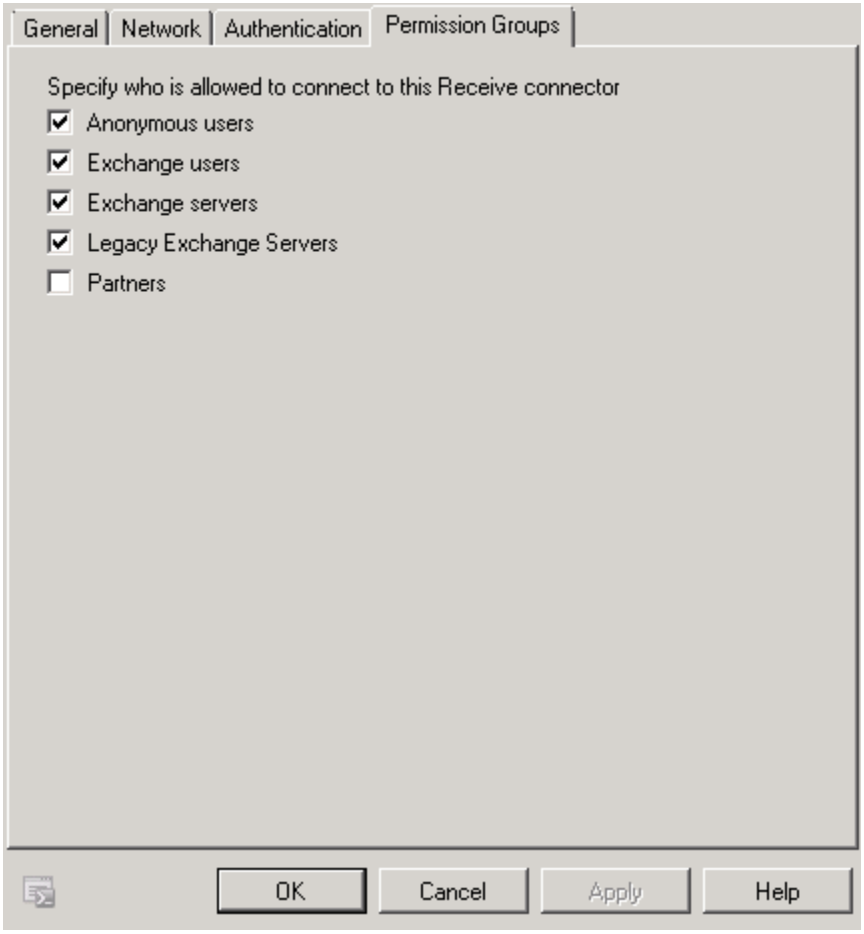


6. Under "Receive mail from remote servers that have these addresses:" find the entry that says *0.0.0.0-255.255.255.0* and **delete** the record.

7. Under "Receive mail from remote servers that have these addresses:" click **Add**. Input the first ExchangeDefender IP range/netmask. Repeat this step for each ExchangeDefender IP network in the deployment guide.



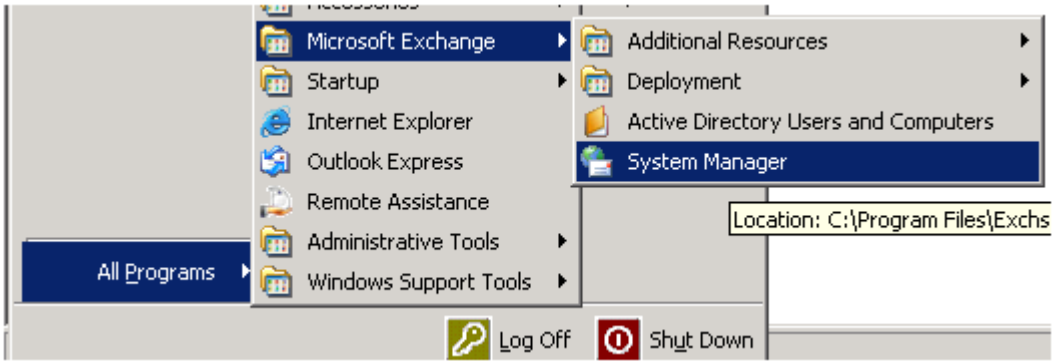
8. Please ensure under the Authentication tab that "Anonymous" delivery is allowed from our ranges.



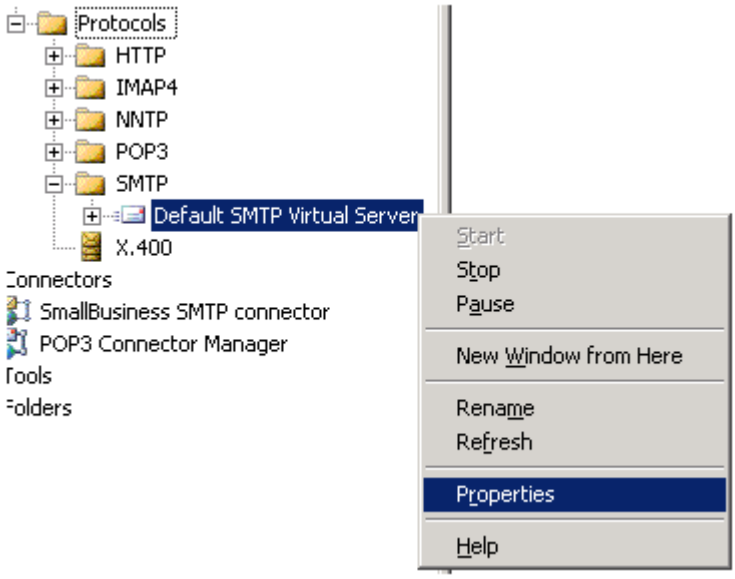
Exchange 2003

1. Obtain the latest list of ExchangeDefender IPs from the ExchangeDefender Deployment Guide under *'Configuring IP Restrictions'*

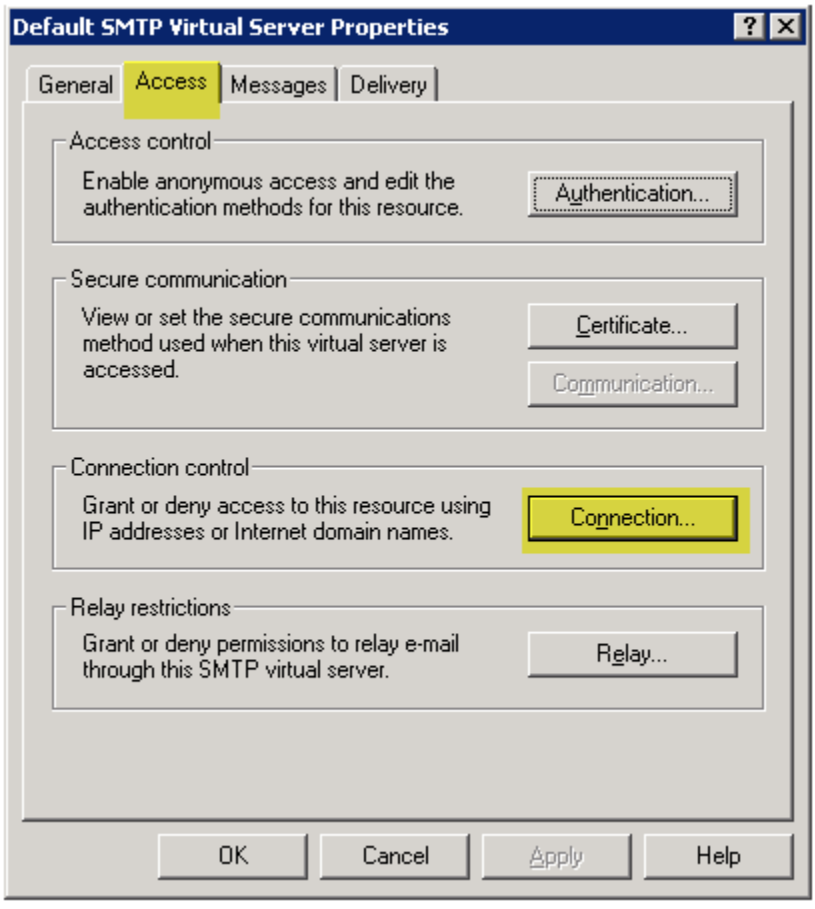
2. Login to your Exchange 2003 server and open *System Manager*



3. Expand Servers, ServerName, Protocols, SMTP - right click *"Default SMTP Virtual Server"* (Or the active receive connector name) and select properties

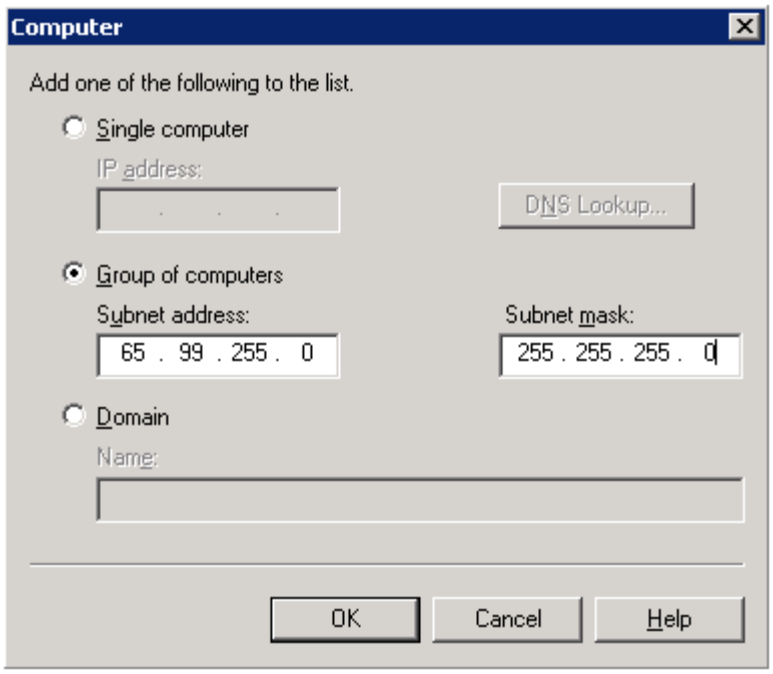


4. Navigate to the *Access tab* and then select the *Connection button*.



5. Remove any entries from previous providers or entries that have the IP range *0.0.0.0 - 255.255.255.0*

6. Click **Add** to enter a new IP restriction. Select the *Group of computers* option, insert the first IP range for ExchangeDefender and set the subnet mask to *255.255.255.0* - click **OK**. Repeat this step for each ExchangeDefender network.



7. Restart the *Simple Mail Transfer Protocol (SMTP)* service to apply the changes.

Warning: Do not enforce IP restrictions until at least 72 hours after the MX record change. Enforcing IP restrictions while your old DNS zone is still cached on the Internet will result in a permanent mail loss and mail delays.

Should the IP restrictions be applied on the firewall or on the mail server? We are frequently asked this question and the answer depends on whether you have external users or third parties attempting to relay mail through your mail server. If you have external connections to your SMTP server (from third party vendors or mobile users) then it is easier to enforce restrictions on the mail server and enforce password protected SMTP access there. However, if you do not have external connections the restrictions should be enforced on the firewall in order to free up resources on the mail server.

Install Client Desktop Software

Own Web Now Corp recommends deployment of Client Software Suite solutions over email Daily and Intraday digest reports for several reasons:

- Over 99% of all email SPAM reports are ignored or filtered to junk mail.
- Outlook and Desktop addins allow for realtime access to SPAM quarantines and settings.
- Client Desktop solutions work the way users do, in the applications they use.
- Client Desktop solutions are interruptive, they alert the users when necessary.

ExchangeDefender Client Software Suite was designed to give the user a more familiar experience, closely tied to the way they access their email and messaging. Outlook 2007 addin is perfect for Outlook power-users that never want to leave their Outlook experience. Similarly, Windows Desktop agent "annoyarizer" was designed for sales professionals, travel agents, financial industry employees and anyone that needs frequent alerts telling them that SPAM has been blocked from their inbox.

For more information about Client Software Suite please see the following page:
http://www.exchangedefender.com/features_client_software.php

Documentation, branding and deployment instructions are available in the individual downloads.

Advanced Deployment Considerations

ExchangeDefender is a very flexible security solution and we encourage our more technically advanced partners to use ExchangeDefender to improve reliability and failover of their own sites with ExchangeDefender's help.