MailGuard and Microsoft Exchange 2010

Contents

Introduction

Viruses are becoming more prevalent and sophisticated every day. Microsoft Exchange, when used in conjunction with MailGuard, can offer full protection from viruses even before they've been officially recognised and anti-virus software is capable of detecting them.

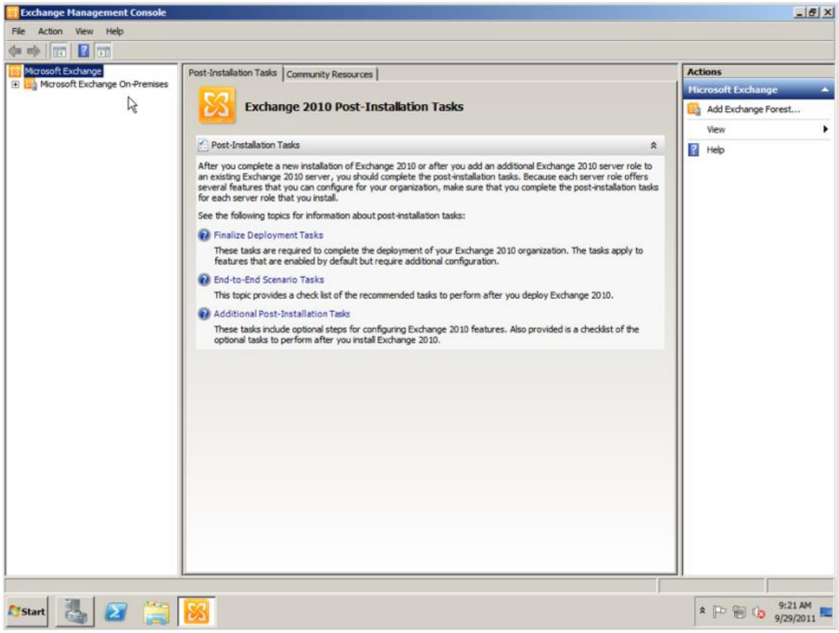
The section **Protecting OUTBOUND email** outlines the procedure for setting up your Microsoft Exchange server to direct all outbound email (that is, email originating from within your organisation) to MailGuard for scanning. Even if you are running anti-virus software locally, and despite the fact all your incoming emails are virus free, there are many different ways a virus can infect a computer. Eliminate the possibility of virus emails originating from your company by sending all your outbound emails to MailGuard for scanning.

Virus authors commonly send infected emails directly to mail servers, bypassing the normal delivery mechanism (and hence our filter servers!). The only way to ensure all your emails have been delivered through the proper channels and verified by us as virus free is to instruct your mail server to only accept email deliveries from MailGuard servers. Instructions for doing this are outlined in the section entitled **Preventing unauthorised INBOUND email**.

All steps below are performed in the **Microsoft Exchange Management Console** application.

1. Start the Microsoft Exchange Management Console: **Start**, **All Programs**, **Microsoft Exchange Server 2007**, **Exchange Management Console** (see Figure 1).

Figure 1



Exchange 2010 Post-Installation Tasks

Post-Installation Tasks

After you complete a new installation of Exchange 2010 or after you add an additional Exchange 2010 server role to an existing Exchange 2010 server, you should complete the post-installation tasks. Because each server role offers several features that you can configure for your organization, make sure that you complete the post-installation tasks for each server role that you install.

See the following topics for information about post-installation tasks:

Finalize Deployment Tasks

These tasks are required to complete the deployment of your Exchange 2010 organization. The tasks apply to features that are enabled by default but require additional configuration.

End-to-End Scenario Tasks

This topic provides a check list of the recommended tasks to perform after you deploy Exchange 2010.

Additional Post-Installation Tasks

These tasks include optional steps for configuring Exchange 2010 features. Also provided is a checklist of the optional tasks to perform after you install Exchange 2010.

Protecting OUTBOUND email

Note: the following steps outline the process of ensuring that all e-mail sent from your organisation via this Exchange server is delivered via MailGuard. Given the universal scope of this MailGuard Send Connector, you are advised to either disable or remove any existing Send Connectors to ensure that all mail is indeed routed via MailGuard.

If necessary, please consult your Administrator and amend the relevant steps should you require that certain mail be routed differently.

To configure **Exchange** to send all outbound messages (i.e. messages originating from within your organisation) to MailGuard for filtering, please perform the following steps:

1. Open the **Microsoft Exchange Management Console** as detailed in the **introduction** of this document.
2. **Create new** SMTP Send Connector:

   FOR 'HUB' TRANSPORT TYPE SERVER:

   Under **Organization Configuration,** right click **Hub Transport** and then **left click** the resulting **New Send Connector...** option (see Figure 2a).

   FOR 'EDGE' TRANSPORT TYPE SERVER:

   Under **Edge Transport**, right click the empty space in the **Send Connectors** tab, then left click the resulting **New Send Connector** option (see Figure 2b).

Figure 2a

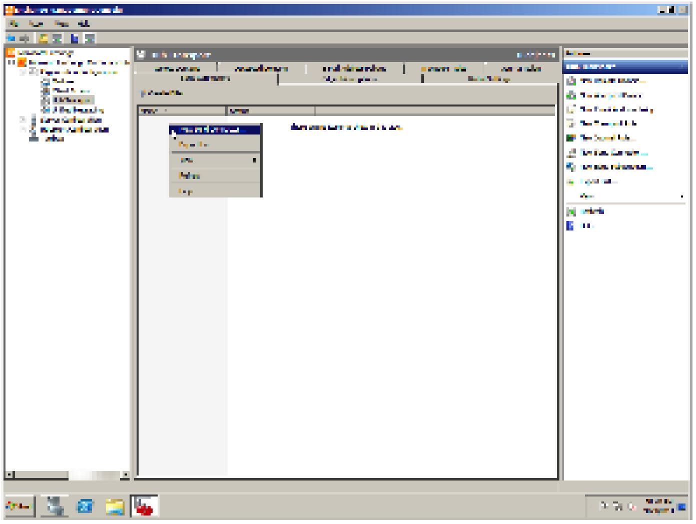
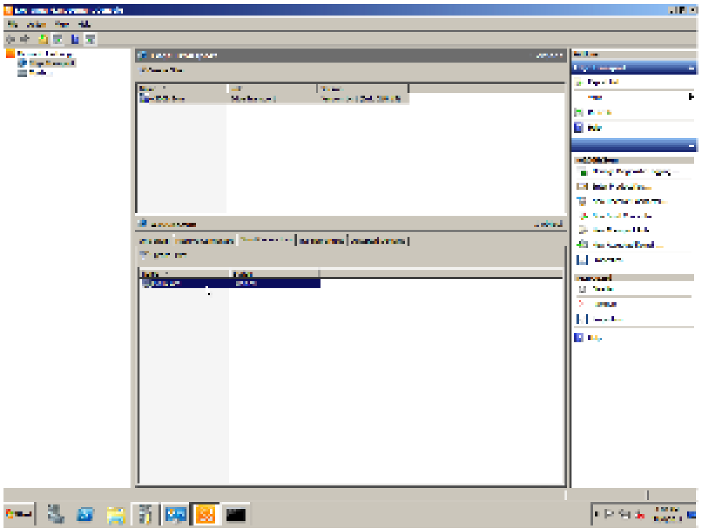


Figure 2b

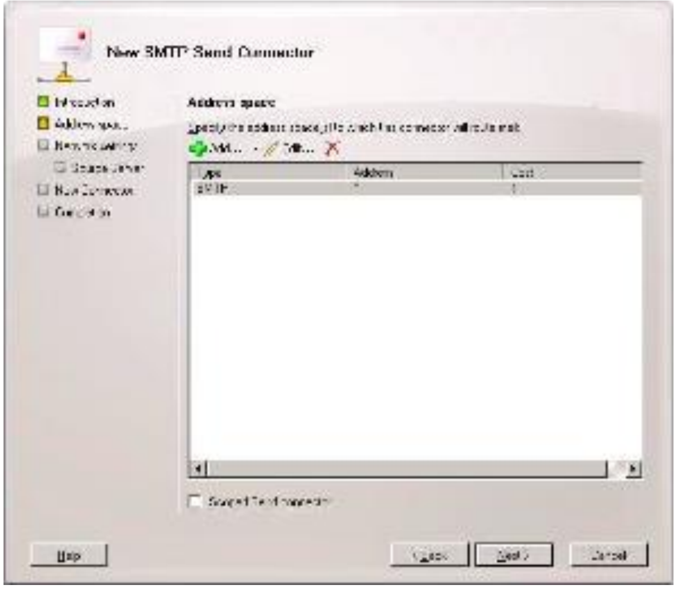


3. Enter the desired Name for the new **SMTP Send Connector** e.g. MailGuard.
4. Ensure that the selected use for this **Send Connector is** set to **Custom**. Click **Next**.
5. Add a new **SMTP Address Space**. To ensure that this Connector will route mail to all domains enter the wildcard character * in the **Address** field. The **Include all subdomains** checkbox will default to checked given this **Address**.

   Leave the **Cost** field at the default value of 1. Click **OK**.
6. Under most typical configurations, the **Scoped Send connector checkbox** will remain unchecked. Consult your Administrator if you are unsure whether this Connector should be made available to all Hub and/or Edge Transport servers in the **Exchange Organization**.

7. Click **Next** (see Figure 3).

Figure 3



8. Under **Network Settings** select the **Route mail through the following smart hosts** radio button. Click **Add**.
9. Under the **Add smart host** pop-up, select the **Fully qualified domain name (FQDN)** radio button.
10. Enter the name of your outgoing filter server. The name of your outgoing filter server takes the format:

    filter.xxxxxx-x.mailguard.com.au

    (where **xxxxxx-x** is the unique MailGuard code allocated to your domain).

    The name of your outbound filter server was included in the welcome message you received upon joining MailGuard.

    If you're not sure of the name of your outbound filter server, please **contact MailGuard Support** or click on the **View** button next to your domain name in the **Domains** tag of the **MailGuard Management Console**.

11. Leave **Use the External DNS Lookup settings on the transport server** checkbox unchecked. Click **Next**.
12. Select the **Basic Authentication** radio button under the **host authentication settings** section.

13. Under most circumstances, ensure that the **Basic Authentication** over **TLS** checkbox is unchecked.

    If you configured your Exchange 2010 Server to use an SSL certificate when you installed it, Exchange 2010 will try to use TLS connections by default regardless of whether or not this option is checked and will only 'fall back' to an unencrypted connection if TLS cannot be utilised. MailGuard's TLS support works in the same way, which ensures the connection is encrypted by default. Please consult your Administrator if you are unsure.

14. Enter the smart host **User name** and **Password**.

    NOTE: This is not the same username and password you use to log into the MailGuard Management Console.

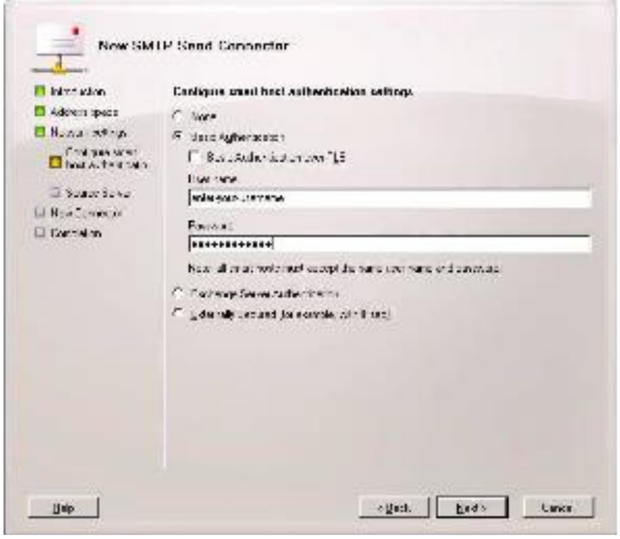
    Your SASL (also called SMTP authentication) username and password was included in the welcome letter you received upon joining MailGuard. If you don't have these details, please **contact MailGuard Support** or click on the **View** button next to your domain name in the **Domains** tag of the **MailGuard Management Console**.

15. Click **Next** (see Figure 4).

    MailGuard offers an alternative method of SMTP authentication. At your request, MailGuard can simply add your static IP to our trusted networks list. Under this configuration you should select an authentication method of None in step 12 above.

    Please note that we offer this alternative authentication method only to clients who have a static IP address. Please **contact MailGuard** should you qualify and have a preference for authenticating in this manner.

Figure 4



Configure smart host authentication settings:

○ None

● Basic Authentication

□ Basic Authentication over TLS

User name: enter your username

Password: ************

Note: all smart hosts must accept the same user name and password.

○ Exchange Server authentication

○ Externally secured (for example, with IPsec)

16. Should you only have a single **Exchange** server, simply click **Next** under the **Source Server** configuration page. Please consult your Administrator should you have a more complex configuration.

17. Review your **Configuration Summary** and correct any mistakes by cycling back through your configuration using the **Back** button. If each item is correct, click **New**.
18. Completion. Click Finish. (see Figure 5a for Hub Transport & Figure 5b for Edge Transport).

Figure 5a

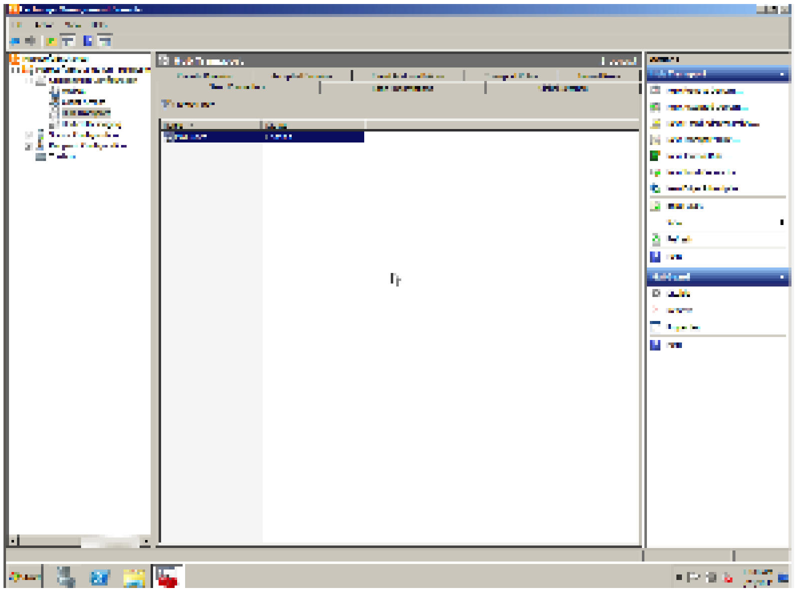
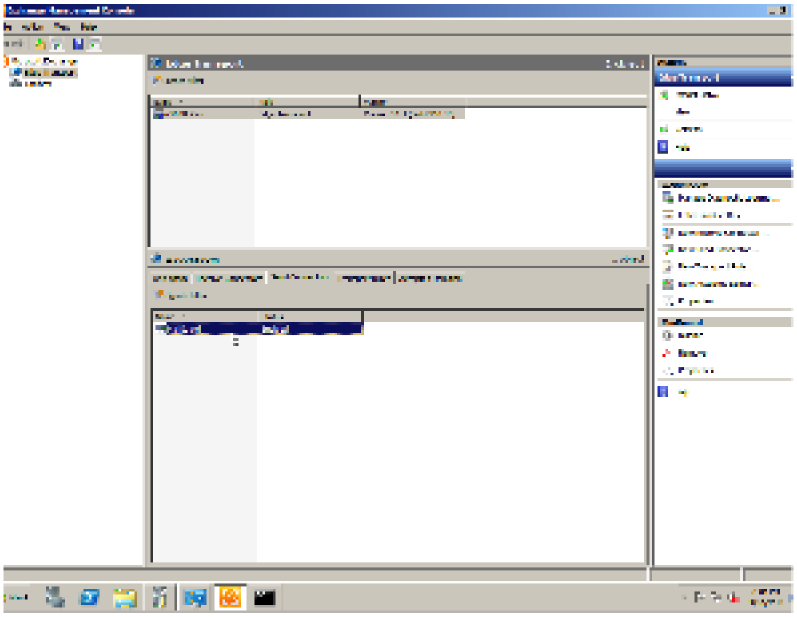


Figure 5b



MailGuard and Sender Policy Framework (SPF)

In computing, **Sender Policy Framework (SPF)** allows software to identify messages that are or are not authorized to use the domain name in the SMTP HELO and MAIL FROM (Return-Path) commands, based on information published in a sender policy of the domain owner. Forged return paths are common in e-mail spam and result in backscatter. (Source: wikipedia).
Should you currently utilise SPF, it is imperative that you amend each record associated with domains relaying mail via MailGuard.

To ensure that your SPF continues to function correctly, please add the following “include” string to your existing SPF:

include:customer.mailguard.com.au

Preventing unauthorised INBOUND email

To prevent malicious users from delivering messages directly to your Exchange Server (thus bypassing MailGuard's servers), perform the following steps:

1. Open the **Microsoft Exchange Management Console** as detailed in the **introduction** of this document.

   FOR 'HUB' TRANSPORT TYPE SERVER:

   a.) Left click the **Hub Transport** sub-item located under **Server Configuration**.

   b.) In the centre panel, double-click the **Default <SERVER NAME> Receive Connector**.

   FOR 'EDGE' TRANSPORT TYPE SERVER:

   a.) Select the **Receive Connectors** tab under **Edge Transport**.

   b.) Double-click the **Default Receive Connector**.

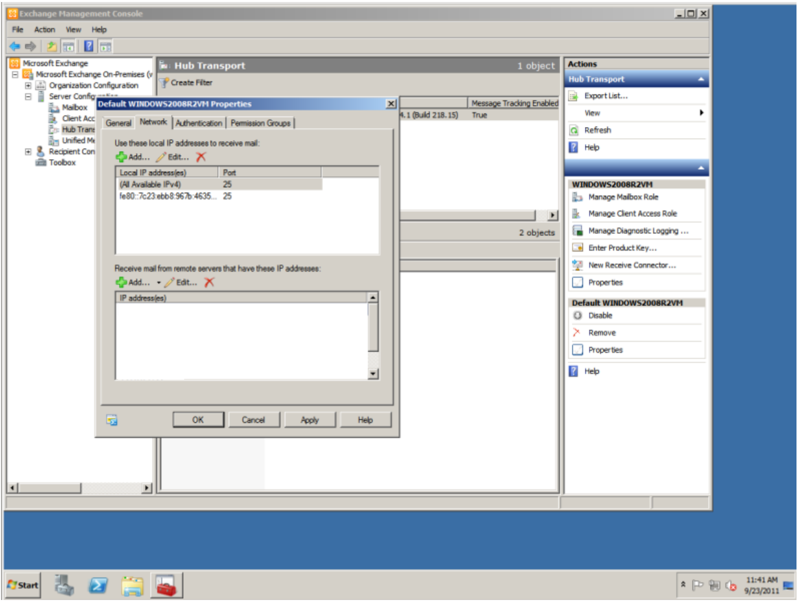
2. Select the **Network** tab.
3. Under the **Remote IP address(es)** table, add each of the following IP Addresses exactly as below:

   50.23.246.238/32
   50.23.252.166/32
   108.168.255.216/32
   108.168.255.217/32
   203.21.125.32/32
   203.21.125.33/32

4. Ensure that all other unauthorised Remote IP address(es) are removed. (see Figure 6a for Hub transport & see Figure 6b for Edge transport)

5. Select the “Permission Groups” tab, and tick the checkbox labelled “Anonymous users”
6. Completion. Click OK.

Figure 6a



Default WINDOWS2008R2VM Properties

General | Network | Authentication | Permission Groups

Use these local IP addresses to receive mail:

Add... Edit...

Local IP address(es)	Port
(All Available IPv4)	25
fe80::7c23:ebb8:967b:4635...	25

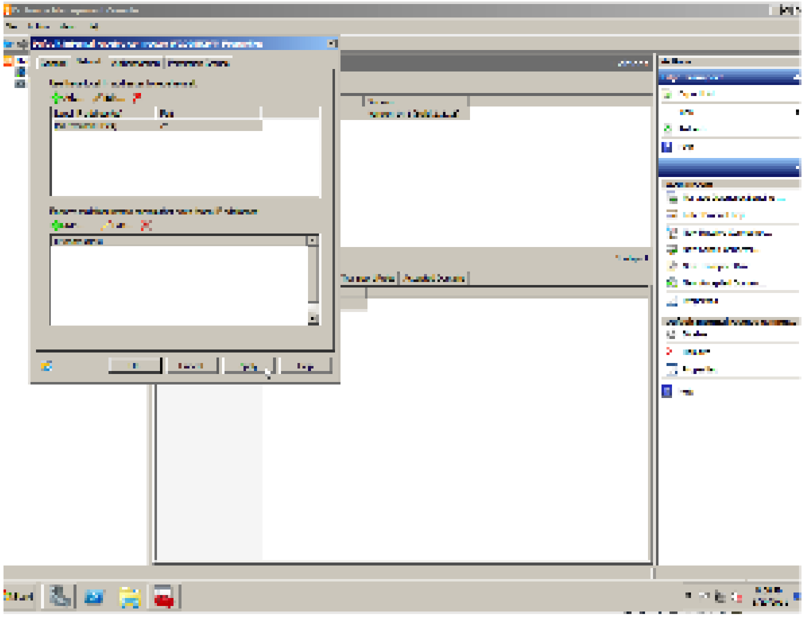
Receive mail from remote servers that have these IP addresses:

Add... Edit...

IP address(es)

OK | Cancel | Apply | Help

Figure 6b

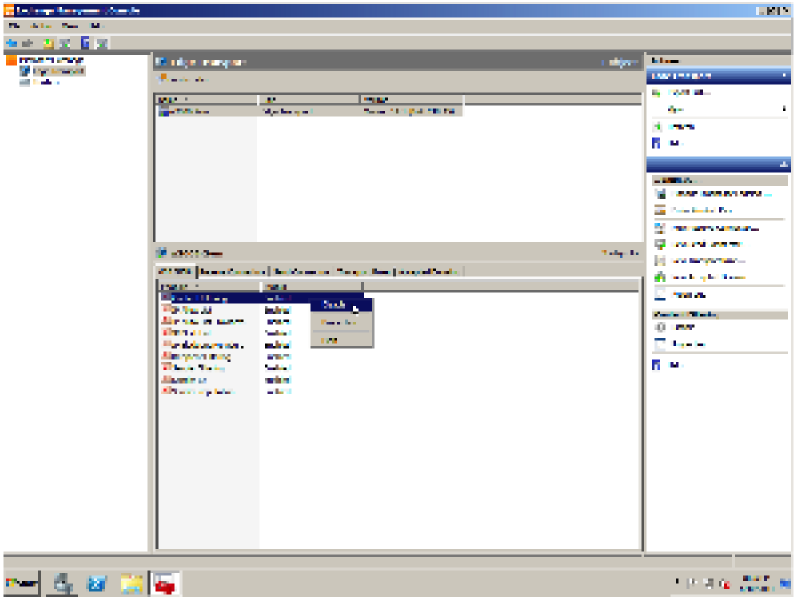


Disabling Content Filtering

The **Edge Transport** version of Exchange 2010 comes with **Microsoft Exchange Content Filtering** included and enabled by default. When using MailGuard, you do not need to maintain a local e-mail security service, therefore it is recommended that Exchange Content Filtering is disabled. To disable Content Filtering, please take the following steps:

1. Open the **Microsoft Exchange Management Console** as detailed in the **introduction** of this document.
2. Select the **Anti-spam** tab under **Edge Transport**.
3. Right-click on **Content Filtering** and select **Disable**.
4. Completion. See Figure 7.

Figure 7



Contact MailGuard

For any queries, comments or suggestions regarding this guide, please feel free to contact the MailGuard Service Desk on 1300 30 65 10 or via email at: **support@mailguard.com.au**.