

## Installing Policy Patrol with Exchange Server 5.5

If you have Microsoft Exchange Server 5.5, you must install Policy Patrol on a separate Windows 2003/2000/XP machine and forward your mails to the Windows SMTP service on the Policy Patrol machine. Depending on your requirements, you will need to forward incoming and/or outgoing mails to the Policy Patrol machine. If you only want Policy Patrol to process outbound mails (for instance for adding disclaimers) you only need to forward outgoing mails. If you only want Policy Patrol to process incoming mails (for instance to block spam) you just need to forward incoming mails. If you want to process inbound as well as outbound mails, you must route all mail through the Policy Patrol machine. Note that Policy Patrol does not offer internal mail filtering or updating of Outlook Sent Items with email modifications for Exchange 5.5.

To use Policy Patrol with Exchange 5.5, follow the steps described below.

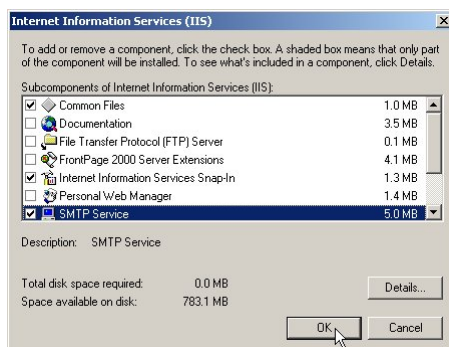
### Step 1. Preparing for installation

#### *System requirements*

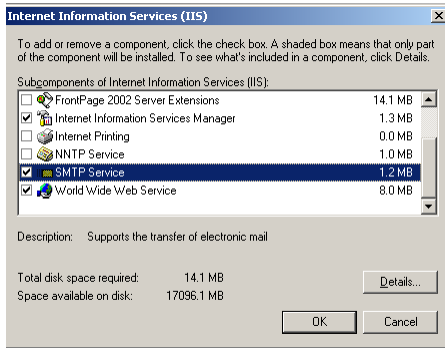
Before you install Policy Patrol make sure that the following is installed on the machine:

- Windows 2000 Professional/Server/Advanced Server, Windows Server 2003 or Windows XP Professional.
- Windows SMTP service (part of Internet Information Services): This is installed by default on Windows 2000 (Advanced) Server and is an option on Windows Server 2003, Windows 2000 Professional and Windows XP Professional.

To install the SMTP service on Windows 2000 Professional and Windows XP Professional, go to **Start > Settings > Control Panel > Add/Remove Programs > Add/Remove Windows Components**. Select **Internet Information Services** and click on **Details**. Check **SMTP service**. Any other required components are checked automatically. Click **OK**. Click **Next** to install the SMTP service.



To install the SMTP Service on Windows 2003 **Start > Settings > Control Panel > Add/Remove Programs > Add/Remove Windows Components**. Select **Application Server** and click on **Details**. Select **Internet Information Services** and click on **Details**. Check **SMTP service** and **World Wide Web Service**(World Wide Web Service is required for Challenge/Response). Any other required components are checked automatically. Click **OK**, then click **Ok** again. Click **Next** to install the SMTP service.

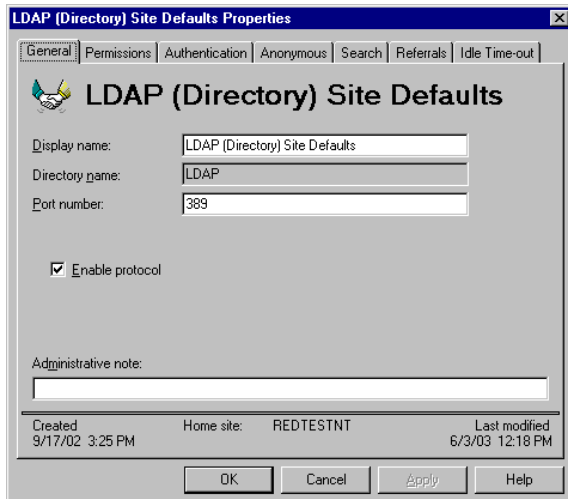


- Microsoft .NET Framework 2.0: If you do not have Microsoft .NET Framework 2.0 installed, the Policy Patrol installation program will download and install this for you.

***If you want to retrieve your users from Exchange 5.5***

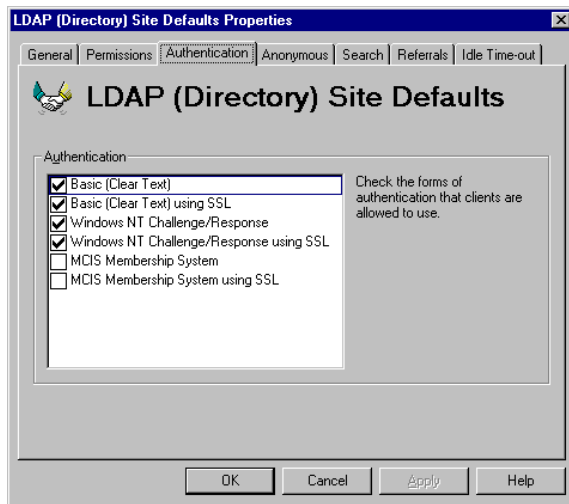
Policy Patrol uses LDAP to retrieve your users. If you wish to retrieve your users from Exchange 5.5, you must make sure that LDAP is enabled and configured as follows:

1. Go to **Microsoft Exchange Administrator > Organization > Site > Configuration > Protocols > Properties > LDAP**. In the **General** tab, make sure that **Enable protocol** is ticked. By default the LDAP service listens on port 389. If your LDAP service is listening on a different port, make sure that the correct port number is entered under **Port number**.

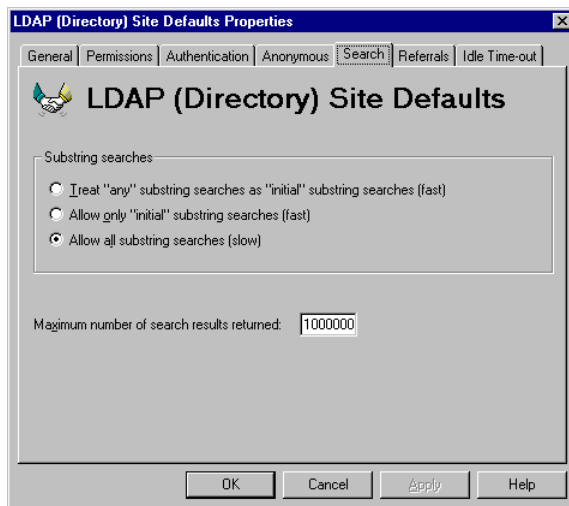


2. Go to the **Authentication** tab and make sure that the following options are ticked:

- Basic (Clear Text)
- Basic (Clear Text) using SSL
- Windows NT Challenge/Response
- Windows NT Challenge/Response using SSL



3. Go to the **Search** tab and select the option **Allow all substring searches (slow)** and set the **Maximum number of search results returned** to at least 10000.

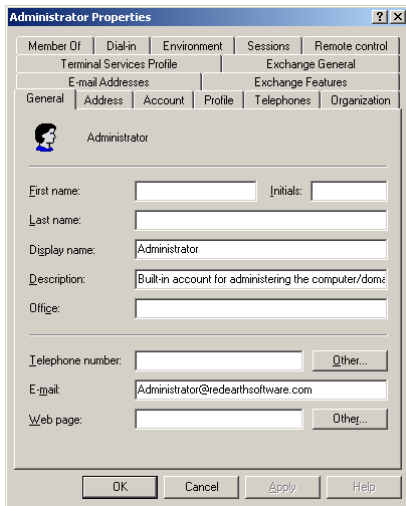


4. When you are ready click **OK** to save any changes.

#### ***If you want to retrieve your users from Active Directory***

If you want to retrieve your users from the Active Directory, you do not need to check any LDAP settings since LDAP is already a requirement for Active Directory. However, you

must make sure that your users have an email address entered in **Active Directory Users and Computers > Users > <User name> > Properties > General** Tab. If there is no email address entered here, Policy Patrol will not retrieve the user.



## Step 2. Install and configure Policy Patrol

---

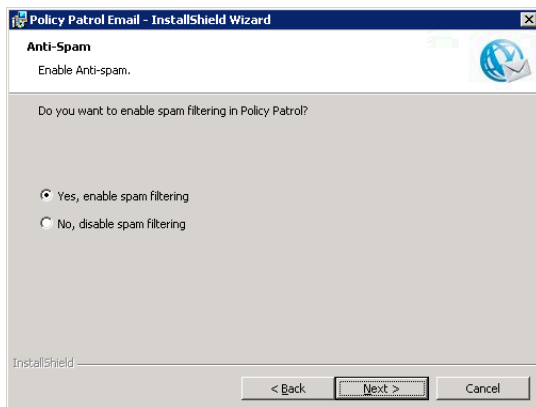
Note: You cannot install Policy Patrol on the same machine as Exchange 5.5, even if it is installed on a Windows 2000 machine. This is because you need to remove the Windows 2000 SMTP service to be able to start the Exchange 5.5 Internet Mail Connector, and Policy Patrol requires the Windows SMTP service to function.

To install Policy Patrol Email:

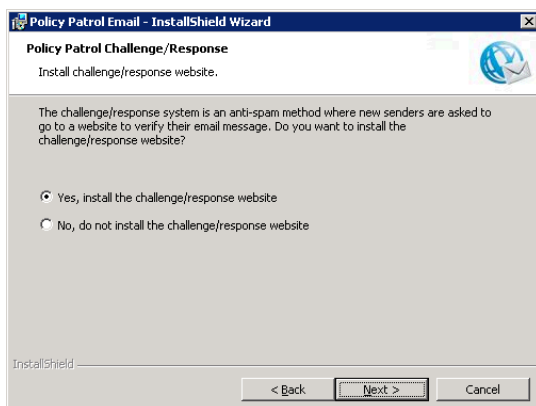
1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 2.0 installed, the Policy Patrol installation program will download it for you.
2. In the Welcome screen, click **Next**.
3. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
4. Select **Complete** as the installation type. Click **Next**.
5. Enter your user name, company name and Policy Patrol serial number. If you are evaluating Policy Patrol, leave the serial number field empty. Click **Next**.
6. **If you did not enter a serial number:** A dialog will pop up asking you to select the evaluation license to be installed. Select the relevant license and click **Next**.

Note: If you are evaluating Policy Patrol and later wish to try out a different Policy Patrol edition you can go to **<server name> > Security > Licenses**, select the license and click **Remove**. Policy Patrol will warn that no valid license is found. Click **OK**. A dialog will now pop up allowing you to select a new evaluation license type.

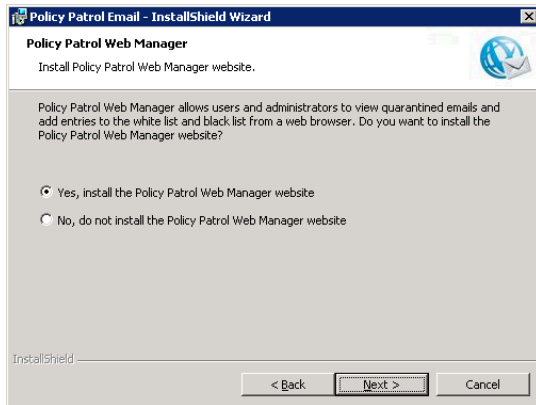
7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email. If you wish to change the location, click **Change** and select another folder. When you are ready, click **Next**.
8. Specify the notification settings. Enter the From:, To:, Cc: and Bcc: fields for the Policy Patrol notification emails. Policy Patrol notification emails inform you about evaluation expiry dates, over licensing issues and new updates to the program. The display name is pre-configured as Administrator, but you can change this by entering the following: "Display name" <email address>, i.e. "Joe Bloggs" <jbloggs@bloggsco.com>. Click **Next**.
9. **Only for Policy Patrol Mail Security Bundle and Mail Server Tools:** Select whether you wish to install the Policy Patrol Kaspersky Anti-Virus engine. Click **Next**.
10. **Only for Policy Patrol Mail Security Bundle:** Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected 'No, disable spam filtering', continue to step 12.



11. **Only for Policy Patrol Spam Filter or Mail Security Bundle with enabled anti-spam:** Select whether you wish to install the challenge/response website. This website is needed if you wish to make use of the challenge/response system that asks new senders to go to a website and verify their email in order for the message to be delivered. Click **Next**.



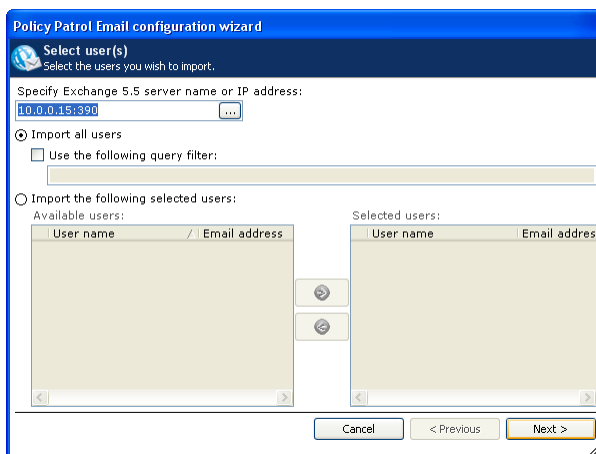
12. **All Policy Patrol editions apart from Policy Patrol Disclaimers:** Select whether you wish to install the Policy Patrol Web Manager website. This website is needed if you wish to allow users and Administrators to view quarantined emails via a web browser (required for quarantine reports).



13. Click **Install** to start installing.
14. When the installation wizard has finished copying the files, click **Finish**.
15. The Policy Patrol configuration wizard will start up. Click **Next** in the Welcome screen.
16. Now you must select where you wish to import your users from. If you want to retrieve your users from Exchange 5.5, select **Exchange 5.5** as the import source and click **Next**. If you want to retrieve your users from the Active Directory select **Active Directory** and click **Next**.
17. Select the users to import into Policy Patrol:

**If you selected Exchange 5.5:**

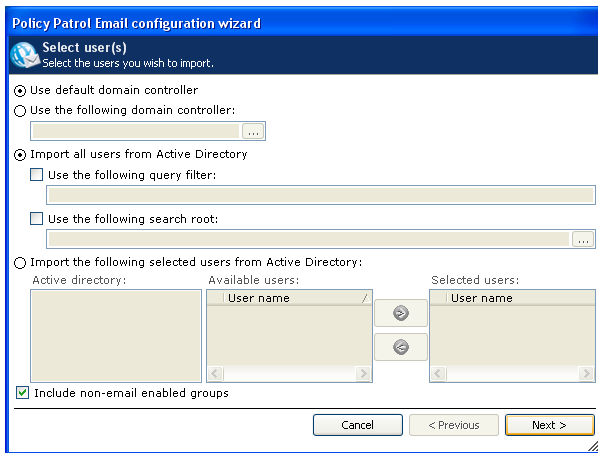
Specify the name or IP address of the Exchange Server, for instance 10.0.0.15. If your LDAP service is listening on a different port than 389, you must also enter the LDAP port as follows: <IP address>:<LDAP port>, e.g. 10.0.0.15:390.



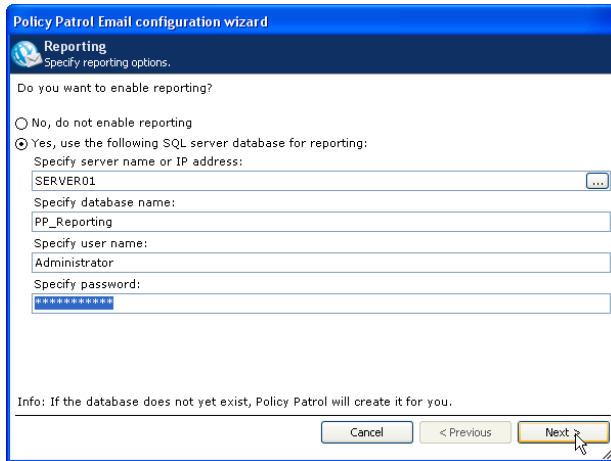
To license all users in Exchange 5.5, select **Import all users**. If you only wish to license certain users, select **Import the following selected users**. Select the users you wish to license in the left pane and press >. The selected users will now appear in the right pane. To select all users, press the >> button. To remove users, press the < button. To remove all users, press << . When you are done, click **Next**. You will now see your users in the Licensed user list in **Settings > Users**.

**If you selected Active Directory:**

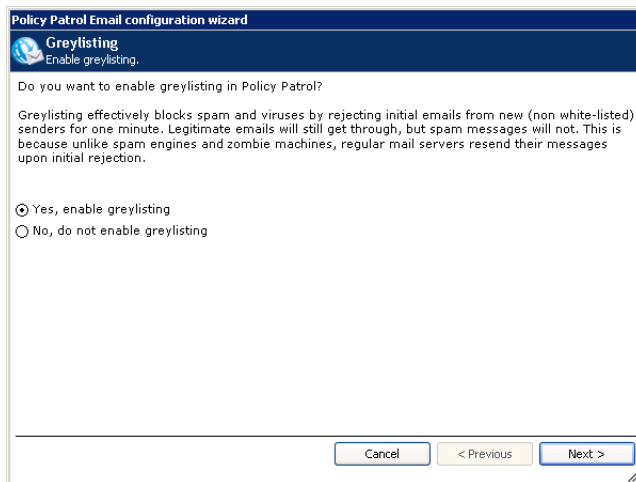
Specify the domain controller to retrieve your users from and select the users that you wish to license. You can either license all users or you can select only certain users to be licensed. For more information on the different options, consult the product manual. Click **Next**.



18. **Only for Policy Patrol Mail Server Tools and Mail Security Bundle:** Select whether you wish to enable Mail Backup. If you enable Mail Backup you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically create the database for you. If you do not have SQL Server, you can also specify an MSDE or SQL Server Express database. Click **Next** to continue.
19. **Only for Policy Patrol Mail Server Tools and Mail Security Bundle:** Select whether you wish to enable reporting. If you enable reporting you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password to be used. Policy Patrol will automatically create the database for you. If you do not have SQL Server, you can also specify an MSDE or SQL Server Express database. Click **Next** to continue.



20. **Only for Policy Patrol Spam Filter or Mail Security Bundle with enabled anti-spam:** Select whether you wish to enable greylisting. Greylisting effectively blocks spam and viruses by initially rejecting messages from new, non white-listed senders for one minute, therefore allowing legitimate emails through without any user intervention, and blocking the non-legitimate emails. Select whether you wish to enable greylisting, and click **Next**.



21. In the Configuration complete dialog, click **Finish**.

### Step 3. Configure Policy Patrol as a mail gateway

---

Before Policy Patrol can actually filter your emails, you must ensure that your mail flows through Policy Patrol. The following scenarios are possible:

- Scenario 1: Policy Patrol processes inbound and outbound mail
- Scenario 2: Policy Patrol processes only outbound mail
- Scenario 3: Policy Patrol processes only inbound mail

Select which scenario applies to your needs and follow the instructions for the appropriate scenario below.

## Scenario 1: Policy Patrol processes inbound and outbound mails

If you want Policy Patrol to filter all your mails, you will need to route all mail through the Windows SMTP service on the Policy Patrol machine, as per Figure 1 below. To do this, follow the next instructions:

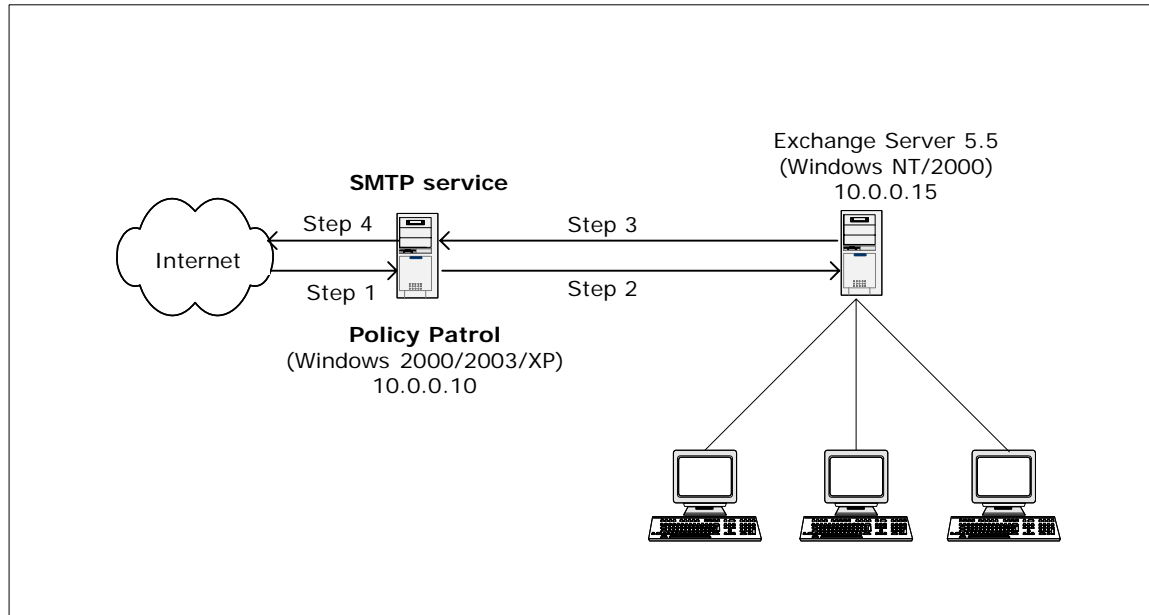
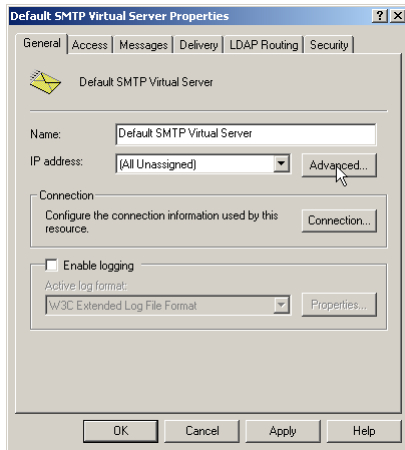


Figure 1 - Policy Patrol processes inbound and outbound mail from Exchange Server 5.5

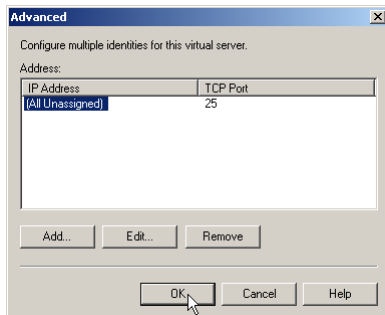
### Step 1. Direct incoming mail to the SMTP service on the Policy Patrol machine

Direct your incoming mail to the Windows SMTP service on the Policy Patrol machine (the external DNS servers for your domain must have an mx (mail exchanger) record pointing to the Policy Patrol machine). Furthermore, check the following settings in the Default SMTP Virtual Server:

- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.
- Right-click **Default SMTP Virtual Server**, and click **Properties**.
- In the **General** Tab, verify that your IP address is listed as **(All Unassigned)**.

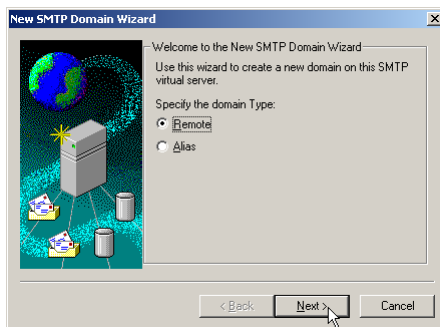


- Click on the **Advanced** button. Verify that the TCP Port is set to 25. Click **OK**.

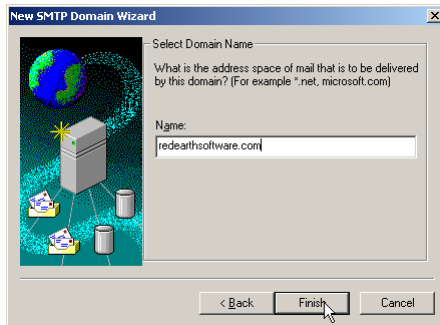


## Step 2. Forward mails from the SMTP service to Exchange 5.5

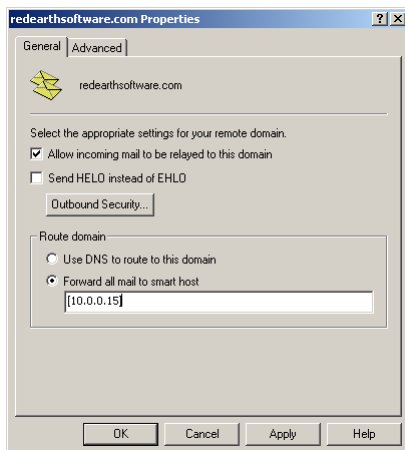
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



- Enter the domain name, for instance `reearthsoftware.com`. Click **Finish**.



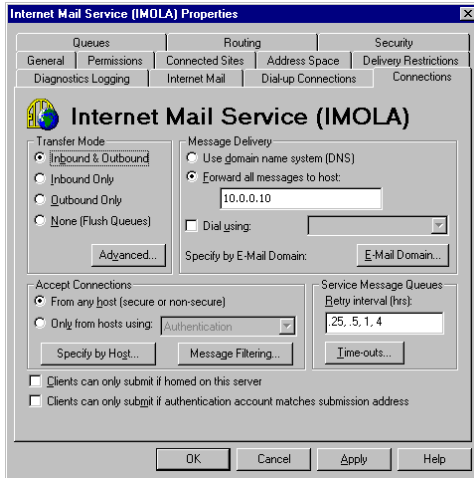
- Select the newly created domain. Right-click and choose **Properties > General Tab**.



- Tick **Allow incoming mail to be relayed to this domain**. In the 'Route domain' section, select **Forward all mail to smart host** and enter the internal IP address (can be the same as the external IP address) of the Exchange Server in between square brackets, e.g. [10.0.0.15] as per Figure 1. Click **OK**. If you use multiple email domains, repeat step 2 for each email domain.

### Step 3. Forward your mails from Exchange 5.5 to the SMTP service

- On the Exchange 5.5 machine, open **Exchange Administrator** and go to **Organization > Site > Configuration > Connections > Internet Mail Service > Properties**.
- In the **Connections** tab go to the 'Message Delivery' section and in the dialog box **Forward all messages to host** enter the IP address of the Policy Patrol machine (10.0.0.10 in Figure 1). Click **OK**.

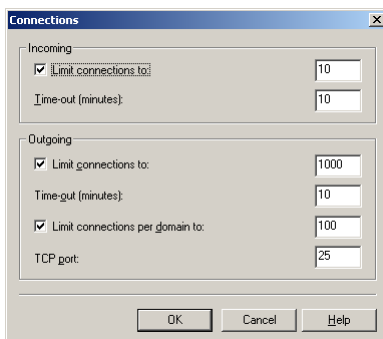


- A dialog will pop up, asking you to restart the Microsoft Exchange Internet Mail Service. Go to **Start > Settings > Control Panel > Services** (Windows NT) or **Start > Settings > Control Panel > Administrative Tools > Services** (Windows 2000/2003/XP). Select 'Microsoft Exchange Internet Mail Service' from the list, right-click and choose **Stop**. When the service has stopped, right-click and choose **Start**.

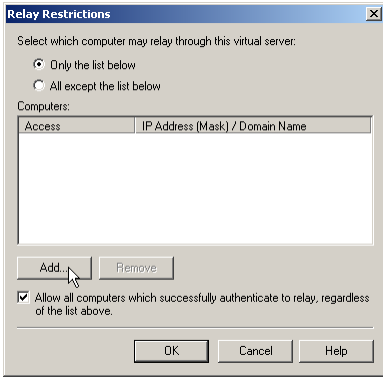
#### Step 4. Configure the SMTP service to send out mails to the Internet

##### If you have Windows 2000 or Windows XP:

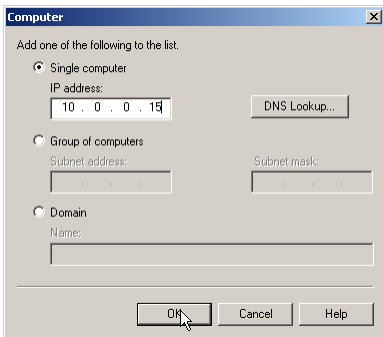
- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.
- Right-click **Default SMTP Virtual Server** and select **Properties**.
- In the **General** tab, click on the **Connection** button. Verify that in the 'Outgoing' section, the TCP port is set to 25. Click **OK**.



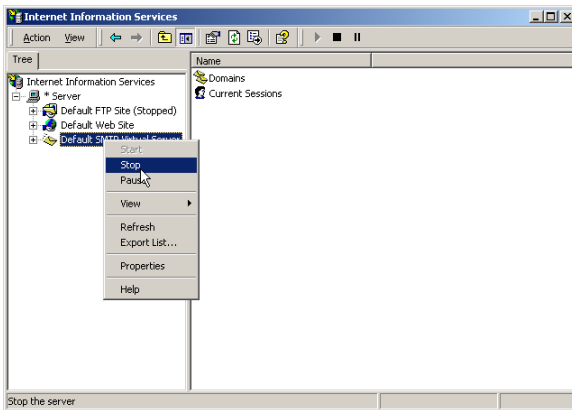
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Exchange Server machine in the **Single computer** dialog (in Figure 2 this is 10.0.0.15) and click **OK**. Note: By entering the IP address of the Exchange Server here, you are effectively blocking relaying for all other machines apart from the Exchange Server, therefore ensuring that your relay server cannot be used for spamming.



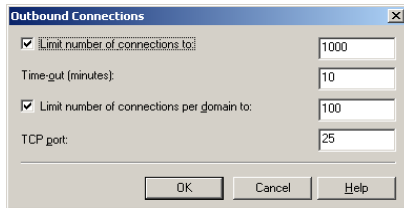
- Right-click **Default SMTP Virtual Server** and choose **Stop**. Then right-click again and choose **Start**.



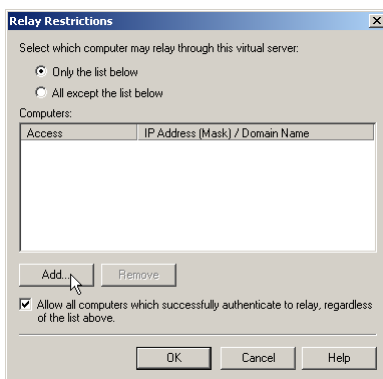
### If you have Windows 2003:

- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.

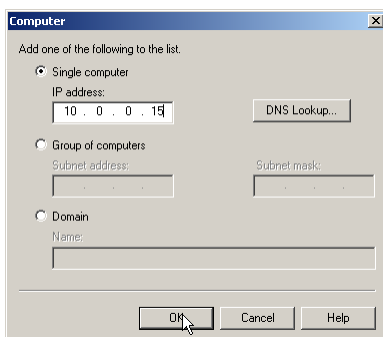
- Right-click **Default SMTP Virtual Server** and select **Properties**.
- In the **Delivery** tab, click on the **Outbound Connections** button. Verify that the TCP port is set to 25.



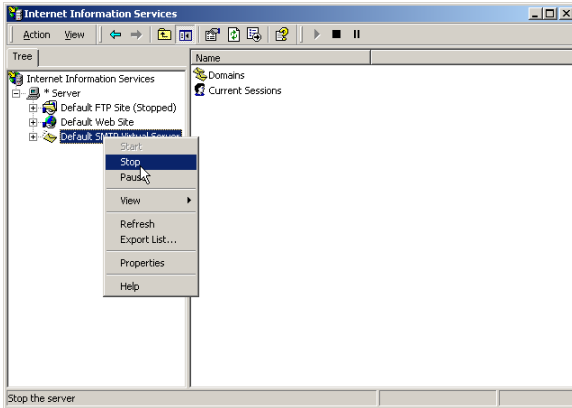
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Exchange Server machine in the **Single computer** dialog (in Figure 1 this is 10.0.0.15) and click **OK**. Note: By entering the IP address of the Exchange Server here, you are effectively blocking relaying for all other machines apart from the Exchange Server, therefore ensuring that your relay server cannot be used for spamming.



- Right-click **Default SMTP Virtual Server** and choose **Stop**. Then right-click again and choose **Start**.



You are now ready to start configuring rules in Policy Patrol to filter all your mails.

## Scenario 2: Policy Patrol processes only outbound mail

If you only require Policy Patrol to process outbound mails (for instance if you only want to add a disclaimer to outgoing messages), you just need to forward outbound mails to the Windows SMTP service on the Policy Patrol machine, as per Figure 2 below. Your inbound mails will still arrive directly at your Exchange 5.5 Server. To configure Policy Patrol to process your outbound mails, follow the next steps:

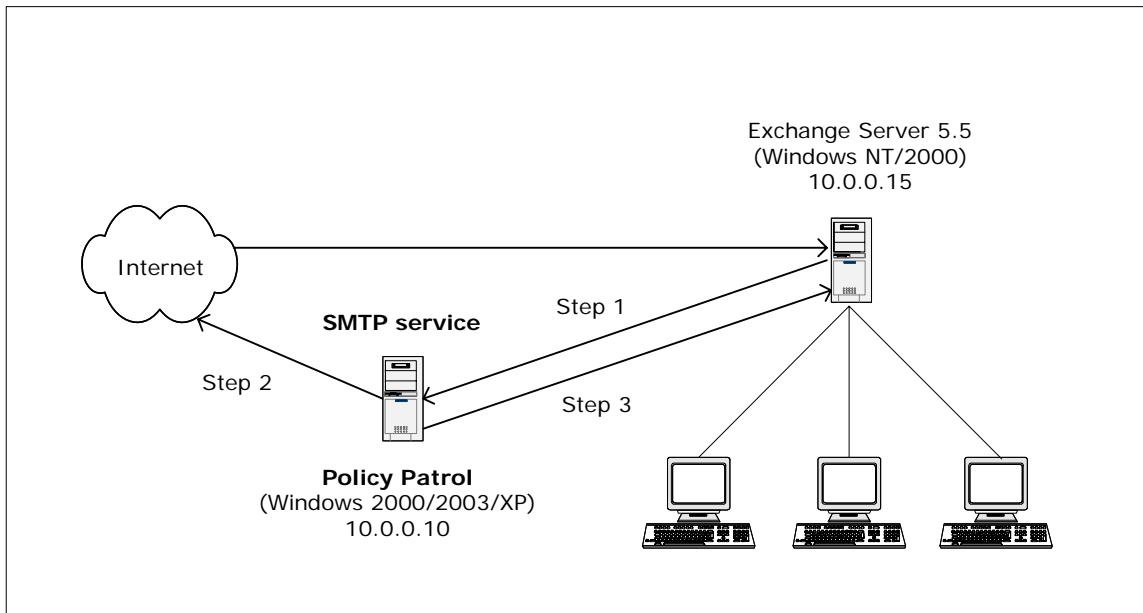
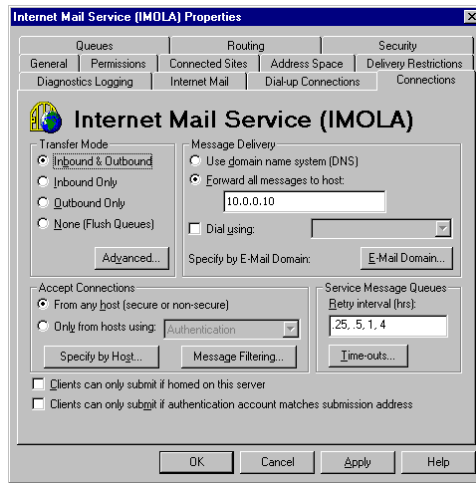


Figure 2 - Policy Patrol processes outbound mail from Exchange Server 5.5

### Step 1. Forward your mails from Exchange 5.5 to the SMTP service

- On the Exchange 5.5 machine, open **Exchange Administrator** and go to **Organization > Site > Configuration > Connections > Internet Mail Service > Properties**.

- In the **Connections** tab go to the 'Message Delivery' section and in the dialog box **Forward all messages to host** enter the IP address of the Policy Patrol machine (10.0.0.10 in Figure 2). Click **OK**.

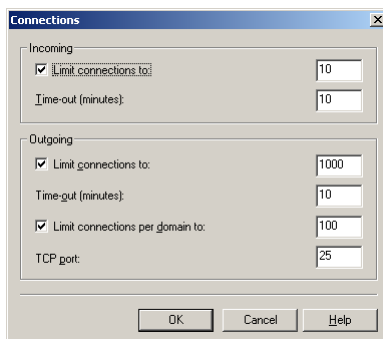


- A dialog will pop up, asking you to restart the Microsoft Exchange Internet Mail Service. Go to **Start > Settings > Control Panel > Services** (Windows NT) or **Start > Settings > Control Panel > Administrative Tools > Services** (Windows 2000/2003/XP). Select 'Microsoft Exchange Internet Mail Service' from the list, right-click and choose **Stop**. When the service has stopped, right-click and choose **Start**.

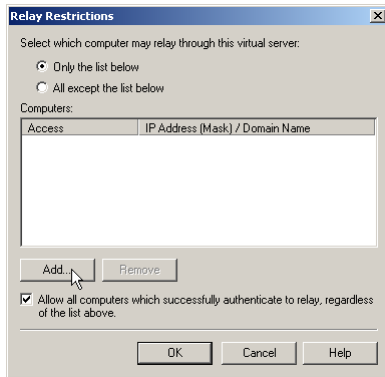
## Step 2. Configure the SMTP service to send out mails to the Internet

### If you have Windows 2000 or Windows XP:

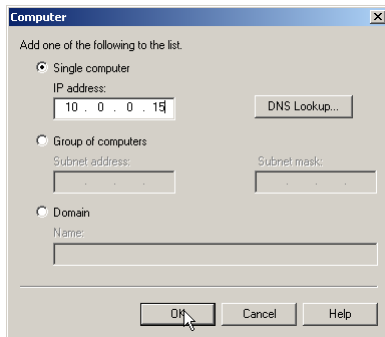
- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.
- Right-click **Default SMTP Virtual Server** and select **Properties**.
- In the **General** tab, click on the **Connection** button. Verify that in the 'Outgoing' section, the TCP port is set to 25. Click **OK**.



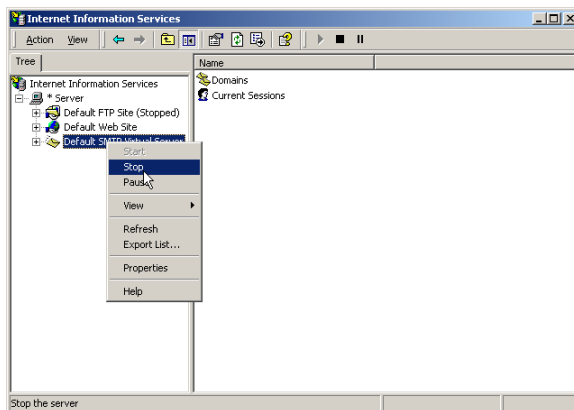
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Exchange Server machine in the **Single computer** dialog (in Figure 2 this is 10.0.0.15) and click **OK**. Note: By entering the IP address of the Exchange Server here, you are effectively blocking relaying for all other machines apart from the Exchange Server, therefore ensuring that your relay server cannot be used for spamming.



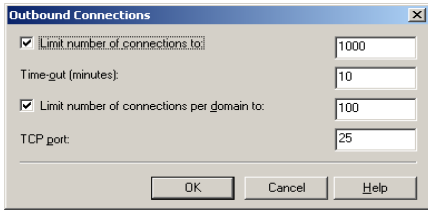
- Right-click **Default SMTP Virtual Server** and choose **Stop**. Then right-click again and choose **Start**.



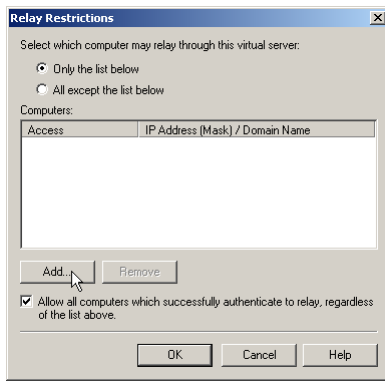
**If you have Windows 2003:**

- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.

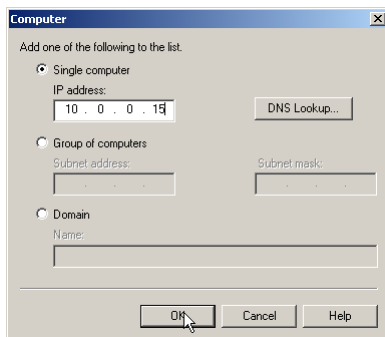
- Right-click **Default SMTP Virtual Server** and select **Properties**.
- In the **Delivery** tab, click on the **Outbound Connections** button. Verify that the **TCP Port** is set to 25. Click **OK**.



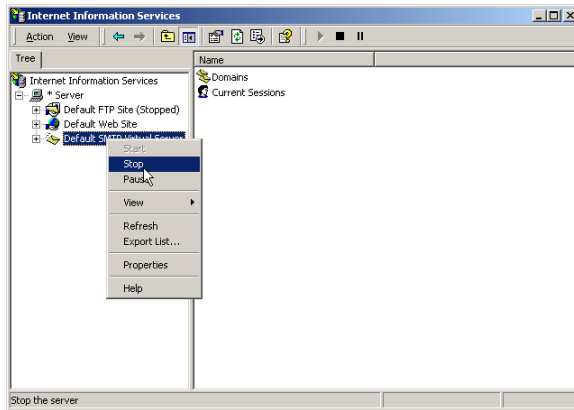
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Exchange Server machine in the **Single computer** dialog (in Figure 2 this is 10.0.0.15) and click **OK**. Note: By entering the IP address of the Exchange Server here, you are effectively blocking relaying for all other machines apart from the Exchange Server, therefore ensuring that your relay server cannot be used for spamming.



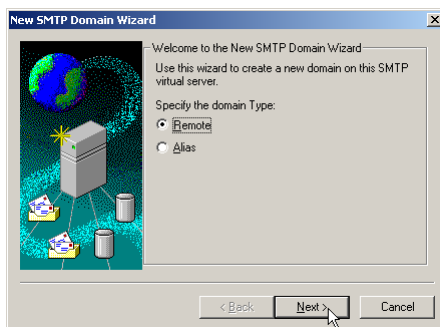
- Right-click **Default SMTP Virtual Server** and choose **Stop**. Then right-click again and choose **Start**.



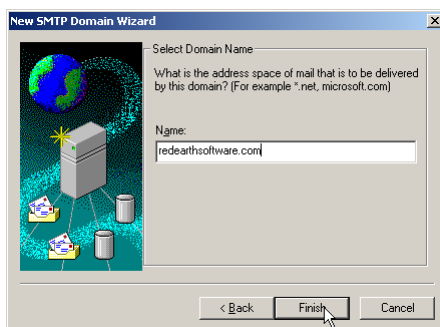
### Step 3. Forward mails (NDRs) from the SMTP service to Exchange 5.5

If the SMTP service cannot deliver a particular message, the Non-delivery messages must be routed back to the Exchange 5.5 Server. Therefore you must configure the SMTP service to forward messages to the Exchange 5.5 Server. In this setup, the only messages that will be forwarded are Non-delivery messages.

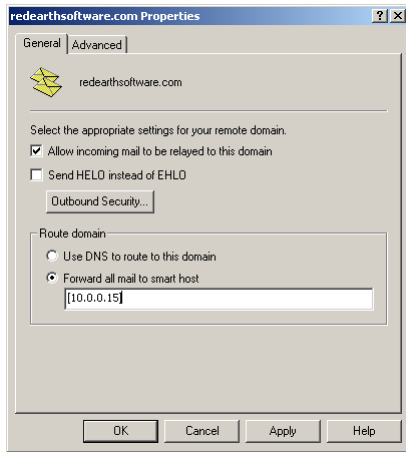
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



- Enter the domain name, for instance `redearthsoftware.com`. Click **Finish**.



- Select the newly created domain. Right-click and choose **Properties > General Tab**.



- Tick **Allow incoming mail to be relayed to this domain**. In the 'Route domain' section, select **Forward all mail to smart host** and enter the internal address (can be the same as the external IP address) of the Exchange Server in between square brackets, e.g. [10.0.0.15] as per Figure 2. Click **OK**. If you use multiple email domains, repeat step 3 for each email domain.
- You are now ready to start configuring rules in Policy Patrol to filter outbound mails.

### Scenario 3: Policy Patrol processes only inbound mail

If you only want Policy Patrol to process inbound mails (for instance to stop spam), you just need to forward incoming mails to the Windows SMTP service on the Policy Patrol machine, as per Figure 3 below. Outgoing mails will continue to be sent out by Exchange 5.5. To configure Policy Patrol to process your inbound mails, follow the next steps:

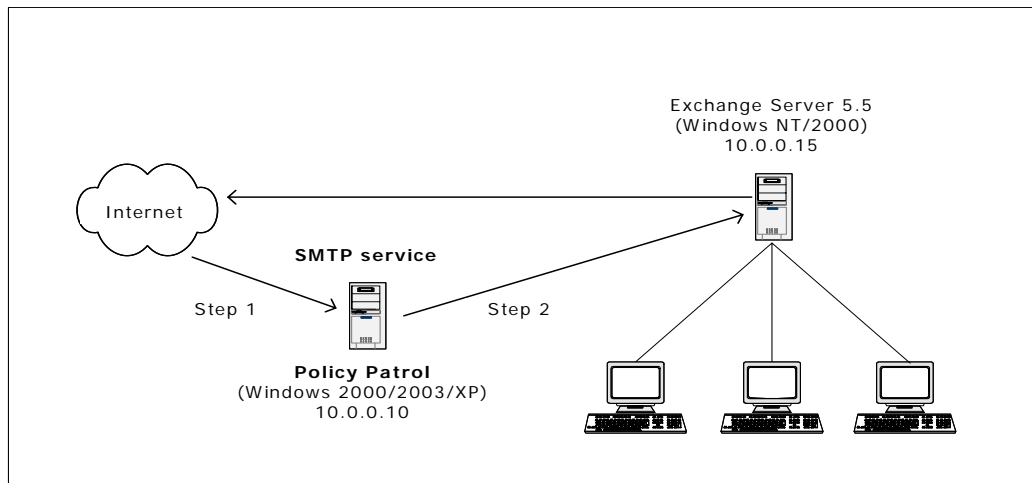


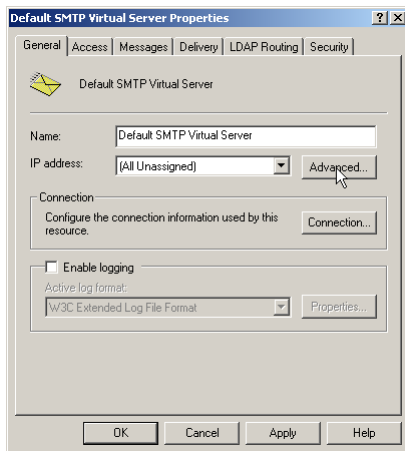
Figure 3 - Policy Patrol processes inbound mail for Exchange Server 5.5

#### Step 1. Direct incoming mail to the SMTP service on the Policy Patrol machine

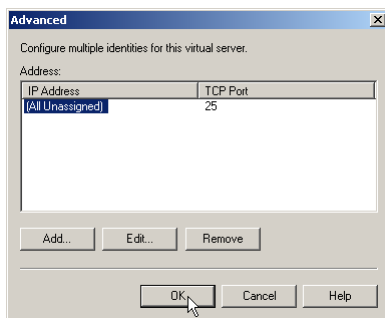
Direct your incoming mail to the Windows SMTP service on the Policy Patrol machine (the external DNS servers for your domain must have an mx (mail exchanger) record pointing

to the Policy Patrol machine). Furthermore, check the following settings in the Default SMTP Virtual Server:

- On the Policy Patrol machine, go to **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.
- Right-click **Default SMTP Virtual Server**, and click **Properties**.
- In the **General** Tab, verify that your IP address is listed as **(All Unassigned)**.

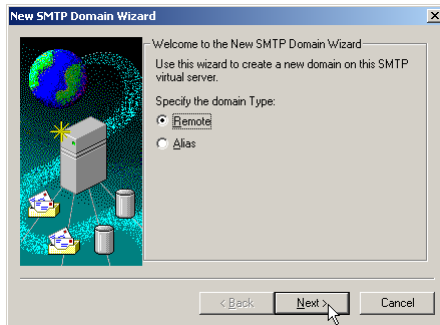


- Click on the **Advanced** button. Verify that the TCP Port is set to 25. Click **OK**.

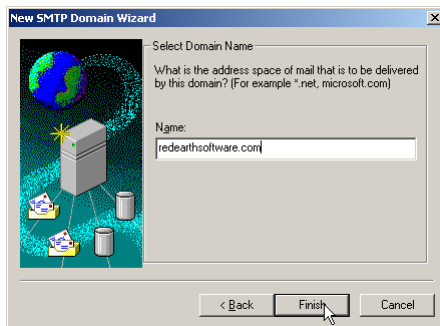


## Step 2. Forward mails from the SMTP service to Exchange 5.5

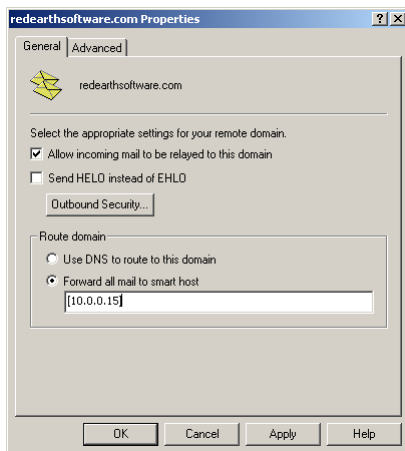
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



- Enter the domain name, for instance `redearthsoftware.com`. Click **Finish**.



- Select the newly created domain. Right-click and choose **Properties > General Tab**.



- Tick **Allow incoming mail to be relayed to this domain**. In the 'Route domain' section, select **Forward all mail to smart host** and enter the internal IP address (can be the same as the external IP address) of the Exchange Server in between square brackets, e.g. `[10.0.0.15]` as per Figure 3. Click **OK**. If you use multiple email domains, repeat step 2 for each email domain.

You are now ready to start configuring rules in Policy Patrol to filter inbound mails.

## More information

---

- ⇒ For more information on how to configure Policy Patrol, please consult the program help or download the product manual from:  
<http://www.policypatrol.com/download.htm>.
- ⇒ For more information on relaying your mail through the Windows SMTP service, consult the following Microsoft Knowledge Base article 'XCON: How to set up Windows 2000 as an SMTP Relay Server or Smart Host' at:  
<http://support.microsoft.com/default.aspx?scid=kb;en-us;293800>.
- ⇒ If you still have questions after reading this document, please consult our online knowledge base at <http://www.redearthsoftware.com/kb.asp>, or send an email to [support@redearthsoftware.com](mailto:support@redearthsoftware.com).

## Contacting Red Earth Software

---

### Red Earth Software, Inc.

595 Millich Drive, Suite 210  
Campbell, CA 95008  
United States  
Toll-free: 1-800-921-8215  
Phone: (408) 370 9527  
Fax: (408) 608 1958  
Sales: [sales@redearthsoftware.com](mailto:sales@redearthsoftware.com)  
Support: [support@redearthsoftware.com](mailto:support@redearthsoftware.com)

### Red Earth Software (UK) Ltd

20 Market Place  
Kingston-upon-Thames  
Surrey KT1 1JP  
United Kingdom  
Tel: +44-(0)20-8328 9830  
Fax: +44-(0)20-8711 5771  
Sales: [sales@redearthsoftware.co.uk](mailto:sales@redearthsoftware.co.uk)  
Support: [support@redearthsoftware.co.uk](mailto:support@redearthsoftware.co.uk)

### Red Earth Software Ltd

Sonic House, Suite 301  
43 Artemidos Avenue  
6025 Larnaca  
Cyprus  
Tel: +357-24 828515  
Fax: +357-24-828516  
Sales: [sales@redearthsoftware.com](mailto:sales@redearthsoftware.com)  
Support: [support@redearthsoftware.com](mailto:support@redearthsoftware.com)

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2009 by Red Earth Software.