Installing Policy Patrol with Lotus Domino

If you have Lotus Domino R5/6/7/8/9 Mail Server, you must install Policy Patrol on a separate Windows 2003/2008/2012 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 Lotus Domino.

To use Policy Patrol with Lotus Domino, follow the steps described below.

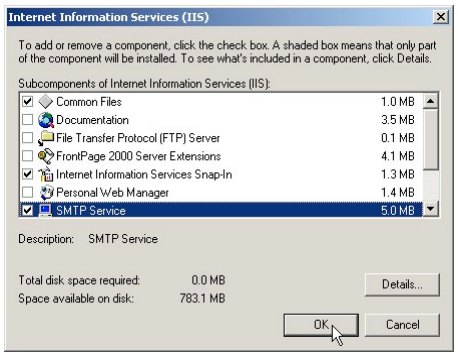
Step 1. Preparing for installation

System requirements

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

☑ Windows 2003, 2008/2008 R2, 2012/2012 R2 Server.

☑ Windows SMTP service (part of Internet Information Services). To install the SMTP service, 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.



☑ 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.

Step 2. Install Policy Patrol

To install Policy Patrol Email:

1. Double-click on **policypatrol.exe** (32-bit) or **policypatrol64.exe** (64-bit). 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**.

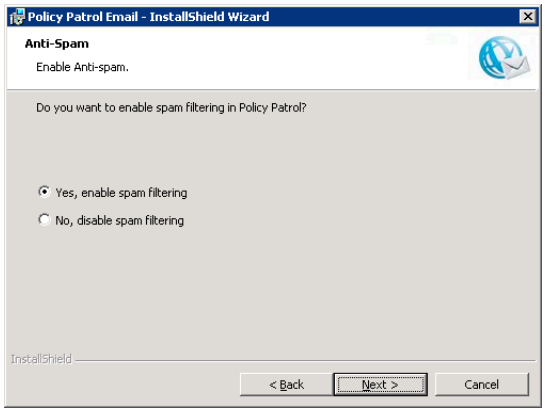
6. **If you did not enter a serial number**: A dialog will pop up asking you to select the evaluation license to be installed. Select the relevant license and click **Next**.

   Note: If you are evaluating Policy Patrol and wish to try out a different Policy Patrol edition after the installation, you can go to **Policy Patrol Administration** > **<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.

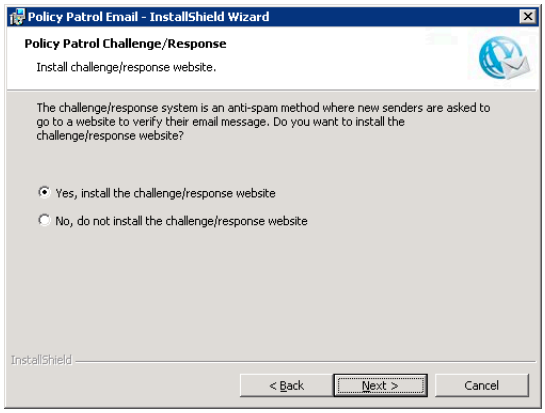
7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email (32-bit version) or C:\Program Files (x86)\Red Earth Software\Policy Patrol Email (64-bit version). If you wish to change the location, 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**.

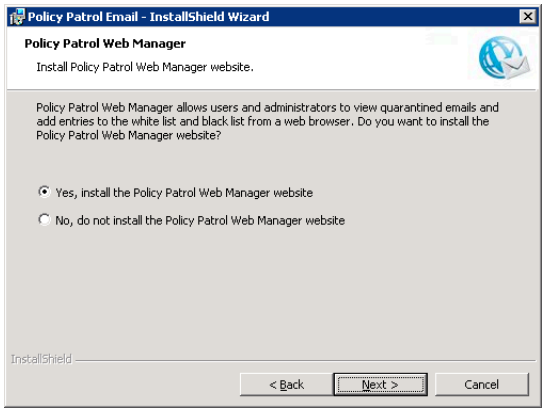
9. **Only for Policy Patrol Mail Security:** Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected 'No, disable spam filtering', continue to step 12.



10. **Only for Policy Patrol Mail Security 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**.



11. **Only for Policy Patrol Mail Security**: 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).



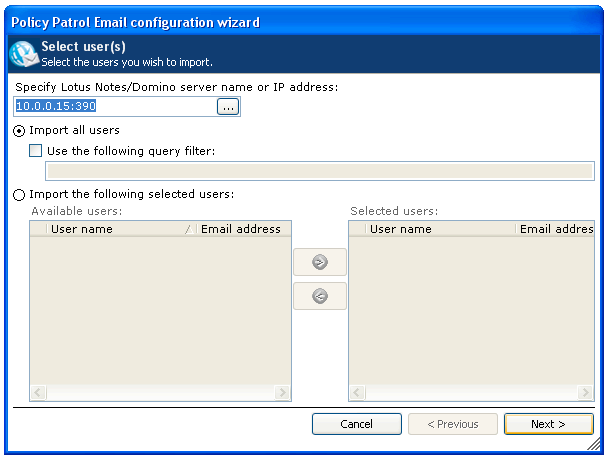
12. Click **Install** to start installing.

13. When the installation wizard has finished copying the files, click **Finish**.

14. The Policy Patrol configuration wizard will start up. Click **Next** in the Welcome screen.

15. Specify the location from where you would like to import your users (Active Directory, Lotus Domino or Manual input) and click **Next**. Note: the 64-bit version only includes the Active Directory and Manual Input options.

16. **If you selected Lotus Domino:** Enter your Lotus Domino server name or IP address, or click on the browse button (**...**) to browse to the computer. 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`.



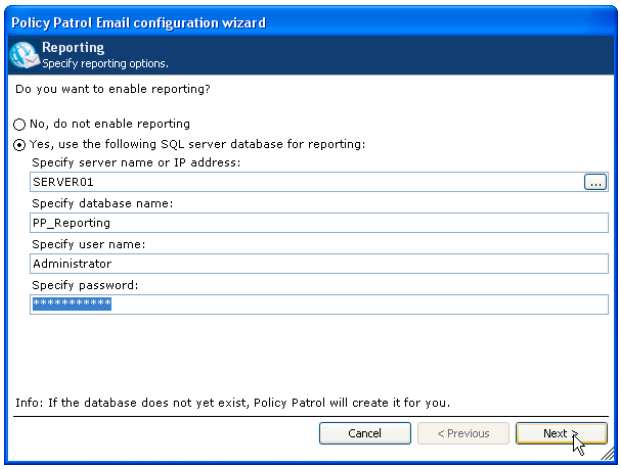
To license all users in Lotus Domino, select **Import all users**. If you only wish to license certain users, select **Import the following selected users**. Select the users you wish to license in the left pane and press ➔. The selected users will now appear in the right pane. To remove users, press the ➔ button. When you are ready, click **Next**.

If you selected Active Directory: Specify the server or domain controller 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 detailed information on the different options in this dialog, please consult the product manual. Click **Next**.

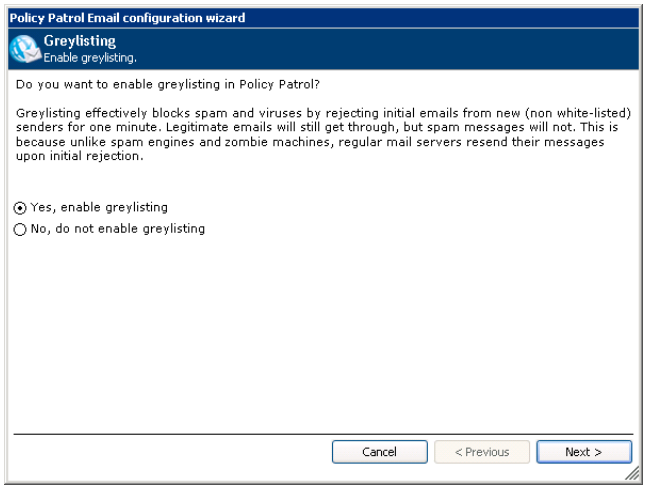
17. **Only for Policy Patrol Mail Security**: Select whether you wish to enable Mail Backup. If you enable Mail Backup you must enter the SQL Server Database settings; enter the IP address or name of the SQL server or SQL server instance and specify the database name. Enter the user name and password 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.

18. **Only for Policy Patrol Mail Security:** 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.



19. **Only for Policy Patrol Mail Security 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**.



20. 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 mail

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:

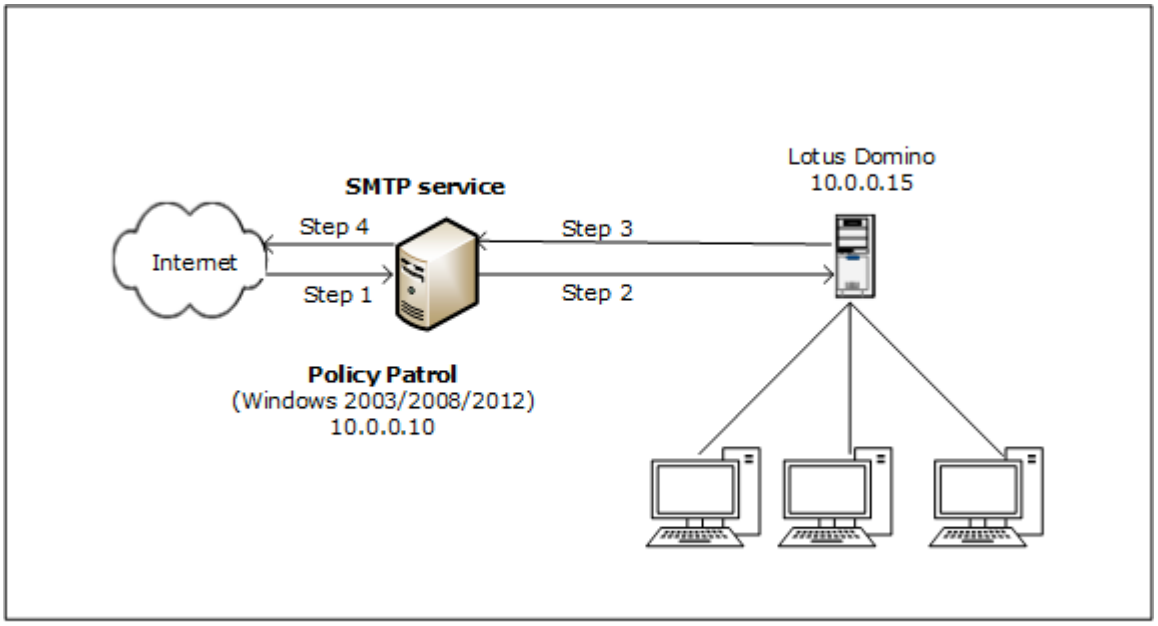
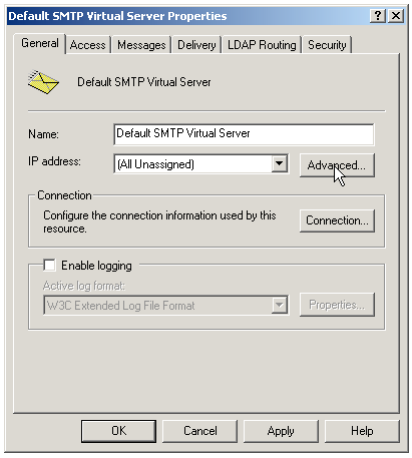


Figure 1 - Policy Patrol processes inbound and outbound mail from Lotus Domino

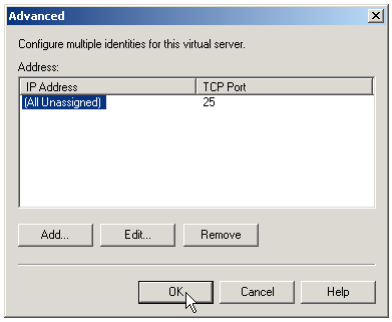
Step 1. Direct incoming mail to the SMTP service on the Policy Patrol machine

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)**.

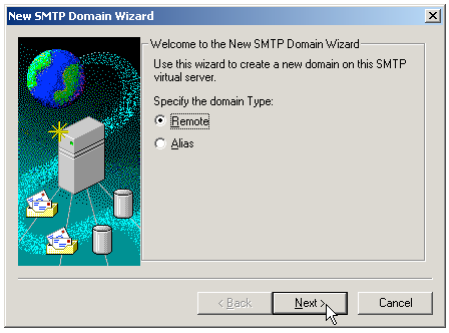


- Click on the **Advanced** button. Verify that the TCP Port is set to 25. Click **OK**.

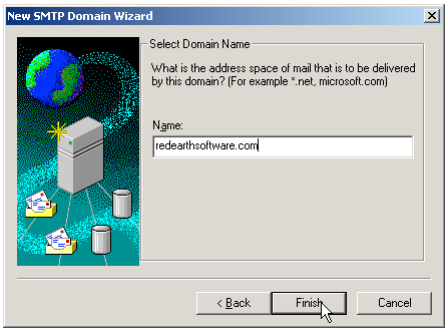


Step 2. Forward mails from the SMTP service to Lotus Domino

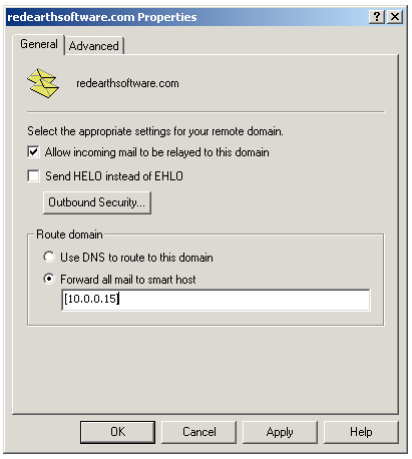
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



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



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

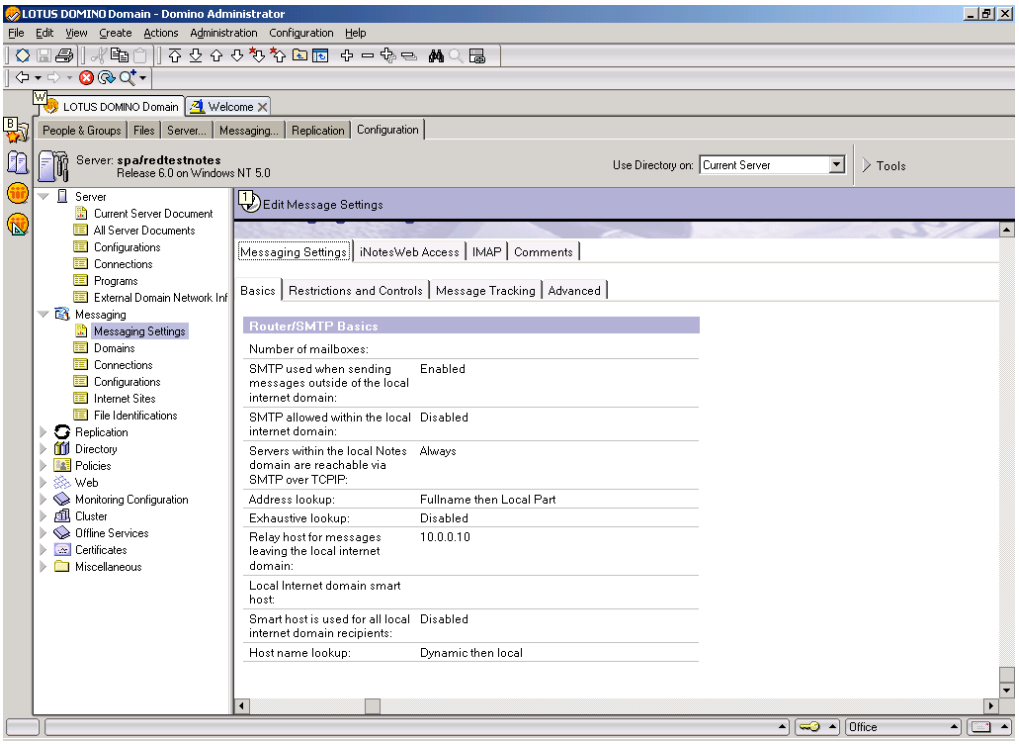


- Tick **Allow incoming mail to be relayed to this domain**. In the 'Route domain' section, select **Forward all mail to smart host** and enter the internal IP address (can be the same as the external IP address) of the Lotus Domino server in between square brackets, e.g. `[10.0.0.15]` as per Figure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

Step 3. Forward your mails from Lotus Domino to the SMTP service

- On the Lotus Domino machine, open the **Domino Administration** and select **Administration** > **Configuration** from the top menu.

- Expand the **Messaging** node and select **Messaging Settings**. Click on **Edit Message Settings** and go to the **Basics** tab.



- Select **Relay host for messages leaving the local internet domain** under the Router/SMTP basics section. Enter the IP address of the Policy Patrol machine, e.g. `10.0.0.10` as per Figure 1. Save the changes by selecting the **Save and Close** button.

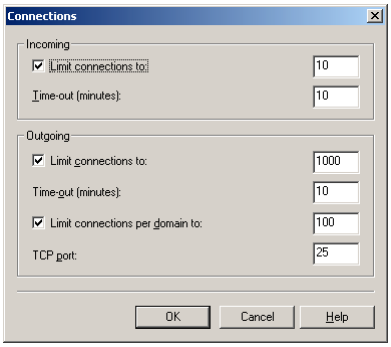
- Now you must restart the Lotus Domino SMTP service as follows: Enter `Tell SMTP quit` from the Domino Server console to stop the Domino SMTP Service. Then enter `load SMTP` to start the Domino SMTP Service again.

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

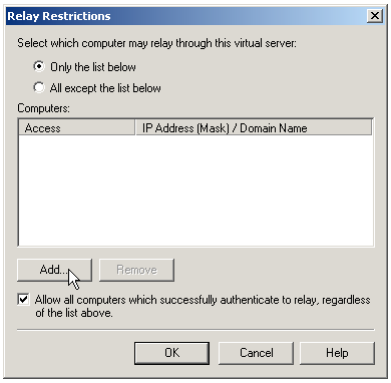
- On the Policy Patrol machine, go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Internet Services Manager**.

- Right-click **Default SMTP Virtual Server** and select **Properties**.

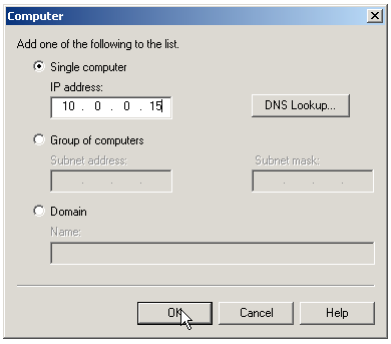
- In the **General** tab, click on the **Connection** button. Verify that in the 'Outgoing' section, the TCP port is set to 25. Click **OK**.



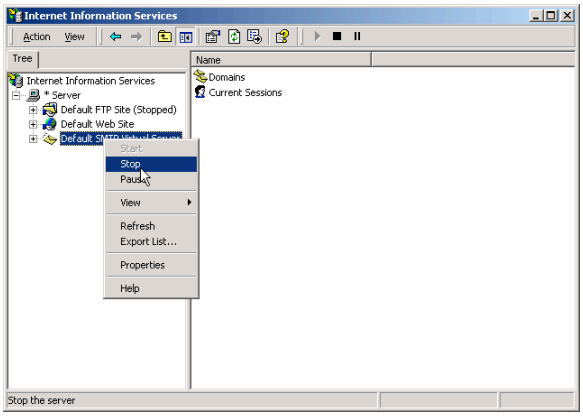
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Lotus Domino server 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 Lotus Domino server here, you are effectively blocking relaying for all other machines apart from the Lotus Domino 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 Lotus Domino server. To configure Policy Patrol to process your outbound mails, follow the next steps:

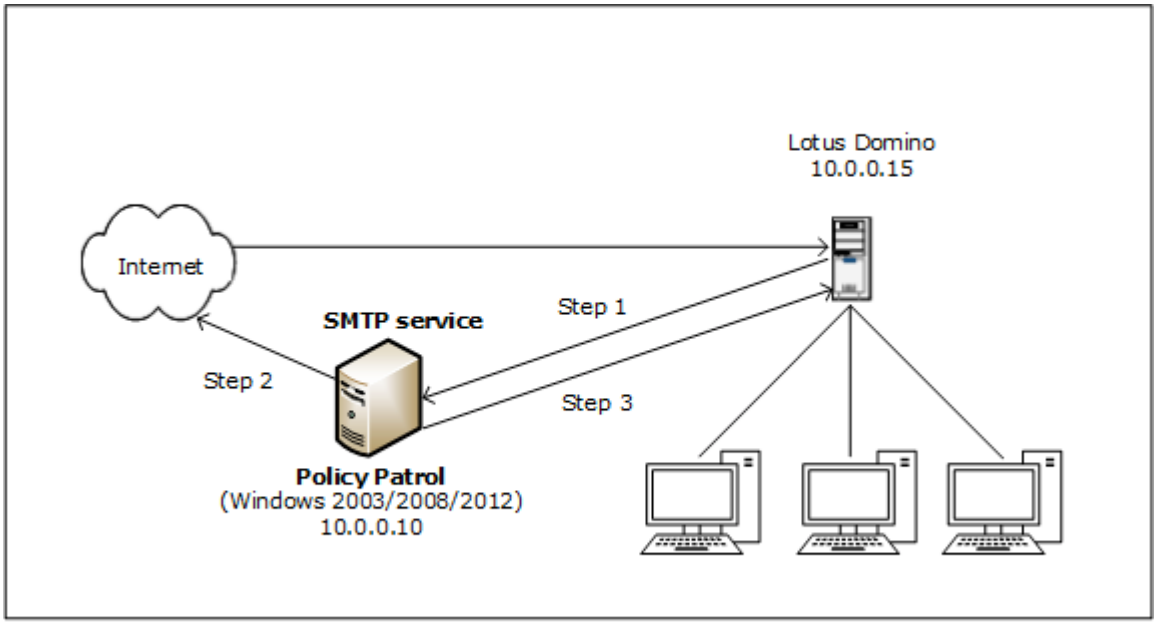
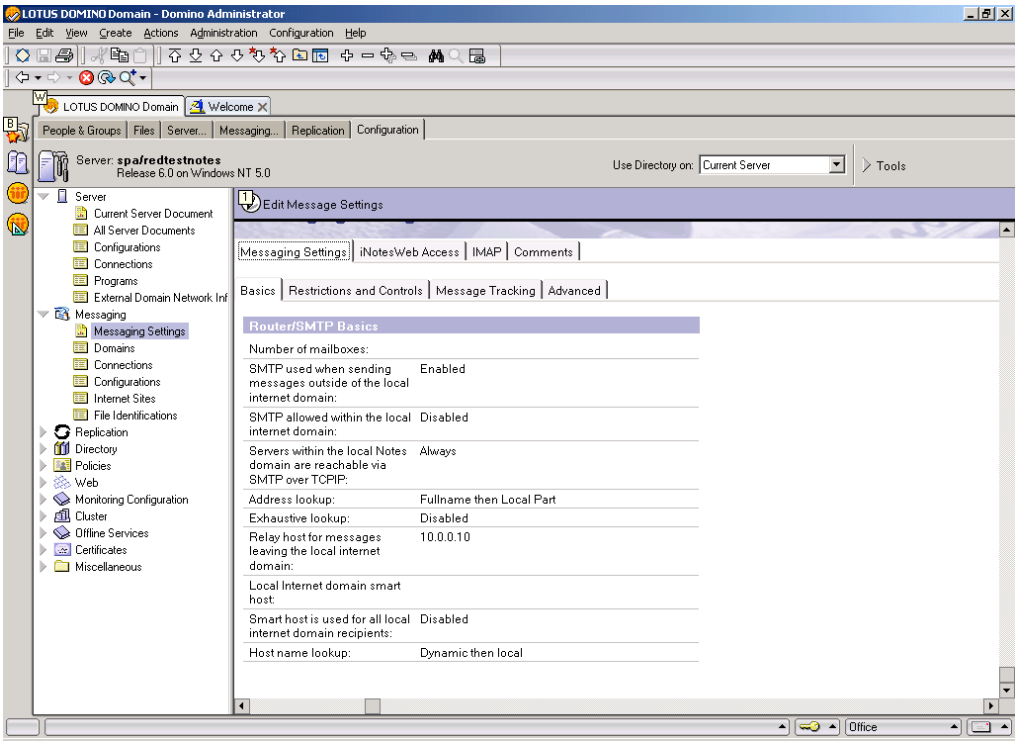


Figure 2 - Policy Patrol processes outbound mail from Lotus Domino

Step 1. Forward your mails from Lotus Domino to the SMTP service

- On the Lotus Domino machine, open the **Domino Administration** and select **Administration** > **Configuration** from the top menu.
- Expand the **Messaging** node and select **Messaging Settings**. Click on **Edit Message Settings** and go to the **Basics** tab.



- Select **Relay host for messages leaving the local internet domain** under the Router/SMTP basics section. Enter the IP address of the Policy Patrol machine, e.g. `10.0.0.10` as per Figure 2. Save the changes by selecting the **Save and Close** button.

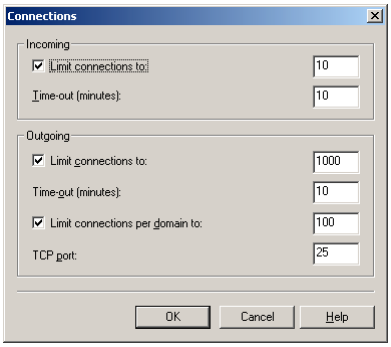
- Now you must restart the Lotus Domino SMTP service as follows: Enter `Tell SMTP quit` from the Domino Server console to stop the Domino SMTP Service. Then enter `load SMTP` to start the Domino SMTP Service again.

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

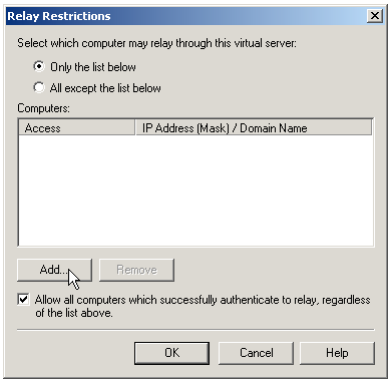
- On the Policy Patrol machine, go to **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Internet Services Manager**.

- Right-click **Default SMTP Virtual Server** and select **Properties**.

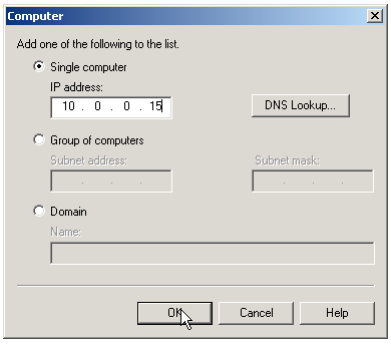
- In the **General** tab, click on the **Connection** button. Verify that in the 'Outgoing' section, the TCP port is set to 25. Click **OK**.



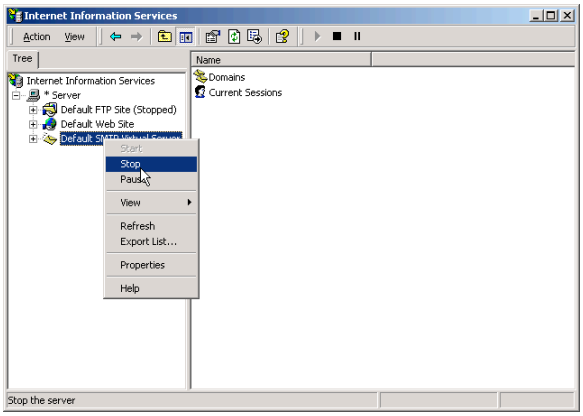
- Go to the **Access** tab and click on the **Relay** button. Select the option **Only the list below** and click on **Add**.



- Enter the internal IP address (can be the same as the external IP address) of the Lotus Domino server 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 Lotus Domino server here, you are effectively blocking relaying for all other machines apart from the Lotus Domino server, therefore ensuring that your relay server cannot be used for spamming.



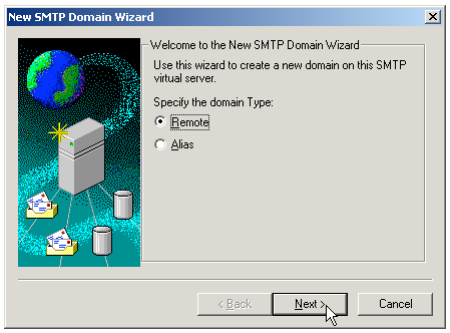
- Right-click **Default SMTP Virtual Server** and choose **Stop**. Then right-click again and choose **Start**.



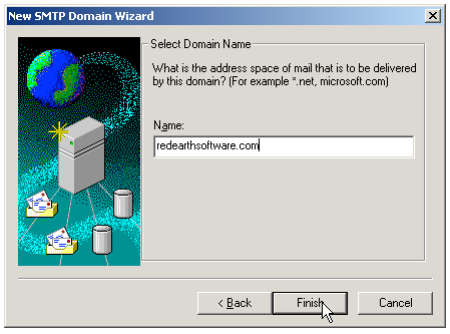
Step 3. Forward mails (NDRs) from the SMTP service to Lotus Domino

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

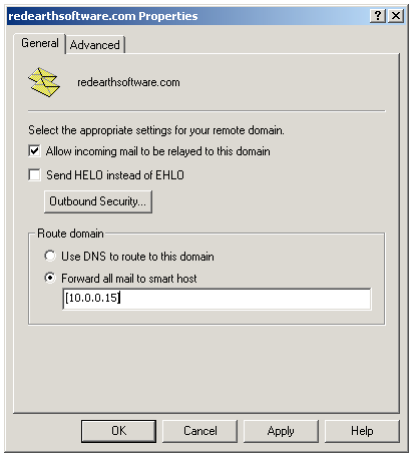
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



- 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 Lotus Domino 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 Lotus Domino. To configure Policy Patrol to process your inbound mails, follow the next steps:

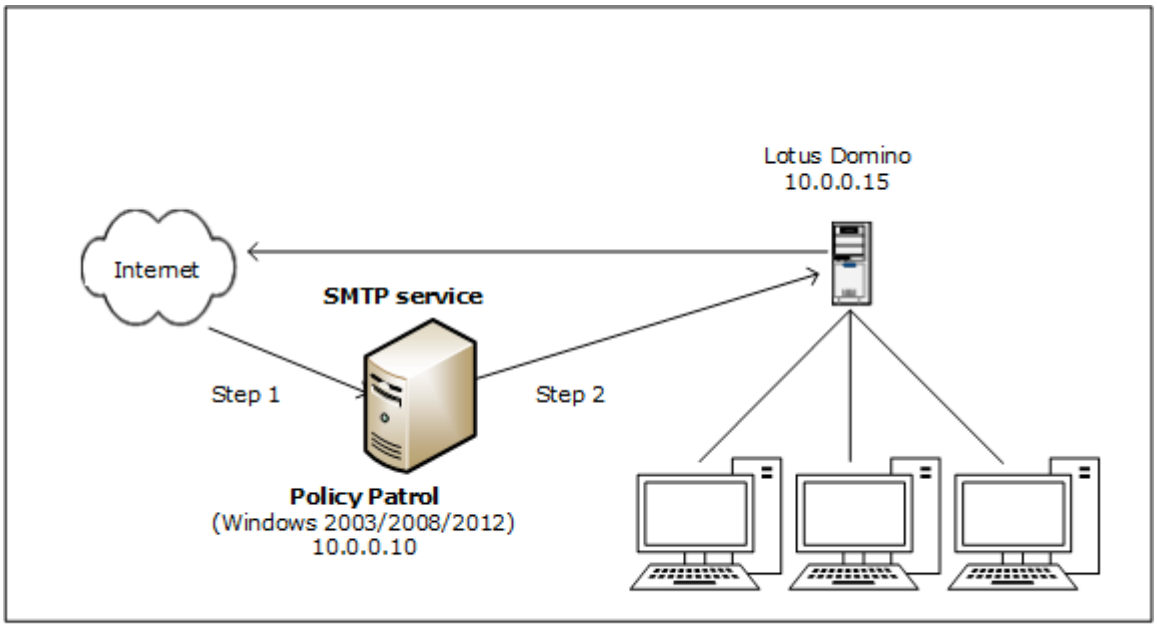
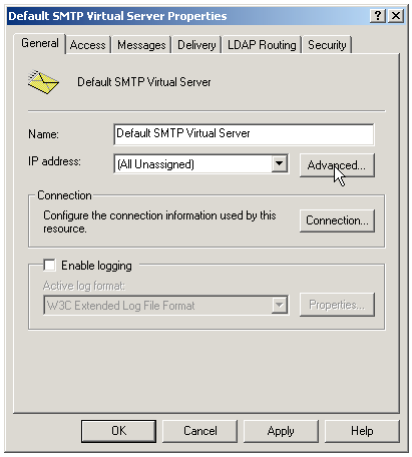


Figure 3 - Policy Patrol processes inbound mail for Lotus Domino

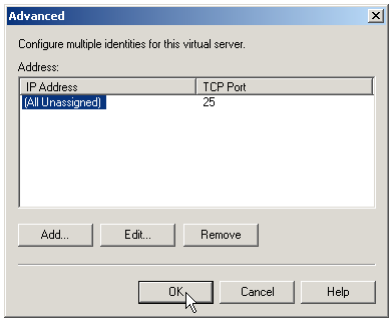
Step 1. Direct incoming mail to the SMTP service on the Policy Patrol machine

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)**.

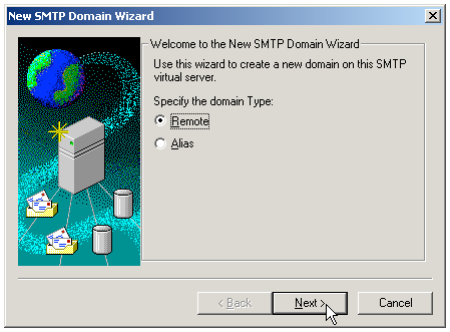


- Click on the **Advanced** button. Verify that the TCP Port is set to 25. Click **OK**.

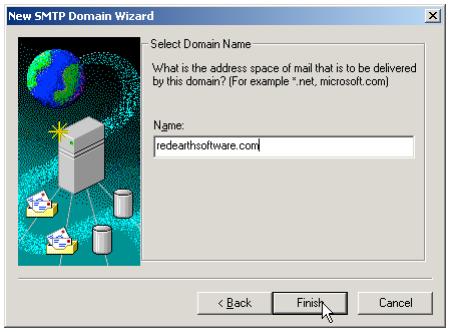


Step 2. Forward mails from the SMTP service to Lotus Domino

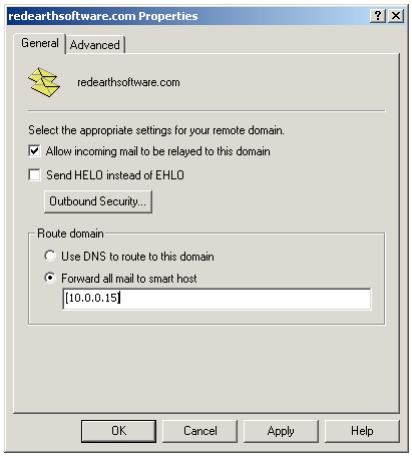
- In the Internet Services Manager, go to **Default SMTP Virtual Server > Domains**.
- Right-click **Domains** and select **New > Domain**.
- The New SMTP Domain Wizard will start up. Select **Remote** and click **Next**.



- 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 Lotus Domino 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/documentation.

⇒ 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 2003 as an SMTP Relay Server or Smart Host' at: http://technet.microsoft.com/en-us/library/aa998368(v=exchg.65).aspx.

⇒ If you still have questions after reading this document, please consult our online knowledge base at http://support.redearthsoftware.com, or send an email to support@redearthsoftware.com.

Contacting Red Earth Software

Red Earth Software, Inc.
4845 Pearl East Circle, Ste 101
Boulder, CO 80301
United States
Toll-free: 1-800-921-8215
Phone: (720) 377-3728
Fax: (720) 554-7950
Sales: sales@redearthsoftware.com
Support: 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
Support: support@redearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2014 by Red Earth Software.