

Installing Policy Patrol in a cluster

Policy Patrol can be installed on Active/Passive clusters. To do this, follow the instructions below. Note that Policy Patrol cannot be installed on Active/Active clusters. An additional server license must be purchased for the clustered node (http://www.policypatrol.com/pricing.htm#additional_server).

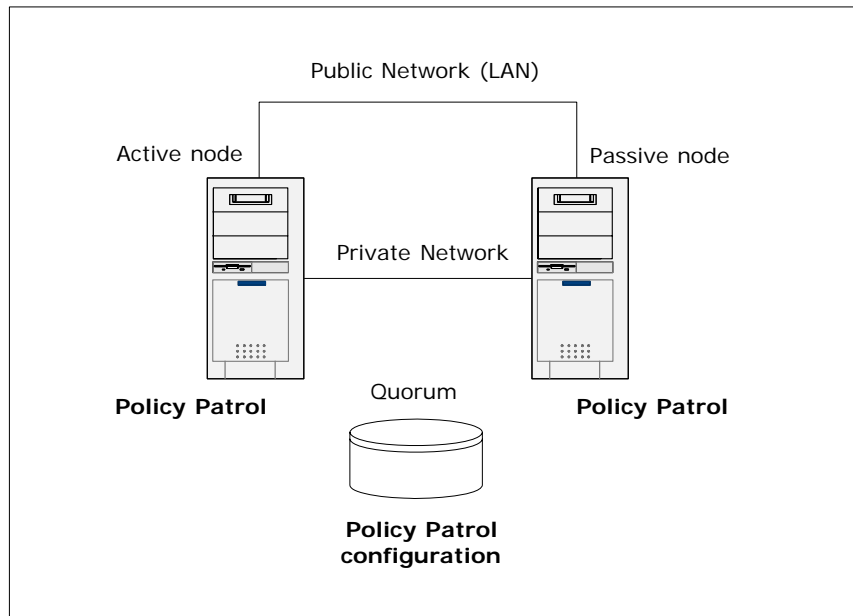


Figure 1. Policy Patrol installed on an Active/Passive cluster

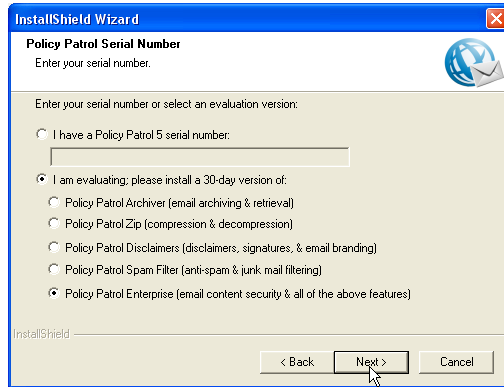
Step 1. Install Policy Patrol on the Active node

Note: If you are upgrading from Policy Patrol v 4, please consult the paragraph 'Upgrading your cluster installation from version 4'.

Install Policy Patrol on the Active node by following the next steps:

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 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 **Yes** to accept the agreement

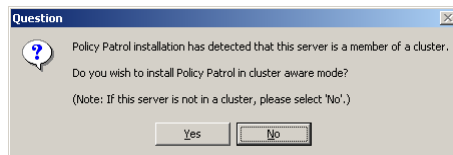
4. Select the installation type. If you select **Complete**, the complete program will be installed. If you only wish to install the Administration console (for remote administration), select **Administration console only**.
5. Enter your Policy Patrol serial number. If you are evaluating Policy Patrol, select one of the 30-day evaluation versions. Click **Next**.



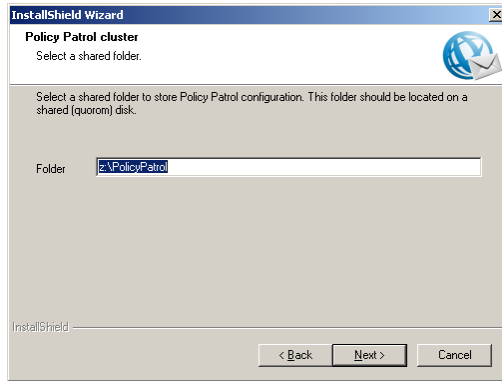
Note: If you are evaluating Policy Patrol and later wish to try out a different Policy Patrol edition you can go to **<server name> > Security > Licenses**, select the license and click **Remove** and **Close**. Policy Patrol will disconnect from the installation. When you connect again, Policy Patrol will allow you to select a new evaluation license type.

If you entered a Policy Patrol serial number, a message will pop up confirming that the serial number was validated and that the respective Policy Patrol edition will be installed.

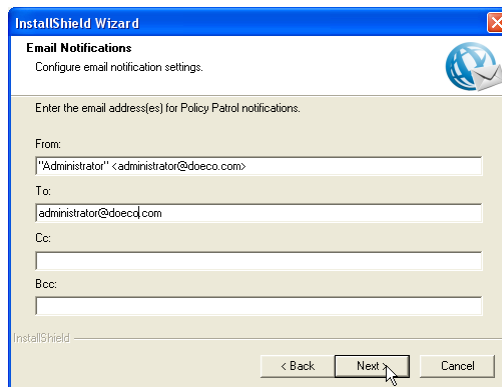
6. Enter your user name and company name. Select whether you wish to make the program available to anyone or only yourself. Click **Next**.
7. Select the destination folder for the Policy Patrol installation. By default the program will be installed in C:\Program Files\Red Earth Software\Policy Patrol Email. If you wish to change the location, click **Browse** and select another folder. When you are ready, click **Next**.
8. A dialog will now pop up saying that the Policy Patrol installation has detected that this server is a member of a cluster. Click **Yes** to install Policy Patrol in cluster aware mode.



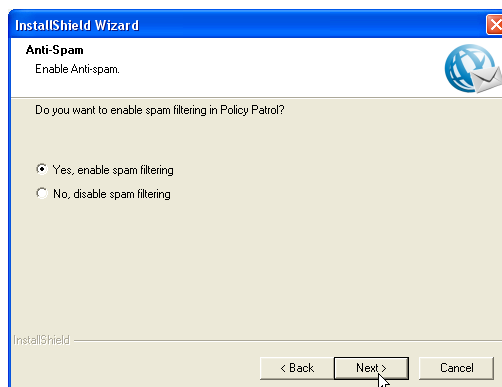
9. Enter the path to the shared folder (quorum) where Policy Patrol should store the configuration files and click **Next**. Note: If you are upgrading from Policy Patrol version 4 this path will automatically be set to the path used in the existing installation.



10. 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**.

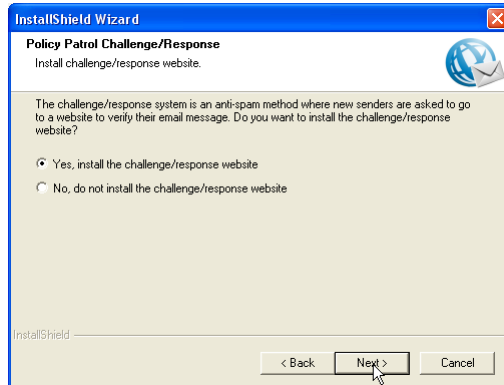


11. **Only for Policy Patrol Enterprise:** Select whether you wish to install the Policy Patrol Kaspersky Anti-Virus engine. Click **Next**.
12. **Only for Policy Patrol Enterprise:** Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected 'No, disable spam filtering', continue to step 16.



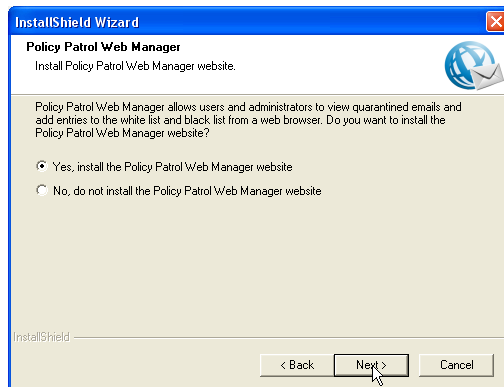
13. **Only for Policy Patrol Spam Filter or Enterprise with enabled anti-spam:**

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**.

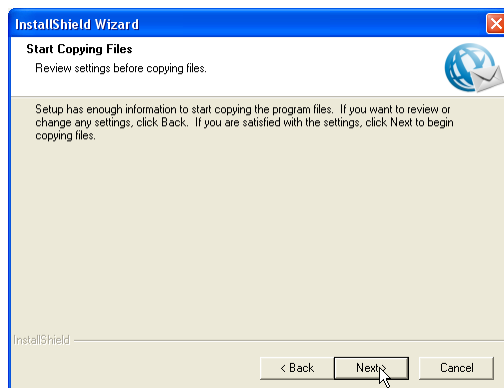


14. **Only for Policy Patrol Spam Filter or Enterprise with enabled anti-spam:**

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.



15. Click **Next** to start copying files.



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

Step 2. Install Policy Patrol on the other node(s)

Install Policy Patrol on the other node(s):

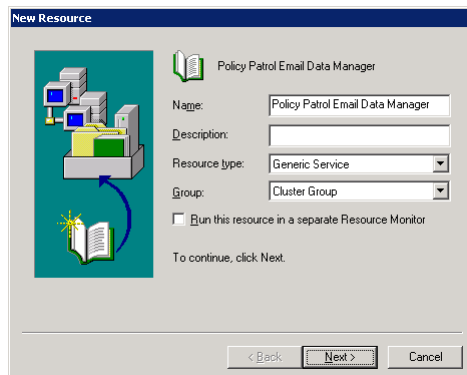
1. Fail over to the Passive node so that it becomes Active.
2. Install Policy Patrol according to the instructions in step 1.
3. Make sure that you specify the same shared configuration path as you did when installing on the first node (see point 9 above).

Step 3: Create the Exchange cluster resources

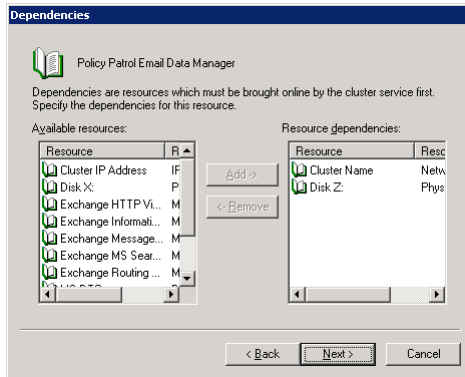
Follow the next steps on the Active node:

Create the Policy Patrol Email Data Manager cluster resource:

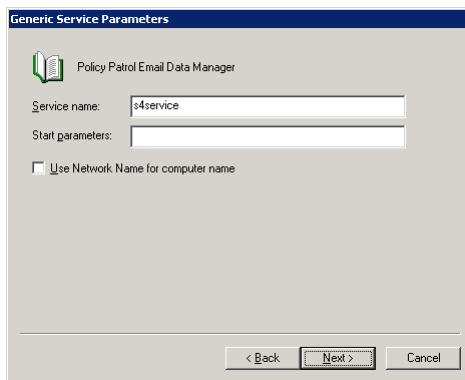
1. Go to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to **Groups**. Right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
2. Enter 'Policy Patrol Email Data Manager' as the name (please use the exact same name). Select **Generic Service** as the resource type. Click **Next**.



3. In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
4. In 'Available resources', select the quorum or shared drive where the Policy Patrol configuration is stored and the cluster network name. Click **Add** and **Next**.



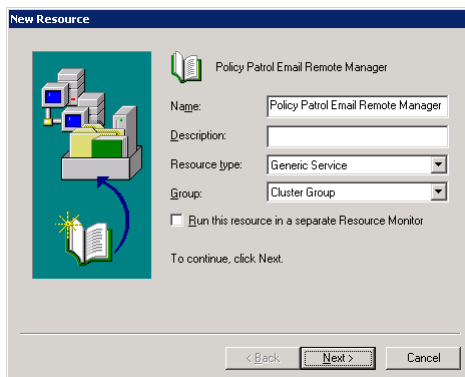
5. Enter `s4service` as the service name and do not enter any start parameters. Click **Next**.



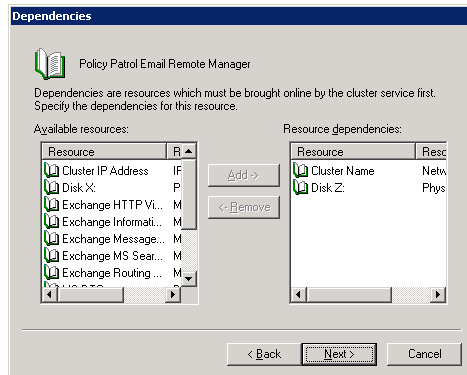
6. Do not add any registry keys and click **Finish** to create the Policy Patrol Email Data Manager cluster resource.

Create the Policy Patrol Email Remote Manager cluster resource:

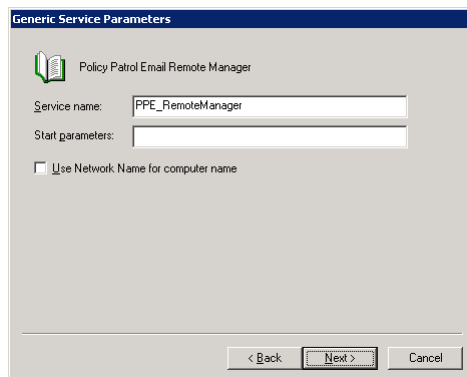
1. Go to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to **Groups**. Right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
2. Enter 'Policy Patrol Email Remote Manager' as the name (please use the exact same name). Select **Generic Service** as the resource type. Click **Next**.



3. In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
4. In 'Available resources', select the quorum or shared drive where the Policy Patrol configuration is stored, and the cluster network name. Click **Add** and **Next**.



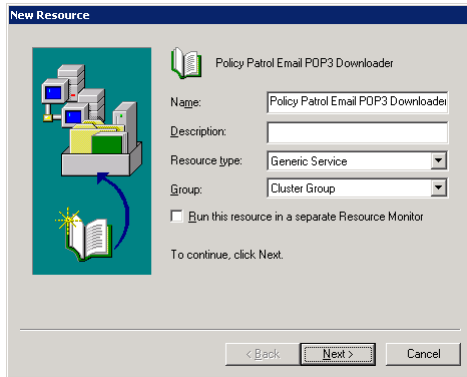
5. Enter `PPE_RemoteManager` as the service name and do not enter any start parameters. Click **Next**.



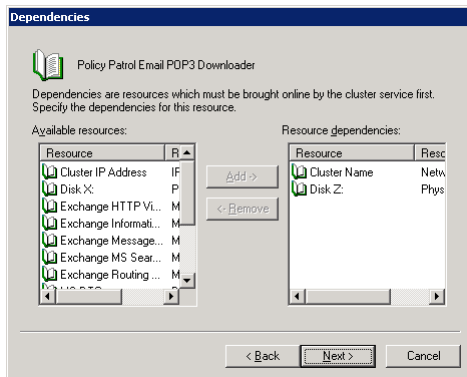
6. Do not add any registry keys and click **Finish** to create the Policy Patrol Email Remote Manager cluster resource.

Create the Policy Patrol Email POP3 downloader cluster resource:

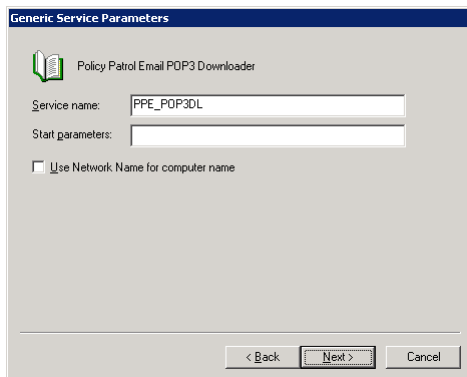
1. Go to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to **Groups**. Right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
2. Enter 'Policy Patrol Email POP3 Downloader' as the name (please use the exact same name). Select **Generic Service** as the resource type. Click **Next**.



3. In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
4. In 'Available resources', select the quorum or shared drive where the Policy Patrol configuration is stored, and the cluster network name. Click **Add** and **Next**.



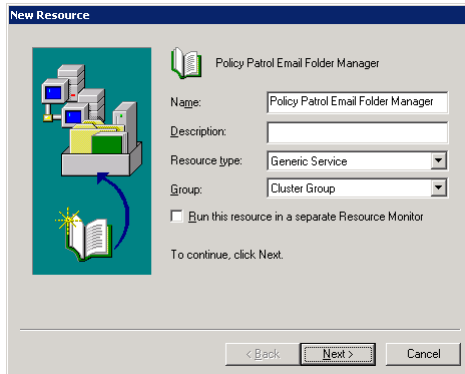
5. Enter `PPE_POP3DL` as the service name and do not enter any start parameters. Click **Next**.



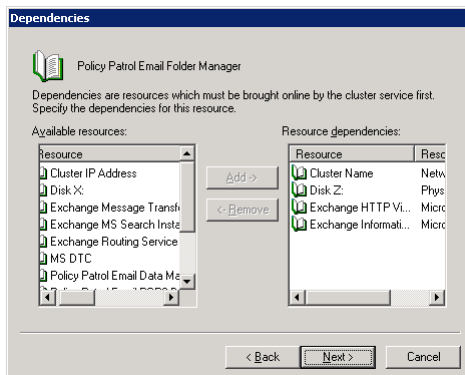
6. Do not add any registry keys and click **Finish** to create the Policy Patrol Email POP3 Downloader cluster resource.

Create the Policy Patrol Email Folder Manager cluster resource:

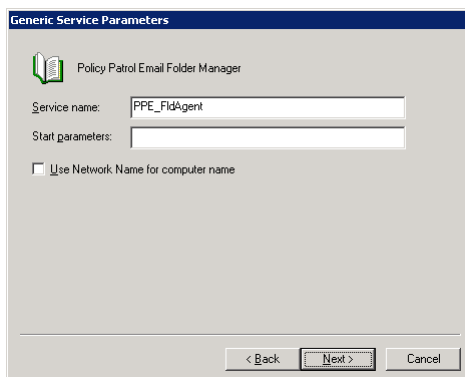
1. Go to Start > Programs > Administrative Tools > **Cluster Administrator**. Go to **Groups**. Right-click the Exchange cluster group and select **New > Resource**. The new resource wizard will now start up.
2. Enter 'Policy Patrol Email Folder Manager' as the name (please use the exact same name). Select **Generic Service** as the resource type. Click **Next**.



2. In 'Possible owners', the two Policy Patrol nodes should be selected. Click **Next**.
3. In 'Available resources', select the quorum or shared drive where the Policy Patrol configuration is stored, the cluster network name, the Exchange HTTP Virtual server and the Exchange Information Store. Click **Add** and **Next**.



4. Enter PPE_FldAgent as the service name and do not enter any start parameters. Click **Next**.



5. Do not add any registry keys and click **Finish** to create the Policy Patrol Email Folder Manager cluster resource.

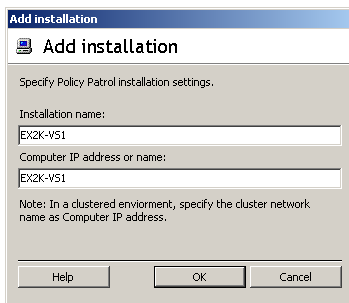
Bring the new resources online:

Select the new cluster group, right-click and choose **Bring Online**.

Step 5. Enable and configure Policy Patrol

Follow the next instructions on the Active node:

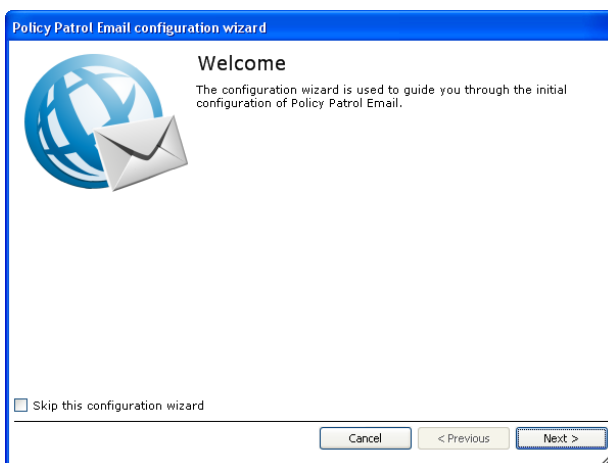
1. Open the Policy Patrol Administration on the Active node, by going to Start > Programs > Policy Patrol Email > **Administration**.
2. Click **Add installation**. Enter an installation name and enter the cluster network name in the Computer IP address or name dialog. Click **OK**.



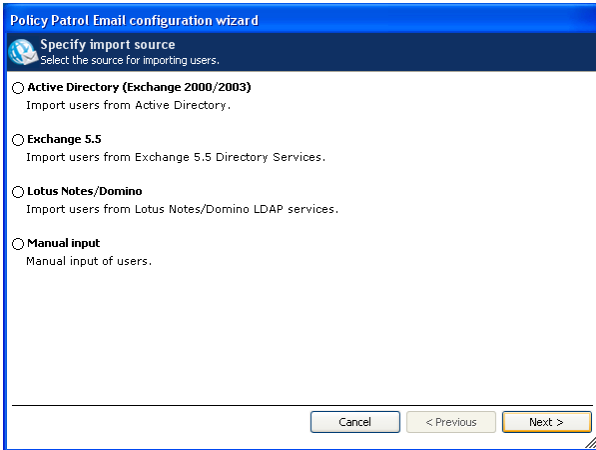
3. Select the installation and click **Connect**.

Note: If you are connecting for the first time, the configuration wizard will now start up:

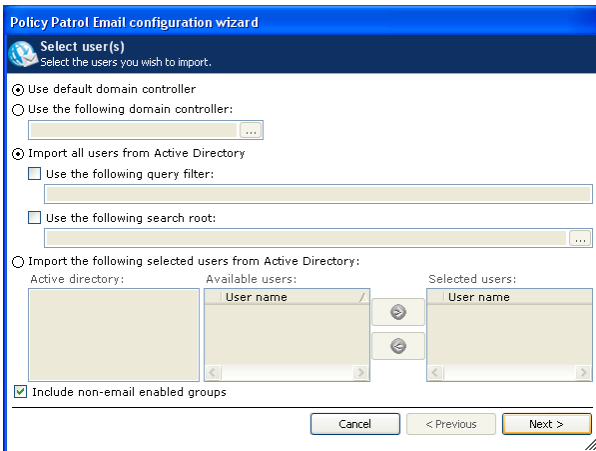
1. Click **Next** in the Welcome screen.



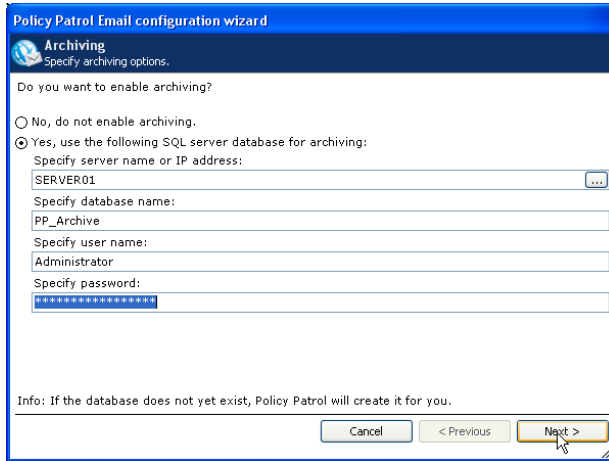
2. Specify the location from where you would like to import your users (Active Directory, Exchange 5.5, Lotus Domino or Manual input) and click **Next**. (Note: the 64-bit version only includes the Active Directory and Manual Input options.)



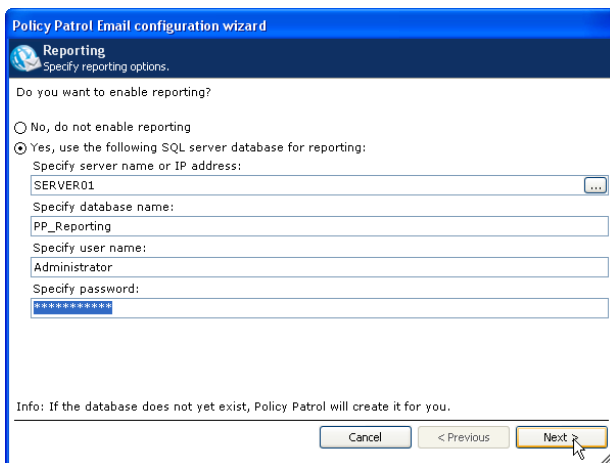
3. Specify the server or domain controller and select the users that you wish to license. You can either license all users or you can select only certain users to be licensed. For more information on the different options, consult the product manual. Click **Next**.



4. **Only for Policy Patrol Archiver or Enterprise**: Select whether you wish to enable archiving. If you enable archiving 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.



5. **Only for Policy Patrol Spam Filter or Enterprise:** 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.

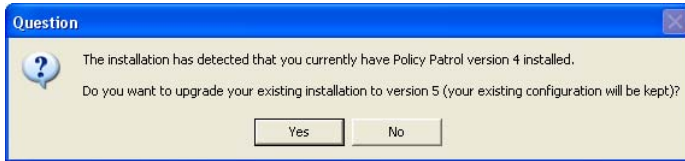


6. In the Configuration complete dialog, click **Finish**.

Upgrading your cluster installation from version 4

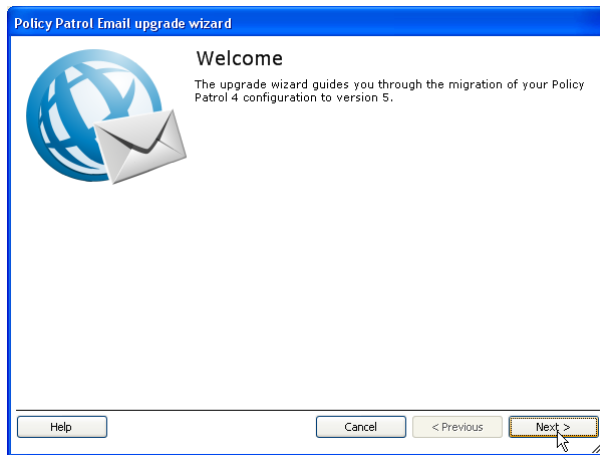
If you are upgrading your existing Policy Patrol 4 cluster installation, please follow the instructions in step 1, 2 and 3. There is no need to uninstall the program first and your existing configuration will be kept.

* Note that in step 1 after you click **Next** in the Welcome screen of the Installation wizard, a message will appear informing you that your existing version 4 installation will be upgraded. Click **Yes** to continue.

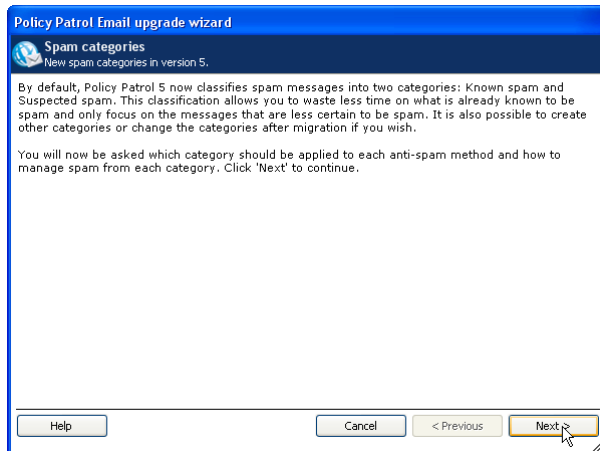


* Note that the configuration wizard (see step 3) will not appear since Policy Patrol is already configured. If you have Policy Patrol Spam Filter or Policy Patrol Enterprise with anti-spam enabled, the upgrade wizard will appear after you connect to the installation for the first time (see step 3):

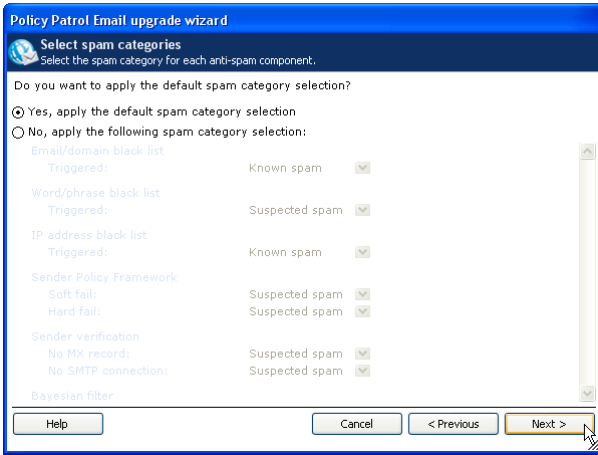
1. Click **Next** in the Welcome screen of the Upgrade wizard.



2. Policy Patrol 5 now allows you to configure spam categories. Read the information in the dialog and click **Next**.



3. Select which spam categories to apply for each anti-spam component. If you want to use the default configuration, select **Yes, apply the default spam category selection**. If you would like to make changes to the default configuration, select **No, apply the following spam category selection** and make the necessary changes. Note that you can also change the spam category selection after installation. When you are done, click **Next**.



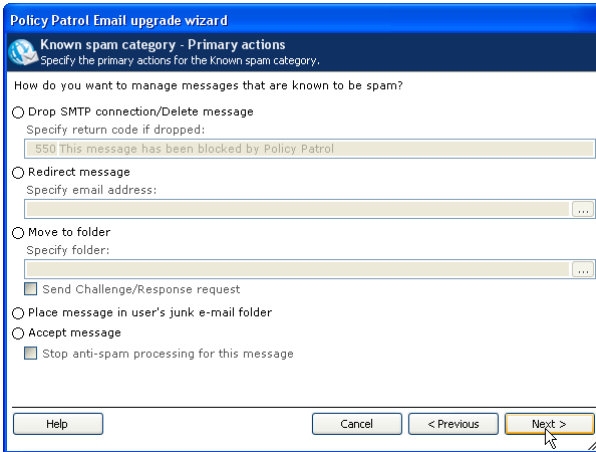
4. Select which action to take if the message is considered to be 'Known spam'. You can select from the following options:

- **Drop SMTP connection/Delete message:** This option will reject (if appropriate) or delete the messages.
- **Redirect message:** This option will redirect the messages to another email address. Enter or select the email address to redirect messages to.
- **Move to folder:** If you select this option Policy Patrol will quarantine the messages in the selected folder. Select the appropriate folder by clicking on the ... button. Note that if you want your users to view their messages in the web manager and receive quarantine reports via email, you must select this option.

If you wish to send a challenge/response message, tick the option **Send challenge/response request**. When the sender verifies the email, the message will automatically be released out of quarantine and delivered.

- **Place message in user's junk mail folder:** Select this option to place the messages in the user's junk mail folder. Note that the junk mail folder should be enabled for the users. For more instructions on how to do this and the required mailbox rights, consult chapter 9.13 'Forwarding spam to the users' junk mail folders' of the product manual.
- **Accept message:** Select this option if you wish to only apply secondary actions or if you wish to process the spam messages by an Enterprise rule (requires Policy Patrol Enterprise). Note that if you select **Accept message**, Policy Patrol will continue anti-spam processing the message to verify whether it belongs to another spam category. If you want to stop any further anti-spam processing, select the option **Stop anti-spam processing for this message**. For instance if you simply want to deliver the message with a tag added, you can select this option.

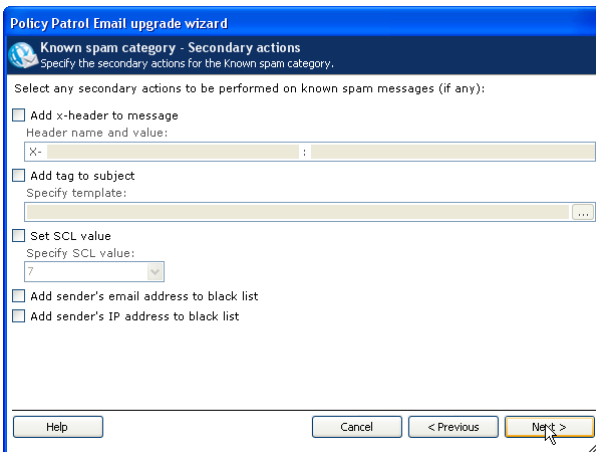
When you are done, click **Next**.



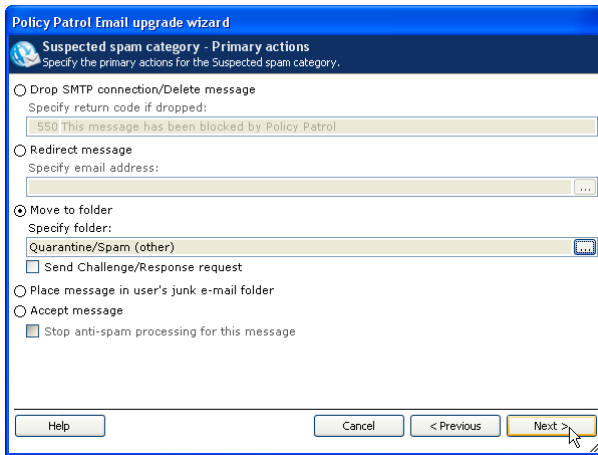
5. Select any secondary actions to be taken for known spam messages:

- **Add x-header to message:** If you select this option Policy Patrol will add an X-header to the message. Enter the header name and value you wish to add, for instance X-PP-KNOWN-SPAM : TRUE.
- **Add tag to subject:** This option will add a tag to the subject. Select the tag template to be used by clicking on
- **Set SCL value:** This option will assign an SCL value to the message that Outlook 2003 can use to determine what action to take for the message. The SCL value can be from 1-9, with 1 indicating a legitimate message and 9 indicating a spam message. Note that this feature requires Exchange 2003 or 2007. It is also possible to increase the SCL value by a certain number (1 to 9). To do this, select one of the options **Increase by n**, where n is the number to increase the value by.
- **Add sender's email address to black list:** Select this option to add the sender's email address to the black list.
- **Add sender's IP address to black list:** Select this option to add the sender's IP address to the black list.

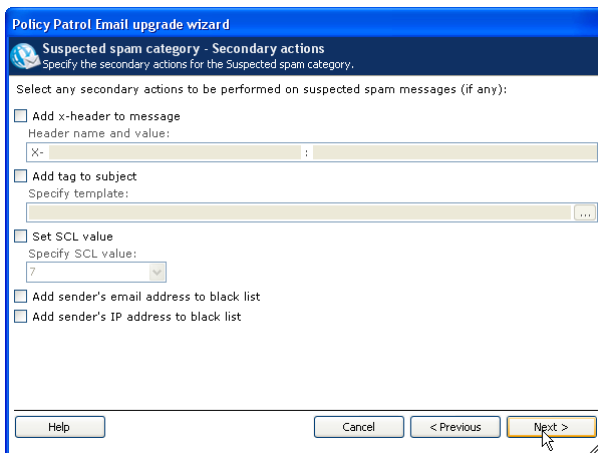
When you are ready configuring secondary actions click **Next**.



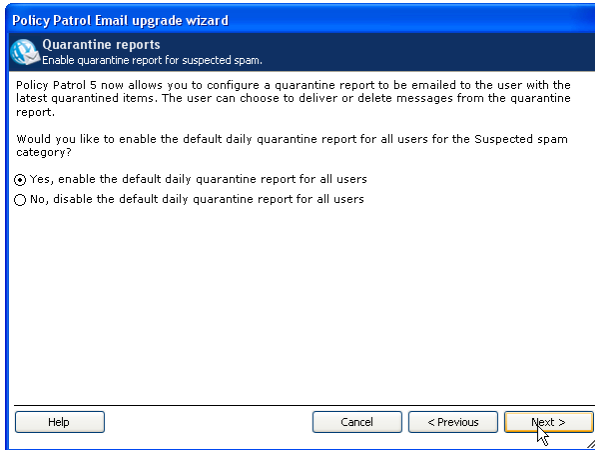
6. Select which action to take if the message is considered to be 'Suspected spam'. The options will be the same as listed in point 4.



7. Select any secondary actions to be taken for suspected spam messages. The options will be the same as in point 5.



8. By default Policy Patrol configures a daily quarantine report for Suspected spam messages. Select whether you wish to enable the default daily quarantine report for all users. Note that you can also enable this after installation. Click **Next** to continue.



9. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 5.

Uninstall Policy Patrol

If you wish to uninstall Policy Patrol Email from the clustered nodes, you must first bring the Policy Patrol cluster resources offline and then remove them. Then uninstall Policy Patrol on the nodes (**No need to failover when uninstalling**). You can do so by going to **Start > Settings > Control Panel > Add or Remove Programs**. Select **Policy Patrol Email** in the list and click **Change/Remove**.

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/docs/download.htm>.
- ⇒ 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.

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
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

Red Earth Software Ltd

Sonic House, Suite 301
43 Artemidos Avenue
6025 Larnaca
Cyprus
Tel: +357-24 828515



Fax: +357-24-828516
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.com

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

