

Quick Start

Policy Patrol 2.5



This guide will help you start using Policy Patrol as quickly as possible. For more detailed instructions, consult the Policy Patrol manual.

Step 1. Prepare for installation

System requirements

Before installing Policy Patrol, check whether you meet the system requirements:

- Windows 2000 Professional/Server/Advanced Server, Windows Server 2003 or Windows XP Professional.
- Exchange Server 2003/2000/5.5, Lotus Domino R5/R6 or other mail server.
- Microsoft .NET Framework 1.1 (If you do not have this installed the Policy Patrol program will download and install it for you).

⇒ If you have **Exchange 2000/2003** you can install Policy Patrol on the Exchange server machine (recommended) or on a separate machine. If you are installing Policy Patrol on the same machine as Exchange, skip this section and proceed to 'Step 2. Install Policy Patrol'. If you install Policy Patrol on a non-Exchange Server machine, Policy Patrol will not process internal mails. All other functionality will be available though. Download the following document for instructions on how to install Policy Patrol on a separate machine:



[Installing Policy Patrol on a separate machine](http://www.policypatrol.com/docs/Installing-Policy-Patrol-on-a-separate-machine.pdf)

(<http://www.policypatrol.com/docs/Installing-Policy-Patrol-on-a-separate-machine.pdf>)

⇒ If you have **Exchange 5.5**, you must install Policy Patrol on a separate Windows 2000/2003/XP machine and forward your mail to the Windows SMTP service on the Policy Patrol machine. Policy Patrol will offer all functionality apart from internal mail filtering. Policy Patrol can retrieve your users & groups from Active Directory or Exchange 5.5. Download the following document for instructions on how to install Policy Patrol with Exchange 5.5:




[Installing Policy Patrol with Exchange 5.5](http://www.policypatrol.com/docs/Installing-Policy-Patrol-with-Exchange55.pdf)

(<http://www.policypatrol.com/docs/Installing-Policy-Patrol-with-Exchange55.pdf>)

⇒ If you have **Lotus Domino R5/R6 Mail Server** (or another mail server), you must install Policy Patrol on a separate Windows 2000/2003/XP machine. Policy Patrol will offer all functionality, apart from processing internal mails. Policy Patrol can retrieve Lotus Domino users & groups, and their user properties for

the user merge fields. Download the following document for instructions on how to install Policy Patrol with Lotus Domino:

 [Installing Policy Patrol with Lotus Domino](http://www.policypatrol.com/docs/Installing-Policy-Patrol-with-Lotus-Domino.pdf)
(<http://www.policypatrol.com/docs/Installing-Policy-Patrol-with-Lotus-Domino.pdf>)

⇒ If you wish to install Policy Patrol in a **clustered environment (active/passive)**, you must install Policy Patrol on both nodes, run the Policy Patrol Clustering Wizard and then create the Policy Patrol cluster resources. For more information on how to do this, consult the product manual or knowledge base. Please note that Policy Patrol cannot be installed on active/active clusters.

⇒ If you have **frontend and backend** Exchange servers you need to determine on which machine(s) you must install Policy Patrol according to the following guidelines:

(1) If you use POP3 clients on the frontend server you must install Policy Patrol on the frontend server.

(2) If you use Outlook, Outlook Web Access (connecting to the frontend or backend server), or POP3 clients connecting to the backend server you must install Policy Patrol on the backend server. Note: If you have the SMTP service installed on the frontend server and all outbound mails are relayed to the frontend server you can also only install Policy Patrol on the frontend server. However, this will mean that Policy Patrol will not process internal mails since these are routed internally on the backend server and will not pass Policy Patrol.

As regards licensing, you will only be charged for one product license, even if you install Policy Patrol on the frontend and backend server. You will have to request an additional serial number though, by sending an email with your purchased serial number to orders@redearthsoftware.com.

⇒ If you have **Policy Patrol 1.x** installed, you must uninstall version 1 before you install version 2. To do this, go to Start > Settings > Control Panel > **Add/Remove programs**. Select **Policy Patrol Disclaimers**. Click **Change/Remove**. Select **Remove** and click **Next**. Click **Yes** to confirm that you wish to uninstall Policy Patrol. After removing the Policy Patrol program you will need to restart the IIS services. Click **Yes** to restart the services. When the wizard is ready, click **Finish**.

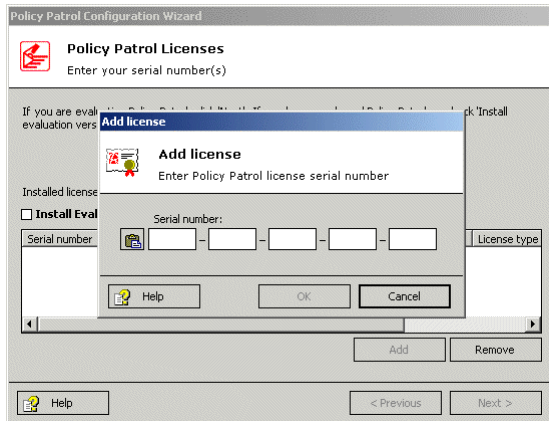
Step 2. Install Policy Patrol

1. Double-click on **PolicyPatrol.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework 1.1 installed, the installation program will install it for you (if the Policy Patrol download included the .NET Framework), or download and then install it for you (if the Policy Patrol download did not include the .NET Framework).
2. In the welcome screen, click **Next**.

3. Read the License Agreement and click **Yes** to accept the agreement.
4. Enter your user name and company name. If you want anyone who is logged on to the computer to be able to access Policy Patrol, select **Anyone who uses this computer (all users)**. If you only wish yourself to be able to access the program, select **Only for me (user name)**. Click **Next**.
5. Select the setup type. If you select **complete**, the complete program will be installed in the default folder C:\Program Files\Red Earth Software\Policy Patrol. If you select custom, you will be able to change the location of the Policy Patrol folder and specify whether you wish to install the mail processor, Administration console, Web monitor and/or sample rules. If you only wish to install the Administration console (for remote administration), select **Administration console**. Click **Next** to continue.
6. Specify the user account that must be used for Synchronization. Make sure that this account has access rights to the Active Directory, Exchange 5.5 or Lotus Domino. Click **Next**.
7. Review the installation settings. If they are correct, click **Next** to start copying files.
8. When Policy Patrol has finished copying the files, the Policy Patrol Configuration wizard will start up. Continue to the next paragraph for instructions on the Policy Patrol Configuration Wizard. When the configuration wizard has run, the Installation Wizard complete screen will pop up. Click **Finish** to exit the Installation wizard.

Step 3. Policy Patrol Configuration Wizard

1. In the welcome screen, click **Next** to start the wizard.
2. If you are evaluating Policy Patrol, click **Next**. If you have purchased Policy Patrol, uncheck **Install evaluation version** and click **Add**. Enter your serial number and click **OK**. If you received your serial number via email, you can copy the serial number from your email and click on the 'Paste' button. Click **Next** to continue.



3. Enter your local domain(s). Your local domain is the part after the @ sign of your email address, for instance `redearthsoftware.com`. If you have installed Policy Patrol on the same machine as your mail server (only possible for Exchange 2000 and 2003), Policy Patrol will retrieve your local domains for you. To add a local domain, click on **Add**. Enter the domain, for instance `redearthsoftware.com`, and click **OK**. To remove a local domain, click **Remove**.

If you do not wish Policy Patrol to process emails from certain mail servers, enter the IP addresses in **Exclude IP addresses**. Click on **Add**, enter the IP address and click **OK**. When you are ready, click **Next**.

4. Select the virtual SMTP server that you wish Policy Patrol to monitor. If you only have one virtual SMTP server installed, the other options will be grayed out. Click **Next**.
5. Enter the email address(es) for the Policy Patrol Administrator. These addresses will be used for Policy Patrol system notifications and Administrator notifications configured in rules. You can enter a To:, Cc: and Bcc: email address. Remember that the From: field must include an existing, internal email address. Click **Next**.
6. You must configure at least one connector so that Policy Patrol can retrieve your users. Select the type of connector you wish to create; **Active Directory/Exchange 2000, Exchange 5.5** or **Lotus Domino** connector. If you selected Active Directory, you can use the default Active Directory domain controller, or you can enter the name or IP address of another server. If you selected Exchange 5.5 or Lotus Domino you must enter the name or IP address of the mail server.

Policy Patrol will synchronize all users from the connector. If you wish to create a more specific connector, or if you wish to pick up users from a text file, uncheck **Create default connector**. You will then be able to configure your connector after installation in 'Connectors'. For instance, if you have a lot of users in your Active Directory and you only want to use Policy Patrol for selected users, it is better to create a more specific connector, rather than synchronizing all the users in your Active Directory. If you wish to use multiple connectors, for instance one Exchange 2000 connector and one Lotus Domino connector, you can create the

default connector during installation, and add more connectors in the Administration console after installation. When you are ready, click **Next**.

Note: The Default connector is not **scheduled**. If you want Policy Patrol to automatically retrieve new users and updated user properties, you must configure scheduling of the Default connector after installation from **Connectors > Default connector > Properties > Schedule** tab.

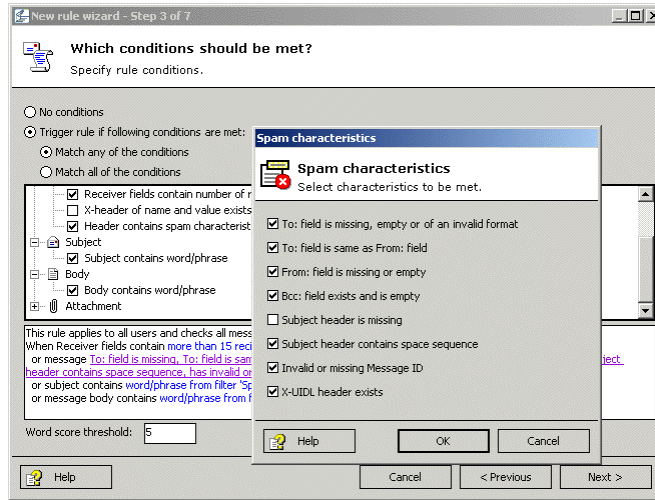
7. Policy Patrol will now display all the users from the default connector. All users will automatically be licensed. If you have more users than licenses, you must remove some licensed users after installation in 'Licensing', since otherwise Policy Patrol will select the licensed users randomly. Click **Next**.
8. If you wish the Administrator to receive an email notification when a new Policy Patrol update is available, check the option **Enable automatic update notifications**. In addition to an email notification, the Policy Patrol Update Wizard icon will appear in the system tray. Note that this option requires an Internet connection on the Policy Patrol machine.
9. If you wish to be able to administer Policy Patrol remotely, you must tick the check box **Enable Remote Administration**. Enter the TCP port to use. By default 8000 is used. If you have multiple Policy Patrol installations that you wish to access remotely, each installation must use a different port. Select **Publish installation** to display the computer in a list that can be connected to from the remote machine. Note that this option is only possible if you have Active Directory.
10. Click **Finish** to exit the configuration wizard.

Step 4. Create rules

You can now start configuring rules in the Policy Patrol Administration console. Go to **Start > Programs > Policy Patrol > Administration**. Select **<server name>** and choose **Connect**. The program includes a number of sample rules. You can use the sample rules or create your own rules. For more information on how to customize the sample rules, consult the manual or help in the program. To create your own rule, go to **Policy rules** and click on the **New...** button. The rules wizard will appear and guide you through the next steps:

1. Which users should this rule apply to? Specify the users and/or groups for the rule and any user exclusions. Domains and Connectors can also be selected here (a system parameter needs to be added for this). Click **Next**.
2. Which messages do you want to check? Specify whether you wish to check all messages, or only internally sent/received or externally sent/received messages. If Policy Patrol is not installed on an Exchange 2003 or 2000 machine, the internally sent/received messages options will be grayed out. Click **Next**.
3. Which conditions should be met? Specify the conditions for the rule. The conditions are sorted in General, Header, Subject, Body and Attachment

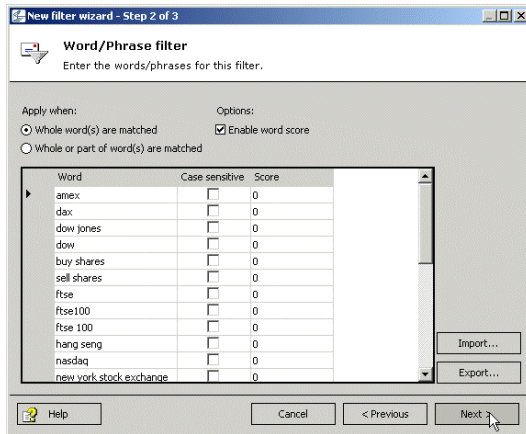
conditions. If you need to set a certain value for a condition, the condition will appear in the rules description with a **red link**. Click on the **red link** to configure the options. If you need to select a filter or template you will be able to create a new one by clicking on the **New Filter** or **New Template** buttons (consult the next paragraph for instructions). If you select a word/phrase condition, enter a word score threshold for the rule to trigger. Click **Next**.



4. Should this rule have exceptions? Select the rule exceptions here. The options will be the same as for the conditions. Click **Next**.
5. What actions should be taken? Select one primary action and any secondary action(s). If further values need to be selected, the action will appear with a **red link**. Click on the **red link** to configure the options. If you select multiple secondary actions and wish to specify the order in which they should be performed, click on the **Change order** button. Click **Next**.
6. Should this rule be scheduled? You can schedule a rule to trigger within a certain date range, or on certain day(s) of the week. Click **Next**.
7. Enter a name for the rule. Enter a name and any comments for the rule. Click **Finish** to create the rule.

Step 5. Create filters and templates

The program includes a number of sample filters and templates. However, you can also create your own.



To create a filter:

1. Go to **Filters > New** (you can also click on **New Filter** in the rules wizard).
2. Select the filter you wish to create: Word/Phrase, Attachment Name, Attachment Type or Domain/Email address filter. Click **Next**.
3. Enter the values for the filter. When you are ready, click **Next**.
4. Enter a name and any comments. Click **Finish** to create the filter.

To create a template:

1. Go to **Templates > New** (you can also click on **New Template** in the rules wizard).
2. Select the template you wish to create: Notification, Tag or Disclaimer template. Click **Next**.
3. Enter the text for the template. You will be able to insert fields, and for the Notification and Disclaimer templates, you will be able to apply formatting and import and export texts. When you are ready, click **Next**.
4. Enter a name and any comments. Click **Finish** to create the template.

Step 6. Configure virus checking

To enable virus scanning you must download and install Kaspersky™ Anti-Virus on the Policy Patrol machine. Depending on the operating system on the Policy Patrol machine, you need to download Kaspersky™ Anti-Virus for Windows 2000 Professional and Windows XP (<http://www.redearthsoftware.com/files/KAVWinWorkstation.zip>), or Kaspersky™ Anti-Virus for Windows 2000/2003 (Advanced) Server (<http://www.redearthsoftware.com/files/KAVNTServer.zip>).

After you have downloaded Kaspersky, follow the next steps to install it:

1. In the Welcome screen, click **Next**.
2. Read the License agreement and click **Yes**.
3. Enter your user name and company name. Click **Next**.
4. Select the installation location for Kaspersky. By default, this is C:\Program Files\Kaspersky Lab\. When you are ready, click **Next**.
5. Enter the program group name in the Start > Programs menu. By default this is Kaspersky Anti-Virus. Click **Next**.
6. In Setup type, select **Custom** and click **Next**. Now select **Kaspersky Anti-Virus Core Components, Kaspersky Anti-Virus Bases, Kaspersky Anti-Virus Updater** and **Kaspersky Anti-Virus Control Centre**. Click **Next**.
7. Review the settings and click **Next** to start copying files.
8. In the Report Viewer Settings screen, select both report viewer associations and click **Next**.
9. Enter the password to be used to remotely access and manage Kaspersky Anti-Virus. Click **Next**.
10. Select the key file in the list and click **Next**.
11. Click **Finish** to exit the installation. Kaspersky will automatically download and apply new anti-virus files daily at 19.30. You can change the scheduling by opening the Kaspersky Anti-Virus Control Centre, right-clicking on **Update anti-virus bases** and choosing **Properties > Schedule tab**.

After Kaspersky is installed, open the Policy Patrol Administration console. To enable virus scanning, go to **Anti virus** and check **Enable Kaspersky™ Anti-Virus**. By default, Policy Patrol checks all messages for possible viruses and tries to clean or delete them. It is highly recommended to enable the sample rule 'Quarantine viruses that cannot be deleted' since in this way if Policy Patrol is not able to delete a virus, the mail will still be quarantined.

Step 7. Configure real time Spam blocker

To use the real time spam blocker, tick **Enable real time spam blocker**. Click **Add** to configure a spam black list. Enter the Zone and Returns for the list. For instance for the Spamhaus Block List (SBL), enter `sbl.spamhaus.org` for the zone and `127.0.0.2` for the Returns. If you select **Reject message and add the following response** the message will not be downloaded by your mail server and will therefore not use up any bandwidth. The response you enter will be sent to the sending mail server. If you want to quarantine or delete the message (with the option to undelete), or add a tag, select **Add the following X-header to message** and enter the header to be added. For instance for the Spamhaus Block List, enter `SPAMHAUS`. When you

are done, click **OK**. You can add as many spam black lists as you wish. For a list of possible spam lists, go to: <http://www.email-policy.com/spam-black-lists.htm>.

To create a rule that processes mails with the X-header SPAMHAUS:

1. Go to Policy rules and click **New**.
2. Select the users for the rule. Click **Next**.
3. Select **Only the following messages** and tick **Externally received**. Click **Next**.
4. Select **Trigger rule if following conditions are met**. Go to **Headers** and select the option **Header of name and value exists**. Click on the link in the description and enter `X-SPAMHAUS` as the name and `TRUE` as the value. Click **OK** and **Next**.
5. If you want to set exceptions, select **Do not trigger rule if following exceptions are met**. For instance you can exclude allowed newsletters and existing contacts by going to **Headers** and selecting the option **Sender field contains domain or email address**. Then click on the link and select the sample 'Automatic white list' and 'Newsletters' filters (you must still enter your newsletter email addresses in this filter). Click **OK** and **Next**.
6. Now specify what actions you wish to take. You can quarantine, delay, delete or accept the message. Furthermore you can select secondary actions, such as sending an email notification, adding a tag, or adding the sender to a filter. When you are ready, click **Next**.
7. Leave the rule unscheduled and click **Next**.
8. Enter a name for the rule and any comments and click **Finish**.
9. Click on **<server name>** and press **Commit** to save the changes.

Apart from using the Spam blocker, Policy Patrol can stop spam by searching for spam headers, spam content, number of recipients and HTML only messages. The sample rule 'Add tag to spam messages' demonstrates how you can search for these conditions in order to block spam. For more information on how to configure Policy Patrol to stop junk mail, please download the following document:



[How to filter spam with Policy Patrol](http://www.policypatrol.com/docs/How-to-filter-spam-with-Policy-Patrol.pdf)

(<http://www.policypatrol.com/docs/How-to-filter-spam-with-Policy-Patrol.pdf>)

Step 8. More information

- ⇒ For more information on how to configure Policy Patrol, please download the product manual from:
<http://www.policypatrol.com/docs/policypatrol2manual.pdf>.

- ⇒ For frequently asked questions, consult our online knowledge base at:
<http://www.policypatrol.com/kb.asp>
- ⇒ If you have any technical or configuration questions please send an email to:
support@reearthsoftware.com.
- ⇒ If you are experiencing a problem with Policy Patrol, please run the Support Wizard by choosing **Help > Support Wizard**. The wizard will gather all the relevant information and send this to Red Earth Software technical support.
- ⇒ If you require any assistance, please contact us at one of the following offices:

Red Earth Software
200 Marcy Street
Portsmouth, NH 03801
United States
Phone: (603) 436-1319
Fax: (603) 457-8455
Sales: sales@reearthsoftware.com
Support: support@reearthsoftware.com

Red Earth Software (UK) Ltd
20 Market Place
Kingston-upon-Thames
Surrey KT1 1JP
United Kingdom
Tel: +44-(0)20-8605 9074
Fax: +44-(0)20-8605 9075
Sales: sales@reearthsoftware.co.uk
Support: support@reearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2003 by Red Earth Software.