

Quick Start

Policy Patrol 3.5



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 you can download Policy Patrol including the .NET Framework or download the Microsoft .NET Framework from the Microsoft website: <http://msdn.microsoft.com/netframework/technologyinfo/howtoget/>).

⇒ 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/PP3-SeparateMachine.pdf)
(<http://www.policypatrol.com/docs/PP3-SeparateMachine.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/PP3-Exchange55.pdf)
(<http://www.policypatrol.com/docs/PP3-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/PP3-LotusDomino.pdf)
(<http://www.policypatrol.com/docs/PP3-LotusDomino.pdf>)

⇒ If you wish to install Policy Patrol in an **Active/Passive cluster**, download the document below for further instructions:

 [Installing Policy Patrol in a cluster](http://www.policypatrol.com/docs/PP3-Clustering.pdf)
(<http://www.policypatrol.com/docs/PP3-Clustering.pdf>)

⇒ 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.

For licensing information regarding frontend/backend servers, please contact sales@reearthsoftware.com.

⇒ If you have **Policy Patrol 1.x** installed, you must uninstall version 1 before you install version 3. 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**.

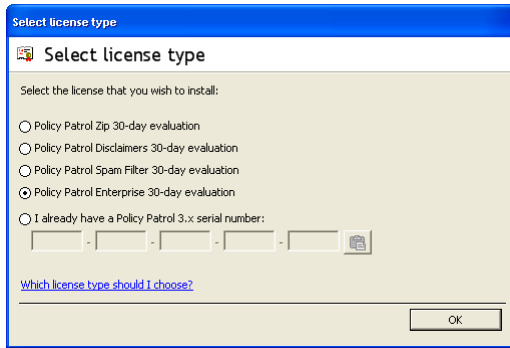
⇒ If you have **Policy Patrol 2.x** installed, you can migrate your existing configuration to version 3. To do this, you must download the migration wizard from: www.reearthsoftware.com/files/migration30.zip. If you do not want to export your configuration it is recommended to uninstall version 2 before you install version 3. To do this, go to Start > Settings > Control Panel > **Add/Remove programs**. Select **Policy Patrol**. Click **Change/Remove**. Select **Remove** and click **Next**. Click **Yes** to confirm that you wish to uninstall Policy Patrol. 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 (and the Policy Patrol download did not include it), the installation program will ask you to install it first (see requirements).
2. In the Welcome screen, click **Next**.
3. Read the License Agreement and select **I accept the license agreement**. Click **Next**.
4. Enter the user name and organization 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 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 only**. Click **Next** to continue.
6. Select the destination folder for the Policy Patrol installation. By default the program is installed in C:\Program Files\Red Earth Software\Policy Patrol 3.0. If you wish to change the location, click **Browse** and select another folder. When you are ready, click **Next**.
7. Select the virtual SMTP server that you wish Policy Patrol to monitor. If you only have one virtual SMTP server installed, leave the default option selected and click **Next**.
8. Enter a user name and password for the Policy Patrol Spam Blocker service. Click **Next**.
9. Confirm that you wish to proceed with the installation by clicking **Next**.
10. Policy Patrol will now start copying the files. When Policy Patrol is ready, click **Finish** to exit the wizard.

Step 3. Configure Policy Patrol

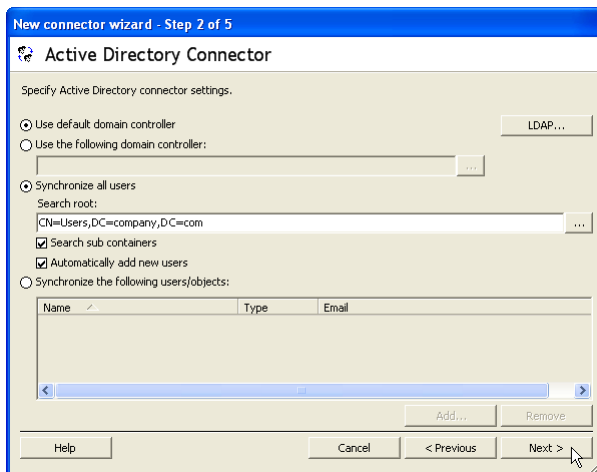
Open the Policy Patrol Administration console by going to **Start > Programs > Policy Patrol > Administration**. Select **<server name>** and click **Connect**.



Select license type: Upon opening the Administration console for the first time, Policy Patrol will ask you which license type you wish to install. If you are evaluating Policy Patrol, select one of the evaluation versions. If you have purchased a serial number, enter the serial number and click **OK**. (If you later wish to try out a different Policy Patrol version 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.

Configure licensed users: Go to **Users > Licensed Users > Connectors** and click on the **New** button. Select the connector type (Active Directory, Exchange 5.5, Lotus Domino or Manual input) and click **Next**. 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.

Click **Next**. Select the objects to be retrieved. You only need to select the objects that you wish to apply rules to. Click **Next**. The user list will now be displayed. All entries with an email address will be counted as a license. Click **Next**. Enter a connector name and click **Finish**.



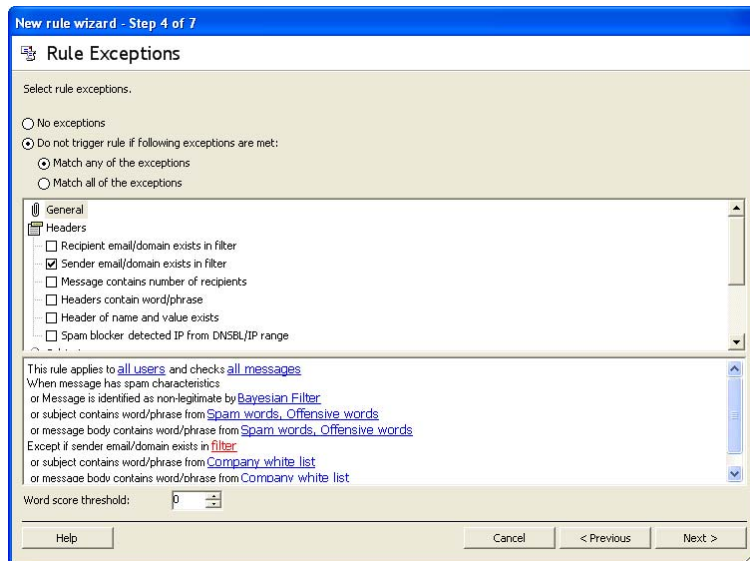
Configure system notifications: Go to **<server name> > Advanced > System Configuration > System notifications**. Enter the email addresses for the Policy Patrol Administrator(s). These addresses will be used for Policy Patrol system

notifications and Administrator notifications configured in rules. You must enter a From: address and at least one To:, Cc: or Bcc: email address.

Step 4. Create rules

You can now start configuring rules. Select **<server name>** and choose **Connect**. The program includes a number of sample rules (see step 6, 7, 8 and 9). You can use the sample rules or create your own rules. To create your own rule, go to **Rules**, select the Rules folder and click on the **New...** button. The rules wizard will appear and guide you through the next steps:

1. Rule users: Specify the users, groups, public folders or domains for the rule and any exclusions. Click **Next**.
2. Rule direction: 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 not be applicable. Click **Next**.
3. Rule conditions: 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 specify a filter or template you can either select an existing one or create a new one by clicking **New**. If you select a word/phrase condition, enter a word score threshold that must be reached for the rule to trigger. Click **Next**.
4. Rule exceptions: Select the rule exceptions here. The options will be the same as for the conditions. Click **Next**.



5. Rule actions: Select one primary action and any secondary action(s). The secondary actions are sorted in Modify message, Message duplication,

Notifications, White lists, black lists and other filter operations and Other actions. 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 **Order** button. Click **Next**.

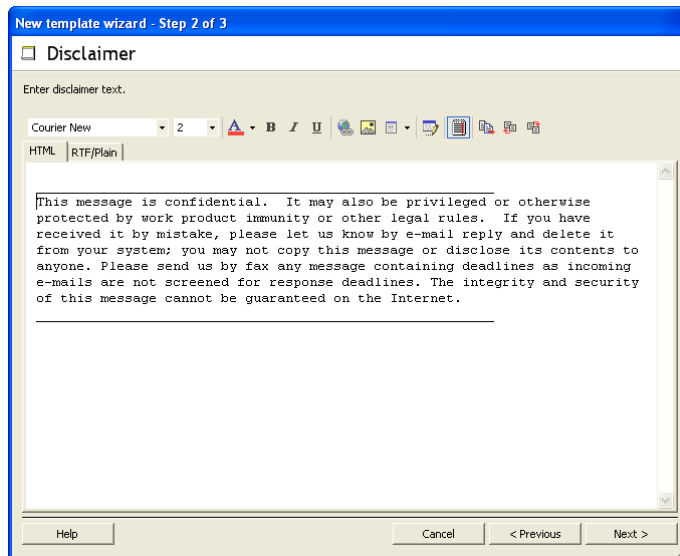
6. **Rule scheduling:** You can schedule a rule to trigger on certain day(s) of the week and on certain times. To specify a date range, click on **Advanced** and select the **Date** tab. In the **Throughput** tab you can configure throttle control options. Click **Next**.
7. **Rule Name:** Enter a name 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 template:

1. Go to **Templates**, select the appropriate folder and click **New** (you can also create a new template from 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.



To create a filter:

1. Go to **Filters**, select the appropriate folder and click **New** (you can also create a new filter from the rules wizard).
2. Select the filter you wish to create: Word/Phrase, Attachment or Email address/domain 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.

Step 6. Compression (Policy Patrol Zip)

The program includes a number of sample compression and decompression rules. To view the rules, go to **Rules > Sample Rules > Policy Patrol Zip**:

- Compress all attachments: Enable this rule if you wish to compress all attachments.
- Compress attachments larger than 50 KB: This rule compresses attachments larger than 50 KB and provides the possibility to exclude messages from compression in the following circumstances: if the attachment is already in compressed format (except for zip since this is already excluded by default), when the code [No compression] is present in the subject, or when a domain or email address exists in the 'Exclude from compression' filter.
- Decompress attachments smaller than 1 MB: This rule decompresses attachments smaller than 1 MB (extracted file size).
- Remove [No compression] from subject: Enable this rule to remove the [No compression] code from the subject before the message is delivered to the recipient.

Step 7. Disclaimers (Policy Patrol Disclaimers)

The program includes a number of sample disclaimer rules. To view the rules, go to **Rules > Sample Rules > Policy Patrol Disclaimers**:

- Add disclaimer for selected recipients: This rule adds a custom disclaimer when sending messages to certain external recipients. Select the disclaimer to be added and enter the recipients in the 'Recipients' filter.
- Add disclaimer with link: This rule adds a prepended disclaimer with a link to an appended disclaimer (only for HTML messages) to externally sent messages. The rule avoids multiple disclaimers by checking whether the appended disclaimer text already exists. Remember that if you change the appended disclaimer text, you must change the word/phrase filter in the exceptions. Tip: You can create another rule that always adds the prepended disclaimer with link at the top of the email. Then remove the prepend disclaimer from the rule 'Add disclaimer with link'.

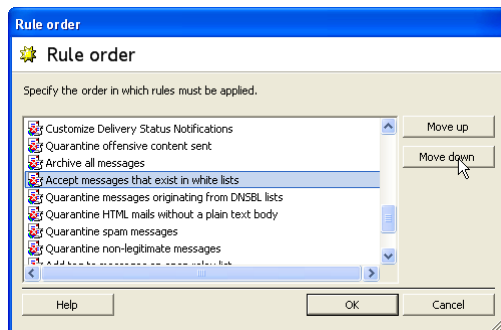
Policy Patrol will now always add the prepended disclaimer, but will only add the appended disclaimer once.

- ☑ Add external disclaimer: This rule adds a disclaimer to all externally sent messages, except if the code [No disclaimer] exists in the subject, or if the disclaimer has already been added. Remember that if you make a change in the 'External disclaimer' template you must change the word/phrase filter in the exceptions.
- ☑ Add internal disclaimer: This rule adds a disclaimer to all internally sent messages, except if the code [No disclaimer] exists in the subject, or if the disclaimer has already been added. Remember that if you make a change in the 'Internal disclaimer' template you must change the word/phrase filter in the exceptions.
- ☑ Add signature: This rule adds a signature to all internally and externally sent messages and attempts to place the signature above the last entered message text. Remember to add your URL in the 'Signature' template.
- ☑ Remove [No disclaimer] from subject: Enable this rule to remove the [No disclaimer] code from the subject before the message is delivered to the recipient.

Step 8. Anti-spam (Policy Patrol Spam Filter)

The program includes a number of sample anti-spam rules. To view the rules, go to **Rules > Sample Rules > Policy Patrol Spam Filter:**

- ☑ Accept messages that exist in white lists: This rule lets all white listed externally received messages through. This includes messages from senders on the 'Newsletters' or 'Automatic white list' filters and messages that include words on the 'Company white list'. After this rule triggers, no further rules are processed (any rules that should still be processed should be ordered above this rule (**Rules > Rule ordering**)). Remember that you must still configure the entries in the 'Newsletters' and 'Company white list' filters and that you must enable the rule 'Automatic white list and Bayesian filter learning'.



- ☑ Accept messages with [New customer] in subject: This rule is to be used in combination with the rule 'Block all messages not on automatic white list' and

- 'Remove [New customer] from subject', and accepts all messages with the code [New customer] in the subject and adds the sender to the Automatic white list.
- ☑ Add tag to messages on open relay list: This rule adds the tag OPEN RELAY: to the subject of messages from senders on the ORDB list.
 - ☑ Automatic white list and Bayesian filter learning: This rule automatically adds recipient email addresses of all outgoing emails (except for Delivery Status Notifications and Out of Office replies) to the 'Automatic white list'. In addition, it adds all outgoing messages (except for Delivery Status Notifications and Out of Office replies) to the Bayesian filter's legitimate database. After enabling the rule, you can simply wait for your Bayesian filter to fill up with legitimate messages (by default maximum is 5000).
 - ☑ Block all messages not on automatic white list: This rule is to be used in combination with the rule 'Accept messages with [New customer] in subject', and blocks all messages from senders that are not listed on the 'Automatic white list' and sends a notification message to the sender requesting the sender to resend the message with [New customer] in the subject. Use this rule with caution since by enabling this rule you will block mails from all new customers and contacts. Remember to enter your company name in the 'Challenge response notification' template.
 - ☑ Delete messages from known spam senders: This rule moves all messages from the 'Spam senders' filter to the Deleted folder. Messages in the Deleted folder that are older than 30 days are automatically deleted.
 - ☑ Quarantine HTML mails without a plain text body: This rule moves all HTML messages without a plain text body (a spam characteristic) to the Quarantine\Spam folder. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.
 - ☑ Quarantine messages from DNSBL and SURBL lists: This rule quarantines all externally received messages from senders on the SBL (www.spamhaus.org) or NJABL (www.dnsbl.njabl.org) real-time black lists, and messages that contain URLs from the SURBL list multi.surbl.org in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.
 - ☑ Quarantine non-legitimate messages: This rule quarantines all externally received messages that have a Bayesian probability score of 0.8 or higher in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder. The Bayesian sample filter already includes over 3000 non-legitimate messages but you still need to add legitimate messages. You can automatically add legitimate messages to the filter by enabling the rule 'Automatic white list and Bayesian filter learning'. Alternatively, you can import messages into the Bayesian filter by going to **Bayesian filtering** > **Sample filter**, selecting **Bayesian filter** and clicking on **Import**. Select to import into the **Legitimate** database. You will be able to import messages from a

mailbox or from a public folder. Note that it is better not to enable this rule until you have at least 2000 legitimate messages in the Bayesian filter.

- Quarantine spam messages: This rule quarantines all externally received messages that have spam words in the subject or body, match spam characteristics, or have a Spam Confidence Level of 7 or higher. The rule quarantines the messages in the Quarantine\Spam folder and adds the sender email addresses to the 'Spam senders' filter. Messages in the Spam folder that are older than 30 days are automatically moved to the Deleted folder.
- Remove [New customer] from subject: Enable this rule to remove the [New customer] code from the subject before the message is delivered to the recipient.

For more information on how to filter spam with Policy Patrol, 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 9. Email content security (Policy Patrol Enterprise)

The program includes a number of sample email content security and management rules. To view the rules, go to **Rules > Sample Rules > Policy Patrol Enterprise** (remember that the sample rules for all other versions are also available to Policy Patrol Enterprise users):

- Archive all messages: This rule archives all messages into the default CSV archive.
- Block spoofed attachments: This rule moves spoofed attachments to the Quarantine\Suspicious folder and sends a notification message to the Administrator.
- Customize Delivery Status Notifications: This rule customizes internally sent Delivery Status Notifications of number 4.4.7, 5.1.1, 5.5.0, and 5.7.1.
- Delay large attachments: This rule checks all external messages and moves messages larger than 1 MB to the Delayed folder for automatic delivery after office hours.
- Print all externally sent messages: This rule prints all externally sent messages on the default printer.
- Quarantine all viruses: This rule moves all messages with viruses to the Quarantine\Viruses folder, sends a notification message to the Administrator and adds an entry to the Windows event log. If the Administrator deletes the message, a notification will be sent to the sender informing them that their message was deleted. Remember to enter your company name and telephone number in the 'Virus deleted' template. For instructions on how to enable virus scanning, go to Step 10.

- ☑ Quarantine dangerous attachment types: This rule moves all messages with dangerous attachment types to the Quarantine\Suspicious folder and sends a notification message to the Administrator.
- ☑ Quarantine externally sent NDRs: This rule moves all externally sent NDR's to the Quarantine\Spam folder.
- ☑ Quarantine offensive content sent: This rule quarantines all internally and externally sent messages with offensive content in the subject or body in the Quarantine\Offensive folder and sends a notification message to the Administrator. Note that externally received messages with offensive content are already caught by the 'Quarantine spam messages' rule in the Sample rules\Policy Patrol Spam Filter folder.
- ☑ Send automatic reply to information request: This rule automatically sends a reply to externally received web forms. Remember that you must still configure the templates and filters to include the necessary information. Note: For the rule to work you must configure the web form to be sent with the submitter of the form as the sender.

Step 10. Install anti-virus (optional)

To start virus-scanning emails, download the Kaspersky Anti-virus plug-in from <http://www.policypatrol.com/files/PPEKAVplugin.exe> and install the program on the Policy Patrol machine:

1. In the Welcome screen, click **Next**.
2. Read the license agreement and click **Yes** to confirm the agreement.
3. Enter an account that has access to the Internet to enable Kaspersky updates to be downloaded. Click **Next**.
4. The Kaspersky files will now be copied on to the machine. When all files are copied, a dialog will appear. If you wish to download the latest anti-virus updates, tick the check box **Update virus definition files** now. Click **Finish** to exit the wizard.
5. If you have purchased the Kaspersky Anti-virus add-on, copy the key file to C:\Program Files\Red Earth Software\Policy Patrol 3.0\Kaspersky. If you have not purchased Kaspersky Anti-virus add-on, you will be able to use Kaspersky Anti-virus for 30 days.
6. Open the Policy Patrol Administration console, connect to the server and select the **Anti virus** node. **Kaspersky Labs Anti Virus** will appear as an installed engine. The expiration date will be listed as well as the date and time that the anti-virus engine was last updated. By default, Kaspersky updates are scheduled to run daily at 8 pm. To change the scheduling of the updater, select **Kaspersky Labs Anti Virus** in the list and click **Schedule**. Select the **Schedule** tab and make the necessary changes. Click **OK**.

Step 11. More information

- ⇒ For more information on how to configure Policy Patrol, please download the product manual from:
<http://www.policypatrol.com/docs/policypatrol3manual.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@redearthsoftware.com.
- ⇒ If you require any assistance, please contact us at one of the following offices:

Red Earth Software LLC
200 Marcy Street
Portsmouth, NH 03801
Phone: (603) 436-1319
Fax: (603) 457-8455
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)20-8605 9074
Fax: +44-(0)20-8605 9075
Sales: sales@redearthsoftware.co.uk
Support: support@redearthsoftware.co.uk

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2004 by Red Earth Software.