

Policy Patrol 6 Upgrade Guide

If you have Policy Patrol 4 or 5 installed you can upgrade to version 6 and keep your existing configuration. Please follow the upgrade instructions below for the respective Policy Patrol edition that you have installed. If you have version 3 or earlier installed, you must uninstall Policy Patrol and follow the instructions in the migration guide: <http://www.policypatrol.com/docs/pp6-migrationguide.pdf>.

Note: You require a new serial number for version 6. If you have a valid maintenance contract the serial number will be provided at no additional cost. If you do not have maintenance you will need to purchase an upgrade. For more information please contact sales at sales@redearthsoftware.com.

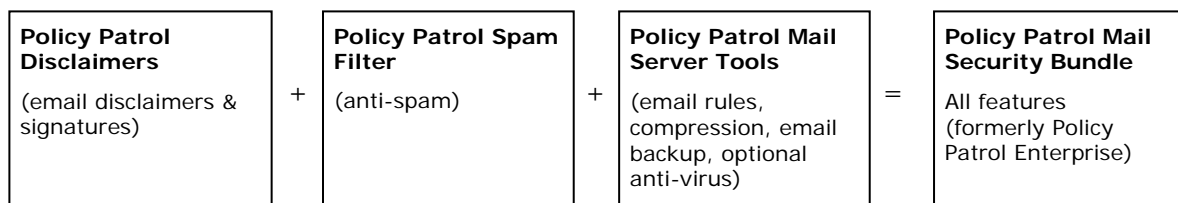
=> If you have a **clustered environment**, please refer to the Clustering guide for instructions on how to upgrade your installation (only applicable for 32-bit clusters): <http://www.policypatrol.com/docs/pp6-clustering.pdf>

=> You must upgrade your server as well as any **remote administration** installations on separate machines.

=> If you are moving to **Exchange Server 2007** (and you will be installing Policy Patrol on the Exchange 2007 machine) you will need to download and install Policy Patrol for Exchange 2007 (64 bit). In this case the upgrade instructions will not apply since you will need to do a new installation. If you would like to keep your existing configuration, you must first upgrade your existing 32-bit installation to version 6 and then export the configuration from the 32-bit version 6 installation (select **Local** and go to **File > Export configuration**) and then import it on the 64-bit installation (select **Local server** and go to **File > Import configuration**). If you want to keep the contents of your monitoring folders, you must also copy the Policy Patrol monitoring folder (by default C:\Program Files\Red Earth Software\Policy Patrol Email\Monitoring) to the Exchange 2007 machine. Policy Patrol for Exchange 2007 (64-bit) can be downloaded from the following link: <http://www.policypatrol.com/files/policypatrol2k7.exe>

New editions

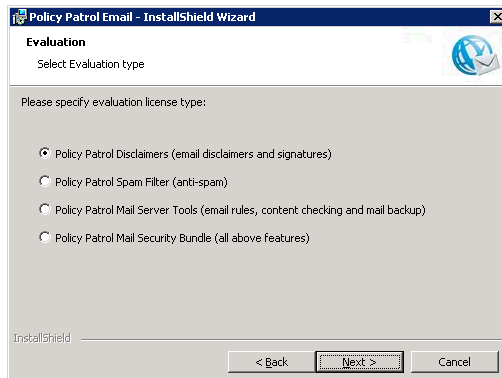
Note that Policy Patrol version 6 is now available in the following editions:



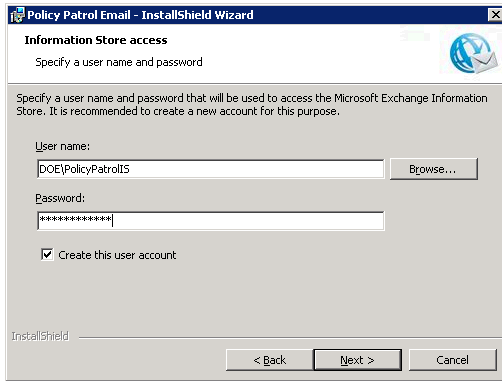
Policy Patrol Mail Server Tools 6 replaces Policy Patrol Archiver and Policy Patrol Zip (newly added features are email rules, reporting, monitoring and optional anti-virus). Policy Patrol Mail Security Bundle 6, formerly Policy Patrol Enterprise, includes all features.

If you are upgrading from Policy Patrol Disclaimers version 4 or 5

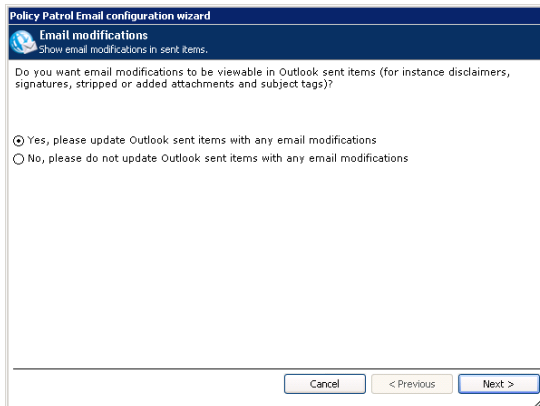
1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.
7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Disclaimers** and click **Next**.



8. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please note that if you want to use an existing account instead of creating a new one, that this account cannot be a member of the Administrators group. If the account does not yet exist, leave the option **Create this user account** enabled so that Policy Patrol will automatically create the user account. When you are ready, click **Next**. Note that this dialog only appears if you are installing Policy Patrol on an Exchange Server 2007, 2003 or 2000 machine.



9. Click **Install** to start copying files.
10. When the installation wizard has finished copying the files, click **Finish**.
11. The Policy Patrol Email Configuration Wizard will start up. Click **Next** in the Welcome screen.
12. Select whether you wish to view email modifications in Outlook Sent Items. If you select **Yes**, any disclaimers or signatures that have been added by Policy Patrol will automatically show in Outlook Sent Items. Click **Next**. Note: This dialog only appears if Policy Patrol is being installed on Exchange Server 2007, 2003 or 2000.



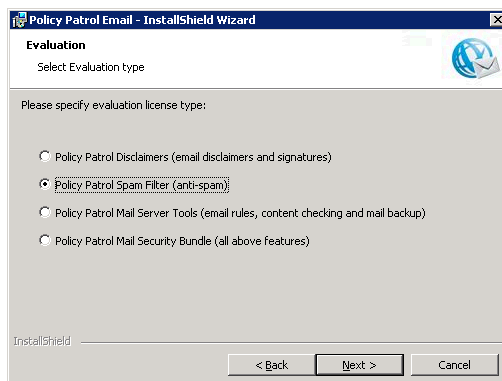
13. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6. The Administration console will start up and your existing configuration will be intact.

New features in Policy Patrol Disclaimers 6:

- Disclaimers and signatures now viewable in Outlook Sent Items
- Preview of AD merge fields when configuring a disclaimer/signature template
- Add a vCard (Business card) to outgoing messages

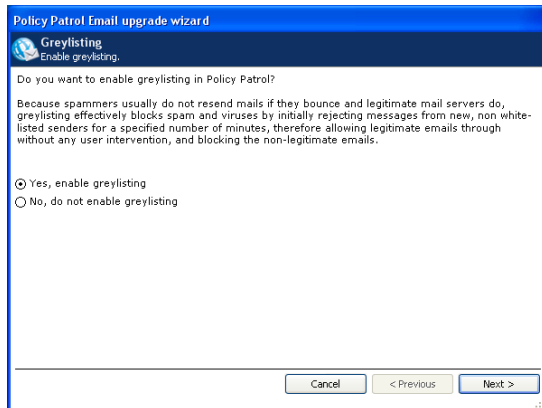
If you are upgrading from Policy Patrol Spam Filter version 5

1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.
7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Spam Filter** and click **Next**.



8. Click **Next** to start copying files.
9. When the installation wizard has finished copying the files, click **Finish**.
10. The upgrade wizard will now start up. Click **Next** in the Welcome screen.
11. If you did not have greylisting enabled: A dialog will pop up asking you to 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. Because most spammers do not resend the message and legitimate mail servers always do, the initial rejection blocks spam mails and automatically

allows legitimate emails through without any user intervention. Select whether you wish to enable greylisting (recommended), and click **Next**.



12. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6.

New features in Policy Patrol Spam Filter 6:

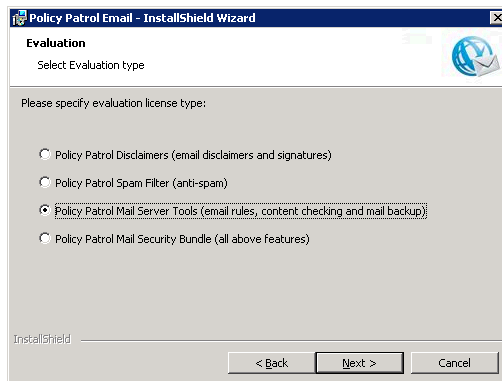
- Block mail from specified countries
- Greylisting improvements (support for IP groups, SQL Server no longer required)
- Import recipients from Sent Items into White list
- Improved Bayesian Filtering (support for more languages)

If you are upgrading from Policy Patrol Archiver/Zip version 4 or 5

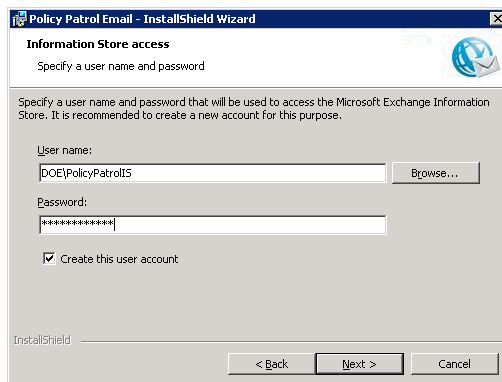
Note that Policy Patrol Archiver 5 and Policy Patrol Zip 5 are being replaced by Policy Patrol Mail Server Tools 6. This means that you will gain access to additional features that were previously not present in Policy Patrol Zip or Policy Patrol Archiver.

1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.

7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Mail Server Tools** and click **Next**.



8. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please note that if you want to use an existing account instead of creating a new one, that this account cannot be a member of the Administrators group. If the account does not yet exist, leave the option **Create this user account** enabled so that Policy Patrol will automatically create the user account. When you are ready, click **Next**. Note that this dialog only appears if you are installing Policy Patrol on an Exchange Server 2007, 2003 or 2000 machine.

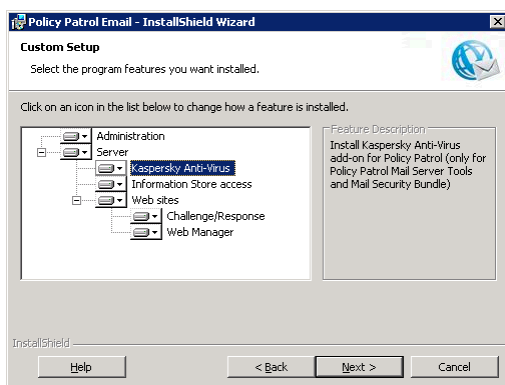


9. Click **Install** to start copying files.
10. When the installation wizard has finished copying the files, click **Finish**.
11. The Policy Patrol Email Configuration Wizard will start up. Click **Next** in the Welcome screen.
12. Select whether you wish to view email modifications in Outlook Sent Items. If you select **Yes**, any modifications (such as subject tags and adding or stripping attachments) that are applied to outgoing emails by Policy Patrol will automatically show in Outlook Sent Items. Click **Next**. Note: This dialog only appears if Policy Patrol is being installed on Exchange Server 2007, 2003 or 2000.

13. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6. The Administration console will start up and your existing configuration will be intact.

Note: In order to content check attachments for words, you need to download and install the appropriate IFilter for the attachment type on the Policy Patrol machine. IFilters can be found on the following page: <http://www.ifilter.org/>.

Note: In order to gain access to all new features you need to install additional components that were not available to you before. Go to **Add or Remove Programs**, select **Policy Patrol Email** and click on **Change**. Click **Next** in the Welcome screen. Select **Modify** and click **Next**. You will be able to select Kaspersky Anti-Virus (note that this does require the purchase of the Kaspersky Anti-Virus add-on) and the Web Manager (this should be installed if you wish to make use of quarantine reports). Select the new components to be installed and click **Next**.



New features in Policy Patrol Mail Server Tools 6:

- Content checking of Office and Pdf attachments (and more)
- Email modifications such as adding/stripping attachments and subject tags will be viewable in Outlook Sent Items.

Policy Patrol Zip users will gain access to the following new features:

- Mail backup (save copies of emails when they are sent or received)
- Email rules (content check emails & attachments, auto-blind copy, remove read/delivery receipts, change Reply To: and From: addresses, and auto-print emails)
- Email monitoring (quarantine emails, receive quarantine reports)
- View Reports on email usage

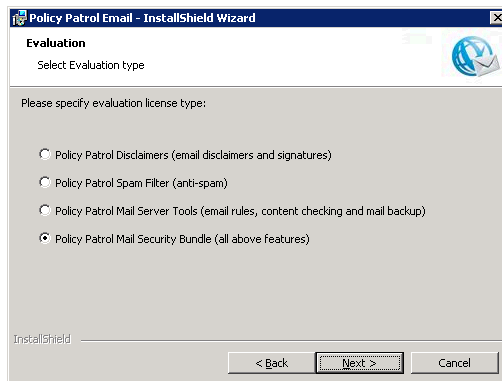
Policy Patrol Archiver users will gain access to the following new features:

- Email rules (content check emails & attachments, auto-blind copy, remove read/delivery receipts, change Reply To: and From: addresses, and auto-print emails)
- Email compression (automatically compress or decompress emails based on conditions)
- Email monitoring (quarantine emails, receive quarantine reports)
- View Reports on email usage

If you are upgrading from Policy Patrol Enterprise version 5

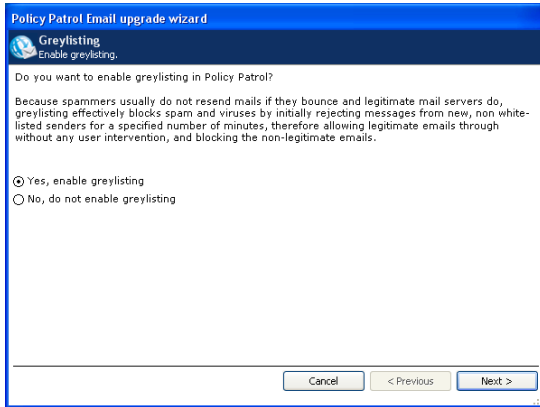
Note that Policy Patrol Enterprise has now been replaced by Policy Patrol Mail Security Bundle. The available features remain the same.

1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.
7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Mail Security Bundle** and click **Next**.

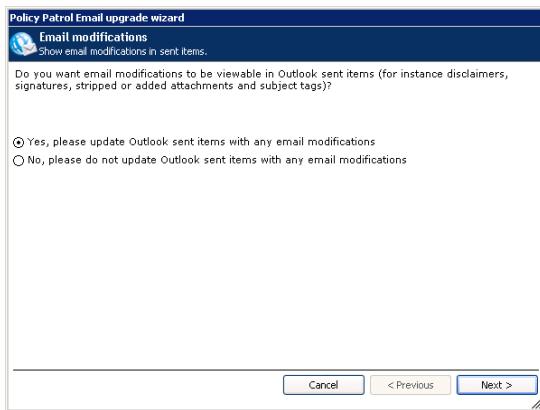


8. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please note that if you want to use an existing account instead of creating a new one, that this account cannot be a member of the Administrators group. If the account does not yet exist, leave the option **Create this user account** enabled so that Policy Patrol will automatically create the user account. When you are ready, click **Next**. Note that this dialog only appears if you are installing Policy Patrol on an Exchange Server 2007, 2003 or 2000 machine.
9. Click **Install** to start copying files.

10. When the installation wizard has finished copying the files, click **Finish**.
11. The upgrade wizard will now start up. Click **Next** in the Welcome screen.
12. If you did not have greylisting enabled: A dialog will pop up asking you to 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. Because most spammers do not resend the message and legitimate mail servers always do, the initial rejection blocks spam mails and automatically allows legitimate emails through without any user intervention. Select whether you wish to enable greylisting (recommended), and click **Next**.



14. Select whether you wish to view email modifications in Outlook Sent Items. If you select **Yes**, any modifications (such as disclaimers, signatures, subject tags and adding or stripping attachments) that are applied to outgoing emails by Policy Patrol will automatically show in Outlook Sent Items. Click **Next**. This dialog only appears if Policy Patrol is being installed on Exchange Server 2007, 2003 or 2000.



13. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6.

Note: In order to content check attachments for words, you need to download and install the appropriate IFilter for the attachment type on the Policy Patrol machine. IFilters can be found on the following page: <http://www.ifilter.org/>.

New features in Policy Patrol Mail Security Bundle 6:

- Block mail from specified countries
- Greylisting improvements (support for IP groups, SQL Server no longer required)
- Import recipients from Sent Items into White list
- Improved Bayesian Filtering (support for more languages)
- Preview of AD merge fields when configuring a disclaimer/signature template
- Add a vCard (Business card) to outgoing messages
- Content checking of Office and Pdf attachments (and more)
- Email modifications such as disclaimers and stripping of attachments are viewable in the Sent Items of Outlook

If you are upgrading from Policy Patrol Enterprise version 4

1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.
7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Mail Security Bundle** and click **Next**.
8. In order to gain access to the Exchange Information Store for updating Outlook Sent Items with email modifications, a new Policy Patrol user account must be created. Specify the User name and Password that Policy Patrol will use. The installation will automatically assign the correct rights. Please note that if you want to use an existing account instead of creating a new one, that this account cannot be a member of the Administrators group. If the account does not yet exist, leave the option **Create this user account** enabled so that Policy Patrol will automatically create the user account. When you are ready, click **Next**. Note that this dialog only appears if you are installing Policy Patrol on an Exchange Server 2007, 2003 or 2000 machine.
9. Select whether you wish to install the Policy Patrol Kaspersky Anti-Virus engine. Click **Next**.
10. Select whether you wish to enable Policy Patrol spam filtering. If you enable spam filtering, Policy Patrol will stop spam out of the box. Click **Next**. If you selected 'No, disable spam filtering', continue to step 12.



11. **If you selected to enable spam filtering:** Select whether you wish to install the challenge/response website. This website is needed if you wish to make use of the challenge/response system that asks new senders to go to a website and verify their email in order for the message to be delivered. Click **Next**.
12. Select whether you wish to install the Policy Patrol Web Manager website. This website is needed if you wish to allow users and Administrators to view quarantined emails via a web browser (required for quarantine reports).
13. Click **Install** to start copying files.
14. When the installation wizard has finished copying the files, click **Finish**. If you did not select to enable spam filtering, your upgrade is now complete.
15. **If you selected to enable spam filtering:** The upgrade wizard will now start up. Click **Next** in the Welcome screen.
16. Policy Patrol 6 now allows you to configure spam categories. Read the information in the dialog and click **Next**.
17. 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**.
18. 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 9.14 '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**.

19. 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**.

20. Select which action to take if the message is considered to be 'Suspected spam'. The options will be the same as listed in point 18.

21. Select any secondary actions to be taken for suspected spam messages. The options will be the same as in point 19.

22. 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.

23. If you did not have greylisting enabled: A dialog will pop up asking you to 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. Because most spammers do not resend the message and legitimate mail servers always do, the initial rejection blocks spam mails and automatically allows legitimate emails through without any user intervention. Select whether you wish to enable greylisting (recommended), and click **Next**.

24. Select whether you wish to view email modifications in Outlook Sent Items. If you select yes, any disclaimers or signatures that have been added by Policy Patrol will automatically show in Outlook Sent Items. Click **Next**. This dialog only appears if Policy Patrol is being installed on Exchange Server 2007, 2003 or 2000.

25. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6.



Note: In order to content check attachments for words, you need to download and install the appropriate IFilter for the attachment type on the Policy Patrol machine. IFilters can be found on the following page: <http://www.ifilter.org/>.

New features in Policy Patrol Enterprise 6:

- Block mail from specified countries
- Greylisting improvements (support for IP groups, SQL Server no longer required)
- Import recipients from Sent Items into White list
- Improved Bayesian Filtering (support for more languages)
- Preview of AD merge fields when configuring a disclaimer/signature template
- Add a vCard (Business card) to outgoing messages
- Content checking of Office and Pdf attachments
- Email modifications such as disclaimers and stripping of attachments are viewable in the Sent Items of Outlook

If you are upgrading from Policy Patrol Spam Filter version 4

1. Download Policy Patrol 6 from <http://www.policypatrol.com/files/policypatrol.exe> (32-bit) or <http://www.policypatrol.com/files/policypatrol2k7.exe> (64-bit). Double-click on **PolicyPatrol.exe**. The Install Program will start up.
2. In the Welcome screen, click **Next**.
3. A notification message will appear asking you whether you wish to upgrade your existing installation to version 6 (your configuration will be kept). Click **Yes**.
4. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
5. Select the installation type. Select **Complete** if you are upgrading Policy Patrol on the server. Select **Administration** if you are upgrading an installation that only includes the Administration console for remote management.
6. 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**.
7. If you did not enter a serial number: A dialog will pop up asking you to select the evaluation license to be installed. Select **Policy Patrol Mail Security Bundle** and click **Next**.
8. 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**.
9. 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).
10. Click **Install** to start copying files.
11. When the installation wizard has finished copying the files, click **Finish**.



12. The upgrade wizard will now start up. Click **Next** in the Welcome screen.
13. Policy Patrol 6 now allows you to configure spam categories. Read the information in the dialog and click **Next**.
14. 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**.
15. 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 9.14 '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**.
16. 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**.

17. Select which action to take if the message is considered to be 'Suspected spam'. The options will be the same as listed in point 15.
18. Select any secondary actions to be taken for suspected spam messages. The options will be the same as in point 16.
19. 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.
20. If you did not have greylisting enabled: A dialog will pop up asking you to 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. Because most spammers do not resend the message and legitimate mail servers always do, the initial rejection blocks spam mails and automatically allows legitimate emails through without any user intervention. Select whether you wish to enable greylisting (recommended), and click **Next**.
21. Click **Finish** in the Configuration complete dialog. You have now successfully upgraded your Policy Patrol installation to version 6.

New features in Policy Patrol Spam Filter 6:

- Block mail from specified countries
- Greylisting improvements (support for IP groups, SQL Server no longer required)
- Import recipients from Sent Items into White list
- Improved Bayesian Filtering (support for more languages)

More information

- ⇒ For more information on how to configure Policy Patrol, please consult the program help or download the product manual from:
http://www.policypatrol.com/download_documentation.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, Ste 210
Campbell, CA 95008
United States
Toll-free: 1-800-921-8215
Phone: (408) 370 9527
Fax: (408) 608 1958
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)20-8328 9830
Fax: +44-(0)20-8711 5771
Sales: sales@reearthsoftware.co.uk
Support: support@reearthsoftware.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.

