

Manual

POLICY PATROL SIGNATURES

FOR OUTLOOK





MANUAL

Policy Patrol Signatures

Version 1

This manual, and the software described in this manual, are copyrighted. No part of this manual or the described software may be copied, reproduced, translated or reduced to any electronic medium or machine-readable form without the prior written consent of Red Earth Software except that you may make one copy of the program solely for back-up purposes.

Policy Patrol® is a registered trademark of Red Earth Software®. All product names referenced in this documentation belong to the respective companies.

Copyright © 2010 by Red Earth Software. All rights reserved.

Contents at a Glance

1	Introduction	5
2	Installation.....	7
3	Creating Email Signatures	13
4	Applying Email Signatures	21
5	Event History.....	24
6	Server Administration	25

Table of Contents

1 Introduction	5	3.4 Deleting an email signature	20
1.1 Policy Patrol Signatures	5	4 Applying Email Signatures	21
1.2 Why do I need centralized Outlook signatures?5		4.1 Selecting email signatures.....	21
1.3 Conventions.....	5	4.2 Applying changes	22
2 Installation.....	7	4.3 Auto licensing	22
2.1 Policy Patrol Signatures components	7	5 Event History	24
2.2 System requirements	7	5.1 Events	24
2.3 Installing Policy Patrol Signatures Server components	8	6 Server Administration.....	25
2.4 Installing the Outlook client	9	6.1 Connection	25
3 Creating Email Signatures	13	6.2 User security	25
3.1 Create a new email signature	13	6.2.1 User access rights.....	26
3.2 User Fields.....	18	6.2.2 Component access rights	27
3.2.1 Force upper case or lower case	19	6.3 Licensing.....	28
3.2.2 Adding more Active Directory fields	19	6.4 System configuration.....	28
3.3 Editing an email signature	20	6.5 System Parameters	29

Introduction

Policy Patrol Signatures for Outlook allows you to centrally manage your Outlook signatures and ensure a uniform corporate appearance as well as utilize your emails as marketing tools.

1.1 Policy Patrol Signatures

With Policy Patrol Signatures for Outlook you can:

- Add professional email signatures & disclaimers
- Control Outlook signatures centrally
- Ensure uniform corporate email 'look'
- Utilize emails as marketing tools
- No Exchange Server needed
- Works with Microsoft Outlook and Outlook Web Access

1.2 Why do I need centralized Outlook signatures?

By controlling and managing your company's Outlook signatures centrally, you can ensure that the company portrays a uniform corporate email look and that emails include the necessary legal disclaimers. This avoids users from having to configure signatures themselves, which can lead to an inconsistent corporate email image and a possible legal loophole. Also, by centrally managing your signatures, it is a simple process to update a signature with a short marketing message regarding an upcoming special or event. This allows you to make full use of emails as marketing tools.

1.3 Conventions

Conventions used in this manual:

- **Bold text** is used to signify a selection or button, for instance the **Deliver** button, or the option **Move to Folder**.



- Courier font is used to signify text that must be entered in the program, for instance `enter price list` and click **Search** to search for the term.
- Paragraph and chapter names are listed in between parentheses, for instance for instructions on how to install Policy Patrol, consult chapter 2 'Installation'.
- Keys are displayed in capitals and in between brackets, such as [CAPS], [TAB] or [DELETE].
- Throughout the manual there are Tips, Info and Notes that contain useful information:

Note type:	Contains:
Tip	Useful information to get the best out of Policy Patrol
Info	More in-depth, background information
Note	Important notes that you should be aware of

Installation

This chapter describes how to install the different server and client components of Policy Patrol Signatures for Outlook and the different system requirements for the server and client.

2.1 Policy Patrol Signatures components

The Policy Patrol Signatures installation consists of three server components that can all be installed on the same machine or on different machines:

- **Administration Console:** The Administration Console is used to configure the program. This component can be installed on any machine. If you wish to configure Policy Patrol from multiple locations, you can install the Administration Console on multiple machines and connect to the same Database Server.
- **Database Server:** The Database Server contains the configuration files. This component can be installed on any machine.
- **Exchange Server Client:** The Exchange Server client is required if you wish to apply Signatures to Microsoft Outlook Web Access. This component needs to be installed on an Exchange Server with the mailbox role. If you have multiple Exchange Servers, you will need to install this component on every Exchange Server with the mailbox role.

Policy Patrol also includes one client component:

1. **Outlook Client:** This component needs to be installed on every client machine for which you wish to control the email signatures in Microsoft Outlook. This installation can be pushed out to the clients through a group policy. Note that you do not need to install the Outlook Client if only Microsoft Outlook Web Access will be used.

2.2 System requirements

The following programs must exist in the network:

- Active Directory

- If using Microsoft Outlook Web Access: Exchange Server 2003, 2007 or 2010
- Windows Operating System on the Policy Patrol server machine
- Microsoft .NET Framework 2.0 on the Policy Patrol server machine

The following programs must exist on the client:

- Microsoft Outlook 2002/XP, 2003, 2007, 2010 and/or Outlook Web Access
- Windows Operating System

2.3 Installing Policy Patrol Signatures Server components

If you have a local Exchange Server: It is easiest to install all components on the Exchange Server (with mailbox role). If you prefer not to install all the components on the Exchange Server machine, you can install the Exchange Server Client on the Exchange Server only, and install the rest of the components on another machine. Note that the Exchange Server Client is only needed if using Microsoft Outlook Web Access.

If you do not have a local Exchange Server: You only need to install the Administration console and Database Server, which can be installed on any machine.

To install Policy Patrol Signatures, please follow the next steps:

1. Double-click on **PPSO.exe**. The Install Program will start up. If you do not have Microsoft .NET Framework installed, the Policy Patrol installation program will install it for you.
2. In the Welcome Screen, click **Next**.
3. Read the License Agreement and select **I accept the terms in the license agreement** and click **Next**.
4. Enter your User name and Organization name. Click **Next**.
5. Select which components you wish to install. You can select from **Administration** (Administration console), **Database Server** (configuration files) and **Exchange Server Client** (connects with Microsoft Outlook Web Access. The first two components can be installed on any machine, the Exchange Server Client however must be installed on an Exchange Server with a mailbox role. When you are ready, click **Next**.
6. Enter your serial number or select **Install a 30-day evaluation license**. Click **Next**.
7. **Only if you are installing the Exchange Server Client:** In order to gain access to the Outlook Web Access signatures, 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**.

8. Click **Install** to start installing the program.
9. When the installation is completed, click **Finish**.

Note

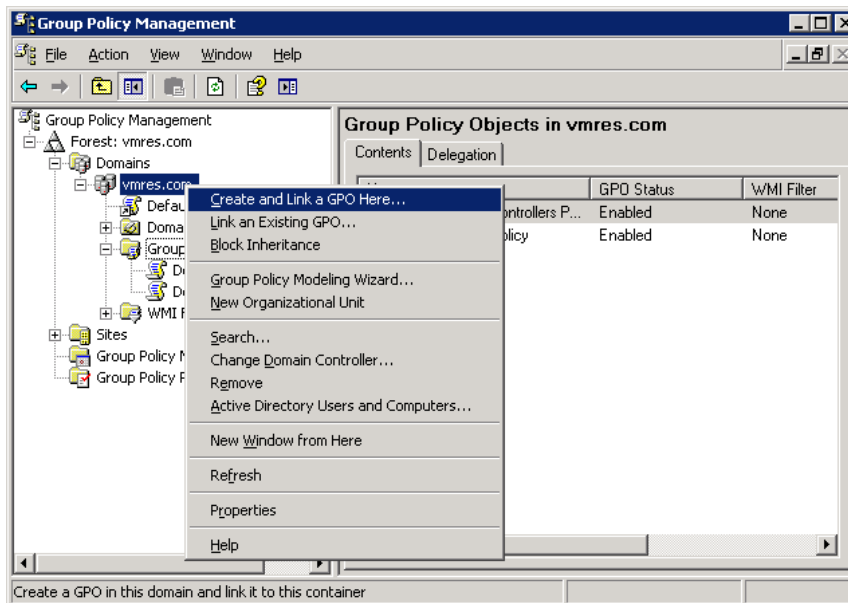
There is no need to reboot the server after installation and no services need to be restarted.

2.4 Installing the Outlook client

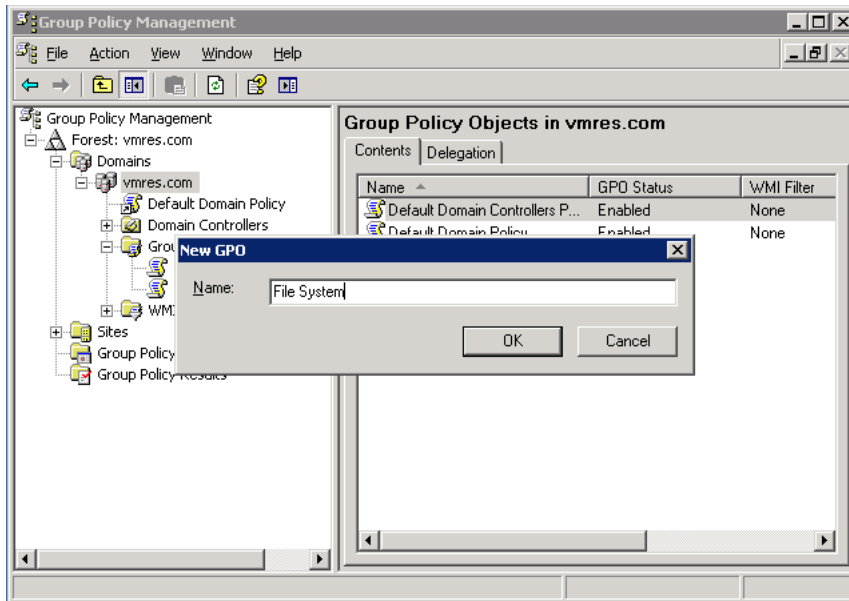
The Policy Patrol Signatures Outlook client must be installed on each machine with Outlook that needs to have the signature updated.

To deploy the Outlook Client to multiple clients in one go, you must create a Group Policy Object. Follow the next steps to create a GPO:

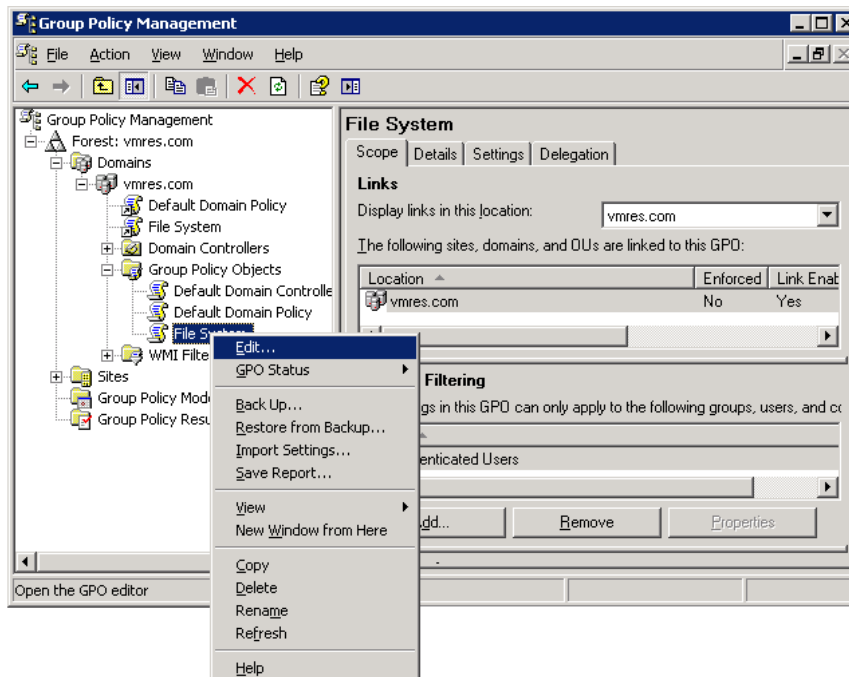
1. Create a shared folder with the .msi files on the Server Domain.
2. Open the Group Policy Management Console, right-click the domain and select **Create and Link a GPO here**.



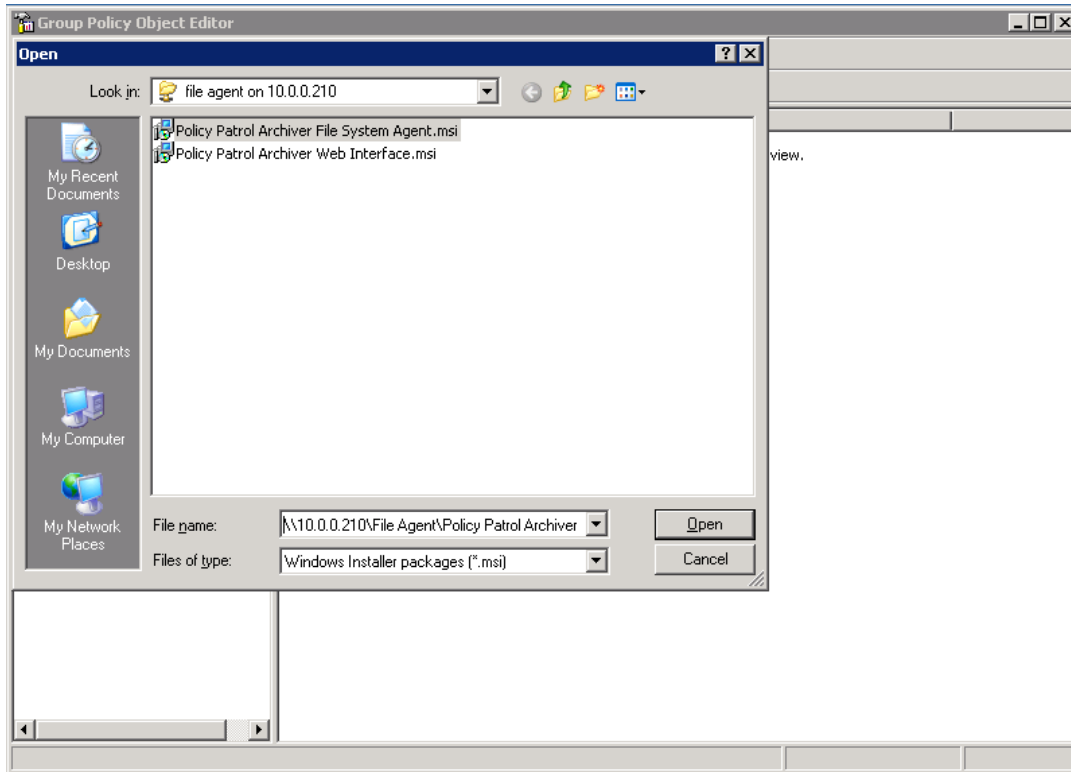
3. Enter a name for the new GPO and click **OK**.



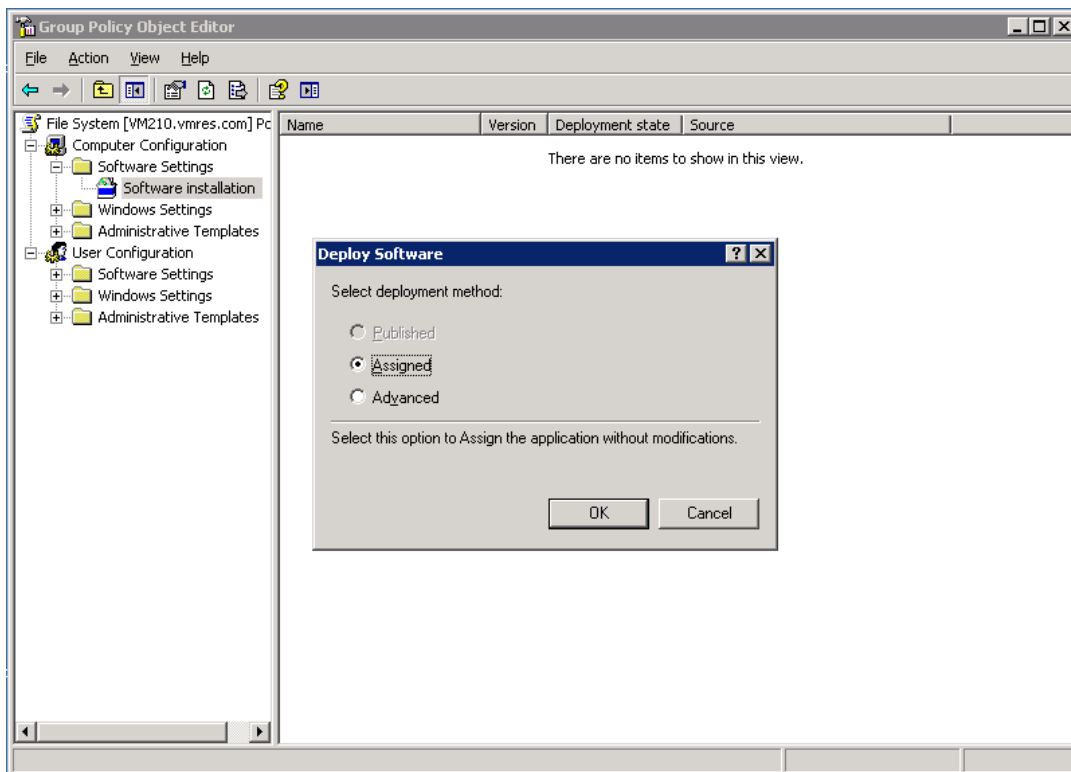
4. Go to Group Policy Objects, right-click on the object that you just created and select **Edit**.



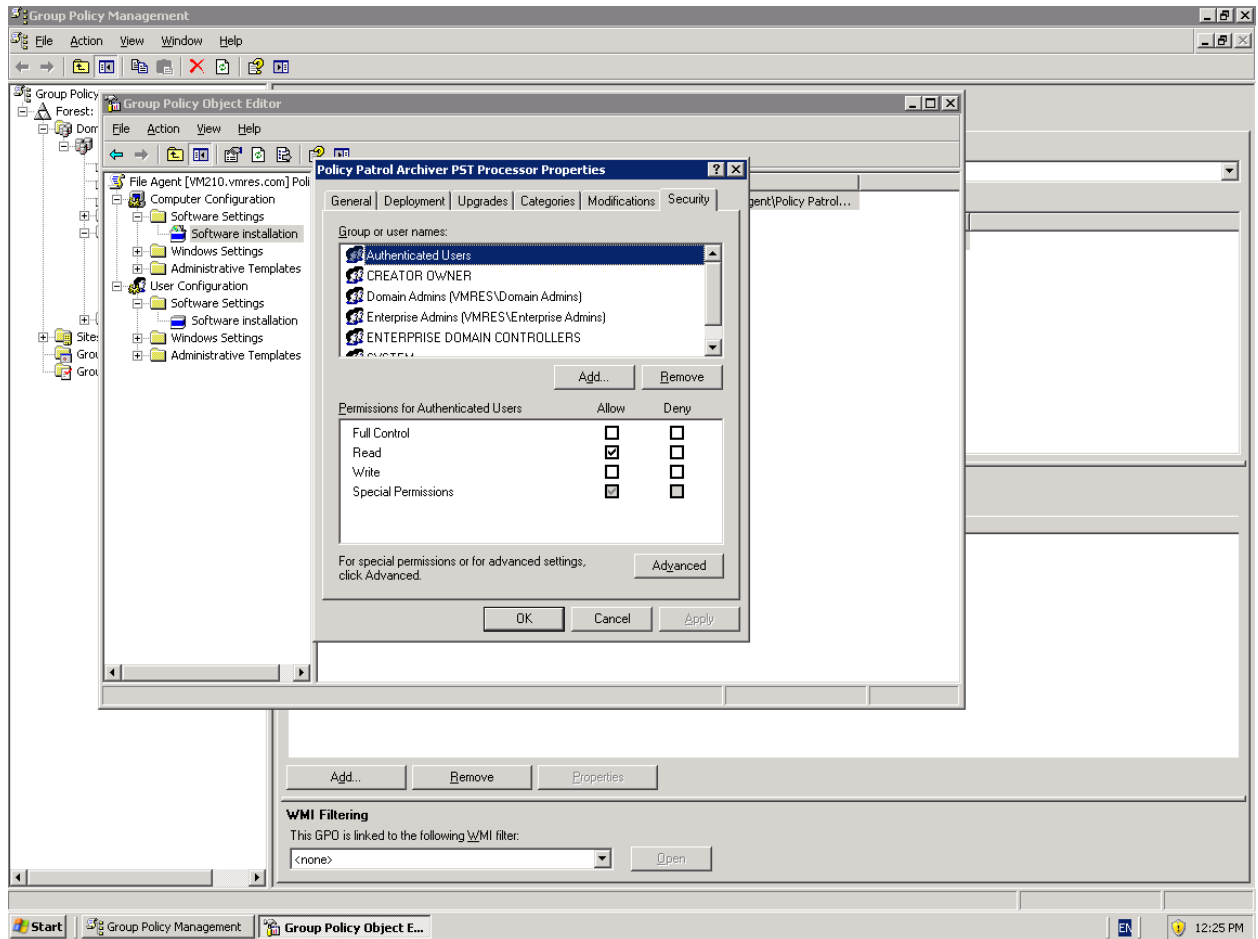
5. Go to **Computer Configuration > Software Settings**. Right-click on **Software Installation** and select **New > Package**.
6. Enter the path for the .msi file, e.g. \\server IP\<>folder name>\Policy Patrol Archiver File System Agent.msi and click **Open**.



7. Select **Assigned** as the deployment method and click **OK**.



- You can check the Permissions by right-clicking on the Software installation package you just created and selecting **Properties** > **Security** Tab.




- Restart the machine. Wait for a while until the machines appear on the web manager site. The installations will start automatically.

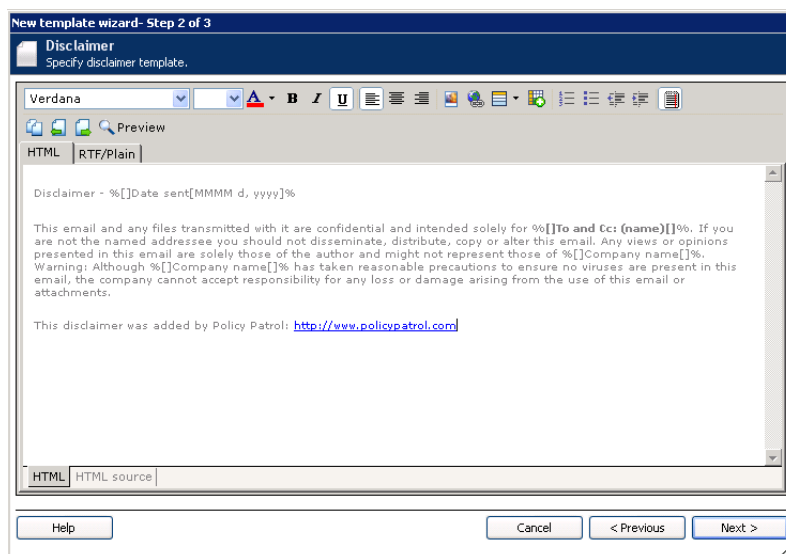
Creating Email Signatures


This chapter explains how to create email signatures and disclaimers that will be used in Outlook and Outlook Web Access.

3.1 Create a new email signature

To create a new email signature, select the **Signatures** node, and click on the **New** button. The New email signature wizard will start up:

1. Click **Next** in the Welcome screen.
2. Enter the email signature text. You can enter the text in two different formats: HTML and RTF/plain text. The text in the HTML tab will be added to HTML messages, and the text in the RTF/plain text tab will be added to rich text and plain text messages. You can apply formatting in the RTF/plain text tab, but this will only apply to rich text messages. The formatting will be removed for plain text messages. To copy text from the HTML tab to the RTF/Plain tab (or vice versa), click on the button **Copy to..** .

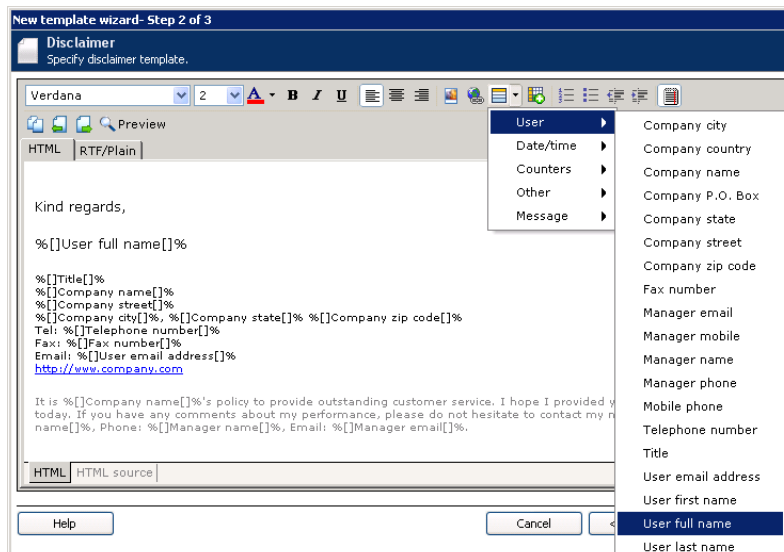



 **Note**

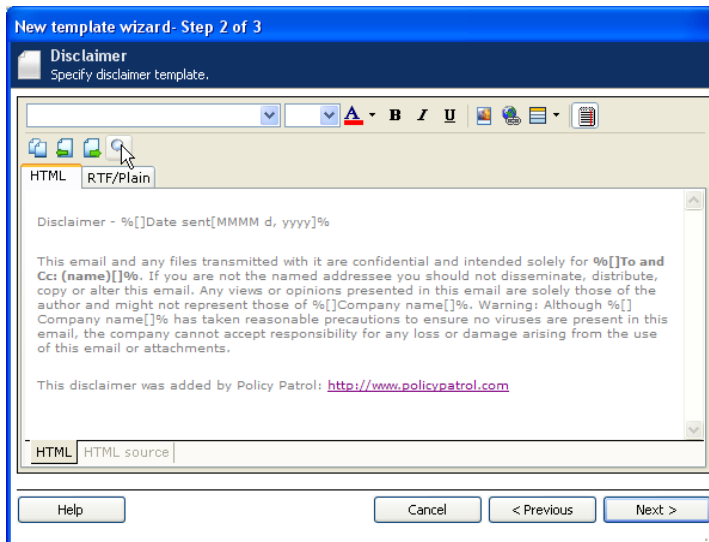
If you don't enter any text in the HTML tab, there will be no signature added to HTML messages. If you don't enter any text in the RTF/plain text tab, there will be no signature added to rich and plain text emails. Because some email clients can only read plain text, you must always enter a disclaimer text in the RTF/plain text tab, even if you only send out HTML messages. However, you only need to enter your text once, since you can copy and paste the text from one tab to another by clicking on the **Copy to..** button.

From the toolbar, you can select font, size, color, bold, italic, and underlined. You can add bulleted lists, numbered lists, indent and align text.

You can insert merge fields by clicking on the **Insert Field** icon and selecting the relevant field. For more information on the available fields, see the 'Fields' paragraph in this chapter.



If you are using fields in your disclaimer or signature, Policy Patrol includes a preview option so that you can check whether the merge fields will be replaced correctly. To see the preview, click on the **Preview** icon  in the toolbar. A dialog will pop up asking you to select a user. Select a user and click **OK**. You will now see the disclaimer/signature with Active Directory merge fields replaced by the Active Directory information for the user. Message fields will be replaced with test data. In case a merge field is still showing in the preview, this means that the field has not been entered correctly. To go back to the normal view, click on the Preview icon again.



Tip

If you are not sure whether a field will exist in every instance, you can specify a **field prefix** that will only be entered if the field is replaced. For instance, if you wish to include a mobile phone number for the user, but not every user has one, you could enter the prefix in between the first square brackets of the field as follows: %[]Prefix]Field name[]%. For instance: %[]Mobile:]Mobile phone[]%. This will mean that the text 'Mobile:' will only be added if the user has a mobile phone number in the user's Active Directory, Exchange 5.5 or Lotus Domino properties.


To **avoid an empty line** when a field does not exist you must enter \n in the field prefix %[]% (this stands for a line break and since it is entered in the prefix it will only be applied if there is a field value). For instance if you want the user name to appear, followed by the title field (if it exists), you can enter the following: %[]User full name[]%[]\n]Title[]%. If you want to combine it with a field prefix, you must enter this as follows: %[]User full name[]%[]\nTitle:]Title[]%...

It is also possible to specify a **default value** in case a field does not exist. For instance, if a user does not have a mobile phone number, you could enter 'Not applicable'. To do this, you must enter the default value in between the last square brackets of the field as follows: %[]Field name[Default value]%. For example: %[]Mobile phone[Not applicable]%.

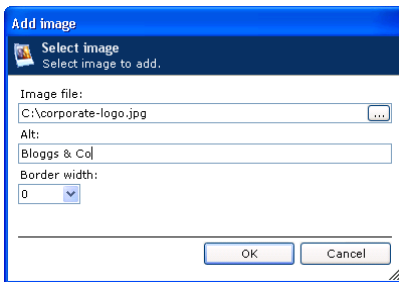
Note that you cannot enter fields as a prefix or default value.

You can import texts from .txt and .html documents by clicking on the **Import** button in the toolbar. Similarly, you can export the text to a .txt or .html file by clicking the **Export** button in the toolbar.

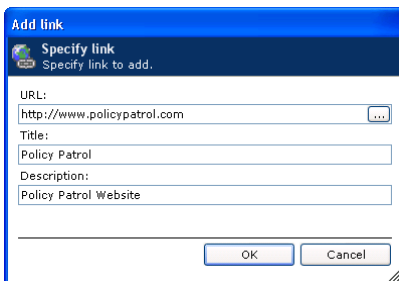
You can insert gif and jpeg pictures by clicking on the **Insert image** button. In **Image file**, enter the path to the picture. Note that this picture must be located on the local drive. Alternatively you can enter the URL to an image on a website. In **Alt**, enter the text that you wish to appear as a tool tip. If you want a border to be applied to the image, set a border width.

 Note

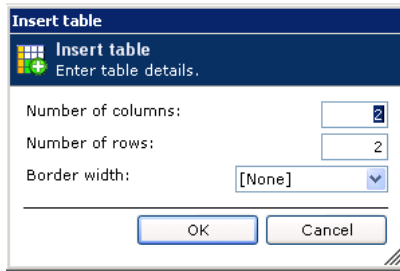
You can only embed images (i.e. use the **Insert Image** option) for Microsoft Outlook signatures. If you are using Microsoft Outlook Web Access signatures, you must include a link to the online image by using the **Insert link** option described below.



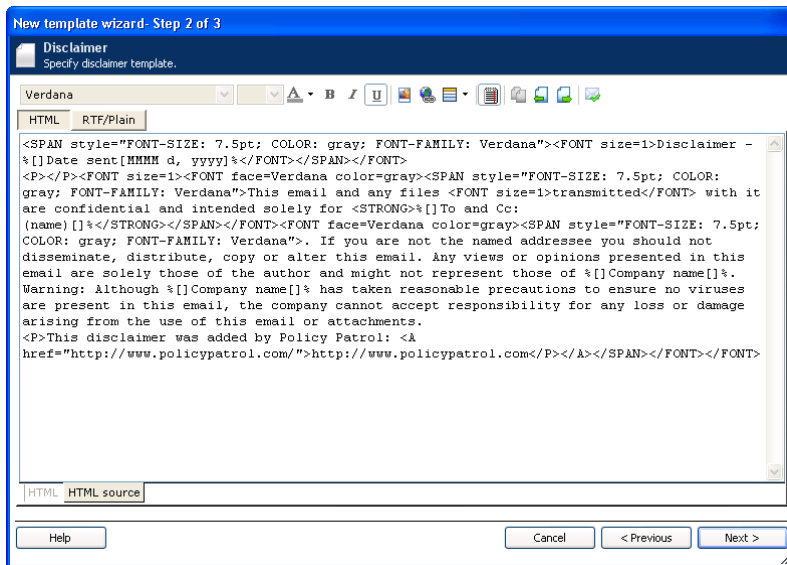
To add a link, click on the **Insert link** button. In **URL:** enter the URL to link to. Enter the text to be displayed in **Title** and enter the description in **Description**.



You can insert a table by clicking on the **Insert table** icon in the toolbar. You can select the number of columns and rows and the border width. Tip: Even if you do not intend to show any borders, you can add the Table with a border first, and then later change the border to 0 in the HTML Code (click on HTML Source tab to see the HTML code); For instance if you configured the table to have a border width of 1, you will see `<TABLE style="BORDER-COLLAPSE: collapse" border=1` in the HTML code. When you have finished designing your text and images in the table, change 1 to 0: `<TABLE style="BORDER-COLLAPSE: collapse" border=0`. When you click back on the HTML tab, the table border will be gone.

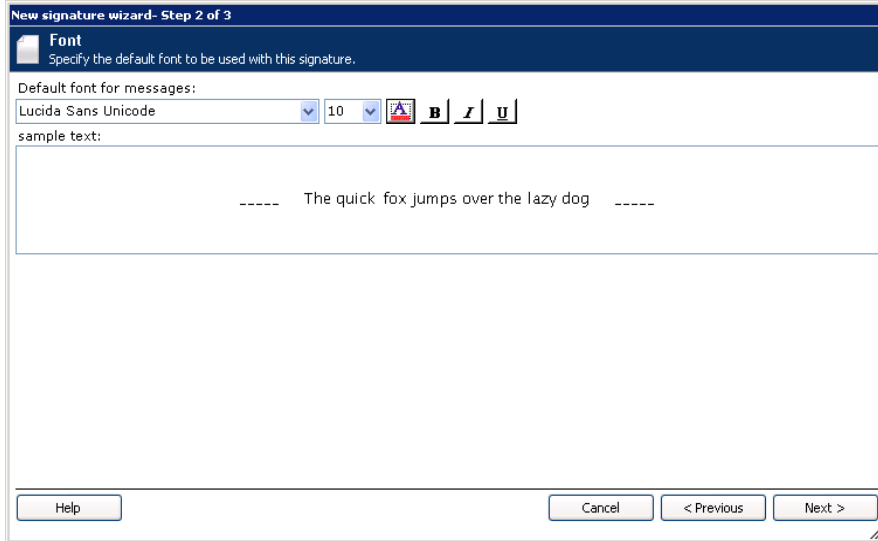


In the HTML tab you can directly edit the HTML source by clicking on **HTML source** at the bottom of the dialog, for instance to add tables or bullets.



When you are ready designing your email signature, click **Next**.

- Now you can select the Default font to be used for messages. You can select font type, font size, color, bold, italics and underlined. A preview of the selected font is shown. When ready, click **Next**.



Note

If you select the Signature template for new messages (see Chapter 4), the font selection will be applied to new messages. If you select the Signature template for replies/forwards, the font selection will be applied to replies and forwards.

4. Enter the signature name and a description. Click **Finish** to create the Signature.

3.2 User Fields

The user fields are taken from the user's properties in Active Directory. Below is a list of the user fields that are included by default. You can add more (or remove) fields by going to **Signatures > Active Directory fields**. More information on how to do this can be found below.

Default field	Description
Company name	Company's name
Fax number	User's fax number
Manager name	Name of user's manager
Manager email	Email address of user's manager
Manager phone	Phone number of user's manager
Manager mobile	Mobile number of user's manager
Telephone number	User's telephone number
Title	User's title
Email Address	User's email address
User first name	User's first name

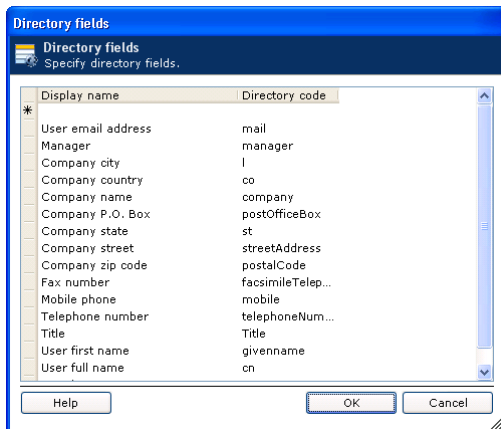
User full name	User's full name
User last name	User's last name
Company street	Company's street address
Company P.O. Box	Company P.O. Box
Company city	Company's city
Company state	Company's state
Company zip code	Company's zip code
Company country	Company's country
Mobile phone	User's mobile phone
User initials	User's initials
Website URL	Company website URL

3.2.1 Force upper case or lower case

If you wish certain fields to be displayed in upper case or lower case, you can add a ^ or a ~ character to a field prefix, where ^ converts to UPPER CASE and ~ converts to lower case. For example if you want the user name to appear in upper case, you can enter ^ in the prefix as follows: %[^]User first name[%]. This will convert the value of the user name to uppercase, i.e. USER NAME. If you wish to add the user name in lower case, you can enter ~ in the field prefix as follows: %[~]User first name[%]. This will convert the value of this field to lower case, i.e. user name.

3.2.2 Adding more Active Directory fields

Directory fields can be configured from **Signatures > Active Directory Fields**. Policy Patrol already includes a number of merge fields taken from Active Directory. You can add more fields by entering the **Display name** (this is the name that will be displayed in Policy Patrol) and the **Directory code** (this is the actual code for the field in the Active Directory – note that these codes are case sensitive). Click **OK**. You will now see the new field(s) when clicking on the **Insert field** button in the toolbar.



To find the correct Active Directory code, follow the next steps:

1. Go to **Start > Run**.
2. Enter `adsiedit.msc` and click **OK**.
3. Expand **Domain**, expand the folder **DC** and expand folder **CN=Users**.
4. Right-click on the user and select **Properties**.
5. Scroll down the list to find the attribute that you want to add, for instance for the company web site, the attribute is 'wWWHomePage'. Enter the attribute name as the Directory code in Policy Patrol. Important: the attributes are case sensitive.

3.3 Editing an email signature

To edit an email signature, select the email signature and click on the **Edit** button. A dialog will appear with the email signature text and default font selection. When you are ready making changes, click **OK**.

3.4 Deleting an email signature

You can delete an email signature by selecting the signature in the list, and selecting **Delete**. Remember not to delete a signature if it is selected for a user.

Applying Email Signatures

Policy Patrol Signatures can apply email signatures and default fonts for your entire organization, Active Directory Groups and individual users. In this Chapter we describe how to make your signature selections.

4.1 Selecting email signatures

To select which signatures should apply to which users, go to the **Users** node in Policy Patrol Signatures. The company domain will be listed.

Apply global email signature: If you want to apply the same signatures for everyone in your domain, you only need to select a signature in the 'Signature New Message' column, and a signature in the 'Signature Replies/Forwards' column. The selections will automatically be propagated to any sub groups and user members. The signature selection that is being propagated will appear in **bold**.

Note

Note that for Outlook Web Access, only the signature that is selected in the 'Signature New Message' column is used, since this is the only option available in Outlook Web Access.

Apply signature per group: If you want to apply different signatures for different Active Directory groups, click on the plus sign next to the company domain and browse to the groups for which you wish to configure an email signature. Select the relevant email signatures per group. The selections will automatically be propagated to any sub groups and user members. The signature selection that is being propagated will appear in **bold**.

Apply signature per individual user: If you want to apply different signatures for different users, click on the plus sign next to the company domain and browse to the individual users for which you wish to configure an email signature. Select the relevant email signatures per user.

Global signature with some group and individual signatures: A combination of all the above configurations is also possible. For instance, if you want to apply one global signature,

apart from one group and 5 individual users, you would first select the signature for the entire domain, then browse to the relevant group and change the signature selection. Then you would browse to the individual users and change their signature selection.

4.2 Applying changes

When you have made any email signature selection changes, you must apply them by clicking on **Apply**.

If you want Policy Patrol to warn if there are multiple signature selections for the same user, check the option **Check for multiple signature selections**. If you do not check for multiple signature selections and a user has multiple signatures configured (e.g. if a user is a member of different groups and each group has a different signature selected), Policy Patrol will randomly apply one of the selected signatures.

If you want to update the Outlook Web Access signatures, check the box **Update Outlook Web Access signatures**. Note that for Outlook Web Access, only the signature that is selected in the 'Signature New Message' column is used, since this is the only option available in Outlook Web Access.

Note

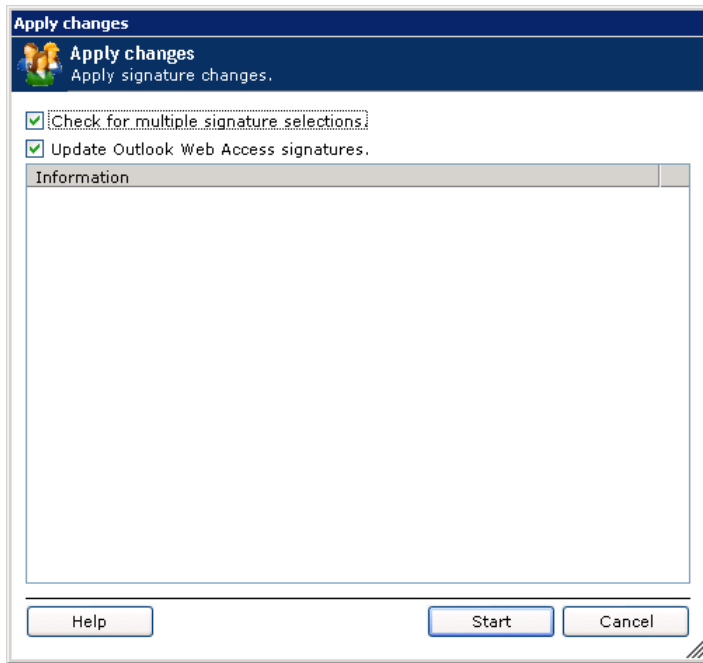
To update signatures in Outlook Web Access, the Exchange Server Client must be installed on Exchange Server 2003, 2007 or 2010. For more information on how to install the Exchange Server Client, please consult Chapter 2.

Click **Start** to begin the update process. Depending on the email client being used, the updates will take effect within the following time frames:

- For Outlook users, the update will take effect within 5 minutes or less (this is the interval that Policy Patrol checks for updates).
- For Outlook Web Access on Exchange 2007 and Exchange 2010 the change will be instant.
- For Outlook Web Access on Exchange 2003, the update will take effect after the user logs on.

4.3 Auto licensing

If you want to automatically apply the email signature selection to new users in your Active Directory, you can check the box **Auto license** next to the domain (for the entire company) or Active Directory group (only for new members of that group) in the User list. If the auto license option is checked, Policy Patrol will automatically apply this signature selection for any new users added to this group.



Event History

The Event History shows a list of events that occurred including the updating of signature texts and selections as well as pushing out signatures to the various clients.

5.1 Events

The Event History lists the following events:

- When the Outlook client queries a new signature
- When a change in the configuration is applied
- When an Outlook Web Access 2003 signature is applied

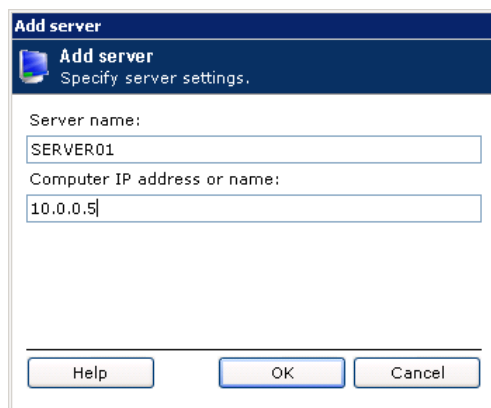
Server Administration

Policy Patrol includes some server options & settings that can be configured from the Policy Patrol server node(s), including user security, system configuration and system parameters.

6.1 Connection

In this section you can connect to the server configuration. Select the server you want to connect to in the left column, and click on **Connect**. By selecting the option **Auto connect to this server when opening Policy Patrol Administration**, the Policy Patrol Administration Console will automatically connect to this server.

It is possible to add several configurations to the same Administration console. To add more servers go to the **Policy Patrol** node and click on **Add Server**. Enter the Server name and IP address. The server will now appear in the left column.



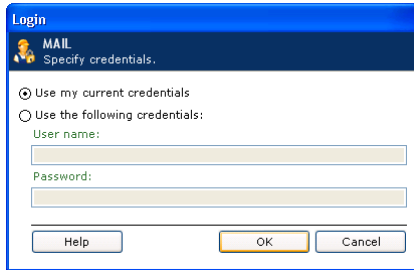
The screenshot shows a Windows-style dialog box titled "Add server" with the subtitle "Specify server settings.". It contains two text input fields. The first field is labeled "Server name:" and contains the text "SERVER01". The second field is labeled "Computer IP address or name:" and contains the text "10.0.0.5". At the bottom of the dialog, there are three buttons: "Help", "OK", and "Cancel".

6.2 User security

In User security you can give selected users access to the Policy Patrol Administration console and grant them certain permissions within the Administrations console. Policy Patrol user security is implemented at three levels; user access rights, component rights and folder rights.

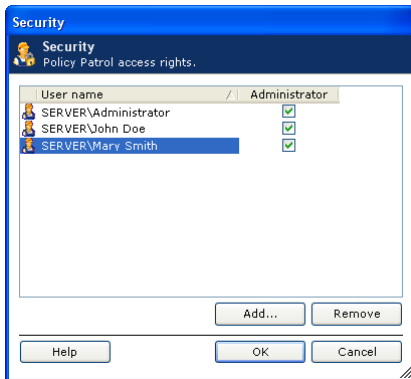
6.2.1 User access rights

When a user connects to a Policy Patrol server, they will be asked for log on credentials. The user can log on with the current credentials or specify another user name and password. Policy Patrol will then check these credentials to see if the user is permitted to access the Policy Patrol Administration console.



By default only the members of the Administrator group are allowed to connect to Policy Patrol installations. To define which users have access rights, follow the next steps:

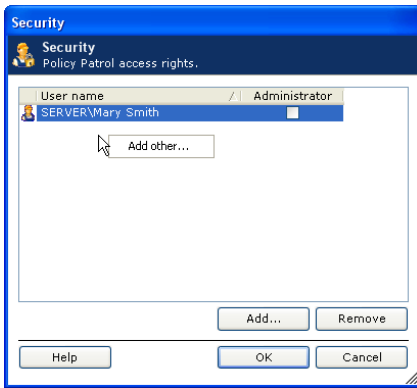
1. Select **<server name>**, expand **Security** and click on **User security**.



2. To add a user with access rights to Policy Patrol, click on **Add**. Select the users you wish to add and click **OK**. To remove a user from the list, select the user and click **Remove**.
3. To give the user Administrator rights, select the user and tick the check box **Administrator rights**. The user icon will now include a small lock to indicate that it has administrative rights. Policy Patrol Administrators have full access to all components and folders and cannot be denied any permissions. You must make at least one user an Administrator so that this user will always be able to access all options in Policy Patrol.

Note

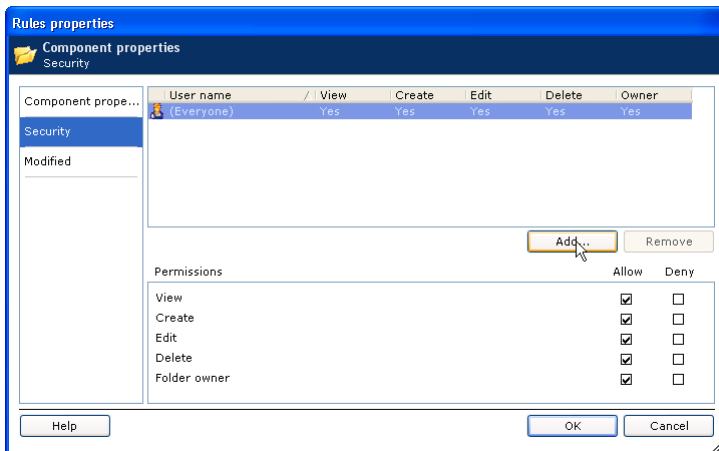
If you wish to grant a user from another domain access rights, you can right-click in the Security list and select **Add other**. This will allow you to specify a user by entering the user name in DOMAIN\Username format.



6.2.2 Component access rights

Now that you have set the access rights to the Administration console, you can specify which Policy Patrol components (i.e. tree nodes) each user has access to. By default, each user has access to all components. To change the access rights for a certain component, follow the next steps:

1. Right-click the component (for instance **Signatures**) and choose **Component properties...**



2. Go to the **Security** tab. By default the (Everyone) group has full access to the component. To change permissions, select the group and change the Allow/Deny permissions. The following rights can be applied:

Right	Description
View	View items
Create	Create new items
Edit	Edit existing items
Delete	Delete items
Folder owner	Change folder permissions

If you only wish certain users to have rights to the component, click on **Add** and select the user(s) with the permissions. Select **Allow** or **Deny** for the relevant rights. Then select **Everyone** and click **Deny** for all rights.

If you wish all users to have access to the component apart from a couple of exceptions, click on **Add** and select the users to be denied access. Select the user(s) and tick the **Deny** check boxes.

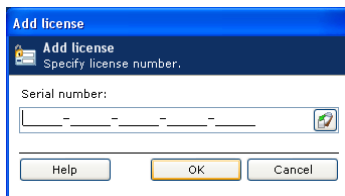
A Folder owner has the right to change the component permissions for the component. Therefore, if you wish to deny permissions for a user, you must also select **Deny** for the **Folder owner** right.

Remember that each component needs to have at least one Folder owner and that Administrators cannot be denied any permissions.

When you have finished editing permissions, click **OK**.

6.3 Licensing

To enter your serial number in Policy Patrol, select **Security** > **Licenses** from the menu. Click **Add**. Now enter your serial number. If you have received your serial number via email, you can copy it and click on the 'Paste' button. The number will automatically be pasted into the dialog. Click **OK** to add the license.



To find out how many user licenses you are currently using, go to the **Users** node. In the top right corner it will list the number of users that are licensed (i.e. configured to use a signature) as follows: x out of x licenses used. For example, if you have configured signatures for 15 users and you have a license for 25 users, it would read: 15 out of 25 licenses used.

6.4 System configuration

System configuration options are found in <server name> > **Advanced** > **System configuration**.

In the System Notifications tab you can specify the options for system notifications. In the From: field, enter the sender of the email. In the To:, Cc: and Bcc: fields, enter the recipients for the system notifications. For internal recipients you can also click on ... and select the recipient from the user list. The recipient addresses entered here will also be taken as the Administrator address(es) when sending notification messages.

The Modified tab displays when and who last updated the component.

6.5 System Parameters

System parameters are found in **<server name> > Advanced > System parameters**. Policy Patrol system parameters are similar to registry keys and must not be changed unless you are asked to do so by Policy Patrol technical support staff.

Policy Patrol® is a registered trademark of Red Earth Software®. Copyright © 2001- 2010 by Red Earth Software.

Index

A

Active Directory · 15, 18
Administrator address(es) · 27

D

Default value · 15
Disclaimer · 13, 14

E

Exchange 5.5 · 15
Export · 15

F

Field prefix · 15

I

Import · 15
Insert Field · 14
Insert image · 16

Internal messages · 27

L

Licensing · 7

P

Permissions · 25, 26, 27
Plain text · 13, 14

R

RTF/plain text · 13

S

System parameters · 28