

1.	CONFIGURATION OF E-POLITE SERVER.....	1
	Configuration.....	1
	Rules.....	5
	Managing default schedules.....	7
	Managing Source and Target objects.....	7
	Queue management.....	8
	Activity Log.....	8
	Licence.....	9
2.	CONTROL of SERVICES.....	9
3.	BACKUP copy.....	14
4.	Configuration of e mail servers.....	14
	If you have Microsoft Exchange Server 4/5/5.5:.....	14
	If you have the Microsoft Exchange Server 2000/2003:.....	15
	If you have the Lotus Notes:.....	15
	If you a have a SMTP/POP3 mail Server:.....	15
5.	DNS CONFIGURATION.....	15
6.	GLOSARIO.....	15

1. CONFIGURATION OF E-POLITE SERVER

Once the installation is completed you will find a shortcut of the program e-Polite.

When you start the program the control panel of e-Polite will pop up asking you to enter the username and password you created during the installation.

Select on the left menu the option **configuration**.

When you finish the configuration you should start the services by clicking the icon on the tool bar. Services will be automatically installed at the moment you start them for the first time.

Once the program is installed it will be possible to change the configuration by connecting remotely to the server from any network linked computer by using the following path:

<http://192.168.0.100/e-polite/>

The IP address must correspond to the IP address of the Server where the e-Polite is installed.

Configuration

General

- **Activity Mode:** You can select the activity mode of this software:

SEVERE: only the authorized e mails are delivered, it means messages sent to addresses that are on the "Authorized e mail Addresses Database".

MODERATE: it blocks the unauthorized messages; it means that all the e mails are delivered except of the e mails belonging to the "Revoked e mail Addresses Database".

- **Sending Mode:** you can choose to resolve e mails through DNS or route all outgoing e mails to another SMTP server.

In case of routing, if the host requests to start session you will click the start session button and enter the username and password.

- **External address:** you have to enter the public IP address of the e-Polite Server, where the automatic authorization and revocation messages are generated.
- **Port:** it's the port from which the Server will catch all the revocation. If you do not fill this field all revocations will be published through the port number 80. If you change the port for the publication of these services, for example port number 5080, some addressee may not access the revocation page because of

firewalls in their network.

- **HOST NAME:** it is the name of the e-mail Server in FQDN (Fully Qualified Domain Name) format which will appear on the header of all the e mails. You have to enter the name of the e-Polite server in your e-mail domain dns server in order to avoid that delivery servers detect them as spam. If you leave this field blank the entire name of the computer will be used.
- **Maximum e mail size:** you should enter the maximum size of messages, expressed in Kb, allowed to pass through the e-Polite. If you do not want to restrict it, chose a high level (not recommended). The default size is 10.000Kb.
- **Maximum number of processes:** it is maximum number of messages that the e-Polite can receive at the same time. In the Enterprise edition the default number is 25.
- **e-mail administrator:** you have to enter an existing e mail address where all the software requests and warning will be sent.
- **Log Detail:** It informs you about the activity Log.
- **Time of storage:** you can specify the maximum time of storage of the log. If you leave this field blank the software will not delete the activity log.

Saving Configuration: when you enter some of these criteria for the first time or you modify them you must save the configuration and reboot the e-polite Listener and the e-Polite Sender services.

• **Static Routes:**

In this table we will introduce the static route that will ignore the DNS resolution or the send through host.

• **Inter-office e- mail Servers:**

In this area you have to enter the IP addresses of your network's e mails servers. Then you have to configure these servers in order to send all the outgoing e mails through e-Polite®.

If you want to increase the security of e-Polite® you can use the addresses of inter-office e mail to generate an Anti-Relay rule:

Source:	List
Relation:	Does not belong
Source Criteria:	Inter-office e mail Server
Target Type:	Grouping
Relation:	It belongs
Target Value:	Any
Action:	Denied. Activity log available

This way you will ensure that e-Polite® will only permit the delivery of messages from your company's internal servers.

• **Corporate Domains:**

In this area you have to enter the domains of your organization that you want to be filtered in order to avoid e-mails sent from those domains join the "Forbidden Addresses" area. You can also generate an Anti-Relay rule by blocking the sending of any e-mail from a source not belonging to the corporate domains.

• **Control Relay:**

In order to control the relay, we have the option of permitting just the sending from the registered corporate domains or also the possibility of receiving only the requests from specific IPs or IP ranks.

Footer of Messages

• **Text at the footer of messages:**

It is the text attached at the footer of all outgoing messages that will allow your company to comply with the current legislation (Statutory Instrument 2003 No. 2426 in the UK or CAN SPAM ACT in the USA), by giving the addressees the possibility to revoke their consent to receive message from your organization in a simple and free of charge manner.

The application provides with a default text which can be modified.

You should insert a link to the **automatic revocation service** in some part of the text in order to allow the addressee to revoke his consent automatically. You can use words like "click here" and link it to <http://#Service#> by clicking on the "insert link" button.

SME Version: e-Polite® SME allows to insert a single text as footer. This text can be modified from the HTML editor.

ENTERPRISE Version: e-Polite® ENTERPRISE gives the possibility to chose a different text to insert at the footer of your e mails for different departments, languages or any other criteria. The choice of the text at the footer of the outgoing messages depends on the **Filtering Options**. The program is provided with a default text that you can modify the way you like most. The default text will be attached to all the outgoing messages not filtered by the **Filtering Option's rules**.

You can create or modify texts from the HTML editor.

- **Exceptions:**

These are source e mail addresses with no footer message. WARNING, sending messages from these e mails addresses means that you may not be complying with the law, so we recommend a very limited use of them. You can use them in order to inform your clients or suppliers about some service they have hired from you or to warn them in case of the services failure.

Authorization

e-Polite® allows to publish a service on the corporate web site of your organization in order to allow the addressees to authorize you to send them e mails. You only need to create a link to the page authorize.asp of the external e mail address of the e-Polite server: <http://SiteServicios.e-Polite/autoriza.asp>

SME Version: The SME e-Polite® allows to configure one single page of authorization for only one language.

ENTERPRISE Version: The ENTERPRISE e-Polite® is a Multilanguage tool, so that the authorization web page will be shown automatically in the language of the user's browser, as long as you configured this language. If you did not configure it, the authorization page will be shown in the default language.

- **Language:** it shows the configuration of the authorization service in the chosen language.

New Language: it permits to configure a new language.

Save Language: it allows you to save the configuration of a new language or changes of an existing one.

- **Title:** header of the window in the authorization page.

- **Text:** message shown in the page where the user will enter his e mail address in order to authorize your company to send him e mails. The aim of this message is giving the user accurate instructions on how to do it.

- **Background colour:** You can customize the background colour of the title and the colour of the button area of the window.

- **Background colour of the text:** you can customize the background colour of the text.

- **"Accept button" text:** you must insert the text "Accept" or "Send" in the language you are configuring.

- **"Cancel button" text:** you must insert the text "Cancel" in the language you are configuring.

- **Alert Text:** Warning shown by clicking on "Accept".

Default Authorization: You have to choose if the language you are configuring is the Default Language. You can only choose a default language.

- **Confirmation e-mail (double opt-in):**

In order to avoid that someone else send you a faked authorization, e-Polite will create a specific message for the e-mail address that have authorized you to send e mails. You can insert all the information about this e mail address by clicking on **#e mail address#**.

You have to include a link to <http://#Service#> somewhere in the text in order to allow your potential customers to authorize you. Only if the customer clicks on this link his e mail will be included in the "Authorized e mail List".

This software keeps a Log of all the received authorization.

- **Confirmation Message:** Message shown on the authorization page as soon as the user confirms his authorization

Revocation

e-Polite® allows users to revoke their consent to receive e mails by clicking on the link at the footer of all your e mails. After clicking on that link a window will pop up and the user will be informed that by that moment he will never receive further e-mails from your company.

ENTERPRISE Version: e-Polite® ENTERPRISE is multilingual, so that the revocation page will be automatically shown in the user's browser language, As soon as you configured it. If you did not do it, the revocation page will be shown in the default language.

- **Language:** it shows the configuration of the authorization service in the chosen language.

New Language: it permits to configure a new language.

Save Language: it allows you to save the configuration of a new language or the changes of a previously configured one.

- **Title:** Header of the window in the revocation page.
- **Text:** Message that will be shown to the user in order to inform him about the effects of the revocation. You can also insert information of the revoked address by filling the field #Address#. The aim of this message is to provide the user with accurate instructions on how to do it.
- **Background colour:** You can customize the background colour of the title and the colour of the button area of this window.
- **Background colour of the text:** You can customize the background colour of the text.
- **Text of the "Accept" button:** For every new language that you configure you should change the text "Accept" into the new language you are configuring.
- **Text of the "Cancel" button:** you have to translate the text "cancel" into the new language you are configuring.
- **Alert text:** Warning shown by clicking on "Accept".

Default revocation language: you have to choose a default language. You can only choose one default language.

Denial

- **Failure Notification:** is the text of the notification received by the sender when one of his e mails has been blocked by the e-Polite active filter. This is how the text of a failure notification is structured:

#From#	Sender of the e mail blocked.
#Para#	Addressee
#FechaHora#	Date and Time of the process.
#Filtro#	Name of the active filter.
#NumRegla#	number of the rule which denied the delivery.
#MailAdministrador#	e mail address in charge of receiving all requests.

All fields must be filled between the symbols #field# and they are Key Sensitive, (distinguish between capital letters and small letters).

The software will provide you with a default text that can be modified

SME Version: The SME e-Polite only allows one single denial text message.

ENTERPRISE Version: e-Polite allows you to chose among different denial notifications depending on languages, departments and other criteria. The text sent to the sender, as warning of a failed delivery, will be assigned by the **Filtering Options**.

- **Sending a Copy:** You can include more e mail addresses in order for them to receive a copy of your message. They should be separated by this symbol: " ; "

Notifications

This software generates notifications in different situations and it can be configured to send a copy of these notifications to several e mail addresses.

- **Error Notifications:** It is the warning message received by the sender when his e mail has been blocked by

the server because of some error. You can configure the software in order to send a copy of this message to other e mail addresses.

- **Notification of Authorization:** this is the warning message received by the e-Polite administrator when a user joins the "Authorized e mail address List". You can unselect the administrator's e mail address if you do not want to receive this kind of notifications, or just select a different e mail address that will receive a copy of them.
- **Notification of Revocation:** this is the message received by the e-Polite administrator when a user joins the "Forbidden e mail Addresses List". You can unselect the administrator e mail address if you do not want to receive this kind of notifications, or just select a different e mail address that will receive a copy of them.

Rules

Thanks to the Filtering Options you can be able to define how the software acts when processing all messages.

For each operating mode of the software exist a basic filter which do not permit to edit or to delete messages, and that follows one of the default lists:

OPERATING MODE	FILTER	WORKING LIST
MODERATE	- Moderate Basic -	Forbidden
SEVERE	- Severe Basic -	Authorized

If you are working on the MODERATE mode and you did not create any personalized filter, the only active filter will be the **Moderate Basic**, which will not permit the delivery of any e mail from the corporative domain to the **Forbidden e mail address list**.

If you are working on the SEVERE mode and you did not create any personalized filter, the only active filter will be the Severe Basic, which will not permit the delivery of messages from the corporative domain to any e mail address that is not on the **Authorized e mail address list**.

There will always be an active filter, just one. The active filter will not permit to edit anything, so if you need to make any modification you will have to copy this filter and make all the modifications on this copy and then define it as the active one.

Rules Edition (See/ Modify Filters)

To see or modify an existing filter you need to select it with the Mouse. The Rules Modification dialog will automatically pop up.

Name: you can modify the name of the filter.

- **Active:** you can define this filter as active. There can only be one active filter.
- **Rules List:** list of rules defining this filter.

New: you can register new rules in a filter.

To modify a rule it is necessary to select it first with the Mouse and then you will be able to edit it.

- **Rules parameters:**

- Kind of origin: it can be an e mail address, an IP address, a domain or a Group list (lists and Group Lists must be managed by clicking on the *Origin objects* option).
- Source Relation: Choose between if it belongs or not belongs
- Origin: depending on the kind of origin you have to select or enter the corresponding object.
- Kind of addressee: it could be an IP addressee, an e mail address a domain or a Group List (lists and Group Lists can only be managed from the option Addressee Objects).
- Destination Relation: It permits to choose between if it belongs or not belongs
- Addressee: Depending on the selected kind of addressee you will have to select or enter the corresponding object.
- Action: You can deny or give permission and in any case you can do it with or without log
- Footer / Return: It permits to choose the message at the footer of your e mails, or the failure delivery message that will be used when the delivery is not authorized.
- Authorization: you can choose the message to send automatically to the addressees who are not in the authorized list for the severe rules. For choosing this option, the rule should be severe,

which means, that it only allows to send e-mails to authorized addressees (You should select as "destination type" a "list", the "relation" should be "Not belongs", the "destination" the "authorized" and the "action" as "denial" with or without log). So you will have the opportunity to send the authorization request to those persons who are not authorized without sending commercial information.

- **Order:** It informs about the way the rules will be applied. This order may be changed by clicking in the arrows *Up* and *Down*. The rule number 1 permits no changes of order.

Save: It permits to save a new rule or changes of an existing one.

Delete: It permits to delete a rule.

Close: to close the rule's edition

Save: It permits to save all modifications of the filter you are editing.

Delete: It permits to delete the filter you are editing.

Close: it permits to close the dialogue of filter edition.

Creating new filters

Any filter will be based on one of the available configurations, the moderate and the severe one. It means that any new filter at the beginning will contain as default rule the Basic acting rule.

The steps you have to follow in order to create a new filter are:

- Select the option New Filter.
- Give the filter a name.
- Register all the rules that you wish.
- When you finish registering all the rules you must click *close* or just click NO when the computer asks you to create a new rule.
- Select the option *Active* if you want it to be the active filter of the application.
- If you want to save all modifications click on **save** in the dialog box.
- In order to see the rules of the new filter you created, you must select the filter.
- We recommend you to check the coherence of the rules before activating a new filter bearing in mind that the first law that complies with all the conditions will be the one to be applied.

Copy Filter

You can create a new filter on the basis of an existing one. You have to click on the "*Copy Filter*" button.

- **Filter to copy:** you have to select the filter you wish to copy.
- **New Filter:** you have to name the new filter. (give the new filter a name)

Once you have copied it you can modify that by selecting it with the mouse.

Authorization Message

You have to define the messages for sending automatically the authorization request.

This e-mail will be selected in the severe rules and if the rule specifies so, the original email will be replaced by the text defined here




The automatic messages will be defined for the authorization request

This E-mail will be selected in the severe rules and will replace the original e-mail if the rule says so. The text of this message must not contain commercial information, because the target of this message is just to request the addressee's authorization.

Sent authorizations

We can check all the sent authorizations, the destination addresses, the date where the authorization was sent and the status of the authorization.

The different status are:

- Authorized 
- Not authorized 
- Pending of answer 

Managing default tables

The default schedules of the application are:

Authorized e-mail addresses: e-mail addresses that explicitly authorized your company to send them e mails. We recommend to keep a register of these authorizations either on printed or on electronic version. The schedule will automatically register all authorizations through the Authorization Service. The administrator can delete records from the schedule.

Forbidden e-mail addresses: e-mail addresses that did not authorize the delivery of messages from your organization. We recommend to keep a register of these revocations either on printed or on electronic version. The schedule will automatically register all the revocations through the Revocation Service.

These schedules are mutually exclusive: the same e mail address could never be registered in both schedules.

Managing Source and Target objects

We can concentrate (gather) objects into a source and target **List** facilitating the configuration of filters, in order for them to have a lesser number of rules and better performances.

If you want to create a new List you have to click on *New*. If you want to modify an existing List it is necessary to click on it with the mouse.

A dialog box will pop up to *Register or modify the List*.

- **Name of the List:** You have to name the List.
- **Description:** You can specify how you would use that List.
- **Kind of list:** There are four kind of lists:
 - Addresses: List of e mail addresses.
 - Domains: List of domains.
 - IP: List of IP addresses.
 - Group: Group of all kind of Lists.
- **Object List:** List of all the objects included into a specific List.

New: Necessary to register new objects into a specific List.

An existing object can only be modified by selecting it with the mouse.

- **Options of the Register/Modify menu of an object on the list:**
 - Save: it allows you to save a new object or changes of an existing one.
 - Delete: It allows you to delete the object you are editing.
 - Close: Exit the edition of the object.

Save: It allows you to save modifications on the List you are editing.

Delete: it allows you to delete the list you are editing.

Close: Exit the edition of the List.

Operators

It is possible to register different kind of users to log in the application, with different profiles such as "users", "Advanced users" and "administrators" of the tool. The administrators will be able to log in all the application, the "advanced users" will be able to log in the lists and the "users" only to their own registers.

Queue list

You can visualize the e mail delivery status by clicking on Queue Management.

To refresh the process you have to click on *Refresh Queue*.

• Queue parameters:

- IP Origin: Sender's IP address.
- From: Sender's e mail address.
- To: Addressee's e mail address.
- Allowed: if it turns green it will be delivered, but if turns red the sender will receive a delivery failure notification.
- Date: Date of delivery of the message in the queue.
- Status: Status of the e mail sending process.
 - Delivering: the message is being delivered.
 - Filtered: the message is being processed by the Filtering rules.
 - In queue: message filtered and waiting to be sent.
 - Sending: The message is being sent.
 - In hold: the message presents some error and is in hold for the second attempt of delivery.
 - Deleting: the message has been processed and it's being deleted from the queue.
- Size: Size of the message in bytes.
- Attempts: number of delivery attempts
- Notes: explanation of errors in previous delivery attempts.

Activity Log

Clicking on this area you can visualize a record of all the e mail sent from your organization. You must take in account that in case of messages processed by a defined rule with "No Log", or messages that did not comply with any rule, the target e mail address will not be saved.

Log parameters:

- Source: sender's e mail address.
- Target: Addressee's e mail address.
- Date: Day that the message was processed.
- Allowed: If it turns green the message has been authorized. But if it turns red, the sender will receive a delivery failure notification.
- Filter used: It informs you about the filter activated when the message was sent.
- Number of rule: It informs you about the number of the rule applied to this message. If instead of the number of rule appears the word "none" it means that the message did not comply with any of the rules and was sent anyway.
- Sent: If it turns green, the message has been sent. If it turns red the sender will receive a failure notification. If it is white, it means that the messages have not been sent yet.

If the 'complete log' is configured we will be able to see the communications detail clicking on the message.

Statistics

Activity Log

In this section we will be able to check the sent emails, breaking down between the authorized and denied e-mails. To do it, we will select the initial and end period of the search

Licence

Here you can visualize all the information about your product and register your licence.

If you do not register the licence of your product you will not be able to access the associated support service.

Here, it will be able to check the e-polite® users pressing the button "See users", and activate/deactivate or even eliminate users.

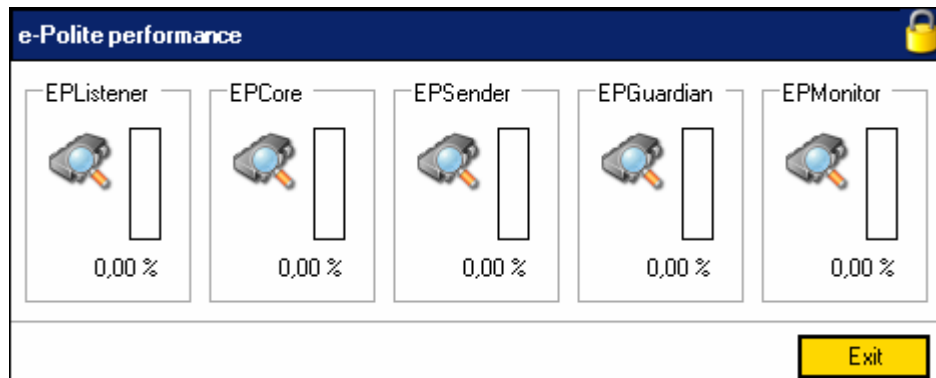
2. CONTROL OF SERVICES

The application installs a control tool in the tool bar of your computer. If it is disabled you can start it by clicking on Start/ Programs/ Adiciona/ Control Service.

Functionalities:

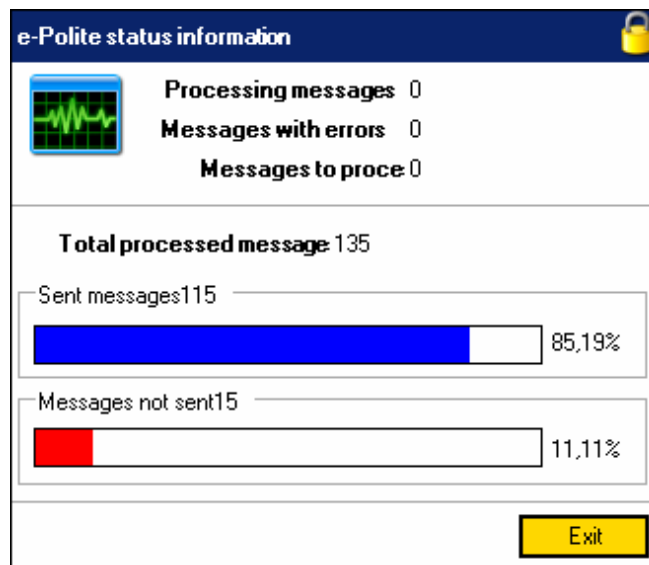
- **System performance**

It allows to check the system resources used for each E-polite module.



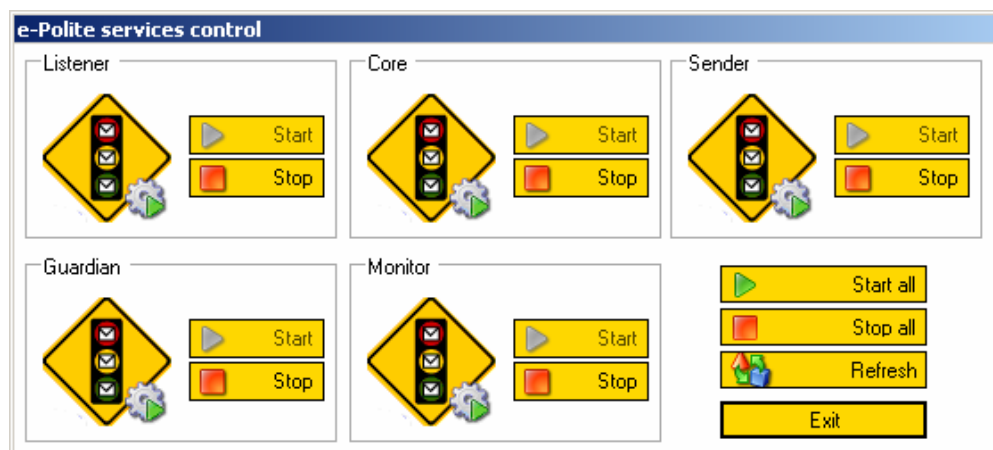
- **Status Information (Only Enterprise version)**

- Message being analyzed: number of messages enlisted to be sent.
- Error messages: Number of messages stopped because presenting some kind of problem and enlisted for the second attempt of sending.
- Messages to be treated: number of messages enlisted for being sent or deleted.
- Total number of treated messages: number of all treated messages in the log.
 - Sent Messages: revised and successfully delivered messages.
 - Not delivered messages: revoked messages or messages that could not be delivered because of some error.



• **Control of services:** It allows you to start, pause and stop software services:

- Listener: Service that receives and checks all messages. Name of the executable: Eplistener.exe.
- Core: Service processing all delivered messages through the active filter. Name of the executable: EpCore.exe.
- Sender: Service in charge of sending all messages previously filtered by the Core. Name of the executable: Epsender.exe.
- Guardian: Service in charge of checking the status of Listener, Core and Sender, and to reboot them if they are stopped. This service also controls event report, sending an alert if errors of e-Polite are detected. Name of the executable: Epguardian.exe
- Monitor: Service in charge of monitoring the messages for the alarms processing



• **Configuration:**

1. Configuration

- SMTP port: It permits to change the listening port of "Listener" and/or the send port of "Sender".
- Ret attempts: It allows configuring the number of reattempts and the waiting time between them.

- **Temporary messages directory:** It allows modifying the directory where all messages, received by the Listener in order to be checked, are stored. Once the Sender checks them they will be eliminated from this folder.
- **Expender Performance:** It allows to configure the e-mails processed every X milliseconds

Configuration

Configuration | Database | Monitoring | Notifications | Connection

Ports (SMTP) configuration

Listener port: 25
IP:
Sender port: 25

Retries

Retries number: 8
Waiting time between retries (minutes): 5
The return time of a message is 40minutes

EPSender performance

Collect: 1 Mails each: 3000 milliseconds

Temp directory of messages

C:\Documents and Settings\dperez\Mis documentos\

2.Database:

It allows to configure the database parameters.

Configuration

Configuration | Database | Monitoring | Notifications | Connection

SQL server: (local) SQL server name or instance. In case of instance, please show ServerName\InstanceName

Port (optional): Connection to SQL server port. If you leave empty this box, it will connect to default port. If it is a firewall, it is recommended to specify one port.

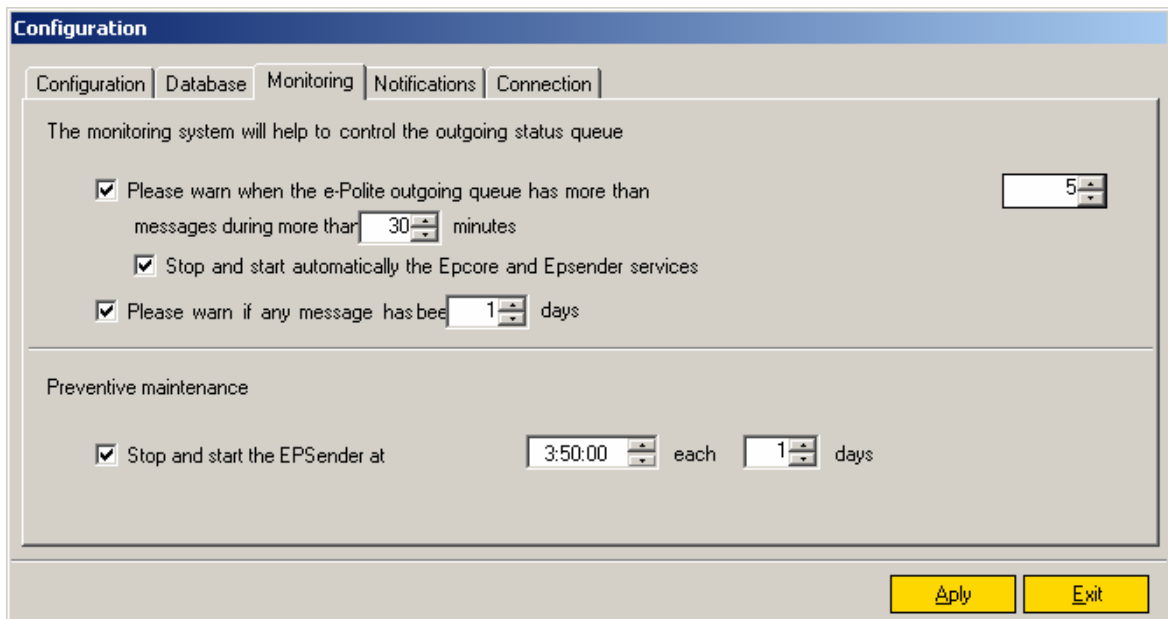
Database: AD_ePolite Database name. Default AD_ePolite

User: sa User to SQL server connection

Password: *** Password for SQL Server connection

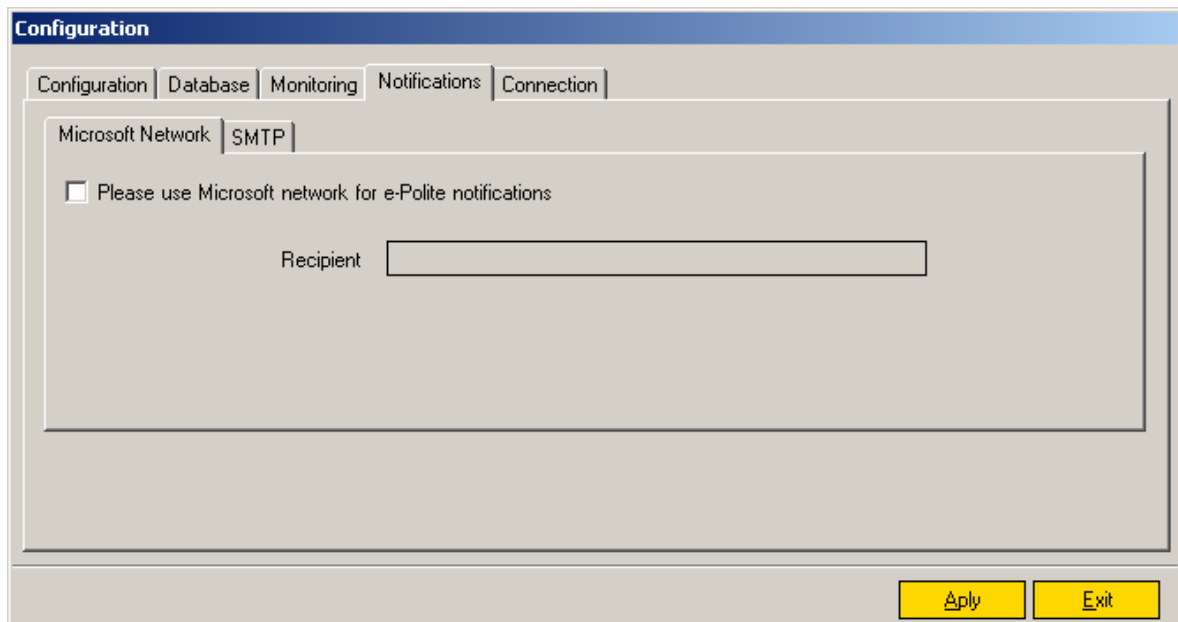
3. Monitoring:

It allows to configure the monitoring parameters to control the E-polite outgoing queue, allowing to configure the notifications and other services for the correct E-polite running.

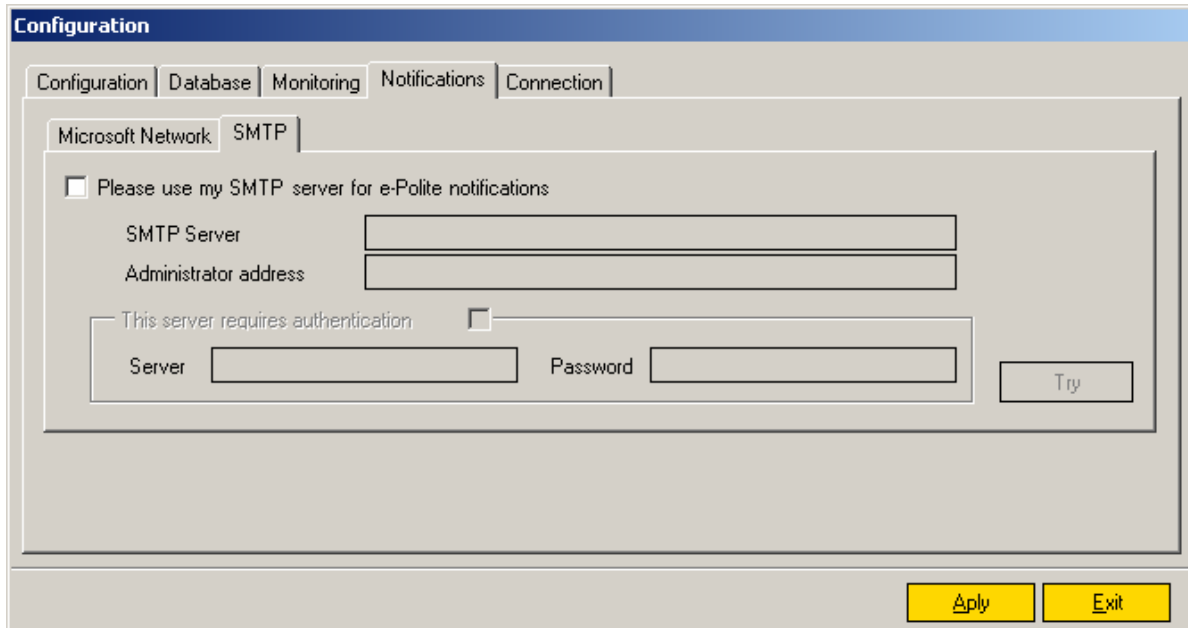


4. Notifications:

- Microsoft Network: you can use Microsoft Network for sending alerts detected by the Guardian. It requires that the service for sending messages is started both in the Server and from the customer. It allows you to enter the name of your computer, a username and an IP address.

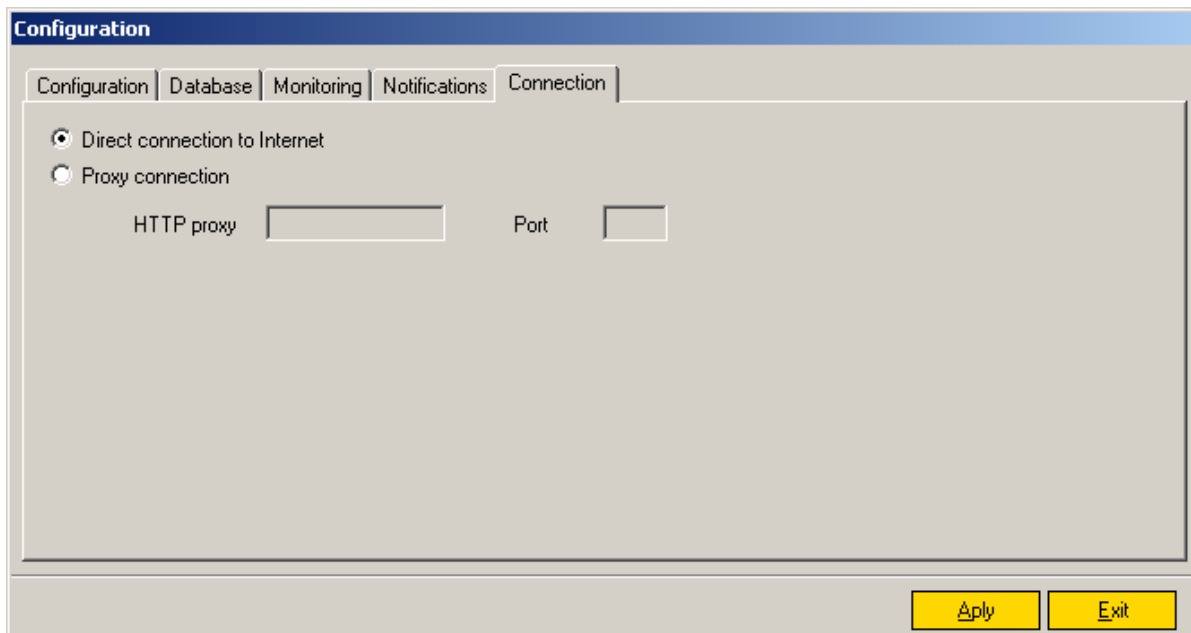


- SMTP: it allows using a SMTP Server in order to send the alerts detected by the Guardian. In this case we recommend no to use the e-Polite since if there is an error affecting the sending process, the alert would not be delivered.
 - SMTP server: you have to enter the SMTP server.
 - Administrator e mail address: you need to enter the e mail address to which all the alerts will be delivered. Use the same e mail address as source address of the message.
 - If the server asks for identification you have to enter the username and password.

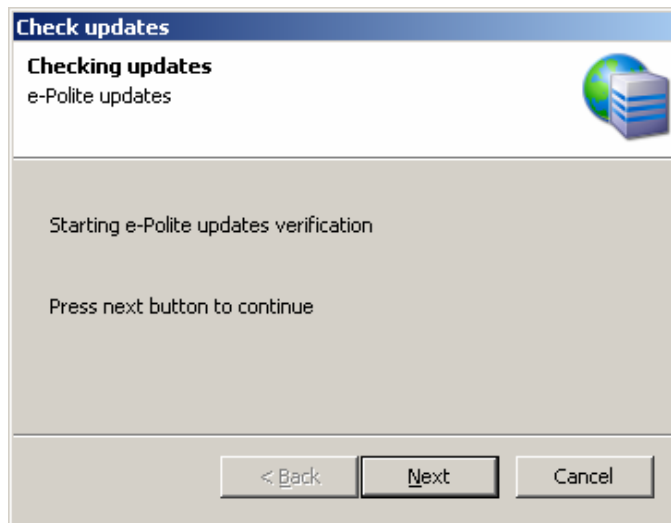


5. Connection:

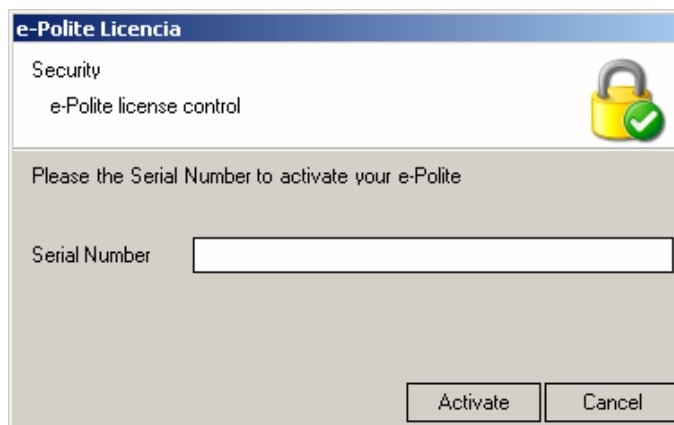
It allows to configure the connection to Internet.



- **Update checking:** Automatic update service.



- **Licence:** It allows to activate the E-polite serial number.



- **Exit:** Close the e-Polite control panel.

3. BACKUP

We recommend you to make a daily copy of the AD_ePolite database of the SQL Server in order to save all the information and avoid a log's critical storage level.

4. CONFIGURATION OF E MAIL SERVERS

In the Enterprise edition of e-Polite® you do not need to modify the of client's e mail configuration of your organization's users, you just need to make sure that mail servers send all the outgoing e mails (not the inter-office mail) to the e-Polite server, instead of resolving it through DNS.

The host where all the outgoing e mail must be sent is the IP address of the e-Polite® server.

If you have Microsoft Exchange Server 4/5/5.5:

1. Start the Microsoft **Exchange Administrator** and click on Configuration / Connections.
2. Find the **Internet Mail Service** and make double click on it in order to configure it.
3. Go to **Connections**.
4. In the section Message Delivery, select 'Forward all messages to host'. Enter the name or the IP address of the server on which the e-Polite® is installed.

5. Click on Accept and reboot the **Internet Mail Service**. You can also make this procedure from the services area.

If you have the Microsoft Exchange Server 2000/2003:

You will need to start a SMTP connector sending all the e mails to e-Polite®:

1. Start the node connector ->New-> SMTP Connector and create a new SMTP connector. You will be asked to choose a name for it.
2. Now select the option "Forward all e mails through this connector to the smart host" and enter the IP address of the e-Polite® Server (the server in charge of re transmit e mails) in parentheses [] for ex: [100.130.130.10]. Now click on Accept.
3. Select the SMTP Server where the SMTP Connector will work. Go to the Address Area and click on Add. Select the SMTP and click on accept.
4. Click on Accept to exit the process. Now all the outgoing e mail will be sent to the server running the e-Polite®.

If you have the Lotus Notes:

1. Double click on the Address Book button of Lotus Notes
2. Click on the Server element in order to open its sub-elements
3. Now click on Domains
4. Click on Add Domains
5. In the section Basics select the SMTP external Domain in the field Type of Domain.
6. In the section "Messages addressed to" enter '*' in the field "Internet Domain".
7. In the section "Must be routed to" enter the IP address of the e-Polite® machine into the field Internet Host.
8. Save and reboot the Lotus Note Server.

If you have a SMTP/POP3 mail Server:

1. Start the configuration program of your e mail Server.
2. Look up for the option for re transmitting all the outgoing e mails through another e mail server. This option is called "Forward all outgoing messages to the Host". Now enter the name or the IP address of the computer running the e-Polite®.
3. If necessary, click on Accept and reboot your e mail Server.

5. DNS CONFIGURATION

Some e-mail services make inverse resolution of the server IP that is in the header of the message before accepting it. To avoid these servers reject the e-mails sent by E-polite, we should register the IP Server in the Inverse resolution area (PTR register).

6. GLOSARIO

- **Filter:** Set of rules for processing messages.
- **Authorized e-mail addresses:** e-mail addresses that explicitly authorized your company to send them e-mails. We recommend you to keep a register of these authorizations either on printed version or on electronic version.
- **Forbidden Addresses:** e-mail addresses that did not authorize the delivery of messages from your organization. We recommend you to keep a register of these revocations either on printed version or on electronic version.

- **List:** Set of source and target objects. It could contain specific objects such as: e mail addresses, domains, IP addresses or groups.
- **Agrupación:** Conjunto de Listas de origen o destino. Puede contener Listas de cualquier tipo: direcciones de correo, dominios o direcciones IP.