



# **Software602 Groupware Server 6.0**

## Administration Manual

## Table of Contents

Introduction .....	3
System Requirements .....	4
Groupware Server Console.....	5
Server Status .....	6
Real-time Log.....	6
Current Connections.....	6
Message Queue .....	6
Statistics .....	6
Upstream Proxy.....	6
License .....	6
System.....	7
Services .....	7
Internet Connection .....	7
SSL Certificate .....	8
Full-text .....	11
Documents .....	11
Notifications.....	11
Logging.....	12
Debug.....	12
Backup.....	13
User Management .....	14
Domains.....	14
Users.....	14
Groups.....	15
User Import.....	16
Mail Services .....	17
SMTP .....	17
POP3 .....	20
IMAP.....	20
Attachment Filter .....	21
LDAP .....	21
Archive .....	21
IM Services .....	22
Web Services.....	23
FTP Services .....	25
Anti-virus.....	26
Anti-spam .....	27
Message Classification .....	27
Real-time Filter.....	27
Bayesian Filter .....	27
SMTP Whitelist & Blacklist .....	28
DNSBL .....	29

## Introduction

Software602 Groupware Server administration can be performed from a web browser by connecting to the built-in Groupware Server web server (not IIS) using the predefined virtual directory `groupwareadmin` (see [Groupware Server Console](#) for more information). Only users that are members of the `Administrator` group can perform administration.

The default URL for accessing Groupware Admin:

<http://localhost:8080/groupwareadmin>

-or-

<http://localhost/groupwareadmin>

The screenshot shows the Groupware Server Admin console. The top navigation bar includes icons for Status, Users, Groups, Log, and Queue. The left sidebar contains a tree view with categories: Administration (Status, Real-time Log, Current Connections, Message Queue, Statistics, Upstream Proxy, License), System (Services, Internet Connection, SSL Certificate, Full-text, Documents, Notifications, Logging, Debug, Backup), User Management (Domains, Users, Template), and Admin. The main content area displays the following information:

- NOTIFICATIONS**: None
- GENERAL**
  - Uptime: 19 hours
  - Disk space used: 42.2 GB
  - Disk space free: 27.03 GB
  - Last anti-virus update: 7/2/2008 11:11 AM
  - Last backup: 7/2/2008 7:11 AM
- STATISTICS**
  - Server started: 7/1/2008 4:51 PM
  - Messages transmitted by SMTP server: 23
  - Messages received by SMTP server: 4294
  - Messages rejected by SMTP server: 5458
  - Messages caught by anti-spam: 1608
  - Messages caught by anti-virus: 6

**NOTE: The correct access URLs can always be found from the Groupware Server 6 Console application.**

# System Requirements

The recommended configuration for Software602 Groupware Server is a dual-core machine with Windows® 2008 Server and 2GB of RAM. Below are the minimum requirements:

## Operating Systems

- Windows® 2000 Professional
- Windows® 2000 Server
- Windows® XP Professional (x86 and x64)
- Windows® Vista (x86 and x64)
- Windows® Server 2003 (x86 and x64)
- Windows® Server 2008 (x86 and x64)

## Memory and Hard Drive Space

- 1024 MB of RAM
- 200 MB for installation
- Additional storage space for user mailboxes, e-mail archive, full-text index, etc.

## Server Requirements

- Microsoft® .NET Framework 2.0 for Windows® 2000
- Microsoft® .NET Framework 3.5 for Windows® XP/Vista/2003/2008
- Microsoft® Internet Information Services 5.0 or higher

## Client Requirements

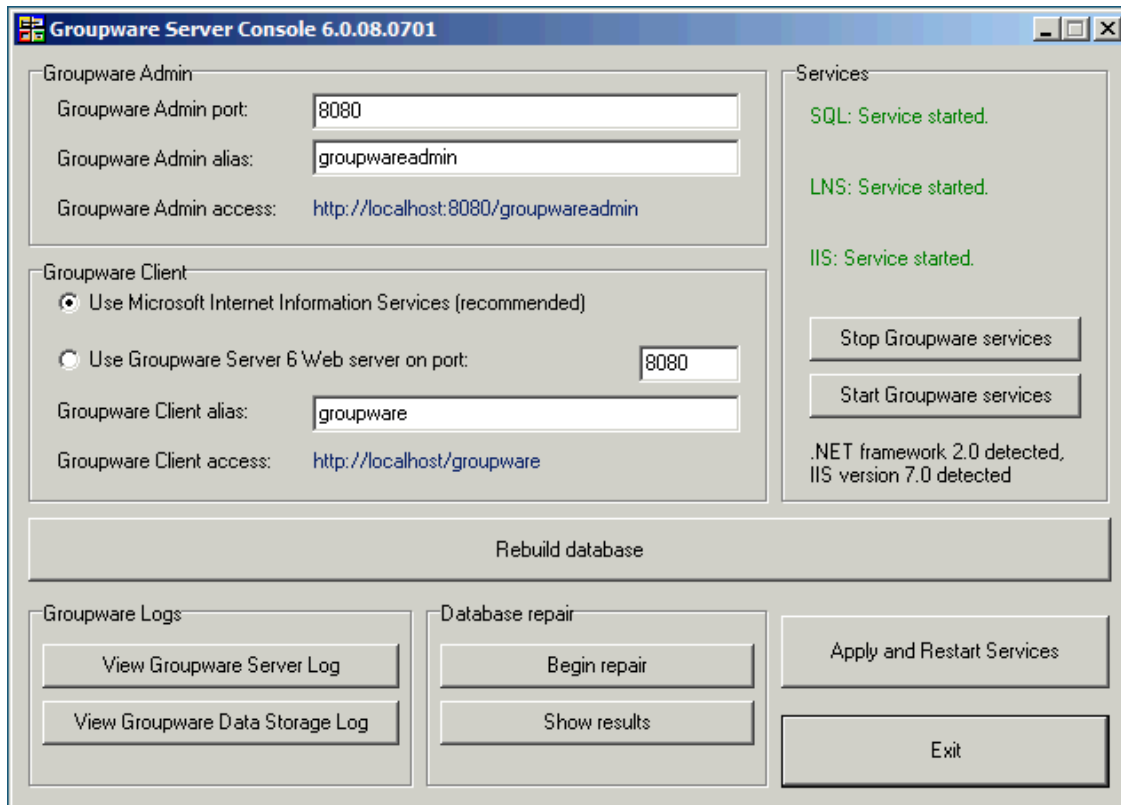
- Microsoft® Internet Explorer 6.0 or higher
- Mozilla® Firefox® 2.0 or higher

## Client Access Options

- Outlook Connector requires Microsoft® Outlook 2002 or higher
- Windows® SMAPI extension requires Windows® 2000 or higher

# Groupware Server Console

The Software602 Groupware Server Console is a Windows application that can define the Groupware Admin settings, the Groupware Client settings, view the Groupware log files, and repair the database. If you make any changes, please click `Apply` and `Restart Services`.



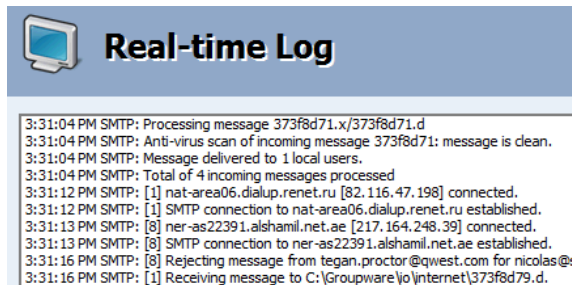
- **Groupware Admin port:** Enter the port the Groupware web server will listen on.
- **Groupware Admin alias:** Enter the alias to access the Groupware Admin.
- **Groupware Admin access:** Click this link to access Groupware Administration.
- **Use Microsoft Internet information Services:** Select this to access the Groupware Client from IIS (recommended for 10+ users).
- **Use Groupware Server 6 Web server on port:** Select this to access the Groupware Client from IIS (recommended for less than 10 users).
- **Groupware Client alias:** Enter the alias to access the Groupware Client.
- **Groupware Client access:** Click this link to access the Groupware Client.
- **Rebuild database:** This will rebuild the database into
- **View Groupware Server Log:** This will open the Groupware server log.
- **View Groupware Data Storage Log:** This will open the Groupware SQL server log.
- **Begin repair:** This will begin the database repair process.
- **Show results:** This will open the database repair process log.

## Server Status

The status section displays critical notifications, general system overview, server statistics, as well as product and database information.

### Real-time Log

View the real-time log of the Groupware Server. You can also reload the SMTP queue, force collection of POP3 mail, disable POP3 collection, and disable queue processing from here.



### Current Connections

This section shows how many users are currently connected to the Groupware Server.

### Message Queue

View all SMTP messages waiting to be processed by the Groupware Server.

### Statistics

Displays the numbers of bytes transferred since the server started.

### Upstream Proxy

If your Groupware Server does not have Internet access, you can enable upstream proxy support for anti-virus updates, Commtouch filter communication, and license activation.

### License

License activation is a seamless process using the license management system. Just insert your purchased `Registration Key` and click `Add`. If you need to add multiple keys, add one key at a time. Added keys will show under `List of Active Registration Keys`. Once you are finished adding keys, just click `Activate` to finish the online activation process.

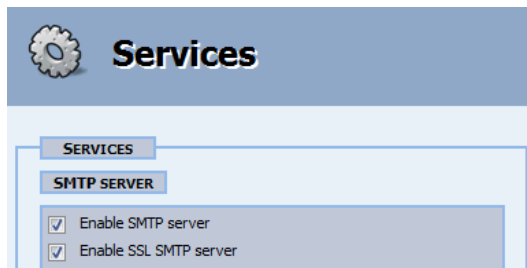
Groupware Server is installed as a fully functional 30-day trial. License activation must be performed before the end of the 30<sup>th</sup> day and requires an Internet connection.

## System

All system-level configuration is performed under this section.

## Services

This section allows you to enable or disable all Software602 Groupware Server services.



## Internet Connection

If the Internet connection is a permanent line (DSL, Cable modem, T1, etc.), there is no need to establish a dial-up connection. If you make a connection via a dial-up line (analog dial-up, ISDN) and you want Software602 Groupware Server to establish and terminate the connection, enable the Dial-up connection and complete the Dial-up schedule. Software602 Groupware Server can work with any Windows Dial-up Networking connection.

### Dial-up Connection Details

From the `Connection name` list, select the dial-up profile name you want to use to establish the Internet connection (all information contained in the profile is from your provider, the connection itself is pre-setup in the Windows environment). Fill in the User name and your Password to the connection. You can obtain this data from your Internet provider.

### Secondary connection (VPN)

To configure a secondary connection (VPN connection) click the `After connection` button. A VPN (Virtual Private Network) is the way to establish a private connection by encoding, authentication or tunneling through public lines.

The `ONCONN.BAT` file is used for editing the routing table or to start a process. If you need to run a process with the VPN connection, create the file `ONCONN.BAT` and save it to the folder where Software602 Groupware Server is installed and check the `Run ONCONN.BAT` checkbox.

### Permanent Schedule

Enable `Connect permanently` to provide a permanent connection to the Internet. Simultaneously, this activates the button `Permanent Schedule`. It opens a table that you can use to specify the weekly schedule when the permanent connection is enabled or disabled. This weekly table is divided into half-hour intervals. A green field means that a connection can be established a red field prohibits the connection.

### **Periodic Schedule**

Enable `Connect every`, if you want to connect to the Internet on a regular basis – after a specific time interval. Enter the interval in minutes into the field to the right of the switch and enter the minimum connection time into the next field. The request for a periodic connection activates the button `Periodic Schedule`, which opens a table to specify the weekly schedule for the connection.

### **E-mail Schedule**

Enable this when you want Software602 Groupware Server to connect to the Internet after e-mail has been waiting to be sent. Use the `E-mail Schedule` button to specify when you want Software602 Groupware Server to obey this rule.

### **POP3 Schedule**

Use this option to tell Groupware Server to connect to the Internet when a POP3 mailbox needs collecting, specified under `Administration -> E-mail -> POP3`. Use the `POP3 Schedule` button to specify when Software602 Groupware Server should obey this rule.

### **SSL Certificate**

The SSL (Secure Socket Layer) protocol runs between the network level and application level protocols. It provides server authentication, an encrypted connection and client authentication (optional).

How Secure Socket Layer works:

- Communication via SSL has a pair of keys: a public key and a private key.
- The Private key is used by the server to encode data.
- The Public key (certificate) is used by the client to decode the data. The certification authority (CA) usually undersigns the public key so the client can be sure that it is communicating with the correct server. The easiest configuration is by using a self-signed certificate (the server functions as a CA).

Secure Socket Layer provides:

- SSL server authentication allows a user to confirm a server's identity.
- An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software.
- SSL client authentication allows a server to confirm a user's identity.
- The handshake of the SSL protocol consists of the following steps:
  - Authenticate the server to the client.
  - Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
  - Authenticate the client to the server (optional).
  - Use public-key encryption techniques.
  - Establish an encrypted SSL connection.

Secure Sock Layer is required for the following services:

- SSL web server
- SSL SMTP server
- SSL POP3 server
- SSL IMAP server
- SSL IM server
- LDAPS server
- FTPS server

If you want to communicate securely, you must first create the public and private key. Enter your information for public and private key setup:

- **Organization:** Name of your organization
- **Common name:** The IP address or domain name of the computer running Groupware
- **Contact e-mail:** The administrator or webmaster e-mail address
- **Country:** Select your country
- **State or province:** Select your state or province
- **Key length:** A longer key means better security, but more data to transmit.



**SSL Certificate**

**SSL SETTINGS**

**SSL INFORMATION**

Organization: (example: Company, Inc.)  
Company, Inc.

Common name: (example: secure.yourdomain.com)  
www.company.com

Contact e-mail: (example: admin@yourdomain.com)  
webmaster@company.com

Country: United States of America

State or province: Florida

Key length: 1024 bits

Now you have the two options: create a self-signed certificate or have your public key signed by a Certification Authority (CA).

- **Create Self-signed Certificate:** A self-signed key is free, but will not be recognized by web browsers, and will consequently offer a warning upon accessing the SSL server.
- **Signed Certificate by Certification Authority:** A certificate purchased from a reputable certificate authority such as Thawte or Verisign will be widely recognized and the web browser will automatically accept this as valid.

If your server is accessed only by employees or individuals that are familiar with your organization, a self-signed certificate may be the best choice. If you are offering secure access to the public, you should purchase a certificate from a well know Certificate Authority to instill confidence in your sever security. Both certificates are equally effective.

To create a self-signed certificate click the `Create Self-signed Certificate` button. The public key and private key are stored in a file `SERVER.PEM` (root of your Groupware Server directory). Your information (Organization name, domain name, etc.) is stored in the file `SSLEAY.CFG` (root of your Groupware Server directory). If the key expires, you can always re-generate it. The file `SERVER.CRT` (root of your web server folder) is also generated, which enables you to add the certificate into the list of CAs.

If you want a CA to sign your public key, click the `Create` button. When the `CERTIFICATE REQUEST` is generated, insert it into a CA form on the Internet. The certificate you receive from the CA must be saved to Software602 Groupware Server. Click the `Input Signed Certificate` button and input your signed certificated.

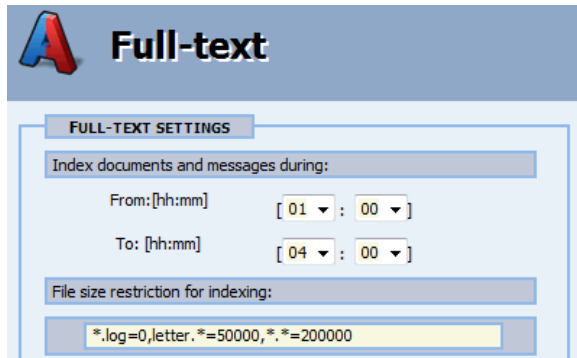
## Advanced SSL

- **Client verification using certificates:** Used to switch on certificate verification of the client certification authority (if not checked the client only verifies the server certificate). The following two checkboxes are accessible only if this check box is active.
- **Certificate required:** After activating this checkbox, client certificate verification will be required for further communication.
- **Verify only once:** Checking this box, the WWW server will only accept certificates confirmed directly by the certification authority (and not by sub-authorities).
- **Don't use any certificates:** Certificates (self-signed or signed by a CA) will not be used for server or client authentication.
- **Server Certification File:** Holds the access path to the certificate file, which includes the public and private keys certified by the certification authority.
- **Server private key:** If the certification file does not include the private key, enter the access path to the file that includes this key into the field `Server private key` (if encrypted in a separate file).
- **CA files directory:** Enter the access path to the directory with files including the public keys of each certificate authority into the field `CA files directory`.
- **CA database file:** Files with public keys can also be merged into a single file called a CA database file. This can be done by copying all individual certificates into a single file.
- **Just talk SSLv2:** Groupware will communicate with clients by SSL version 2 only.
- **Just talk SSLv3:** Groupware will communicate with clients by SSL version 3 only.
- **Do not generate a temporary RSA key:** No temporary RSA key for default SSL authentication will be generated.
- **Turn on SSL bug compatibility:** Some older browsers contain an SSL bug. If you have problems with SSL connections using an older browser, enable this option.

You can use various encoding methods for communication among SSL servers and clients. Use the `Ciphers` checkboxes to specify the methods that will be accepted by the server.

## Full-text

Full-text indexing is available for basic object information at all times. Indexing of complete object content is executed at off-peak times (i.e. usually at night). It is recommended to set the index time interval so that it does not overlap with the backup time.



**Full-text**

**FULL-TEXT SETTINGS**

Index documents and messages during:

From: [hh:mm] [ 01 : 00 ]

To: [hh:mm] [ 04 : 00 ]

File size restriction for indexing:

\*,log=0,letter.\*=50000,\*.\*=200000

## Documents

- **Data Consistency Verification:** This verifies that the database object and the local file system object exist.
- **Format Recognition:** This section should only be used to recognize a file format that is unrecognized. You must first add the new file type to the `fileformats.xml` file (this file is located in the installation folder under the `SQL` subdirectory) and then click `Begin format recognition`.
- **Full-text Index:** This section should only be used to re-index documents if you are experiencing problems searching for documents.

## Notifications

Groupware Server provides a notification system that will inform users of actions performed by the server (e.g. received a new e-mail) or events that are about to take place (meeting time reminder). The user is informed through the web-based Groupware Client.

Notifications are stored in the database and the client (web browser) regularly queries the server for these notifications. The server remembers the last status and within the time interval provides updates. Both of these actions take place regularly and can, in the case of a higher number of active users, increase the load on the server/database.

- **Refresh time (client – server):** A short period is better for the user (they will be certainly informed in time), but will load down the server.
- **Refresh time (server - database):** If this interval is substantially longer than the client-server refresh time, then the client will repeatedly receive obsolete data.
- **Delete notification records after:** If a user does not login to Groupware for a long time, then his/her new message notifications will accumulate in the stack. Therefore the server will automatically delete old notifications.

- **Delete reminder records after:** If a user does not login to Groupware for a long time, then his/her reminder notifications will cumulate in the stack. Therefore the server will automatically delete old notifications.
- **Current Statistics:** Serves as an overview for the administrator concerning the number of notifications in the stack.
- **Delete all older than:** Maintenance can be performed in a single action and will delete all notifications older than a pre-set number of days. The notification age is evaluated according to the e-mail time or, beginning of an event, or time of an event.
- **Delete all after:** If the stack contains notifications to an event or task in the future, it is also possible to delete them.

## Logging

Software602 Groupware Server provides the ability to log all server activity in a plain-text log file as well as in the W3C format for later analysis by W3C log analyzers.

- **Log to file SMMDDYYI.LOG:** Records the Software602 Groupware Server activity to a file. The file can be found in the Groupware Server installation directory, with the name SMMDDYYI.LOG (MM = months, DD = day and YY = the last two digits of the year).
- **Delete log files after:** This will rotate log files after the number of days specified here.
- **Maximum size of statistics file:** Other statistic log files exist as well: `lansuite.csv`, `infected.csv`, and `spam.csv`. The maximum file size is limited to the value specified here. After reaching this size, the server will delete older records after midnight.

Use the section `Log messages from` to specify the services to monitor reports from:

- Web/FTP/FTPS server
- Dial-up connection
- SMTP server
- POP3 server
- IMAP server
- LDAP server
- External Anti-virus scanning
- IM server

Most web servers offer the option to store log files in either the [W3C common log format](#) or a proprietary format. Software602 Groupware Server can provide web server logs in W3C format. W3C log files are recorded in a format readable by analysis tools.

## Debug

When troubleshooting a problem with Software602 Groupware Server, it is possible to record debugging information to a separate debug log file. Just enter the `Directory to store report files` then select the `Debug level` and which `Debug modules to watch`. The `Debug GWAPI` section will determine what functions and/or SQL commands to capture.

## Backup

Software602 Groupware Server is able to create backup copies of all data for restoration in the event of a hardware failure. The database file (.FIL) and full-text index file (.FTX) are copied at the pre-set time to the selected directory, the registry (.GRG) backup is created and a directory is created where the files stored outside the database are copied.

Important backup information:

- The backup directory can be a local or network disk.
- It must be a disk with a file system that allows [hard links](#).
- The result of the last backup is displayed at the top.
- The result of the backup is also saved to the Windows Event Log (Application Log).
- An incomplete backup is immediately deleted from the disk.
- Restoration from a backup can be performed using the installation program or by manually renaming and copying files to their correct locations.

During each backup, 3 files and 1 directory are created in the following format:

- **YYMMDDHHNN.FIL:** The database
- **YYMMDDHHNN.FTX:** The full-text index
- **YYMMDDHHNN.GRG:** Windows Registry entries
- **YYMMDDHHNN.GWDATA:** Directory containing files stored outside of the database.

File name description: YY = year, MM = month, DD = day, HH = hour, NN = minute

Each backup creates a directory with a complete copy of all files that are stored outside the database. If the disk contains multiple backups, these directories will take up an enormous amount of disk space. To avoid this situation, the files that have not changed since the last backup are maintained using a hard link. The new backup will only contain hard links (reference) to the same file in the older backup set. If the older backup is deleted, the file system guarantees that the data is not lost and remains valid for the later backups.

It is recommended to save the backup to another computer or network volume. If you set the backup directory as a UNC path, please ensure that the Software602 Groupware Server Windows service has access to the network disk by observing the following rules:

- By default, the Software602 Groupware Server service is running as the system account that cannot connect to network disks. Launch the service under a specific user account to gain sufficient permissions.
- The service will connect to the remote computer under the same user name and password, thus it is necessary to create the same user on the remote computer.
- From the Windows service you cannot access mapped network drives (e.g. M:\backup)
- On Windows 2000 it is impossible to create hard links using UNC. Backup is only possible to a local disk with the NTFS file system.

# User Management

Manage your domain, users and groups, or import users from LDAP or Active Directory.

## Domains

The `default domain` is used as the default e-mail domain for sending Internet e-mail. `Domain aliases` are other domains that all users can use.



**Domains**

**E-MAIL ADDRESSES**

Default domain:

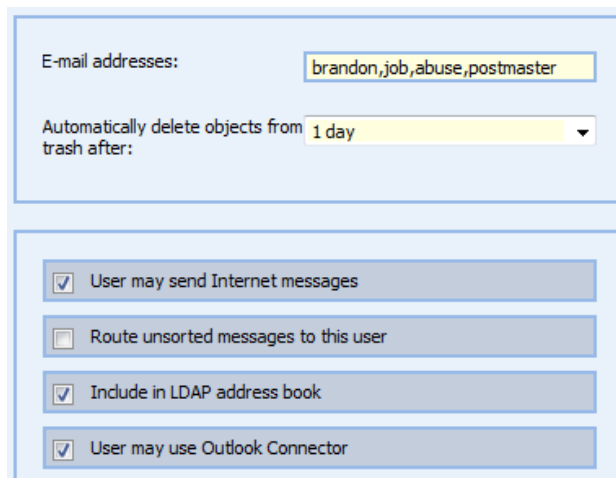
Domain aliases:

## Users

Users consist of local users and external users (e.g. a customer) that can login to the Groupware Client. They are allowed access to public folders in Groupware Documents and do not need to be listed within the `Local User` list.

Within user details, it is possible to add the user to a system groups (for permissions) or a user group (for group management). It is also possible to modify contact information, determine used space, change the password (provided the user is not imported from Active Directory) and change e-mail settings.

User `E-mail addresses` can be entered separated by a comma, the first address is considered the default, and the others will be aliases.



E-mail addresses:

Automatically delete objects from trash after:

User may send Internet messages

Route unsorted messages to this user

Include in LDAP address book

User may use Outlook Connector

A **Resource** is a Groupware user account that provides scheduling of time utilization of some resource by means of the Calendar (e.g. conference room or projector).

Resource requirements:

- A resource is an account within Groupware that consumes a user license.
- It is created like a normal user (cannot be external) and then specified as a resource.
- The resource can be listed in the Groupware Client under **Contacts** among **Local Users** or not. If it will not be listed, it is advised to enter this contact manually under **Shared Contacts**, so that other authorized users can make use of it.
- The Administrator user list will show resource accounts with a different icon.
- To give a user permission to take a resource from the Groupware Client, the resource account must allow such user read and write access to the resource's calendar.
- If a resource is taken from a calendar message, it can only be verified by the organizer/sender e-mail address.
- After creation of a resource, it is necessary to login to the Groupware Client under this account and share the calendar for both read and write access.
- To allow calendar message processing, the resource must have an e-mail address.
- A resource is radically different from a standard user since it will automatically process calendar messages with an event. If the resource is available at the required time, it will confirm the request. If it is in conflict with another event, it will reject the request.

If a resource receives a message that is not a Calendar request (e.g. a normal e-mail), it will be **DELETED**. This prevents the aggregation of unwanted messages to this account.

## Groups

Software602 Groupware Server supports two types of groups: user groups and system groups. System groups are described as follows:

1. System groups for allowing access to services:
  - **Instant Messaging users:** Users listed here can access the IM server.
  - **LDAP users:** Users listed here can login to the LDAP server.
  - **Mail users:** Users listed here can send messages to the Internet.
  - **Outlook connector users:** Users listed here can use the Outlook Connector.
  - **Unsorted mail operators:** Incoming messages where it is impossible to identify a recipient will be copied to the inbox of users specified here.
2. System groups for defining access permissions to shared folders:
  - **Administrators:** Read and write access to Public Folders and Shared Folders.
  - **Customers:** Read access to Public Folders.
  - **Everyone:** Read access to Public Folders.
  - **Power Users:** Read and write access to Public Folders and Shared Folders.
  - **Users:** Read access to Public Folders and Shared Folders.

**NOTE: System groups cannot be deleted.**

## User Import

### Active Directory Synchronization

Once the object list is loaded from the domain controller, select the users that should also be Groupware users, and then start synchronization. The selected users will be loaded into Groupware and they will be permanently bound to the Active Directory user. Among other things, these users will login to Groupware using their Active Directory password.

If any user data is modified within Active Directory, re-synchronization with Groupware will be required. A user bound to Active Directory cannot be deleted from Groupware directly; first, the user must be unbound from Active Directory, either by clicking the button under user details or during an Active Directory synchronization (uncheck the user). The same procedure can be used for synchronization of user groups from Active Directory.

**NOTE: In order to connect to Active Directory, the Software602 Groupware Server service must be started under an administrator account.**

### Groupware Import

Users can be imported from another Groupware Server. The import takes place using the LDAP server of the opposite Groupware Server. Login to LDAP is simplified in this case, since the LDAP data structure for Groupware is already known.

### LDAP Import

Users can also be imported from an LDAP server.

Syntax of the connecting string:

```
LDAP://server[:port]/keys
```

**Example 1:** LDAP://mail602:389/c=CZ

**Example 2:** LDAP://www.openldap.com:389/dc=OpenLDAP,dc=org

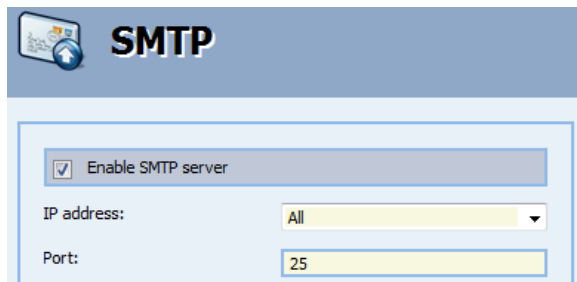
**Example 3:** LDAP://x500.bund.de:389/l=Berlin,ou=BAKS,o=Bund,c=DE

## Mail Services

Configure the following mail services: SMTP, POP3, IMAP, LDAP and the e-mail archive.

### SMTP

Enable or disable the SMTP services using the `Enable SMTP server` and `Enable SSL SMTP server` checkboxes. It is also possible to select the TCP/IP interface where the SMTP services will operate. All interfaces are selected by default, but you can choose a specific interface from the `IP address` pull-down box. This allows you to run the SMTP service on only one interface for security or functionality reasons (e.g. set the SMTP server to the Internal LAN interface will only allow users from the LAN to access the SMTP services). Software602 Groupware Server also includes an SSL SMTP server that provides a secure server to client connection. The default port where the SSL SMTP server listens is 465. In order to use SSL security you must first generate an [SSL certificate](#).



#### SMTP Delivery: Directly via MX records

The standard method of routing e-mail uses DNS (Domain Name System) services to request the MX record information about where the e-mail for a particular domain is to be directed. DNS evaluates your request and if it does not find a corresponding MX record, it forwards the request to the nearest DNS. This procedure is repeated until the corresponding record is found and the destination address is found. To choose this delivery method select the `Directly via MX records` option.

#### SMTP Delivery: Relay to ISP SMTP server

The simplest situation for delivering e-mail is if you can offload delivery to your Internet Provider's SMTP server. In this case, enter its address, either in the IP or domain form into the field and select `Relay to ISP SMTP Server`.

#### SMTP Delivery Options

- **Maximum number of outbound threads:** An excessive number of simultaneously transmitted messages will burden the connection and transmission will take longer.
- **Delivery retry interval:** Time interval between attempts at message transmission.
- **Return the message if not delivered after:** After the specified number of days, the message will be returned to sender with reason for failure.

- **Send warning to sender if not delivered after:** The server will warn a sender that it has not succeeded in delivering the message. The server will continue to attempt delivery until the `Return the message if not delivered after` option is reached.

### SMTP security settings

- **Maximum number of messages per hour from one IP address:** Protection against spam or an attempted denial-of-service attack on the server.
- **Maximum number of concurrent SMTP connections from one IP address:** Another form of protection against spam or a DoS attack on the server.
- **Maximum number of unknown recipients (directory harvest attack protection):** Protection against spam by attempts to send e-mail to random recipient addresses.

### Additional SMTP settings

- **Block if sender e-mail domain is not found in DNS:** Protection against spam from non-existent e-mail domain names.
- **Maximum number of recipients in a message:** Protection against sending spam to an unusually high number of recipients.
- **Maximum number of failed commands in an SMTP session:** Protection against an incorrectly operating external mail server.
- **Limit maximum incoming SMTP message size to:** Limitation to incoming total message size (header + letter + attached files).
- **Limit maximum outgoing SMTP message size to:** Limitation to outgoing total message size (header + letter + attached files).
- **Maximum number of accepted received headers (hops):** A record is added to the message header during each pass through an SMTP server. If a message is roaming during delivery, there will be a high number of these records.

### Request messages from SMTP server

Some ISPs support ETRN or ATRN as an e-mail collection request. If your ISP supports SMTP spooling via ETRN or ATRN, enable the `Request messages from SMTP server` option and click the `Edit Details` button.

### Preset routes

Under certain circumstances, it may be necessary to route messages for certain mail domains to a particular host. Preset routes can contain domains and target computers.

### Custom HELO/EHLO

An SMTP session between two servers starts with the HELO command (EHLO in ESMTP) that should be followed by the name of the calling server. The Software602 Groupware Server SMTP server will read this name from Windows (the Computer Name). If the server should report another name, this name can be defined here (e.g. `mail.domain.com`).

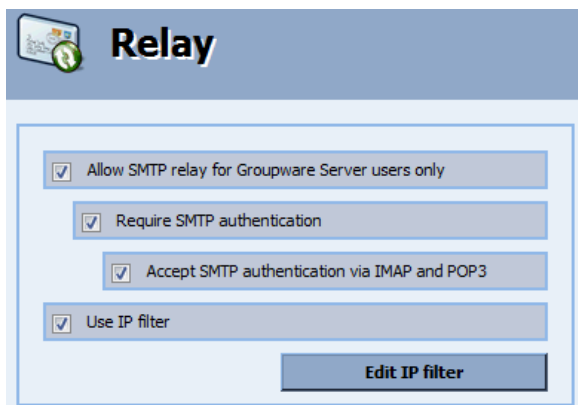
## SMTP Relay

SMTP relay functions provide message routing for users that do not have an account (mailbox) on the Software602 Groupware Server. This function is necessary for users who send messages from an SMTP client application (e.g. Outlook, Thunderbird). By default, the SMTP server will only work for Software602 Groupware Server users (enable `Allow SMTP relay for Groupware Server users only`). The SMTP server will check the Internet address of the sender (i.e. the address in the FROM: field) and if the user's e-mail address does not correspond with any local account or e-mail alias, the SMTP server will not relay for the user. If you check `Require SMTP authentication`, the SMTP server will only work for users who successfully authenticate (using their login name and password). If you want to disable all protection on the SMTP server, disable all checkboxes.

**NOTE: The SMTP server will be vulnerable to SPAM abuse if all checkboxes are disabled! If you want to protect SMTP processing by the IP filter, enable the IP Filter and setup the SMTP relay IP filter.**

Available SMTP relay settings:

- **Allow SMTP relay for Groupware Server users only:** SMTP server verifies sender e-mail address and provides relay only to valid local users.
- **Require SMTP authentication:** SMTP server requires authentication, however not all client programs support this function.
- **Accept SMTP authentication via IMAP and POP3:** Enabling this option will require a user to login successfully via IMAP or POP3 first, and for 120 minutes, the relay will work for this user.



**Relay**

Allow SMTP relay for Groupware Server users only

Require SMTP authentication

Accept SMTP authentication via IMAP and POP3

Use IP filter

[Edit IP filter](#)

## SMTP Relay IP Filter

The SMTP relay IP filter defines what connections are able to relay mail through the SMTP server. The IP filter rules are checked from top to bottom with each rule superseding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited – a RED icon means access denied, a GREEN icon means permit access.

## POP3

Post Office Protocol 3 (POP3) is the name of the protocol used for collecting the contents of mailboxes on the Internet. By enabling the POP3 server, you provide access to Software602 Groupware Server user mailboxes via the POP3 protocol. You can also specify rules for collecting messages from external POP3 mailboxes and deliver them to local user mailboxes.

Enable the POP3 Server to provide POP3 access to user mailboxes. It is possible to select the IP address where the service will operate on. All interfaces are selected by default, but you can choose one interface for the POP3 server from the `IP address` pull-down box. Software602 Groupware Server also includes an SSL POP3 server that provides a secure server to client connection. The default port where the SSL POP3 server listens is 995. In order to use SSL security you must first generate an [SSL certificate](#).

### POP3 Collection

Click the `Add` button and enter the POP3 account information into the input fields to create a collection rule. If you need to access a POP3 server on a different port, enter this value after the address separated by the colon character (e.g. `pop.server.com:999`). If you want to delete an item from the list, select the item and click the `Remove selected` button.

Messages from a POP3 mailbox can be collected and sorted to a local user mailbox:

- **According to the addresses:** When your ISP routes all e-mail to a domain into one POP3 account (e.g. `bob@company.com`, `john@company.com`) this will automatically sort the e-mail to the specific user. A recipient address is found in a message from the `FOR` item of the `RECEIVED` keyword, and this information has priority over other keys.
- **According to the addresses (alternative method):** Same as above, but uses different header analysis. Try this option if you are having problems with the first sorting method. The `FOR` item has no priority and other keys contained within the header are used for analysis.
- **To a specific user:** To direct all collected e-mail from the POP3 account to a specific user, select the user from this list.

POP3 mailbox collection can occur in a set time that will be repeated or at specific times:

- **Every X minutes:** Enter the time interval in minutes you want to collect the POP3 mailbox contents.
- **At predefined times:** Enter times in 24-hour format separated with a comma when you want to collect the POP3 mailbox contents.

## IMAP

[IMAP](#) (Internet Message Access Protocol) is an application layer Internet protocol operating on port 143 that allows a local client to access e-mail on a remote server. The current version, IMAP version 4 revision 1 (IMAP4rev1), is defined by RFC 3501.

SSL IMAP is the same protocol operated within a secured SSL channel. The server listens for communication on a certain port. In the default configuration, port 143 is for IMAP and 993 for SSL IMAP. If a computer has multiple IP addresses, it is possible to select one IP address where the (SSL) IMAP server will listen.

## Attachment Filter

Incoming and outgoing messages can include attached files. It is possible to block message attachments with specific file extensions. Messages including these attachment extensions will be processed according to the following settings:

- **Check delivered e-mail messages for unwanted attachment extensions:** Enable or disable attachment filtering.
- **Unwanted attachment extensions:** Enter the extensions of attached files that will be blocked by the attachment filter.
- **Don't check:** Choose if you want to check messages for/from Administrators or local messages.
- **Incoming/Outgoing message:** Here you can define an action if a message includes an unwanted attachment extension.

**NOTE: This filter does not check the file content, only the file name extension.**

## LDAP

The [LDAP](#) (Lightweight Directory Access Protocol) server allows clients to find contact information (e-mail addresses) of other users from the Software602 Groupware Server. Searching is generally performed by the e-mail client (e.g. Outlook Express, Thunderbird).

If you want to make the LDAP service available, enable the LDAP server. If the computer running Software602 Groupware Server is connected to the Internet and you have multiple IP addresses, you have several possibilities under the `IP address` option. Due to security reasons it is recommended to select the internal IP address. This will prevent the address list from being accessible from the Internet.

The default port the LDAP service is listening on is 389. A common method of securing LDAP communication is using SSL. The default port for LDAP over SSL (LDAPS) is 636.

## Archive

Archive messages sent and received by the Software602 Groupware Server. This read-only archive is compressed and encrypted. Different archive settings can be defined for incoming messages and outgoing messages. A limit on attachment size is also available.

`Archive administration` gives you the ability to remove old messages from the archive and export them into the .EML format.

## IM Services

eXtensible Messaging and Presence Protocol (XMPP) is an open, XML-inspired protocol for near real time, extensible instant messaging (IM) and presence information. Unlike most instant messaging protocols, XMPP is based on open standards. Like e-mail, it is an open system where anyone who has a domain name and a suitable Internet connection can run their own Jabber server and talk to users on other servers.

**IM SERVICES**

eXtensible Messaging and Presence Protocol (XMPP) is an open, XML-inspired protocol for near real time, extensible instant messaging (IM) and presence information. Unlike most instant messaging protocols, XMPP is based on open standards. Like e-mail, it is an open system where anyone who has a domain name and a suitable Internet connection can run their own Jabber server and talk to users on other servers. You can obtain client software for the IM server, [here](#).

Enable IM server

Domain name:

IM port for communication between server and clients:

IM port for communication between servers:

Enable SSL

SSL communication port:

IP address for SSL communication:

**Synchronize IM configuration**

The IM server has been tested with the following Instant Message clients: Psi, Miranda, Qip, and Pidgin. You can obtain client software for the IM server, [here](#).

The following client settings are required:

[x] Use SSL encryption / Force old SSL (**port 5223**)

-or-

[x] Allow Plaintext Login / Allow plaintext auth over unencrypted streams (**port 5222**)

**NOTE: Do not use the plain-text login over untrusted networks (e.g. the Internet).**

Click the `Synchronize IM configuration` button when you have added or deleted users from the `Instant Messaging users` group. This will ensure that the buddy list of the IM server is synchronized with active Groupware users.

## Web Services

This section provides access to all settings related to the built-in Web/WebDAV server.

### Web Server/SSL Web Server

Enable `Web/WebDAV server`, if you want to use the functionality of the web server. It is possible to select the IP interface on which the server will listen from the `IP address` field. The default value is all interfaces, but you can select a specific interface if needed. Use the `Port` field to specify the port used for communication (default value is 80).

Software602 Groupware Server also includes an SSL web server that provides a secure client connection. Setup the SSL web server just like the web server (above). The default port the SSL web server listens on is 443 (Installation of an [SSL certificate](#) is required).

**NOTE: The built-in Software602 Groupware Server web server is REQUIRED for administration. Either the web server or the SSL web server MUST be enabled.**

The web server provides the following functionality:

- **Home directory:** Path to the root directory in the field.
- **Index file name:** File name that will be used as the index page (e.g. index.htm or index.html).
- **Script directory:** Directory with CGI or FastCGI scripts.
- **Environment variables for scripts:** Environment variables used with scripts.
- **IP filter defines access:** The IP filter rules are checked from top to bottom with each rule superseding those above it. Enter the IP address and mask of the computer or network that sends the request to the field IP address and IP mask. It is also necessary to define if the item is allowed or prohibited (RED = denied, GREEN = permit).
- **Enable directory browsing:** This will allow web visitors to browse directories on your web server that do not include an index page.

### Virtual Directories

Virtual directories are web directories generally located outside of the basic web directory structure and have various special features (authentication, launching various type applications, etc.).

To use an `Alias` on the web server, define them using the following values:

- **Alias:** Define the Alias as to how it will be accessible from the WWW server.
- **Path:** Define the local path you would like to alias.
- **Environment variables:** It is possible to include an application (EXE file) to the URL request. Separate each parameter with a semicolon.

Adding a virtual directory with `ASP.NET (.aspx)` support creates a virtual directory where the web server processes [ASP.NET](#) web application framework pages. Use the `Environment`

`variables` field, to add additional items to environment variables that the launched application receives from the system. The variables are entered in the following format:  
<variable\_name1>=<value1>;< variable\_name2>=< value2>

To use a `Mapped application`, register the application by defining the following values:

- **Mapped application name:** Application name that will be presented in the list.
- **Extension:** Enter the file extension (e.g. `.php`).
- **Path to EXE file:** Enter the application EXE file name with full path. The WWW server will run this application upon URL request with the included extension entered in the extension field.
- **Environment variables:** It is possible to run the mapped application with specific parameters. Separate each parameter with a semicolon.

WebDAV (Web-based Distributed Authoring and Versioning) refers to the set of extensions to the Hypertext Transfer Protocol (HTTP) that allows users to collaboratively edit and manage files on remote web servers.

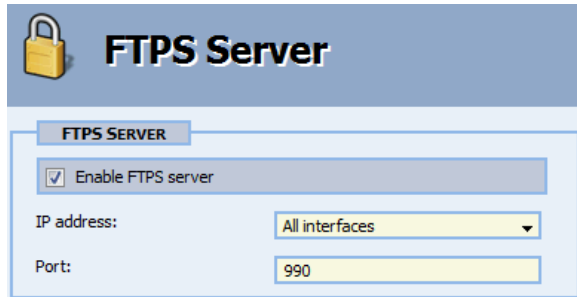
**NOTE: WebDAV access to Software602 Groupware Server folders is only accessible using the built-in web server or SSL web server.**

## Administration

Software602 Groupware Server Administration can be used on a different port for enhanced security. Once this option has been enabled, administration will not be available on the standard web server. Access will only be available from this port. It is possible to enable SSL (`https`) communication on this port by enabling the `Use SSL protocol` option.

## FTP Services

The included [FTP/FTPS](#) server provides access to documents stored within the Software602 Groupware Server document storage. The FTP/FTPS server must be enabled and the interface selected. The default port for FTP is 21, and for FTPS is 990.



The screenshot shows a configuration window for the FTPS Server. At the top, there is a blue header with a yellow padlock icon and the text "FTPS Server". Below this, a tab labeled "FTPS SERVER" is active. The configuration area includes a checked checkbox for "Enable FTPS server". Below the checkbox, there are two fields: "IP address:" with a dropdown menu set to "All interfaces", and "Port:" with a text input field containing the value "990".

Local users and external users can access `Public Documents`. Public access (FTP path `/public/`) is for read only access. For write access (create/modify/delete), use the following path `/documents/shared/public/`.

## Anti-virus

Software602 Groupware Server includes the BitDefender anti-virus engine. All e-mail messages, local server files, and Groupware Server objects will be scanned using this anti-virus engine. The Groupware Client also includes an ActiveX component to provide scanning of client files from within Microsoft Internet Explorer.

Seamless integration with BitDefender provides an enhanced virus warning system. All infected parts of an e-mail can be removed, an e-mail notification to the recipient can be sent and the entire message can be delivered to a special account for later review. To activate scanning, `Enable anti-virus scanning of delivered e-mail messages`.

If the message is infected, you have the following options:

- Send to recipient
  - Notification
  - Notification with original message body
  - Notification with original message body and attachment(s)
- Send to special account – select an account from the combo box
  - Notification
  - Notification with original message body
  - Notification with original message body and attachment(s)
- Send a notification to administrator(s)

All scanned e-mail can be stamped with a `Certification` tag. Here you can enable certification if desired and define the certification message.

New viruses are released daily. To keep your virus protection up-to-date we recommend checking the `Enable automatic Anti-virus updates` checkbox. It is possible to enter an interval in hours that you wish to update the virus database. If you want to update the virus database manually, click the `Update Now` button.

# Anti-spam

Software602 Groupware Server uses the latest technology to block unsolicited e-mail and prevent your system from abuse. Multiple protection options include: Commtouch real-time filter, SMTP security, DNSBL lookup, Bayesian filtering, Blacklist, Whitelist and IP filtering.

## Message Classification

If the Real-time filter or the Bayesian filter classifies an e-mail message as Junk, it is possible to select one of three actions:

- **Delete:** Deletes the message immediately
- **Send to user:** Send the message to the user
- **Send to Anti-spam account:** Send the message to the Anti-spam account for further processing. The Anti-spam account can be assigned to any Software602 Groupware Server user, but we recommend creating a dedicated user account for junk e-mail. A message will be sent to this account on each Bayesian update request.

You can define the following options regardless of action:

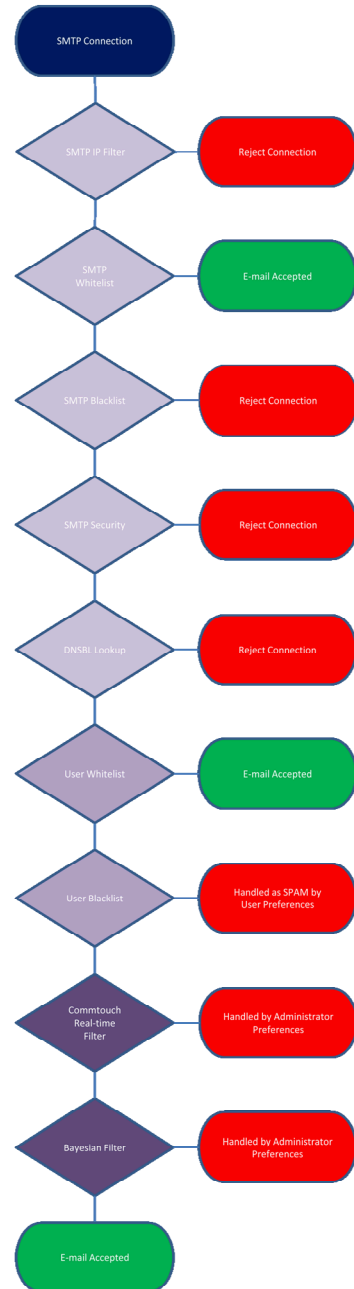
- Add X-LNS Spam-Check header to the message
- Add the following subject text to Junk E-mail

## Real-time Filter

The real-time filter is based on Commtouch’s Anti-spam service. Commtouch analyzes billions of transactions in real-time to identify new spam, malware and zombie outbreaks as they are initiated. Real-time messaging security based on Recurrent Pattern Detection (RPD)<sup>™</sup> technology provides a maintenance-free solution that works out-of-the-box.

## Bayesian Filter

The architecture of the Bayesian anti-spam filter system has a few distinct parts. The first, and most obvious, is the content engine that takes an e-mail message and breaks it up into a series of words. At this moment it takes words out of the text part of the message, stripping out various HTML code and other bits of unneeded information. A variety of e-mail header interpretation and internal serialization goes on as well.



**Technical description of the Bayesian filter:** <http://spambayes.sourceforge.net/>

The Bayesian filter will attempt to classify incoming e-mail messages as Junk (spam) or Not Junk (good e-mail). This means you can have Junk messages automatically filed away into a different e-mail folder where it will not interrupt your e-mail reading.

The Bayesian filter **MUST** be trained to identify Junk and Not Junk e-mail. Essentially, you will show the Bayesian filter a number of e-mail that you like (Not Junk) and a number of e-mail you do not like (Junk). The Bayesian filter will then analyze the e-mail for clues as to what makes the messages different. For example: different words, differences in the e-mail headers and content style. The system will then use these clues to examine new messages.

The Software602 Groupware Server Bayesian filter will classify incoming e-mail messages and the outcome of this classification will be entered into the e-mail header. If incoming e-mail is classified as Junk, Groupware Server can (according to the settings) insert a text string into the e-mail subject and insert a score into the e-mail header.

Users can train the Bayesian filter in several ways:

- **Groupware Client:** Users can classify received e-mail by clicking the `Junk` or `Not Junk` buttons from the inbox. It is also possible to use the option `Automatically learn from senders listed in the white list` found under `Settings` to train the Bayesian filter automatically.
- **Any third-party e-mail client:** Users can classify received e-mail by forwarding the message to: `junk@junk` for Junk or `notjunk@junk` for Not Junk.

### **Bayesian filter learning**

- Enabling the `Automatically learn from senders listed in the white list` option will automatically train the Bayesian filter from these senders.
- Select a method on how the Bayesian filter will be updated when users classify e-mail as Junk or Not Junk.

### **Bayesian filter backup**

The Bayesian anti-spam database can be saved at anytime. We recommend backing up the database to fix a situation when a large amount of messages has been improperly trained or [Bayesian poisoning](#) has occurred. In these cases you can restore a previous database.

### **SMTP Whitelist & Blacklist**

Software602 Groupware Server SMTP server supports a blacklist and whitelist. The SMTP server will reject / accept incoming messages based on these lists. Here you can enter a specific host or sender from which you do not want to accept e-mail from (Blacklist) OR from which you always want to accept e-mail from (Whitelist).

Description of host and sender:

- **Host:** A host would be the mail host of the sender. If the mail host for e-mail address bob@company.com is mail.company.com enter mail.company.com.
- **Sender:** The sender would be the complete e-mail address of the sender. To block/allow bob@yahoo.com, enter bob@yahoo.com. To block/allow ALL addresses from company.com enter \*@company.com.

**NOTE: A host can send e-mail for multiple domains. So, you could possibly be blocking mail from more than one domain.**

## DNSBL

Software602 Groupware Server will immediately reject incoming messages according to the outcome of a request sent to a DNS lookup service. Protection via DNS Blacklist (DNS-bl) is a cooperative effort by providers across the Internet to deny service to known spam domains. Some provide this service for free (in Groupware Server the Anti-spam list includes the keyword [FREE]) and some of them are a paid service (keyword [PAY]).

There are many anti-spam database categories:

- **Spam:** Includes confirmed spammers. Highly recommended.
- **Dial-up:** Includes dynamic assigning IP addresses. Recommended.
- **Open Relays:** Includes unsecured e-mail servers on the Internet that will relay e-mail for anyone. Highly recommended.
- **Combined:** Includes any combination of the above. Use at your own discretion.

Add a service by clicking the `Add service` button. Here are the available options:

- **Service name:** Descriptive name of a DNS lookup service provider.
- **DNS lookup domain:** The lookup domain on which the service runs.
- **IP address returned when host is listed:** The anti-spam service provider defines the returning IP address if the domain from which the e-mail is coming is in the spam database.
- **Response if denied:** Define the text message to send if the incoming e-mail is from a spam domain.