



602LAN SUITE 5.0 Groupware

Administration Manual

Table of Contents

Table of Contents	2
Introduction	3
System Requirements.....	4
602LAN SUITE Groupware Console.....	5
License	6
Console	6
User Management.....	6
Users	6
Groups.....	7
User Import.....	8
Connection	9
Mail.....	11
SMTP	11
POP3.....	14
IMAP.....	15
Anti-spam	15
Attachment Filter.....	17
Archive	17
Fax Server	18
Internet	20
Proxy	20
NAT	24
Firewall	25
Web Server/SSL Web Server.....	25
SSL	27
DHCP.....	29
LDAP.....	30
FTP/FTPS.....	30
Content Filter	31
Anti-virus.....	33
Maintenance.....	34

Introduction

602LAN SUITE Groupware administration can be performed from a web browser by connecting to the built-in 602LAN SUITE web server (not IIS) using the predefined virtual directory `groupwareadmin` (see [602LAN SUITE Groupware 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 displays the 602LAN SUITE Groupware Admin interface. The top navigation bar includes icons for Status, Users, Groups, Console, and Queue. The left sidebar shows a tree view of administration options: Administration, License, Console, User Management (Users, Groups, Import), Connection, E-mail, Fax, Internet, Content Filter, Anti-virus, and Maintenance. The main content area is divided into two sections: PRODUCT and DATABASE.

PRODUCT	
Update	
Product:	602LAN SUITE 5 Groupware
Operating system:	Microsoft Windows NT 5.0.2195.0
.NET framework version:	1.1.4322.2032
Application version:	5.0.07.1012
Last update:	Never

DATABASE	
Database server name:	GROUPWARE
Database application name:	GW
Application creation date:	10/12/2007 1:57 PM
602SQL version:	Windows 10.0.2.919
Database schema (language/version):	US/88
Index file storage:	C:\Program files\Software..... 5 Groupware\SQL\DATABASE

NOTE: The correct access URLs can always be found from the 602LAN SUITE 5 Groupware Console application.

System Requirements

The recommended system configuration for 602LAN SUITE Groupware is a dual-core machine with Windows® 2003 Server and 1GB RAM. Below are the minimum requirements:

Operating Systems

- Windows® 2000 Professional
- Windows® 2000 Server
- Windows® XP Home
- Windows® XP Professional
- Windows® XP Professional x64 Edition
- Windows® Vista
- Windows® Vista x64 Edition
- Windows® Server 2003
- Windows® Server 2003 x64 Edition

Memory and Hard Drive Space

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

Groupware Server Requirements

- Microsoft® .NET Framework 1.1 with Service Pack 1 (SP1)
- Microsoft® Internet Information Services 5.0 or higher (optional)

Client Requirements

- Microsoft® Internet Explorer 6.0 or higher
- Mozilla® Firefox® 2.0 or higher
- Outlook Connector requires Microsoft® Outlook 2002 or higher
- Thunderbird Connector requires Mozilla® Thunderbird 2.0 or higher

602LAN SUITE Groupware Console

The 602LAN SUITE Groupware 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**.

The screenshot shows the 602LAN SUITE Groupware Console 5.0.07.0906 application window. It is divided into several sections:

- Groupware Admin:** Fields for Groupware Admin port (8080), Groupware Admin alias (groupwareadmin), and Groupware Admin access (<http://localhost:8080/groupwareadmin>).
- Groupware Client:** Radio buttons for "Use Microsoft Internet Information Services (recommended)" (selected) and "Use 602LAN SUITE 5 Groupware Web server on port: 8080". Fields for Groupware Client alias (groupware) and Groupware Client access (<http://localhost/groupware>).
- Services:** Status for SQL, LNS, and IIS services (all "Service started."). Buttons for "Stop Groupware services" and "Start Groupware services".
- Groupware Logs:** Buttons for "View Groupware Server Log" and "View Groupware Data Storage Log".
- Database repair:** Buttons for "Begin repair" and "Show results".
- Bottom Section:** Buttons for "Apply and Restart Services" and "Exit".

- **Groupware Admin port:** Enter the port the 602LAN SUITE 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 602LAN SUITE 5 Groupware 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.
- **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.

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.

602LAN SUITE Groupware is installed as a fully functional 30-day trial. License activation must be performed before the end of the 30th day and requires an Internet connection.

Console

Console

View the real-time activity log of the 602LAN SUITE Groupware server.

Queue control

Basic commands for server queue control (reload queue, force collection of POP3 mailboxes, disable POP3 collection, and disable queue processing).

Connection statistics

Display the numbers of transferred bytes since server start.
(Statistics of space used by users is found in Maintenance section).

User Management

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

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 and fax 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. Assignment of the fax MSN number (CAPI only) provides delivery of incoming faxes to this user (more information under [Fax Server](#)). This user will also receive faxes sent from devices with the fax IDs specified, comma separated.

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 (a local user, it cannot be an external user) and then it is 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

602LAN SUITE Groupware supports two types of groups: user groups and system groups. System groups are described as follows:

1. System groups for allowing access to services:
 - **Unsorted mail operators:** Incoming messages where it is impossible to identify a recipient will be copied to the inbox of users specified here.
 - **Unsorted Fax Operators:** Delivered faxes that are not sorted by Fax ID or CAPI MSN number will be delivered to users specified here.
 - **Fax users:** Users listed here can send faxes.
 - **LDAP users:** Users listed here can login to the LDAP server.
 - **Internet mail users:** Users listed here can send messages to the Internet.
 - **Proxy users:** Users listed here can use the HTTP proxy (provided it requires authentication, otherwise all users have permission).
2. System groups for defining access permissions to shared folders:

- **Administrators:** Read and write access to Public Folders and Shared Folders.
- **Everyone:** Read access to Public Folders.
- **Customers:** Read access to Public Folders.
- **Users:** Read access to Public Folders and Shared Folders.
- **Power Users:** Read and write 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 602LAN SUITE 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

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 602LAN SUITE Groupware to establish and terminate the connection, enable the Dial-up connection and complete the Dial-up schedule. 602LAN SUITE Groupware 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 602LAN SUITE Groupware 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.

On Request Schedule

If you want 602LAN SUITE Groupware to connect to the Internet upon a client request for SOCKS, DNS or any Proxy services, enable `Upon client request to proxy server`. You must check this if you want the server to connect to the Internet if a client makes a request for the proxy. Enter the number of minutes into the `Disconnect` field.

If you do not want to establish a dial-up connection from a DNS request, set this option under `Administration -> Internet -> Proxy`.

E-mail Schedule

Enable this when you want 602LAN SUITE Groupware 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 602LAN SUITE Groupware to obey this rule.

POP3 Schedule

Use this option to tell 602LAN SUITE Groupware 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 602LAN SUITE Groupware should obey this rule.

Release TAPI Device Schedule

This setting allows 602LAN SUITE Groupware to share a single dial-up modem for both faxing and Internet access. When a specified number of fax messages are waiting to be sent, 602LAN SUITE Groupware will automatically release the Internet connection long enough to send the faxes. It will then re-connect to re-establish the connection.

Mail

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. All combinations of user names, the default domain, domain aliases, and user aliases, will be shown here. The red icon denotes the default (first) address of that user.

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). 602LAN SUITE Groupware 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 computer. Preset routes can contain e-mail 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 602LAN SUITE Groupware 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 602LAN SUITE 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 602LAN SUITE Groupware users (enable `Allow SMTP relay`

for 602LAN SUITE 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 602LAN SUITE 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 authentication by IMAP and POP3 authentication method, too:** 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.

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.

SMTP Whitelist & Blacklist

602LAN SUITE Groupware 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

602LAN SUITE Groupware 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 602LAN SUITE Groupware 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.

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 602LAN SUITE Groupware 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. 602LAN SUITE Groupware 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.

Anti-spam

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

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.

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 602LAN SUITE Groupware 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, 602LAN SUITE 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.

If the Bayesian filter classifies e-mail 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 602LAN SUITE Groupware 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

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.

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.

Archive

Archive messages sent and received by the 602LAN SUITE 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.

Fax Server

The 602LAN SUITE Groupware Fax server allows sending and receiving of faxes using an analog fax modem (TAPI) or ISDN (CAPI) device. Enable the `Fax server` and select either `TAPI device` or `CAPI device` depending on what fax device you will be using.

Here is a list of available options:

- **Fax identification:** Enter a string into the field Fax identification that includes the identification information about the fax sender. This information is transmitted to the counterpart fax machine during the first stage of transmission and allows the receiving party to identify you. This should include your fax number.
- **Print received faxes using:** If you wish to automatically print all incoming faxes to a printer, select the printer here.
- **Activate fax server:** Number of seconds the fax server should check the fax queue.
- **Resend interval:** If a sending attempt was unsuccessful, the server will send the unsuccessful fax message after the entered amount of minutes.
- **Max attempts for delivery:** The number of times to attempt delivery. The first attempt consists of four dial attempts and the next attempt will consist of two dial attempts.
- **Add this header line to each fax message:** It is possible to enter a message into the field Header line text that will be printed first on a fax message. This information can include, for example, your identification.

TAPI

This tab sets the TAPI device parameters. All available TAPI devices are listed in the `TAPI device` list. All TAPI options are as follows:

- **Settings:** Modem commands to configure your modem.
- **Modem reset:** Modem commands to reset your modem.
- Controlling commands: Fax modems have several sets of control commands in their fax section. The option Controlling Commands enables you to select this set directly or let the server attempt auto-detection.
 - **Class 1:** The oldest of the three classes, lets the computer carry out most of the fax operations and thus leaves most of the operation up to the computer. This set was arranged into a standard and therefore is frequently implemented in fax modems and control programs. The original standard did not include a definition of how the modem should distinguish a data call from a fax call when receiving a message. Older types of US Robotics modems support Class 1. Class 1 and Class 2 are supported by all modems based on the ROCKWELL chipset.
 - **Class 2:** The fax modem carries out a number of communication operations (checking for a common protocol with the counterpart fax, page confirmation, transmission termination) itself or as a response to a single AT command. This set was never arranged into a standard; it was only formed as a set of recommendations

that manufacturers sometimes did not adhere exactly to. This is the reason why there are some problems with this class. Differentiation between fax and data is not clearly defined here. This set is widely used with fax modems. ZyXEL supports this class in all FW versions, US Robotics has not implemented this class because it is not an official standard.

- **Class 2.0:** The latest version, with its structure of commands and method of operation, is very much like Class 2, but the commands are shorter and there are some extra commands that solve the problems with Class 2. This set is fully standardized and is not widely used yet, but its popularity is increasing. ZyXEL Elite, ZyXEL 1496 FW 6.12+ and US Robotics support this standard. ROCKWELL does not support it.
- **Transmission/Reception speed limit:** Enables you to decrease the maximum fax transmission speed to the specified limit and thus adjust it to the line quality. There is a standard range of speeds from 2,400 to 14,400 bit/s or select unlimited.
- **Pickup after ring count:** Specifies the number of rings after which the server will answer the incoming call.

CAPI

ISDN data terminal devices usually offer control using the CAPI 2.0 interface (Common ISDN API) and can support fax functions. Provided that the CAPI interface was detected in Windows (CAPI2032.DLL file exists in Windows) and fax support was detected during CAPI initialization, CAPI can be used for faxing. To connect the CAPI interface, enter a phone number assigned to this phone line (MSN = Multiple Subscriber Numbering). If you do not enter a number, the server will reply to all calls on this line. If you have multiple MSNs, it is possible to assign individual users these MSNs and faxes will be delivered directly to them.

Internet

The *Internet* section deals with Internet services for your network. This includes proxy services, web services and LDAP services.

Proxy

A proxy server runs on a computer that is connected to the Internet via a permanent or dial-up line. The proxy server receives requests from clients on the network and forwards them on its own. Fulfilled requests (web pages) are then delivered to the proper clients.

A proxy server provides two functions:

- **Proxy:** It proxies clients on the network with a connection to the Internet via the HTTP/HTTPS/HTTP-FTP application protocols.
- **Security:** Because all communication goes through the server, it can check every computer that wants to communicate with any client computer on the Internet via the HTTP/HTTPS/HTTP-FTP application protocols.

All proxies are setup for unrestricted access by default. These settings will not need to be altered or changed for most users, but can be modified depending on your individual desires or security concerns. You may activate/deactivate any proxy service by enabling/disabling the respective checkbox. Simply alter the port number in the respective port field will change the port the service is listening on. All ports are set to industry standards by default.

Individual proxy services may be enabled/disabled or have ports modified as follows:

- **HTTP/HTTPS/HTTP-FTP proxy:** This is the proxy that provides access via the hypertext transfer protocol. Web pages and files downloaded by this proxy can be checked by the [Anti-virus](#) engine and [Content Filter](#).
- **SOCKS proxy:** This controls the SOCKS protocol, which is frequently used by instant messaging programs as well as programs that do not provide direct proxy support. The SOCKS 4 and SOCKS 5 standards are supported.
- **FTP proxy:** This proxy controls the FTP (File Transfer Protocol), which is commonly used for the transfer of files over the Internet.
- **Telnet proxy:** This proxy service allows the communication of telnet applications.
- **RealAudio proxy:** This proxy is specifically designed to allow the use of the popular RealAudio program from Real Networks, Inc.
- **DNS proxy:** While not a true proxy service, this option allows 602LAN SUITE Groupware to process DNS (Domain Name Server) requests for other computers on the network.

The HTTP/HTTPS/HTTP-FTP proxy listens on port 80 by default. If you are running a third party web server (e.g. Microsoft Internet Information services) you may need to alter this number to avoid port conflicts.

Automatic proxy discovery

The `Enable automatic discovery` feature allows you to distribute WPAD information from the included `DNS proxy`. To enable automatic discovery, do the following:

1. Enable the `HTTP/HTTPS/HTTP-FTP proxy`.
2. Enable `Automatic discovery`.
3. Enable the `DNS proxy`.
4. Click `Save` to save the settings.
5. Configure the network user's TCP/IP information to use the IP address of 602LAN SUITE Groupware as the DNS server.
6. Configure the network user's web browser to `Automatically detect settings` (Internet Explorer) or `Auto-detect proxy settings for this network` (Firefox).

NOTE: If you are using a third party DNS server, you simply need to add a "wpad" record as an Alias and point it to the IP address of 602LAN SUITE Groupware. Please consult your DNS server documentation for information on adding a record.

Advanced proxy settings

This is recommended for slow connections where bandwidth is a major concern. By enabling this feature, you activate proxy cache that stores web pages on the server allowing them to be retrieved quickly from the hard drive as opposed to over a slow Internet connection.

The following options are recommend to be enabled for effective cache use:

- **File info required:** Most web servers provide information on a file, this allows 602LAN SUITE Groupware to determine if the file has been downloaded completely, with this option checked, only files verified complete will be saved to the cache.
- **Do not cache CGI queries:** 602LAN SUITE Groupware will not cache results from a CGI request (dynamic web page).
- **Allow cache control by HTTP commands:** 602LAN SUITE Groupware will obey HTTP caching commands (example: `Pragma: no-cache`)

Proxy IP filter

The IP filter defines what connections are possible to establish through the Proxy and SOCKS services. Through the IP filter we can define which connections can be established through the SOCKS or Proxy Server. You will create a list of networks and stations and define if access to them is allowed or prohibited. The IP filter rules are checked from top to the 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 `Source IP address` and `Source mask`. Enter an IP address and mask to the `Destination IP address` and `Destination mask` where the request is pointed. It is also necessary to define if the item is allowed or prohibited – a RED icon means access denied, a GREEN icon means access enabled.

A TCP/IP computer network is defined by the IP address and mask. The IP address defines the value addressed in the network and mask defines the size of the network (the maximum amount of IP addresses in a particular network). Mask examples:

```
255.255.255.255 -- single user, the computer with IP address given above
255.255.255.0 -- all computers on the Class C network
255.255.255.224 -- subnetwork with 32 addresses
0.0.0.0 -- all IP addresses (all Internet)
```

With the IP filter it is possible to verify whether a connection between two specific computers are allowed (e.g. a user wants to connect to `www.software602.com`). 602LAN SUITE makes a logical decision with the IP address of the computer that wants to establish a connection (source IP address); with the IP address of the destination computer (destination IP address) and the IP Filter follows the logic operation:

To grant access, the following must apply:

```
SOURCE_IP AND SOURCE_MASK = WHO_IP AND SOURCE_MASK
DESTINATION_IP AND DESTINATION_MASK = WHERE_IP AND DESTINATION_MASK
```

The connection will be established if the results of both logic operations are true and the rule is green. IP filter rules are checked from top to bottom

Example:

- Restrict three employees with following IP addresses – 192.168.1.25, 192.168.1.35, 192.168.1.38
- Allow all others Internet access
- Outside users from the Internet need to have access to only one computer with the 192.168.1.1 IP address.

Solution:

- The first three rules deny the three computers 192.168.1.25, 192.168.1.35, 192.168.1.38 access to any computer through the firewall (i.e. this restricts these three employees access the Internet).
- The fourth rule grants all users of the 192.168.1.0 network communication with any computer through firewall (i.e. it allows all users including 192.168.1.25, 192.168.1.35, and 192.168.1.38 users access to the Internet). But, since the IP filter rules are checked from top to the bottom, users 192.168.1.25, 192.168.1.35, 192.168.1.38 do not have access to the Internet.
- The fifth rule grants any communication with 192.168.1.1 through the firewall (i.e. this rule allows ANY Internet users access to the 192.168.1.1 computer).

NOTE: If the fourth rule were in the first position, it would not be able to restrict the users 192.168.1.25, 192.168.1.35, or 192.168.1.38.

Site Access

Restricted/allowed users are specified by their IP address and mask. It is possible to restrict/allow specific URLs for a single computer or sub-network. To specify the entire network input 0.0.0.0 for the `Source IP Address` and `Source Mask`. If only a specific machine or group of machines need to be denied/allowed access, put the specific IP (i.e. 192.168.1.23, mask 255.255.255.255) or group (i.e. 192.168.1.0, mask 255.255.255.0). Unlike the IP filter, the restricted/allowed sites are defined by their name or part of their name where * and ? symbols can be used (convention: * = alias all, ? = mask).

By using * and ? characters, you can construct common masks. Enter the IP address and mask of the computer or sub-network that the URL will be restricted/allowed.

Examples: *.hate*. * restricts access to servers in which the domain name begins "hate" for all services (HTTP, HTTPS, FTP) *.shopping.??? restricts access to the domain shopping in all 3 digit endings(i.e. www.shopping.com, www.shopping.org, etc.) for all services (HTTP, HTTPS, FTP), www.espn.com restricts access to the server of the given name.

Mapped Links

Mapped links provide an alternative to establishing a connection between a workstation on the LAN and a host computer on the Internet. It is a useful alternative when an application does not supports SOCKS/PROXY and connects with only one computer on the Internet.

If a client program on a network workstation needs to establish a TCP/IP connection with a particular computer on the Internet. Instead of using the address of that computer, the IP address of the 602LAN SUITE Groupware server is entered into the program in which a mapped link is used to specify that if a connection to this port, all packets should be sent to a particular computer on the Internet. It is like a re-director between two computers.

You need to setup these entries for a Mapped link:

- **Protocol:** Select the Protocol (TCP or UDP, UDP1, UDP2) for each mapped link.
- **Connection from client:** The information you enter in this section is for the machines that are allowed to make the connection. Enter the IP address and IP mask of the computer that will need the mapped link.
 - **IP Address:** You should enter the network address or the IP address of the machine/machines you wish to allow access to this link. Example: If you wish to allow everyone on your network and no one else access to this link, enter your network address. If you are unsure what your network address is, you can obtain it by take taking the IP address of the 602LAN SUITE server and changing the last value to a 0 (i.e. 192.168.1.0). To let only one machine access it, enter in that machines IP Address. To allow anyone to access this link use 0.0.0.0.
 - **IP Mask:** This is the subnet mask for the machines you wish to allow. The detailed explanation of how a mask works is beyond the scope of this document. The general idea of how to use it is if you only wanted one machine to access this link, it would be 255.255.255.255. If you want your entire network to access it, then enter 255.255.255.0. If you want to give everyone access, make it 0.0.0.0.

- **To this computer:** This is what interface the mapped link will be accessible from.
 - **IP Address:** Set to all interfaces. The only reason this would need to be changed is if you wanted to increase security for access to the mapped link.
 - **Port:** This is the port that this machine will listen on for requests coming through this link. This will vary based on what you wish to accomplish. You cannot have a port that is already in use added here. If you already have a mapped link that listens on port 9000, then you cannot add another port 9000 link. You can't use ports 80, 21, 23, and 1080 if you are using them for your proxy server. The link will not work if the port is already in use.
- **Map to:** Enter the Host address and Port. Enter the IP address and port of the host the client needs to establish a connection with.
 - **Host address:** You can enter the domain name or IP address of the computer you are trying to contact.
 - **Port:** This is the port that the computer you wish to connect to is listening on. Unlike the port under To this computer, you can reuse this port.

NOTE: You cannot have two services using the SAME port on the SAME interface.

NAT

NAT requires that at least two interfaces be installed on the computer where 602LAN SUITE is running (e.g. two NICs or a NIC and a Dial-up adapter). To begin using NAT you must first `Enable network address translation`. Next, select the connection you wish to share under `Shared interface`. Now, select the internal network(s) under `Private interface` to define what network(s) will be allowed to access NAT. If an interface has more than one IP address you can select the addresses as needed.

Example:

A computer with 602LAN SUITE Groupware has one internal interface with the IP address 192.168.1.1 and 255.255.255.0 mask. Workstations that need access to NAT must be configured in the following way:

- **IP address:** 192.168.1.x (where x is a number from 2 - 254)
- **Mask:** 255.255.255.0
- **Gateway:** 192.168.1.1

The `NAT IP Filter` defines what connections are allowed to access NAT services. 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 means access denied, GREEN means permit access. If the IP filter includes a rule, all data transmission is prohibited except transmission defined by this rule. If the IP filter does not contain a rule, all data transmission is allowed.

Firewall

The firewall protects the computer where 602LAN SUITE Groupware is running and the entire Local Area Network against unauthorized TCP/IP connections. It is necessary to have at least two interfaces (1 - internal connection to your Local Area Network and 2 - External connection to the Internet).

NOTE: Improper firewall settings can cause disruption of 602LAN SUITE Groupware services such as SMTP, IMAP, POP3, Proxy, etc.

The firewall includes the following options:

- **High:** Direct connections between the internal network and the Internet are denied. Internal network computers must use the proxy server to access the Internet.
- **Medium:** TCP/UDP connections from the internal network to the Internet are allowed.
- **Low:** All TCP/UDP/ICMP communication is allowed except file sharing (NetBIOS).
- **Custom:** Custom firewall settings.

WARNING: The firewall rules supersede the IP filter rules. This means that access to a given service that is denied by the firewall will never get to the IP filter.

For proper firewall functionality, choose the interface to which your LAN is connected (your internal network interface). Interfaces not selected are designated as Internet interfaces.

If you do not check any interface as the internal network interface, only the computer where 602LAN SUITE Groupware is running will be protected. Remember, each set or rule means **ALLOW** access. If no rules are defined then ALL IP communication is **DENIED**.

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).

602LAN SUITE Groupware 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 602LAN SUITE Groupware 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.
- **User home directory:** The directory path where personal user pages will be placed.
- **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.

User home directory

Once the user home directory has been defined, 602LAN SUITE Groupware will create a sub-directory of the user name in this folder when a new user is created. In contrast to a typical web server, user directories can be accessed via `http://computername/~username` regardless of the folder setting.

A user can update their home directory in the following ways:

- **Copy files via file sharing:** Use Windows file sharing to copy files to the appropriate user folder.
- **Upload pages via the FTP protocol:** In this case the user folders must be created as a subdirectory under the main web server directory.

If the user is not an administrator = will access their user folder.

If the user is an administrator = will access the root of the web server.

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 602LAN SUITE Groupware folders is only accessible using the built-in web server or SSL web server.

SSL

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
- 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 where 602LAN SUITE is running
- **Contact e-mail:** The administrator or webmaster e-mail address
- **Country:** Select your country
- **State or province:** Select your state or province
- **Key length:** Select key length. A longer key means higher security, but more data to transmit.

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 602LAN SUITE directory). Your information (Organization name, domain name, etc.) is stored in the file `SSLEAY.CFG` (root of your 602LAN SUITE 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 602LAN SUITE Groupware. Click the `Input Signed Certificate` button and input your signed certificated.

Advanced

- **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:** 602LAN SUITE will communicate with clients by SSL version 2 only.
- **Just talk SSLv3:** 602LAN SUITE 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, check the Turn on SSL bug compatibility checkbox.

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.

DHCP

[DHCP](#) (Dynamic Host Configuration Protocol) provides basic TCP/IP settings for network workstations. Workstations can use the DHCP server to obtain an IP address, mask, DNS and more. Dynamic IP assignment means easy administration and also conserves assigned IP addresses to the amount of in-use workstations only. DHCP uses the UDP protocol on port 67 and 68. DHCP is an open standard, developed by the Dynamic Host Configuration working group (DHC WG) of the Internet Engineering task Force (IETF).

To begin using the DHCP server you must first `Enable DHCP server`. Also make sure that the IP address of the INTERNAL network is selected for the `IP address` option.

Next you will need to define a `Start IP address` and an `End IP address`. We suggest using a [Class C](#) IP address such as 192.168.x.x. The start should be 192.168.1.10 and the

end can be up to 192.168.1.254. Starting with 192.168.1.10 allows 9 IP addresses to use on servers and PCs you wish to not use DHCP (192.168.1.1 - 192.168.1.9). Multiple intervals can be defined.

There are many DHCP options and variables supported, but you only need three:

- **subnet-mask:** This should be set to 255.255.255.0
- **domain-name-servers:** This should be set to the IP address of the computer running 602LAN SUITE Groupware (with the DNS proxy enabled).
- **routers:** This should be set to the IP address of the computer running 602LAN SUITE Groupware (with NAT enabled).

For more information on DHCP and DHCP options please visit <http://www.dhcp.org>.

LDAP

The [LDAP](#) (Lightweight Directory Access Protocol) server allows clients to find contact information (e-mail addresses) of other users from the 602LAN SUITE 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 602LAN SUITE Groupware 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.

FTP/FTPS

The included [FTP/FTPS](#) server provides access to documents stored within the 602LAN SUITE Groupware 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.

Content Filter

602LAN SUITE Groupware includes content filtering through the HTTP proxy. To begin using the Content Filter you must first enable the `Check HTTP proxy requests with the Content Filter` option.

The Content Filter provides the following features:

- **Use SafeSurf classifying information:** Enables the use of the SafeSurf PICS rating system when classifying a web page. More information here: <http://www.safesurf.com/>
- **Use ICRA PICS classifying information:** Enables the use of the ICRA PICS rating system when classifying a web page. More information here <http://www.icra.org/>
- **Cache previously classified URLs:** Enables the caching of previously classified web pages. This provides immediate classification of frequently visited web pages.
- **URL cache directory:** Specifies the directory that will be used to store the classified URL cache.
- **URL cache disk size:** Specifies the disk size in MB that will be used to store the classified URL cache.
- **Clear URLs in cache after:** Specifies the time (in hours) that a URL will remain in the classified URL cache. After this time the URL will be reclassified on the next user request.

The Content Filter will process rules in the following order:

1. IP Filter under the Proxy section
2. Site Access under the Proxy section
3. Whitelist Rules under the Content Filter (If the requested URL is found here, the next two steps are ignored, and the URL will be shown)
4. Blacklist Rules under the Content Filter (If the requested URL is found here, the next step is ignored, and the URL will be filtered)
5. Content Filter Rules under the Content Filter

Rules are defined on the following sections:

- **Content Filter Rules:** URLs matching these rules will do the action specified.
- **Whitelist Rules:** URLs entered here will always be allowed.
- **Blacklist Rules:** URLs entered here will always be denied.

Adding a Content Filter Rule:

- **Filter access to web pages classified in these categories:** Select the categories you want to filter.
- **For users / hosts:** Specify what 602LAN SUITE users or hosts this rule will apply to.
- **Add users:** Proxy authentication must be enabled to use this feature.

- **Add hosts:** You can specify hosts by any of the following methods: any address, single address, subnet, and IP range.
- **Time schedule:** Specify the time you would like this rule to be active.
- **Action:** Select one of following four actions:
- **Block access and show error page:** This will deny access to the URL and show a predefined HTML error page (this page can be found in the ERRORS folder with the file name cfblock.html).
- **Block access and show blank page (no graphics or text):** This will deny access to the URL and return nothing to the browser. This is useful for blocking access to specify images (e.g. ads, etc.).
- **Redirect to URL:** This will redirect the user to the URL specified.
- **Log access:** User activity is always logged, but this option will perform no other action except log the access. Please note that the `Web/Proxy/FTP` option must be enabled under `Maintenance -> Logs` for this to work.

Adding a Whitelist/Blacklist Rule:

- **(Don't) Filter access to these web pages (URLs):** Enter the URLs to allow (Whitelist) or deny (Blacklist) here. URLs can be defined with * and ? symbols (convention: * = alias, ? = mask).
- **For users / hosts:** Specify what 602LAN SUITE users or hosts this rule will apply to.
- **Add users:** Proxy authentication must be enabled to use this feature.
- **Add hosts:** You can specify hosts by any of the following methods: any address, single address, subnet, and IP range.
- **Time schedule:** Specify the time you would like this rule to be active.
- **Action:** Select one of following four actions (this only applies to the Blacklist):
- **Block access and show error page:** This will deny access to the URL and show a predefined HTML error page (this page can be found in the ERRORS folder with the file name block.html).
- **Block access and show blank page (no graphics or text):** This will deny access to the URL and return nothing to the browser. This is useful for blocking access to specific images (e.g. ads, etc.).
- **Redirect to URL:** This will redirect the user to the URL specified.
- **Log access:** User activity is always logged, but this option will perform no other action except log the access. Please note that the `Web/Proxy/FTP` option must be enabled under `Maintenance -> Logs` for this to work.

Anti-virus

602LAN SUITE Groupware includes the BitDefender anti-virus engine. All e-mail messages, local server files, and proxy requests 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.

Maintenance

Administration

602LAN SUITE Groupware 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.

Program Update

602LAN SUITE Groupware can automatically check the Software602 update server for new updates. If you want 602LAN SUITE Groupware to check for new updates automatically enable the `Check for a new 602LAN SUITE update every` checkbox.

When an update is available, choose one of the following:

- **Send notification e-mail to administrator(s):** An update notification will be sent to all administrators.
- **Download update and send notification e-mail to administrator(s):** The new update will be downloaded and an update notification will be sent to all administrators.

If you want to limit the time in which the update will be downloaded, enable the `Limit update time` checkbox and enter the required time values.

If 602LAN SUITE Groupware is connected via a Dial-up Internet connection and you want to automatically establish a Dial-up connection to download the update, enable the `Establish dial-up connection to download update` option.

If you do not want to use the automatic option, you can still check the update server for a new 602LAN SUITE Groupware update by clicking the `Check for update` and `Download update` buttons.

The previous build of 602LAN SUITE Groupware will be automatically saved. If any error occurs during startup of the new build, the previous build will be restored.

Statistics

The statistics show the current status of used disk space and the number of objects for each 602LAN SUITE Groupware user. Click a user to display a detailed statistics.

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.

Logs

602LAN SUITE Groupware 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 602LAN SUITE Groupware server activity to a file. The file can be found in the 602LAN SUITE Groupware installation directory, with the name SMMDDYYI.LOG (MM means months, DD means day and YY means 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/Proxy/FTP
- SOCKS server
- Dial-up connection
- DNS proxy
- DHCP server
- SMTP server
- POP3 server
- IMAP server
- LDAP server
- Fax server
- NAT server
- Local Anti-virus scanning

Most web servers offer the option to store log files in either the [W3C common log format](#) or a proprietary format. 602LAN SUITE Groupware provides the following logs in W3C format:

- **W3CA_MMDDYY.LOG:** Web server log file
- **W3CP_MMDDYY.LOG:** Proxy server log file
- **W3CC_MMDDYY.LOG:** Proxy cache log file
- **W3CNAT_MMDDYY.LOG:** Network Address Translation log file

W3C log files are recorded in a format readable by analysis tools. A header specifying the data type is recorded at the beginning of each log file.

Firewall messages can be logged to the `FWMMDDYY.LOG` file. The options that are checked will define what will be logged to the file. Here is a description of the options:

- **Log dropped packets:** Dropped packets will be logged.
- **Log successful connections:** Only successful connections will be logged.
- **Log all packets:** All traffic will be logged (WARNING: Should only be used for debugging purposes!).

Backup

602LAN SUITE Groupware 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 602LAN SUITE Groupware Windows service has access to the network disk by observing the following rules:

- By default, the 602LAN SUITE Groupware 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.

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 & Reminders

602LAN SUITE Groupware 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, or from the 602LAN SUITE Groupware InfoPanel Windows application.

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

- **Refresh time (client – server):** the short period is comfortable for the user (will be certainly informed in time), but loads more the server.
- **Refresh time (server - database):** it has influence upon the workload. If this interval is substantially longer than the client-server refresh time, then the client receives repeatedly obsolete data.
- **Delete notification records after:** if a user does not login to Groupware for a longer time or does not use the client that processes the messages (e.g. SMTP/IMAP client), then his/her messages cumulate in the stack. Therefore the server automatically deletes old messages.
- **Delete reminder records after:** if a user does not login to Groupware for a longer time or does not use the client that processes the notices (e.g. SMTP/IMAP client), then his/her messages cumulate in the stack. Therefore the server automatically deletes old notifications.
- **Current Statistics:** serves as an overview for the administrator concerning the number of messages and notifications in the stack.
- **Delete all older than:** the maintenance can be also done in a single action and delete all messages and notifications older than the pre-set number of days. The notification age is evaluated according to the postponement time or, in case of still nonvisual notification, since the event beginning, or time of performance.
- **Delete all after:** if the stack contains notifications to an event or task in far future, it is also possible to delete them.

Debug Options

When troubleshooting a problem with 602LAN SUITE Groupware, 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.