IceWarp Unified Communications

Mail Service Reference

Version 11.4



Published on 2/9/2016

Contents

Mail Service 4

About 4
7-Zip License Requirements 4
Reference 5
General 5
Spool Manager – Main Features 5
Delivery 5
Routing 9
Advanced 10
Security 18
General 18
Submission Port (RFC4409) 19
DNS 20
Intrusion Prevention 21
Advanced 24
Rules 25
Content Filters 25
Adding a New Filter 26
Editing a Filter 39
Deleting a Filter 39
Exporting Filters 39
Importing Filters 40
Bypassing Filters 40
Understanding the SMTP Protocol and Message Headers 40
Rules 42
Auto Clean 48
External Filters 51
Archive 52
Mail Archive 53
ETRN Download 55
SMTP Errors 57

Mail Service

Registered Trademarks

iPhone, iPad, Mac, OS X are trademarks of Apple Inc., registered in the U.S. and other countries. Microsoft, Windows, Outlook and Windows Phone are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Android is a trademark of Google Inc. IceWarp is a registered trademark in the USA and other countries.

About

The **Mail** node contains five sub-nodes:

- **SMTP Service** – various settings for the SMTP service.
- **Security** – comprehensive set of options for stopping unwanted use of your server, defining advanced options such as delays, policy banner, server title, etc.
- **Rules** – allow you to define content filters, rules, auto clean and external filters.
- **Archive** – allows you to define backup policy for received/sent e-mails.
- **ETRN Download** – allows you to define ETRN (or ATRN) collection options.

7-Zip License Requirements

IceWarp Server uses 7-Zip *.exe* and *.dll* files for archive operations. 7-Zip is licensed under the GNU LGPL license. The source code can be found here: ***www.7-zip.org***.

For more info, refer to this web page: ***http://www.7-zip.org/faq.html***.

Reference

This part of the document describes administration console sub-nodes of the **Mail** node. These sub-nodes are:

- General
- Security
- Rules
- Archive
- ETRN Download

General

The **SMTP** (Simple Mail Transfer Protocol) service is the core of IceWarp Server's functionality, as it is the protocol used for sending messages from one server to another.

See also the **AntiSpam Flowchart** chapter within the **AntiSpam Reference** guide.

Spool Manager – Main Features

(the **Mail – General – Advanced** tab)

- Independent emails going to the same target domain are sent using one SMTP session.
- It is possible to set limits for messages sent to one domain per one minute.
- It is possible to set limits for messages sent from one domain per one minute.
- There are five queues with different sending speed. The appropriate queue is chosen according to:
  - message priority in the message header
  - wheter it is a mailing list / backup domain delivery / distributed doman delivery
  - wheter it is a retry attempt

Internal outgoing queues are sorted by Priority (0-4), where 4 is the fastest. Sending speeds are relative - every queue is 2x as fast than a queue with the closest lower priority. Administrator can see current message priority queue in Logs - Message Queue section of the administration console.

Priority flags are respected and standard email is prioritized over:

- Mailing lists
- Backup domains
- Distributed domains
- Any entries

Example:

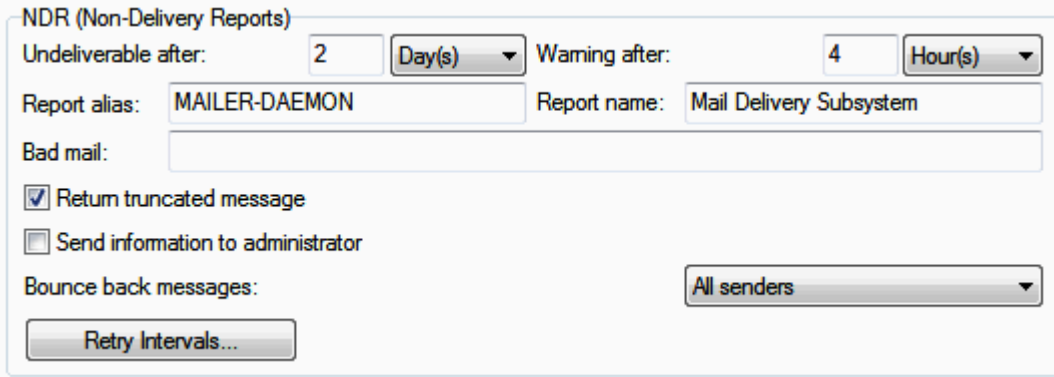
Priority 1 or 2 are emails sent via mailing list or coming from backup domains. If retried they would be showing Priority 0.

Delivery

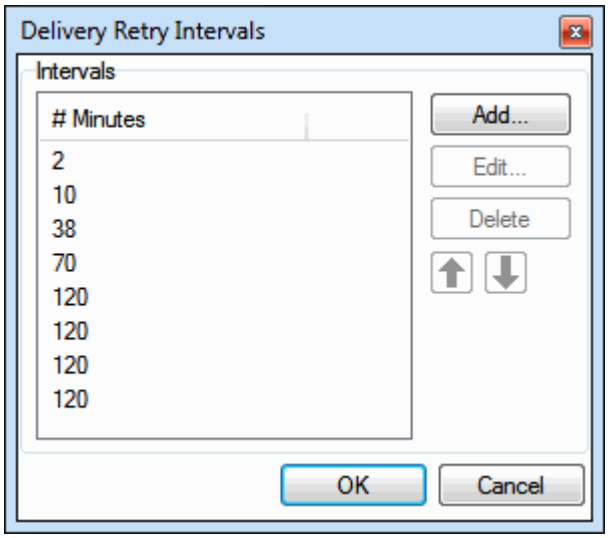


Field	Description
Use DNS lookup	Select this option if your server is going to send messages directly. When sending a message, IceWarp Server will query DNS servers to locate the receiving server's DNS MX record. DNS servers can be specified in the **System – Connection** node.
Use relay server	Select this option if you wish IceWarp Server to use a relay server to send messages. This is useful when the place where IceWarp Server is installed has a dynamic IP address and a broadband Internet (ADSL, cable, etc.) which are usually listed on major blacklists, your domain has no public IP address or you are on a slow dial-up connection via an ISP that allows you to use their email server to send messages. Connections to your ISP's mail server tend to be faster than other servers on the Internet so your messages may be delivered more quickly, keeping your connection costs down. Enter the hostname or IP address of the relay server. If your relay server requires authentication, this can be achieved by using one of the following 'full URL' forms of the hostname: ***<username>:<password>@<MyISPhostname>*** or *<username@domain.com>:<password>@<MyISPhostname>* The second option is to be used if your username is a full email address. **Example:** *john@doe.com:johnspassword@mail.MyISP.com* You can specify multiple relay servers here, separated by semicolons. If IceWarp Server cannot connect to the first relay server, it will try the second one etc. *NOTE: Relay servers may use different ports for SMTP service then the default one (25).* *In this case, you have to specify it:* ***<username>:<password>@<MyISPhostname:port>*** *or* *<username@domain.com>:<password>@<MyISPhostname:port>*
Public Hostname	Hostname or alias of the server where IceWarp Server runs. This field must not be left blank as it is used when IceWarp Server authenticates or introduces itself to another mail server. This should be the hostname of your IceWarp Server which is registered on DNS. You may also want to ensure your IceWarp Server's IP address has a PTR record registered as this is a spam-fighting requirement that some receiving mail servers require. *NOTE: This value is the same as in the **System – Services – SmartDiscover – Public Hostname** field. When changed in one field, it is changed within the second one accordingly.*
Deliver messages via relay server when direct delivery	Checking this option only has an effect if you have selected the ***Use DNS lookup*** option and you have defined a relay server (or servers) in the ***Use relay server text*** box.

fails	IceWarp Server will attempt delivery via these servers if all direct delivery attempts fail. *NOTE: This option overrides the SMTP retry interval settings and will use the retry settings defined on the server where IceWarp Server will relay to.*
Max message size	Check this box and enter a value to limit the size of messages that can be sent or received via IceWarp Server (in the above screenshot 10MB). If a user tries to send a message larger than the specified size it will be rejected. *NOTE: This limit will be overridden by any non-zero domain-specific limits or user-specific limits if **Override global limits** is checked within **Domains and Accounts – Global Settings – Domains**.* *NOTE: WebClient lets you upload files in a different way. Via SmartAttach or to upload files in groupware objects (such as **Files** object or files attached to contacts, events, etc.). In this case, IceWarp Server uses a **different limit** defined in **icewarp/php/php.ini**. The default is 2 GB (**upload_max_filesize = 2048M**). You can change this setting to match your global maximum message size policy.* *NOTE: There is 30% overhead for messages with attachments (encoded in **base 64**), so for the 10 MB limit, specify 13 MB here.*
Delivery reports	Check this box if you want the delivery reports to be available for users. There are following delivery statuses: ▪ **Delivered** – message delivered (only for local recipients). ▪ **Sent** – message successfully sent outside/relayed. ▪ **Queue** – message was temporally deferred, the server will try to send it later. ▪ **Error** – message was bounced back with an error (check your inbox for a detailed error message). For users, this feature is available in ***IceWarp WebClient – message composer window – Options – Show Delivery Report***. For further information about delivery reports in IceWarp WebClient, refer to **IceWarp WebClient User Guide**.



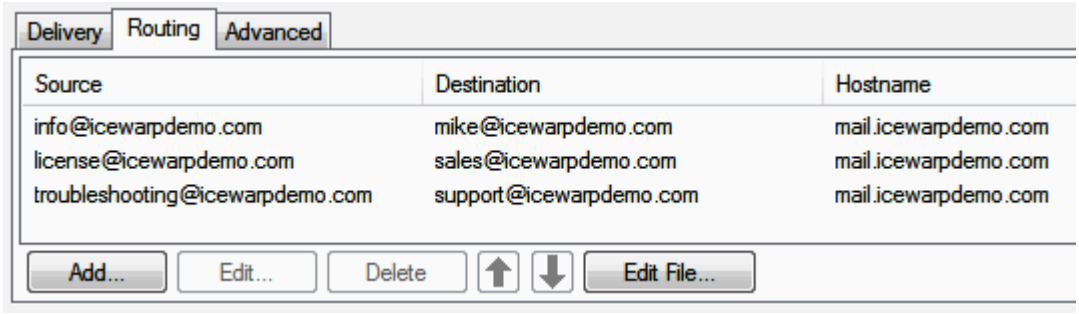
Field	Description
Undeliverable after	If IceWarp Server cannot contact a server to deliver a message it will queue the message and retry delivery at regular intervals. Specify a value and time unit. After this time, delivery attempts are aborted.
Warning after	Specify a value and time unit. If IceWarp Server cannot contact a server for the specified time, the sender is informed. This message is only a warning, IceWarp Server will continue trying to deliver the message. Use the ***Retry Interval*** button to schedule delivery attempts (by default, after 2 minutes / 10 min.

	/ 38 min. – see further). The warning is sent after third unsuccessful attempt.
Report alias / Report name	The report alias and name are used to generate the From: header in any system generated report messages (for example the undeliverable report, disk space monitor report, etc.).
Bad mail	If the sender of a message cannot be ascertained (e. g. there is no From: header) and an undeliverable message report is generated, it will be sent to the recipient(s) listed here. Multiple addresses can be specified, separated by semicolons.
Return truncated message	Check this option and if the message cannot be delivered, approximately 4 KB of the original message are returned as an attachment. This includes the message headers and – in some cases – also part of the original message body.
Send information to administrator	Check this option and all undeliverable messages will be copied to the primary domain administrator.
Bounce back messages	Choose a process option for bounce back messages. **All senders** – process bounce back messages for all senders. **Local senders only** – process only for local senders. **Disabled** – do not process bounce back messages. **Validated senders only** – the server checks SPF (and possibly MX) in the very last step of processing. If the sender does not meet the criteria, the session is marked with a flag in the header of the ***_outgoing*** file (*DontBounce: 1*). When this flag is present, NDR is not generated (regardless of the bounce back mode). *NOTE: In MDA mode a message is accepted and then processed by other filters at a later time. If a message is then refused, a bounce back is sent to the sender. If the sender's address is spoofed than an innocent recipient could get the bounce back which would be considered as spamming – because of this the recommended bounce back level in MDA mode is "local senders".* *If you want to prevent delivery of bounce backs for certain IPs/domains, you can create the **smtpbouncebackbypass.dat** file and place it into the **icewarp/config/** folder. Use the same syntax as for e. g. **spambypass.dat** file (**Anti-Spam – General – Other**).*
Retry Intervals	Click this button to open a dialog allowing you to specify retry intervals (from the previous attempt) for failed deliveries:  Use the ***Add*** button to add a new retry time. Use the ***Edit*** and ***Delete*** buttons to modify or remove a retry time. Use the ***Up*** and ***Down*** arrows to move a retry time in the list.

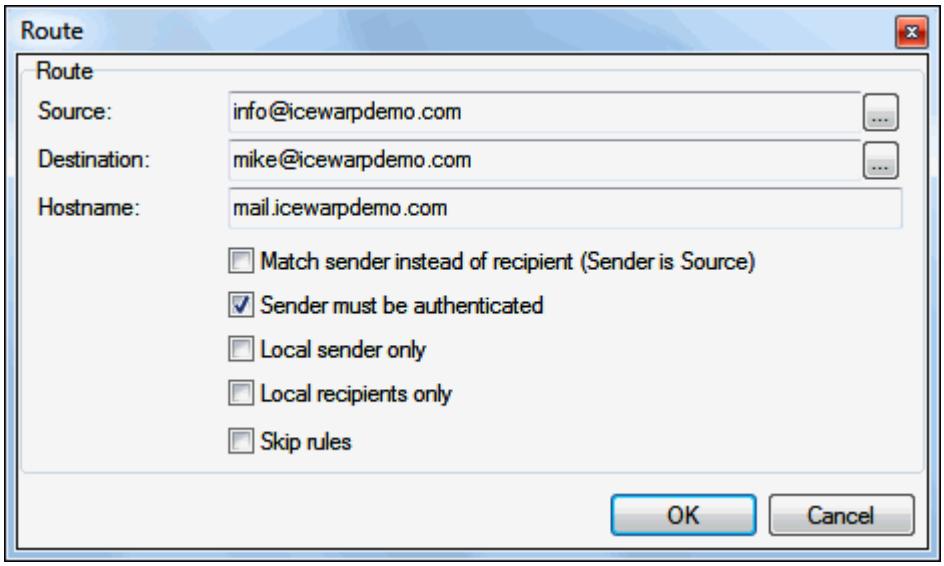
Routing

The SMTP Routing feature allows you to redirect messages based on the recipient address. Also, if your server's IP is blocked on a certain server, you can redirect emails to that destination using another SMTP server.

A list of routing rules is displayed:



Field	Description
Source	This column shows the original recipient.
Destination	This column shows where the message will be redirected.
Hostname	This column shows a name of the server that messages will be forwarded through.
Add	Click the button to add a new routing rule. The **Route** dialog opens.
Edit	Select a rule and click the button to edit this rule. The **Route** dialog opens.
Delete	Select a rule and click the button to remove this rule.
Arrows	Select a rule and use these buttons to move it in the list up or down.
Edit File	Click the button to edit rules in the **redirect.dat** file. To reveal examples, click the ***Comments*** button here.



Field	Description
Source	The email address or domain which should be replaced and redirected. You can use the '...' button to select accounts, domains or groups via the **Select Item** dialog.
Destination	The email address or domain by which the source one is replaced and redirected.

	You can use the '...' button to select accounts, domains or groups via the **Select Item** dialog. **Syntax:** **emailaddress | domain** You can use three variables in this field: ***%%alias%%***, ***%%domain%%*** and ***%%current_recipient%%***. E.g. ***%%alias%%***@***%%domain%%.*** ***%%current_recipient%%*** – uses the current recipient as the destination.
Hostname	A hostname, with an optional port, that will be used for extended routing, using the following syntax: **[user":"password@]hostname [":" port]** Example: ***relay.isp.com*** This causes that corresponding messages will be sent through the ***relay.isp.com*** mail server. ***user:pwd@relay.isp.com*** This causes that corresponding messages will be sent through the ***relay.isp.com*** mail server with SMTP authentification (*user:pwd*). ***username@domain.com:passwd@relay.isp.com:586*** This causes that corresponding messages will be sent directly through the ***relay.isp.com*** server, port 586 instead of using standard DNS lookup with SMTP authentication against full email address.
Match sender instead of recipient (Sender is Source)	Check this box if you want to use routing for senders instead of recipients. In this case, fill in the sender's email address into the ***Source*** field.
Sender must be authenticated	Check this box and all senders of messages processed by this routing must be properly authenticated via SMTP (SMTP AUTH).
Local sender only	Check this box and routing will be performed only for local senders.
Local recipients only	Check this box and routing will be performed only for local recipients.
Skip rules	Check this box and rules will not be processed for routed messages.

Routing Scenario Example

This useful scenario helps you to relay all emails sent from some domain to another server.

Open the **redirect.dat** file (**Mail – General – Routing – Edit File...**) and use the following syntax:

[original_domain]=%%alias%%@%%domain%%;12;[another_server]

Example: *tests.icewarpdemo.com=%%alias%%@%%domain%%;12;mailbackup.server.com*



NOTE: If you have MDA enabled (by default it is off), it might do relay for local emails too. In this case, try to add a rule such as this one, ***before*** *the main rule:*

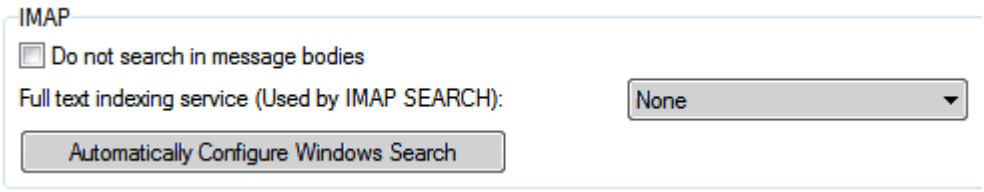
Source : *testes.icewarp.com.br*

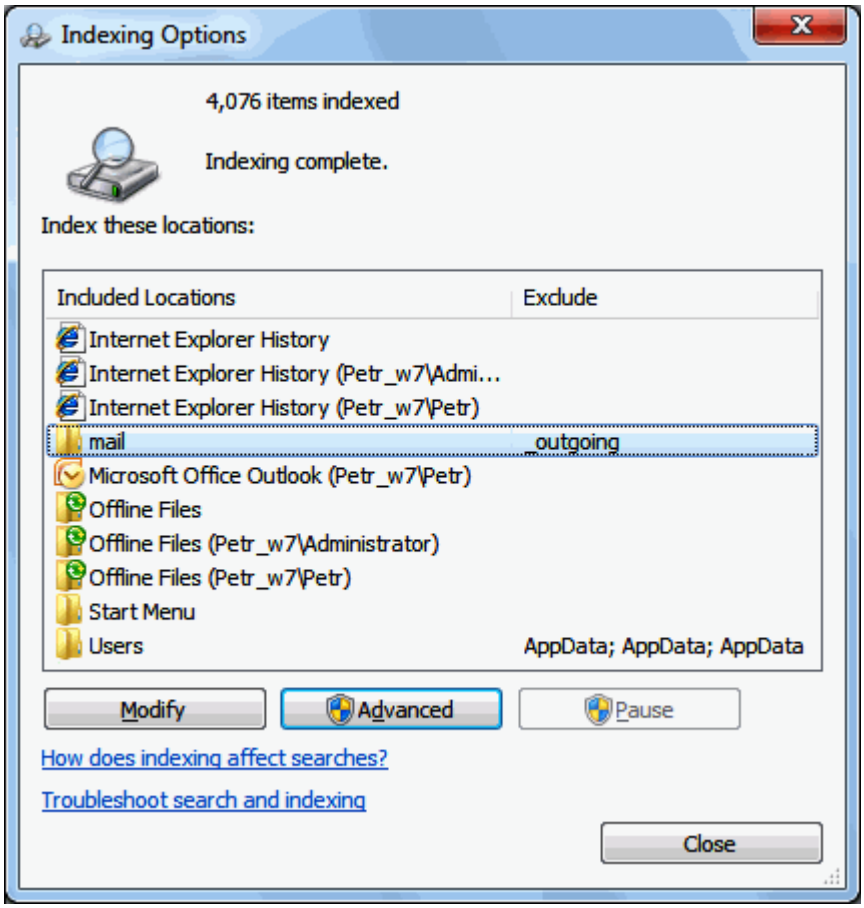
Destination : *testes.icewarp.com.br*

Server: *blank*

Options: *do not mark any*

Advanced

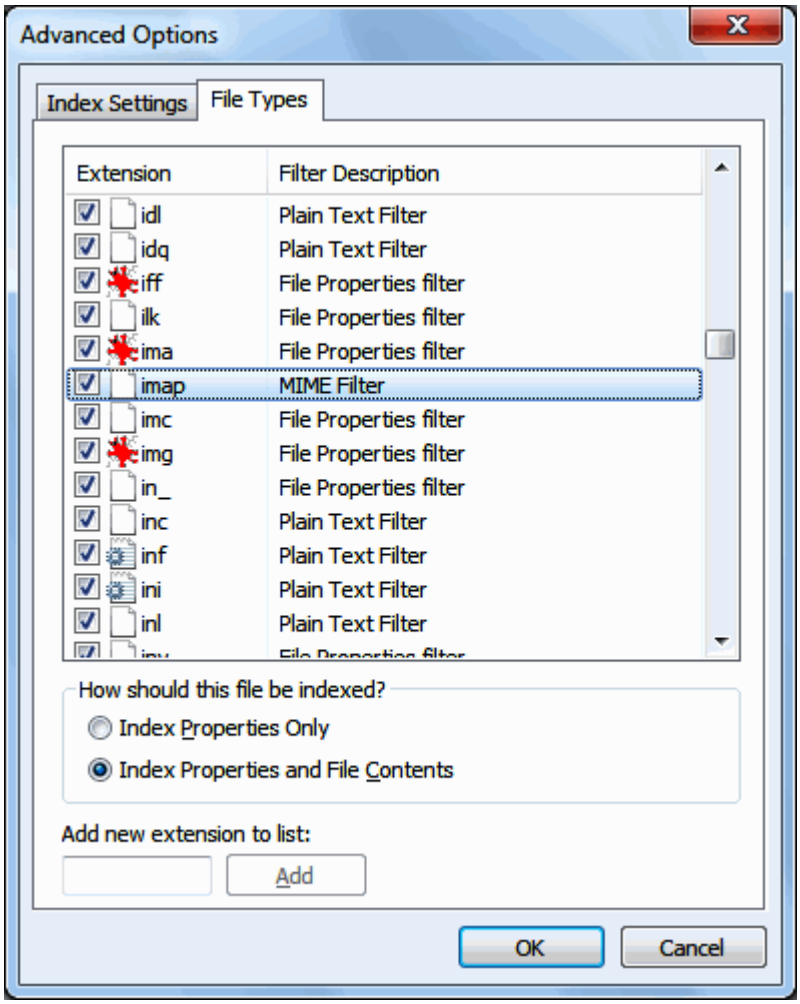


Field	Description
Do not search in message bodies	Tick the box if you want the search not to take into account message bodies even if such a search is requested (*Fulltext* in WebClient).
Full text indexing service (used by IMAP SEARCH)	Select from the list: **None** Full-text search is not used. **Windows Search** Windows Search is used. Provided that you have Windows Search installed (or you use Windows 8 (8.1) / Windows 2008 / Windows 2012 where it is included), you can enable full text search within received email messages. Windows Search indexes all words within a message (including headers and "text based" attachments – not only pain text but also, for example, ***.doc*** files) and saves them to a database with fully qualified paths (with usernames included) to files where these words occur. This allows to distinguish between users as they have to log in. To check whether Windows Search works properly, go to **Control Panel – Indexing Options**. The list has to include the ***mail*** item with the ***Exclude*** property with value of ***_outgoing***: 

This also speeds up searching speed inside IW WebClient.

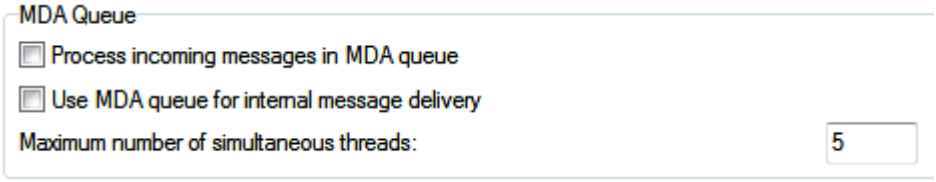
NOTE: Windows Search is installed via Server Manager / Roles.

Click the ***Advanced*** button to open the **Advanced Options** dialog:



You should see something similar to this figure. Note that the ***Index Properties and File***

	Contents option is selected.
Automatically Configure Windows Search	Click the button to tell Windows Search to add email folder(s) to the list of folders that are indexed and start indexing of the folder content. NOTE: Indexing may take some time. Do not select the ***Windows Search*** item (the above feature) immediately after clicking the button. Wait until indexing is done. NOTE: Indexing works for all subfolders of the **<install_dir>\mail** folder (the default one upon **System – Storage – Directories – Mail path**). Should you have set a different ***Mailbox path*** for any user(s), you have to add this path(s) to Windows Search to have these folders indexed too. Example: **C:\mail** NOTE: To index network drive(s) under Windows 7, you need to run the following patch: ***http://www.microsoft.com/downloads/details.aspx?FamilyID=f7e981d9-5a3b-4872-a07e-220761e27283&displaylang=en***



Field	**Description**
Processing incoming messages in MDA queue	Check this option to have the MDA queue used. You should only consider using this option on high-traffic servers or servers that have major AntiSpam and/or IceWarp Anti-Virus processing. *NOTE: Huge MDA queues (e. g. more than 13 000 emails) can cause SMTP not working properly.* *If messages are not flowing, you can:* *· either increase number of threads* *· or run **smtp.exe/systray** using Command Line. In this case, it is not started as a service but as an application.* *As a service, it has timeout set to 30 second and when there is a huge MDA queue it simply does not make it to start in the timely fashion. As an application, it does not have any timeout set.*
Use MDA queue for internal message delivery	Check this option to have all internal messages processed via the MDA queues. This means that any internal message (bounce back, server generated message, Account Forwarder message, etc.) will be processed via an MDA queue and all filter, rule, AntiSpam, IceWarp Anti-Virus, etc. processing will be performed on the message.

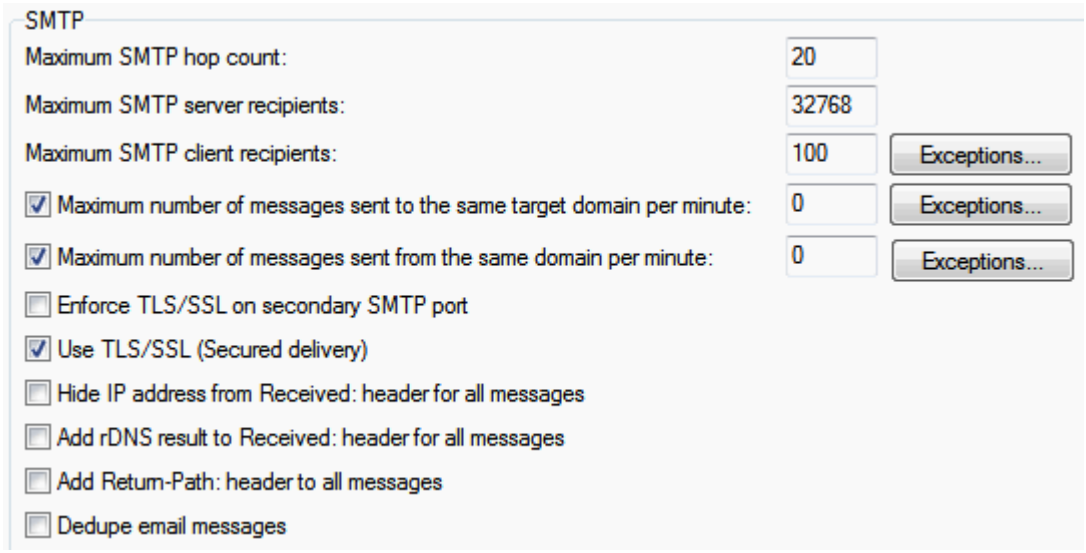
Maximum number of simultaneous threads	Specify the maximum number of threads to use for processing of incoming messages. This can help alleviate problems on high-load servers where the sending server times out, but IceWarp Server still processes and delivers the message. The sending server then tries again, and a duplicate message is received. If you enter a non-zero value here then any incoming messages are stored immediately to an incoming folder, for later processing, and the session is closed so there are no timeouts. Recommended value for non-high-load servers is 8. Increase the value if not sufficient due to the server load. *NOTE: In MDA mode, a message is accepted and then processed by other filters at a later time. If a message is then refused, a bounce back is sent to the sender. If the sender's address is spoofed than an innocent recipient could get the bounce back which would be considered as spam – because of this the recommended bounce back level in MDA mode is **Local senders only**. (**Mail Service – General – Delivery** (on page 5) – **Bounce back messages**.)*

NOTE: Forwarding of local messages to local recipients is not logged unless local MDA is enabled.

*NOTE: When MDA is set, the **<install_dir>/mail/_incoming** folder is used instead of the one defined under **System – Storage – Directories**. Local MDA changes these folders only for local emails.*

*NOTE: If you enable MDA, check also information within the **Mail Service – General – Advanced** section – Bounce back messages option.*

NOTE: Auto-responder will always back-scatted regardless MDA is set or not. For detailed information, refer here: http://www.spamcop.net/fom-serve/cache/329.html.

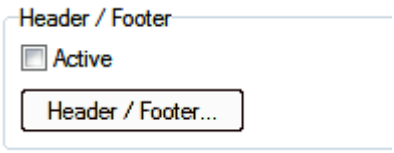


For general information on **Spool Manager**, refer to the **Reference – General** page.

Field	Description
Maximum SMTP hop count	Sometime a message can get into a 'relay loop', where it is being passed between servers trying to find a delivery point. A hop is defined as one pass of the message to a server. Specifying a value here instructs IceWarp Server to count the number of servers the message has been through, compare it with this value, and reject the message if the number of hops exceeds the specified value.
Maximum SMTP server recipients	Specify the maximum number of server session recipients allowed in an outgoing message. (I. e. number of recipient addresses in one message.) This can be used to protect your server from overload.

Maximum SMTP client recipients	Specify the maximum number of client session recipients allowed in an outgoing message. Some systems do not like receiving many emails in one session, this option can split outgoing client sessions based on the number of recipients If the number is exceeded the message will be split into multiple sessions.
Exceptions	Here you can override ***Maximum SMTP client recipients*** for specific target domains. Click the button to open a dialog allowing you enter the target domain and the override value.
Maximum number of messages sent to one domain per minute	Check the box, if you want to enable this feature. Specify the maximum number of incoming messages into the edit field. Messages going to one local/remote domain are aggregated and sent together. Enable this option to throttle the sending speed and specify the maximum number of incoming messages to the same local/remote domain per minute. Emails violating the limit will be held in the retry queue for as long as is necessary. Leave this option disabled for fastest message delivery. To limit number of Incoming connections in specific domain leave the value to 0, open the Exceptions dialog and add your domain and limit the number of client sessions per minute.
Exceptions	Click the button to open the **Maximum number...** dialog. Click the *Add* button to specify a domain name and value to override the value in the edit field. It is even possible to specify one limit to a set of domains (delimited by semicolons). In this case, this group of domains has common limit.
Maximum number of messages sent from one domain per minute	Check the box, if you want to enable this feature. Specify the maximum number of outgoing messages into the edit field. Enable this option to throttle the sending speed and specify the maximum number of outgoing messages from the same domain per minute. Emails violating the limit will be held in the retry queue for as long as necessary. Leave this option disabled for fastest message delivery. Internally some messages can have higher sending priority and skip ahead of others, but there is no way to influence it. See ***Mail Service - General - Spool Management*** for details. To limit number of Incoming connections in specific domain leave the value to 0, open the Exceptions dialog and add your domain and limit the number of client sessions per minute.
Exceptions	Click the button to open the **Maximum number...** dialog. Click the *Add* button to specify a domain name and value to override the value in the edit field. It is even possible to specify one limit to a set of domains (delimited by semicolons). In this case, this group of domains has common limit.
Enforce TLS/SSL on secondary SMTP port	Check the box if you want to enforce the secondary SMTP port (587) to communicate using this protocol(s). *BE AWARE: When these commands are turned on:* *c_mail_smtp_delivery_messagesubmission* *c_mail_smtp_delivery_enforcetlsonsecondarysmtpport,* *this combination of settings can cause fails to send out email by PHP mailer because of not STARTTLS command is supported.*
Use TLS/SSL	Check this box and IceWarp Server will connect to remote servers using TLS/SSL, if the remote server is capable of this. *NOTE: If you want to use TLS instead of SSL while sending/receiving mails, use the basic ports in email client (25 for SMTP) and mark to use TLS. (For SSL, use the usual SSL ports).*
Hide IP address from Received: header for all messages	Checking this option tells IceWarp Server not to put the IP address in a messages Received: header. This effectively stops people from being able to work out your local network configuration.

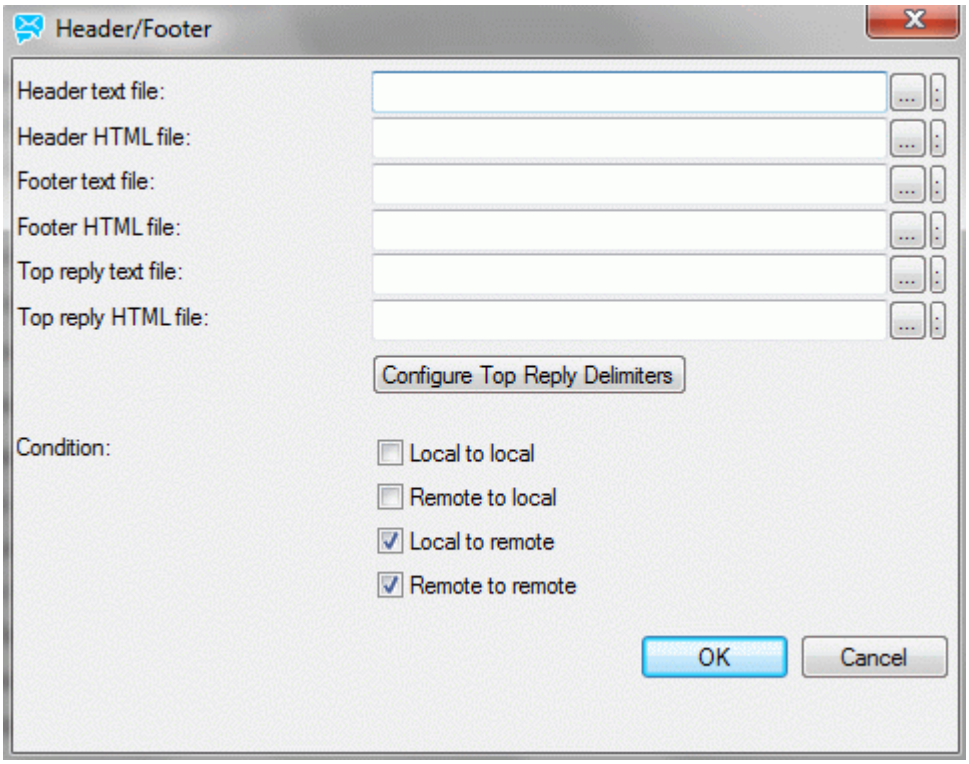
Add rDNS result to Received: header for all messages	Check this option and a reverse DNS lookup will be performed for each incoming message and the result added to the message headers. *NOTE: Using this option improves security but can severely impact performance on high-load Servers.*
Add Return-Path header to all messages	Check this option and IceWarp Server will add a Return-Path header to the email. This can be useful for debugging and checking where an email came from.
Dedupe email messages	If a user has multiple aliases and a message is sent to more than one of the aliases the end User will receive multiple copies. Also, if a user is a member of more mailing lists (or groups) and these lists (groups respectively) receive the same message, this user will receive multiple copies. Check this option and IceWarp Server will check for duplicate message to the same end user and only deliver one of them. *NOTE: If the **Bounce back for failed recipients** feature in WebClient (**Tools – Administrator Options – Mail – General**) is enabled, this option can not be used. As a result of enabling of both options, users would receive duplicated messages.* BE AWARE: The following scenario can cause a loss of messages that could be completely deleted : • standard domain • static route –> forward to a host (relay server) • catch-all forward to this static route (2) Do NOT use the *Dedupe email messages* option in this case!



IceWarp Server can automatically insert a header and/or footer to messages using this option.

This will affect all domains within your server. If you want to specify different headers and footers for different domains you should use the domain-based **Header/Footer** button in **Domain – Options** – but you must enable the facility in this panel.

Field	**Description**
Active	Tick the box to enable header/footer processing.
Header/Footer	Click the button to define header/footer files. The **Header/Footer** dialog opens.



Field	Description
Header text file	A fully qualified path to a text file which will be inserted as a header to text format messages.
Header HTML file	A fully qualified path to an HTML file which will be inserted as a header to HTML format messages. *NOTE: The extension of this file must be **htm** or **html** for this function to work correctly.*
Footer text file	A fully qualified path to a text file which will be inserted as a footer to text format messages.
Footer HTML file	A fully qualified path to an HTML file which will be inserted as a footer to HTML format messages. *NOTE: The extension of this file must be **htm** or **html** for this function to work correctly.*
Top reply text file	A fully qualified path to an text file which will be defined at the end of the top reply within an email.
Top reply HTML file	A fully qualified path to an HTML file which will be defined at the end of the top reply within an email. *NOTE: The extension of this file must be **htm** or **html** for this function to work correctly.*
Configure Top Reply Delimiters	Click this button to configure top reply delimiters. This file contains additional patterns used to detect end of top reply in email message.
Local to local	Header and footer will be inserted into a message if both the sender and recipient are local.
Remote to local	Header and footer will be inserted into a message if the sender is remote and recipient is local.
Local to remote	Header and footer will be inserted into a message if the sender is local and recipient is remote.
Remote to remote	Header and footer will be inserted into a message if both the sender and recipient are remote.

*NOTE: If you are using HTML headers or footers you should **only** use HTML found within the <BODY> tag.*

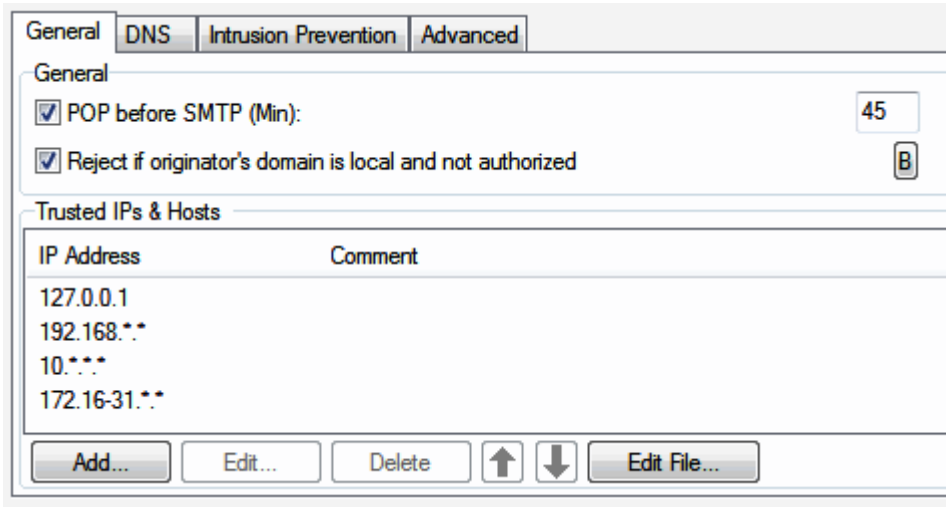
NOTE: It is recommended to specify both HTML and plain text files as IceWarp Server will add the appropriate header/footer according to message format.

*NOTE: You can use **vCard variables** for header / footer. All variables are available in example directory - **variables.dat.html**.*

Security

One of the most important areas of IceWarp Server – the SMTP Security options – are designed to protect your server from unwanted access and use.

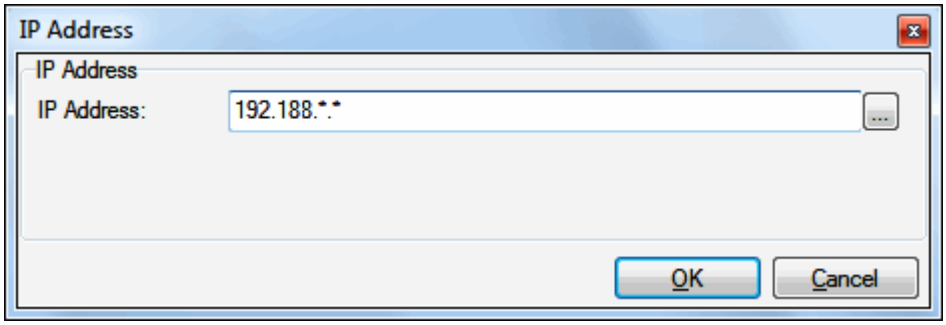
General



Field	Description
POP before SMTP (Min)	Check this option and a local email address which has made a successfully authenticated POP or IMAP connection will be allowed (for specified number of minutes) to initialize SMTP session (from the same IP address which was used for the POP or IMAP connection) with the same rights as if it was successfully SMTP authenticated.
Reject if originator's domain is local and not authorized	If the sender of the message is a local user (claims to be from your local domain), they have to authorize themselves. Authorization can be done using the SMTP authentication, relaying from IP address or the POP before SMTP feature. This option can reject also local users if they authenticate against different SMTP server, e.g. their ISP SMTP server. *NOTE: Whitelist and blacklist are skipped if the remote side tells us the sender is local, but the session is not authenticated nor comes from a trusted IP. The email is then processed as usually – other rules are applied.* *It can be turned off only using API Console – the* ***SpamSkipBypassLocalUntrusted*** *variable.* *Bypass reason code – H. For more information about reason codes, refer to the* ***AntiSpam – Reason Codes*** *chapter.* *NOTE: This option can cause problems if user is in a place where Internet access is offered (e. g. hotels) that forces their SMTP to users.*
Add	Click the button to add a new IP address. The **IP Address** dialog opens. CIDR notation/ranges can be used.
Edit	Select an IP address and click the button to edit this address. The **IP Address** dialog opens.
Arrows	Use the buttons to move addresses up or down in the list.
Edit File	Click the button to open the simple text file containing the IP ranges. Examples are given there.

The **Trusted IPs** list shows the IP address ranges you consider trustworthy. SMTP connections from these IP addresses will be allowed without authentication.

*NOTE: This list of trusted IPs is also used by the AntiSpam engine's whitelist as a bypass list, if the **Whitelist trusted IPs and authenticated sessions** option is checked in **Antispam – Black & White List – Whitelist – General**.*



Field	Description
IP Address	Fill in an IP address. You can use masks, as shown above, and ranges, for example 192.168.0.1-50 *NOTE: You can use host names as well as IP addresses.*

Submission Port (RFC4409)

This port is used as a way to avoid SMTP abuse. Users are forced to use port ***587*** that requires authentication. In this case, the standard port 25 is used ***only*** for communication that is not authenticated (between SMTP servers). It means that all possible spam attempts etc. go via antispam and antivirus filters/rules set on the server for unauthenticated communication.

If you want to use this feature:

1. Enable SMTP AUTH via API:

   tool modify system ***c_mail_smtp_delivery_messagesubmission 1***

2. Inform users to change their email clients to use port 587 for SMTP.
3. Check whether the SMTP service has set the ***2nd basic service*** field to 587. (**System – Services – General – SMTP dialog – Properties tab**). If not, change it – it works only if set as 2nd basic!.

BE AWARE: Since WebClient requires authentication by default, it is also necessary to change the port in the ***SMTP Server*** field (**Console – WebClient – General**).

E. g. ***mail.icewarpdemo.com:587***.

The same applies to EAS and Spam reports.

*NOTE: Submission port (if enabled via API) PERMITS MAIL FROM **account@localdomain.com** (where **localdomain.com** is created on the IceWarp Server where submission port is enabled).*

*But it still REJECTS due to submission if MAIL FROM is **xxx@localdomain.com** where **xxx** is an account that doesnt exist in the local domain. Then the submission bypass is required.*

Submission Port Bypass

You may want to bypass the submisiion port for local users (when *MAIL FROM* is local). In this case, do the following:

1. Create the **submissionbypass.dat** file.

2. Use the standard bypass file syntax – "**l:**" – as for *Local Sender*.
3. Save this file into the **<install_dir>/Config/** directory.

Submission Username and Password

You can also use two variables – *<smtp_user>* and *<smtp_pass>* – for unauthenticated operations (e. g. on login screen, in reports, etc.) to authenticate to SMTP. In this case, add these variables (tags) into the **server.xml** file (**<install_dir>/config/_webmail**).

Use credentials of the account that will be used for SMTP authentication by WebClient in the case a user is not logged in.

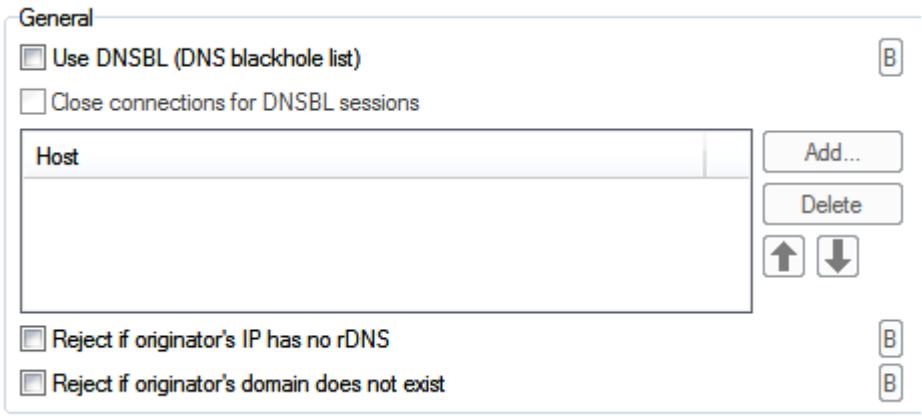
Another way how to deal with such operations is to add *localhost* or *127.0.0.1* to trusted hosts (default settings) – SMTP will not require authentication.

DNS

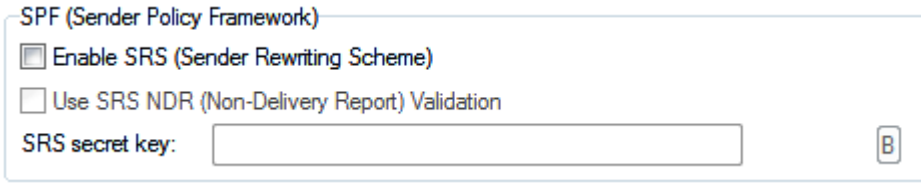
A DNSBL is basically a DNS server which only lists IP addresses of known spammers.

If you query an address against a DNSBL server and get a positive result, the address is most likely that of a known spammer.

This can be used as an AntiSpam technique.



Field	Description
Use DNSBL	Check this option to use DNSBL checking. Use the ***B*** button to specify a list of IP addresses, domains and email address that you will not perform the DNSBL check for (effectively a list of trusted addresses).
Close connections for DNSBL sessions	Check this option and all connections from IP addresses which are listed on the blacklist will be closed immediately.
Host	Here you must define a list of DNSBL server(s) you wish to query. Use the ***Add*** and ***Delete*** buttons to populate and de-populate the list. *NOTE: You can use as many DNSBLs as you wish but you should be aware that each query will add some processing time.*
Reject if sender's IP has no rDNS	Check this option to enable rDNS (reverse DNS) checking. Any connection from a server that does not have an rDNS record (PTR record) will be rejected.
Reject if originator's domain does not exist	Check this option to check for the existence of a DNS A record for an incoming message senders domain. If the sender's domain has no A record, the message is rejected.



Field	Description
Enable SRS (Sender Rewriting Scheme)	Activates the SRS technology fixing the SPF forwarding mail issue, by forcing the agent to change the "mail from" address. *NOTE: When using SRS, it builds the MAIL FROM always referring to the primary domain. You may have a reason not to show your primary domain but still use this feature.* *The solution is to have SRS enabled + enable the **Use domain IP address for outgoing connection** feature (**Domains and Accounts – Global Settings – Domains – Other**) or set the **C_Accounts_Global_Domains_IPAddress** API variable to **1**.*
Use SRS NDR (Non-Delivery Report) Validation	Activate this feature if you want the server to validate whether incoming NDRs (bounce backs) contain the correct SRS hash (see SRS secret key). If not, these NDRs are not delivered into users' mail boxes.
SRS secret key	The secret key is any arbitrary string you can make up – it is your own pass phrase. The secret key will be used for ciphering the data (for hash creation). This field must not be left blank.
'B' button	Use this button to open and edit the SRS bypass file – **srsbypass.dat**. See the example in the bypass file for the correct syntax.

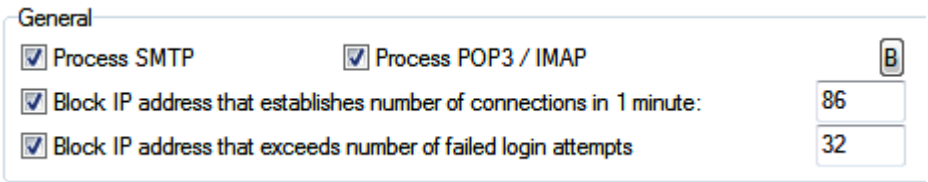
Intrusion Prevention

Intrusion prevention (also known as tarpitting) allows you to block any IP address performing suspicious activities.

This option serves e. g. as protection against spammers who are trying to spam your IceWarp Server accounts based on email address dictionary attacks or DoS (Denial of Service) ones.

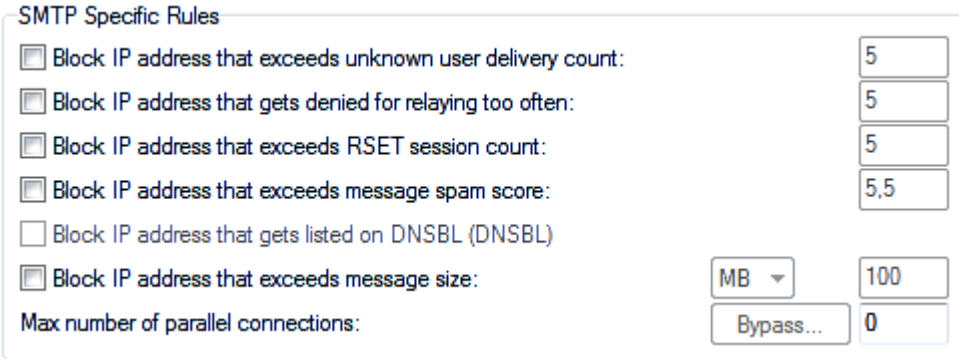
Most of these rules do not affect authenticated users, except # of connections per minute and RSET (since authentication is lost when RSET command is sent).

There is an option to create a "bypass list" of IP addresses which will never be blocked.



Field	Description
Process SMTP	Enables the feature for SMTP.
Process POP3/IMAP	Enables the feature for POP3/IMAP. Supported options are limited to ones included in the **General** section.

"B' (Bypass) button	Click the button to edit the standard **Bypass** file. If the session is authenticated or comes from trusted IP, it is automatically bypassed even if bypass file is empty. *NOTE: Several of the conditions are evaluated in early stage of the SMTP session, when not enough information about the session is present.* E. g.: The ***Local Sender*** condition can not bypass ***Block IP address that exceeded number of failed login attempts***, because a sender is not known when authentication is done.
Block IP address that establishes number of connections in 1 minute	Check this option and specify a value. In the above example an IP address that establishes 86 (or more) connections in one minute will be automatically blocked.
Block IP address that exceeded number of failed login attempts	IP address will be added to blocked list after unsuccessful login attempt which exceeds the number of failed attempts specified.



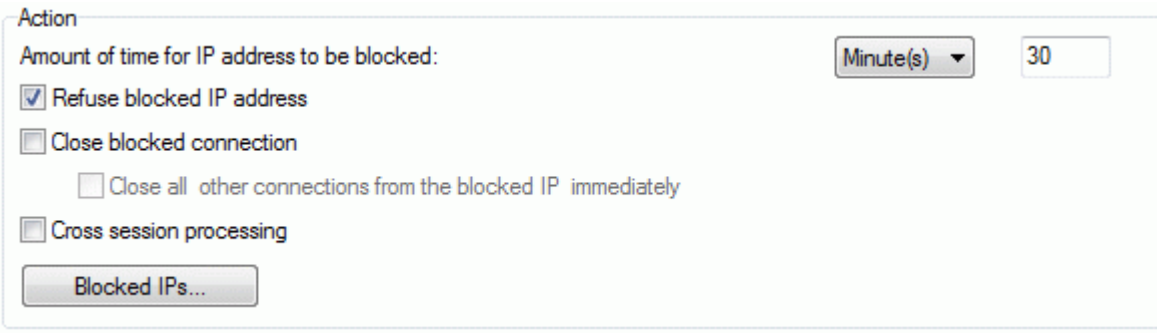
Field	**Description**
Block IP address that exceeds unknown user delivery count	Check this option and specify a value. When activated, the server will monitor all suspicious activities. If the number of activities from one server exceeds the threshold setting, this IP address will be blocked (denied access) for a specified amount of time. In the above screenshot, an address will be blocked after it attempts to deliver 5 messages to unknown users.
Block IP address that gets denied for relaying too often	Check this option to automatically block addresses that attempt to relay through IceWarp Server more than the number of times specified.
Block IP address that exceeds RSET session count	Check this option and specify a value. In the above example any connection that issues more than 5 RSET commands in one session will be blocked.
Block IP address that exceeds message spam score	Check this option and specify a value. In the above example any IP address that delivers a message with a spam score higher than 5.5 will be automatically blocked.
Block IP address that gets listed on DNSBL	Check this option and any connection that is refused because it is on a DNSBL will also be blocked.
Block IP address that exceeds message size	Check this option to have the IP address blocked for any connection that attempts to deliver a message greater than the specified size. Specify a value and choose Kilobytes, Megabytes or Gigabytes from the drop-down box.
Max number of parallel connections	If the number of connections coming from a particular IP address exceeds the limit set here, no more SMTP connections are accepted.

	(This value is related to the *MailServer.ParallelIPConnectionsLimit* variable. Zero means no limit.) Click the *Bypass* button to specify an IP address (or a range of IP addresses) where this limit is not applied.

*NOTE: This check differs from the standard SMTP "maximum message size" check in that the connection is closed **as soon as the size threshold is reached** and the IP address blocked. This is useful for stopping potential bandwidth abusers who send large messages.*

For example with the settings shown above, someone sends a 1GB message to one of your users. As soon as the system has received the first 100MB it will close the connection and block the IP address for 30 minutes. The sending SMTP server may try to re-send the message but it will be denied access until these 30 minutes are up, at which point the first 100MB will be accepted then the block happens again. Eventually the sending SMTP server will give up trying to send the message.

The effect on your server is that instead of having a high bandwidth usage for a 1GB duration it will have high bandwidth usage every 30 minutes for a 100MB duration until the sending server gives up, freeing your bandwidth for other send/receive operations in the meantime.



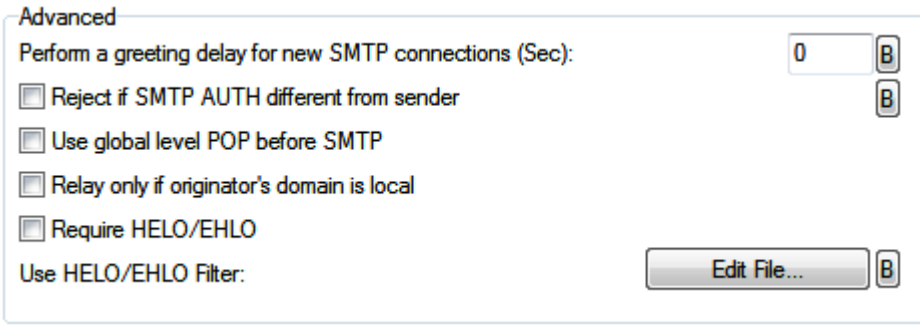
Field	Description
Amount of time for IP address to be blocked	Specify here how many minutes (hours, days) an IP address should be blocked for.
Refuse blocked IP address	Checking this option will store the blocked IP in a database and refuse any further connection attempts. *NOTE: It is meaningful (and recommended) to have ticked at least one of following options: **Refuse blocked IP address**, **Close blocked connection**.*
Close blocked connection	Check this option if you want to have closed immediately all intrusive connections from an IP address that has just been blocked. Other current connections from this IP are not closed. All connections just incoming from this IP address are blocked for the time specified in the ***Amount of time ...*** field.
Close all other connections from the blocked IP immediately	Check this option if you want to have closed immediately all other intrusive connections from an IP address that has just been blocked.
Cross session processing	Check this option IceWarp Server to collect Intrusion Prevention stats across multiple sessions (connections) from the same server. Stats are accumulated over the time selected in ***Amount of time for IP address to be blocked***. In the above example, connections from HostA would be collected and acted upon for 30 minutes. There are some cases where using of this option is senseless. E. g. ***Block IP address that exceeds message spam score***, ***Block IP address that gets listed on DNSBL***, ***Block IP address that exceeds message size***. Contrary, the ***Block IP address that establishes number of connections in 1 minute*** option performs

	Cross session processing automatically.
Blocked IPs	Press this button to jump to the Intrusion Prevention queue, where you can manage blocked IP addresses.

Intrusion Prevention Reason Codes

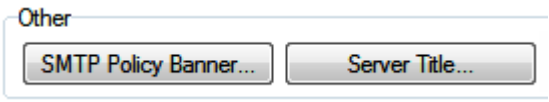
Reason Code	Explanation
C	Tarpitting invoked via Content Filters
I	IP blocked for exceeding connections in one minute
M	IP blocked for delivering oversized message
R	IP blocked for exceeding RSET command count
D	IP blocked for being listed on DNSBL
A	The account that this message was sent to was a "tarpit" account so the sending IP is tarpitted
P	IP blocked for exceeding unknown user delivery count
Y	IP blocked for relaying
S	IP blocked for exceeding spam score in a message
U	IP blocked manually via IceWarp Server's console
L	IP blocked for too many failed login attempts

Advanced



Field	Description
Perform a greeting delay for new SMTP connection	Specify a non-zero value here and IceWarp Server will wait this time (specified in seconds) before responding to an incoming SMTP session. Most spammers systems will time out very quickly as they want to get as much mails delivered as possible within a short time. Genuine connections will wait. A bit more advanced method how to do something similar is greylisting in Anti-Spam.
Reject if SMTP AUTH is different from sender	Check this option to reject any connections where the sender's information differs from the information used in the SMTP AUTH command.
Use global level POP before SMTP	Check this option and any IP address from which a successfully authenticated POP or IMAP connection was made in the past N minutes (N specified under **Security – General – *POP before SMTP (Min)***) will be allowed to initialize SMTP session with the same rights as if it was

	successfully SMTP authenticated.
Relay only if originator's domain is local	Check this option to only allow relaying from local domains.
Require HELO/EHLO	Check this option to deny any connections that do not use the HELO or EHLO commands when they connect. This option should be enabled.
Use HELO/EHLO Filter	Click the ***Edit File*** button to open the **heloehlo.dat** file. Here you can create/edit filters. Syntax rules and examples are given there (click the ***Comment*** button to reveal them).
"B" button	Click the button to open the **Bypass** dialog where you can define items that will bypass defined filters. For more details, refer to the **Bypassing Rules/Filters** section.



Field	Description
SMTP Policy Banner	Press this button to specify banner text that will be presented to any client connected to the server to send messages. Examples are given within the file.
Server Title	By default, IceWarp Server will identify itself to a connecting server. Some hackers can use this information to exploit your server. Click this button to change the identification text so no-one can identify the server software you are running. Examples are given within the file.

Rules

These rules can help you to catch spam and viruses.

If you want to filter messages using advanced rules and make adjustments to messages, we recommend using **Content Filters**. The basic difference between rules and content filters consists in the fact that rules are used for received messages whilst content filters can be defined for both received and sent messages (unless defined differently within the filter itself).

If you just want to restrict message acceptance using keywords, it is better to use **Black & White Lists**.

Additionally, you can design your own filters and create your own filters in any programming language (and then call such filters) in the **External Filters** dialog.

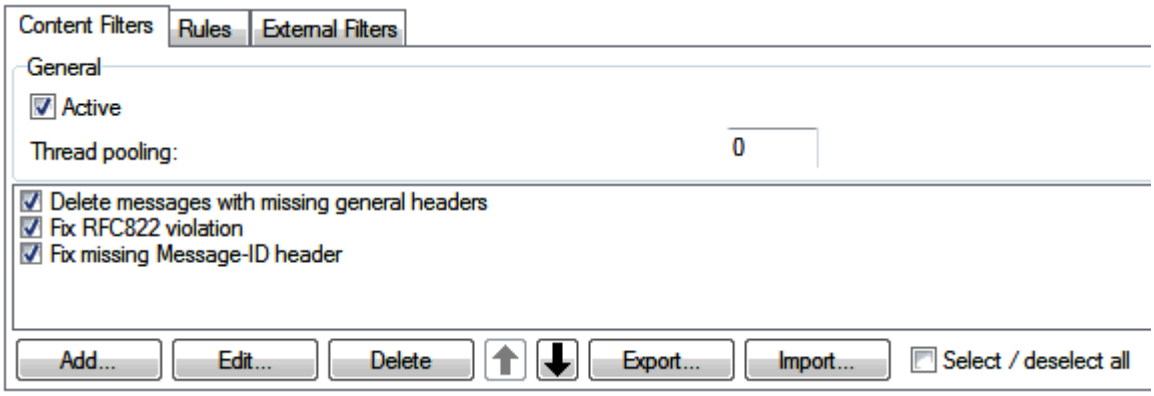


*NOTE: To determine what logs show content filters /rules hits, refer to the **System – Logging – Debug** chapter – **Mail flow...** field.*

Content Filters

Content Filters (CF) are able to parse message content (headers and body) and perform various actions based on the results.

CFs basically work on the server level, however you can set a CF to only act on messages from selected users, domains, etc.



The three filters shown in the above screenshot are pre-defined within IceWarp Server and are discussed later in this section.

Field	**Description**
Active	Check this box if you wish IceWarp Server to process Content Filters. Check the box next to a filter to enable that filter.
Thread pooling	Content filters processing is multi-thread based. Sometimes, this can cause problems on slower servers if the engine takes up too many resources (like 100% CPU). Entering a non-zero value here limits the number of threads that will be run concurrently. Specify here the maximal number of threads to be used when processing content filters.
Add	Click the button to open the **Filter** dialog and add a new filter here.
Edit	Select an existing filter and click the button to edit filter's properties.
Delete	Select a filter and click the button to remove this filter.
Arrows	Select a filter and use these arrows to move this filter up or down in the list.
Export	Click the button to export filters to an XML file.
Import	Click the button to import filters from an XML file.
Select/deselect all	Use this box to ease operations with filters.

The buttons at the bottom of the screen are briefly described here and in detail later in this chapter.



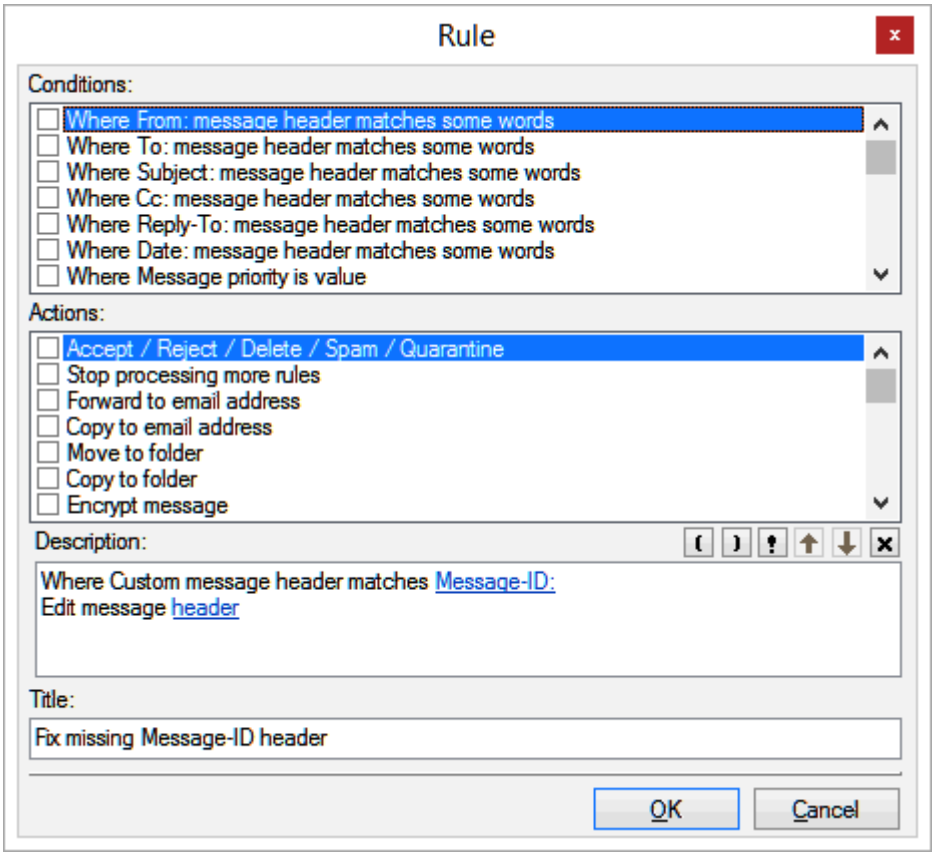
*TIP: Select a rule in the list and hold CTRL while you press the **Add** button, the new rule is positioned above the selected one.*



*TIP: Check the **Server Variables and Functions** chapter (**Manual.chm – Shared Topics**) for system variables which can be used here, for example to forward email to other SMTP server.*

Adding a New Filter

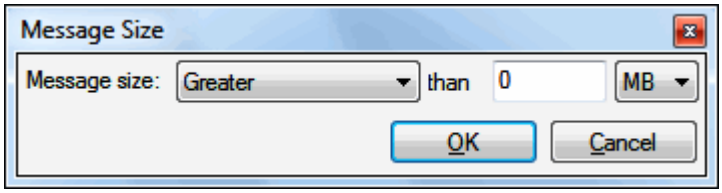
Clicking the **Add** button opens the **Rule** dialog which allows you to define a new filter:



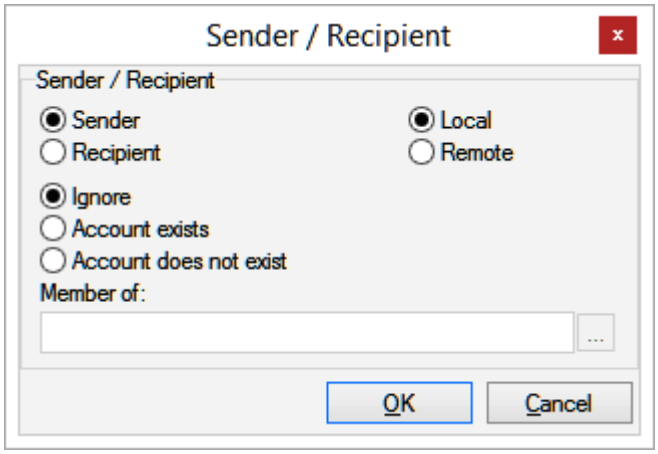
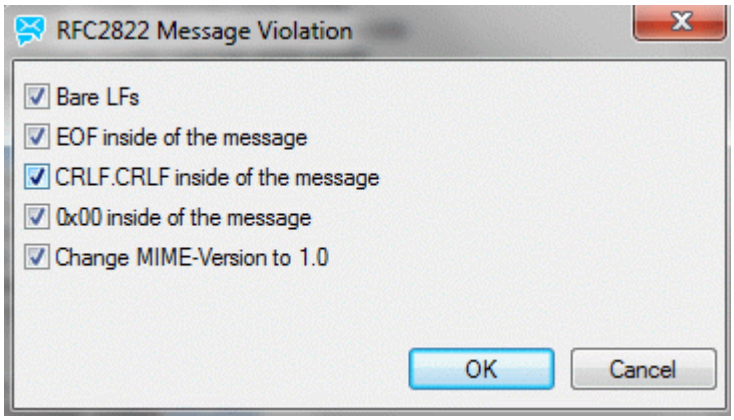
Field	Description
Conditions	All rules consist of one or more conditions. Tick the wished condition(s). For detailed description, refer to the **Filter Conditions** chapter.
Actions	Select the wished action(s) that are to be performed in the case any of rule conditions is evaluated TRUE. For more information, refer to the **Filter Actions** chapter.
Description	This pane shows the rule structure and allows you to add/edit values of conditions and actions. Click the appropriate link(s) do to it. For more information, refer to the **Filter Description** chapter.
Title	Enter a descriptive rule name. In the case the field is left blank, this name is generated automatically.

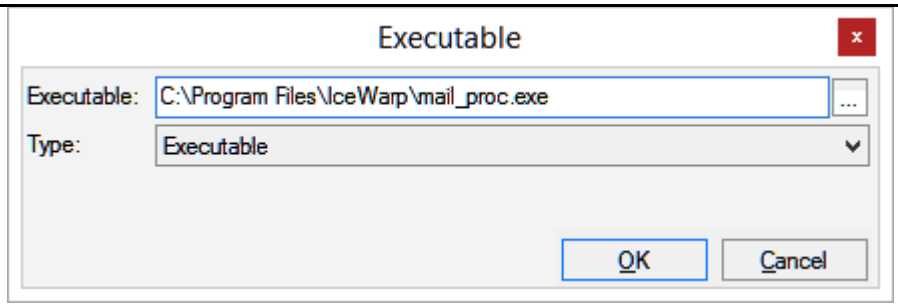
Filter Conditions

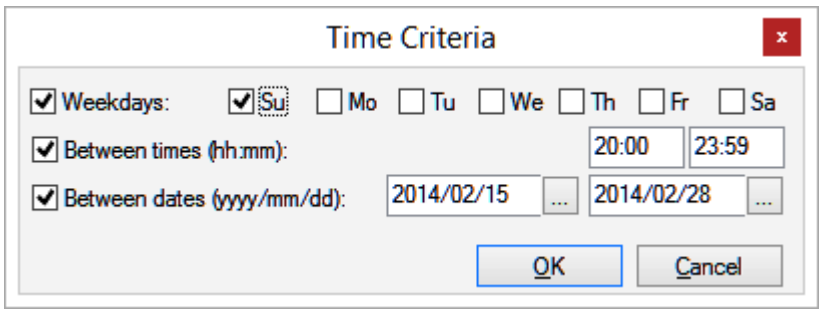
Condition	Use this condition to ...
Where From: message header matches some words	check the From: header for text. Adds a **some words** option to the rule description (explained below).
Where To: message header matches some words	check the To: header for text. Adds a **some words** option to the rule description (explained below). This condition has the ***Multiple Items Matching*** section within the **String Condition** dialog with the following options: ▪ Convert to single string ▪ All items match ▪ At Least one item matches

	For detailed explanation, see further in this section.
Where Subject: message header matches some words	check the Subject: header for text. Adds a **some words** option to the rule description (explained below).
Where Cc: message header matches some words	check the Cc: header for text. Adds a **some words** option to the rule description (explained below). This condition has the ***Multiple Items Matching*** section within the **String Condition** dialog with the following options: ▪ Convert to single string ▪ All items match ▪ At Least one item matches For detailed explanation, see further in this section.
Where Reply-To: message header matches some words	check the Reply-To: header for text. Adds a **some words** option to the rule description (explained below).
Where Date: message header matches some words	check the date: header for text. Adds a **some words** option to the rule description (explained below).
Where Message priority is value	check the priority of the message. Adds **Where message priority is Normal** to the rule description. Click on **Normal** to select a priority.
Where Message is Spam	check if the message is marked as spam
Where message is size	check the size of the message. Adds a **0 kB** option to the rule Description. Click on this to choose whether to check the message for a size Greater than or Less than and a size in selected units (kB, MB, GB). 
Where Message body matches some words	check the whole message body for some text. **Parse XML** function removes all HTML tags from an HTML email body and allows you to search for the text in an HTML part of a message Adds a **some words** option to the rule description (explained below). *NOTE: When creating a content filter that scans a whole message body, you should use the **Where message is size** condition set to some reasonable size (e. g. < 50 kB).* *This condition is to be the first one used in the **Description** field.* *Example:* *Where **Message is** < 50 kB* *and **Where Message body matches** viagra* *Reject message* *and Stop processing more rules.*
Where Custom message header matches some words	check any custom headers for some text. Adds a **some words** option to the rule description (explained below).

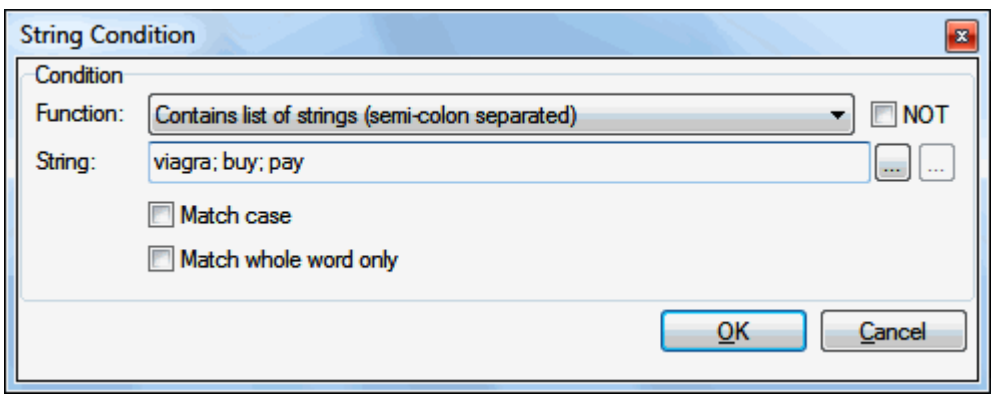
Where Any message header matches some words	check all message headers for some text. Adds a **some words** option to the rule description (explained below).
Where Attachment name matches some words	check attachment names for some text. Adds a **some words** option to the rule description (explained below).
Strip Attachment where name matches some words	Strip any attachment(s) whose name contains some text. Adds a **some words** option to the rule description (explained below).
Rename Attachment where name matches some words	Rename any attachment(s) whose name contains some text. This adds **some words** to the rule Description. This is a special case and usage examples follow: Syntax 1 - newstr;oldstr Syntax 2 - *.new;old Syntax once is a simple string replacement, any occurrence of "oldstr" in an attachment name will be replaced by "newstr" Syntax 2 adds ".new" as an extension to the name of any attachment whose name contains "old" Examples: the rule `dog;cat` would rename attachment `mycat.jpg` to `mydog.jpg` the rule ****.ex_;.exe*** would rename attachment ***Myprogram.exe*** to ***Myprogram.exe.ex_*** it would also rename ***not.an.exe.file.jpg*** to ***not.an.exe.file.jpg.ex_***
Where Message contains attachment	evaluates TRUE if the message contains an attachment.
Where Message charset matches some words	check the messages character set name for some text. Adds a **some words** option to the rule description (explained below the table).
Where Sender matches some words	check the sender's address for some text. Adds a **some words** option to the rule description (explained below the table). *NOTE: In the case you want to use the **Starts with** function (in the **String Condition** dialog), you have to specify also the initial angle bracket.* *Example: Email addresses are **john.doe@domain.com, john.d@anotherdomain.net,** etc. You want to search for all addresses beginning with **john**. In the **String** field, specify this: **<john*****
Where Recipient matches some words	check the recipient's address for some text. Adds a **some words** option to the rule description (explained below). This condition has the ***Multiple Items Matching*** section within the **String Condition** dialog with the following options: ▪ Convert to single string ▪ All items match ▪ At Least one item matches For detailed explanation, see further in this section. *NOTE: If you intend to use the **Starts with** function, see also the note above.*
Where Sender/Recipient is local/remote	specify sender/recipient: ▪ Sender – the defined action will be applied to a sender. ▪ Recipient – the defined action will be applied to a recipient. ▪ Local – the sender/recipient is local (from a local domain).

	▪ Remote – the sender/recipient is remote. ▪ Ignore – ignore the switches and field below. ▪ Account exists – the sender's/recipient's account exists within the selected domain/group/mailing list/... ▪ Account does not exist – the sender's/recipient's account does not exist within the selected domain/group/mailing list/... ▪ Member of – click the "..." button to select the appropriate domain/group/mailing list/... 
Where Sender's hostname matches some words	check the sender and the recipient for some text. Adds a **some words** option to the rule description (explained below).
Where message violates RFC2822	check the message for any RFC2822 violations. Adds **RFC2822** to the rule Description. Click on this to open a dialog that allows you to choose the five most common RFC2822 violations that can cause email clients to hang when trying to receive a message. 
Where Condition is execution of application	run a specific application to process the email message. Adds an **application** option to the rule description (explained bellow). Click this link to define the path to the application. This (custom) application obtains the path to the email file as a parameter. If the application output equals zero, the condition is not met, if the output is differing from zero, the condition is met.

	
Where Sender's IP address matches some words	check the Sender's IP address for some text. Adds a **some words** option to the rule description (explained below).
Where rDNS (PTR) matches some words	check the rDNS record for some text. Adds a **some words** option to the rule description (explained below).
Where Sender's IP address is listed on DNSBL server	check a DNSBL server for the sender's IP address of this message. Adds the **server** expression to the rule description. Click this to enter the name of the DNSBL server you wish to interrogate. (If not set, all servers activated under ***AS – Spam Assassin – RBL*** are queried.) Fill in the ***Regex*** field. Enter the regex expression that you want to use to sort DNSBL server answers. (If not set, any server answer will match the condition.) See the **Simple Regex Tutorial** chapter. *When creating content filters apart from AntiSpam/SpamAsssasin defined ones, consider using a condition Where **NOT** SMTP AUTH, to avoid catching users that authenticate SMTP.* *Example of a regex to check only for result code of 127.0.0.x from list.dnswl.org (which – in this case – is a classification they use for very legitimate senders – HIGH TRUST which is 127.0.0.1 as shown at www.dnswl.org instructions):* ***Where Sender's IP address is listed on DNSBL: Server – list.dnswl.org, Regex – 127.0.\d+.3*** ***Add score: -3.50*** ***Accept message***
Where session is trusted	check whether sender's IP is trusted or the sender has authenticated himself/herself.
Where Spam score is Value	check the spam score assigned by the AntiSpam engine. Adds **0.00** to the rule Description. Click on this to choose Greater or Lower than and a value. Note that the maximum value that the AntiSpam engine will assign is 10, so specifying a rule that says greater than 10 will never evaluate TRUE, similarly less than 10 will always evaluate FALSE unless the score is exactly 10.
Where Bayes score is percentage	check the score (%) assigned by the Bayesian filter processing. Adds **0%** to the rule Description. Click on this to select Greater or Lower and a percentage value.
Where SMTP AUTH	check whether this message was delivered using the SMTP AUTH command (authenticated login).
Where Scanned by Antivirus	check messages that were scanned by the IceWarp Anti-Virus engine. Adds **antivirus** to the rule Description. Click on this to open a dialog where you can choose any of the four IceWarp Anti-Virus engine results.

	 Note that it is not possible to tick both *Message contains a virus* AND *Message does not contain a virus* options.
Where Local time meets criteria	check the local time (of the IceWarp Server). Adds **criteria** to the rule Description. Click on this to open a dialog where you can specify local time checking criteria:  The above example will evaluate TRUE only if: The date is between 15th February 2014 and 28th February 2014 AND it is a Saturday or Sunday AND the time is between 20:00 and 23:59. This condition is supplied so that you could create a rule that only runs at weekends, overnight, etc.
Where SQL returns records value	This option runs a query against the database and if the query returns a result evaluates to TRUE, if the query returns an empty result it evaluate to FALSE. Click on Value in the rule description to specify the Database connection to use and the query to run. Click on reject in the rule description to choose an action if the rules evaluates as TRUE.
All messages	Evaluates TRUE for all messages. This is useful if you want to apply an action to every incoming message.

When **some words** is added to a rule **Description** you should click it to define the text you wish to check for. The **String Condition** dialog is presented:

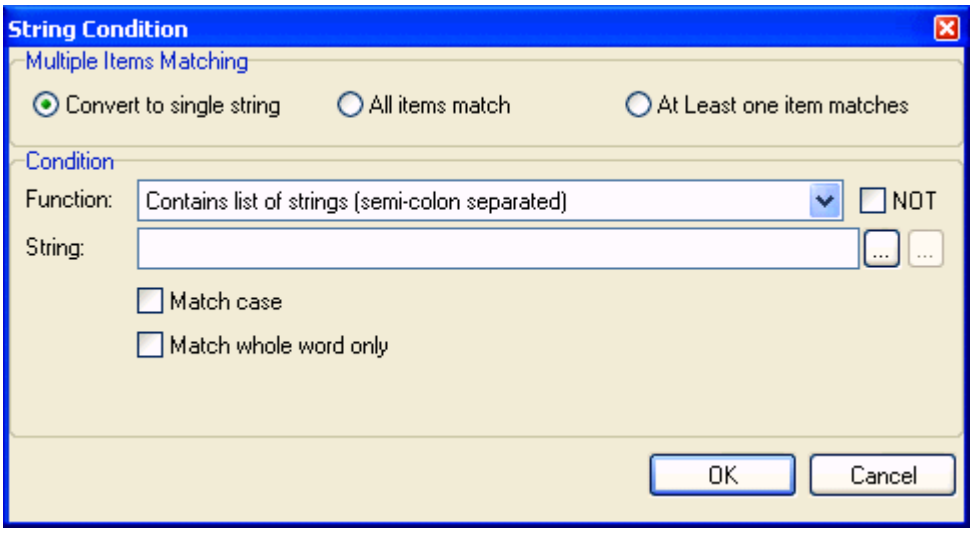


Field	Description

<table>
<tr><td>Function</td><td>Select the type of a test you want to perform against the value specified in the String field.
<table>
<tr><th>Function</th><th>Use this condition to ...</th></tr>
<tr><td>Contains list of strings (semi-colon separated)</td><td>Specify a list of semicolon separated strings.
Each string will be checked against the Condition and TRUE will be returned if any string matches.
Example:
Viagra;Cialis;spam</td></tr>
<tr><td>Regex</td><td>Specify a Regex (Regular Expression).
See Simple Regex Tutorial for more details. See the Mail Service – RegEx Rewrites section for more information about this topic.
For comprehensive Regex information, see http://www.regular-expressions.info/.</td></tr>
<tr><td>Contains string</td><td>Specify a single string.
If the specified string exists in the Condition, TRUE will be returned.
NOTE: Server variables can be used within a string definition. For more information, refer to the Server Variables chapter.</td></tr>
<tr><td>Starts with string</td><td>Specify a string that Condition must start with.</td></tr>
<tr><td>Ends with string</td><td>Specify a string that Condition must end with.</td></tr>
<tr><td>Is string</td><td>Specify a string that must be an exact match with the Condition.</td></tr>
<tr><td>Contains list from file or pattern</td><td>Specify a file name containing a list of strings in the String text box.
This must be a fully qualified path to the file.
The file must contain one string per line.
This Function works like "Contains list of strings" but reads the strings from the file.
To select a pattern (defined upon the System – Advanced – Patterns tab), click the left "..." button.</td></tr>
</table></td></tr>
<tr><td>NOT</td><td>Tick the box if you want to negate the specified function.</td></tr>
<tr><td>String</td><td>Fill in the string you want to evaluate against the Condition.</td></tr>
<tr><td>Match case</td><td>Tick the box if you want the comparison to be case sensitive, i.e. "Viagra" will match "Viagra" but not "viagra".</td></tr>
<tr><td>Match whole word only</td><td>Tick the box if you want the comparison to be true only if the string is not part of another word, i.e. "Viagra" will match "Viagra works" but will not match "Viagraworks".</td></tr>
</table>

Multiple Items Matching

This extended dialog is available for conditions related to the ***To***, ***CC***, ***Recipient*** and ***Attachment*** headers.



Field	Description
Convert to single string	Default. All recipients or attachments are evaluated as one string.
All items match	Condition is evaluated for each recipient/attachment, global match is returned if all recipients/attachments match.
At least one item matches	Condition is evaluated for each recipient/attachment, global match is returned if at least one recipient/attachment matches.

Example #1

Let's have two recipients: ***a@d1.com*** and ***a@d2.com***

Condition: contains string ***@d1***

- If ***Convert to string*** is used, "<a@d1.com>;<a@d2.com>;" string is constructed and tested. Result is ***MATCH***.
- If ***All items match*** is used, <a@d1.com> is tested, result is match, then <a@d2.com> is tested, result is not match. Global result is ***NOT MATCH.***
- If ***At least one item matches*** is used, <a@d1.com> is tested, result is match, then <a@d2.com> is tested, result is not match. Global result is ***MATCH.***

Example #2:

Let's have two recipients: ***a@d1.com*** and ***a@d2.com***

Condition: does ***NOT*** contain string ***@d1***

- If ***Convert to string*** is used, "<a@d1.com>;<a@d2.com>;" string is constructed and tested. Result is ***NOT MATCH.***
- If ***All items match*** is used, <a@d1.com> is tested, result is not match, then <a@d2.com> is tested, result is match. Global result is ***NOT MATCH.***
- If ***At least one item matches*** is used, <a@d1.com> is tested, result is not match, then <a@d2.com> is tested, result is match. Global result is ***MATCH.***



*NOTE: This works and will work for **Content Filters** only.*

Example #3

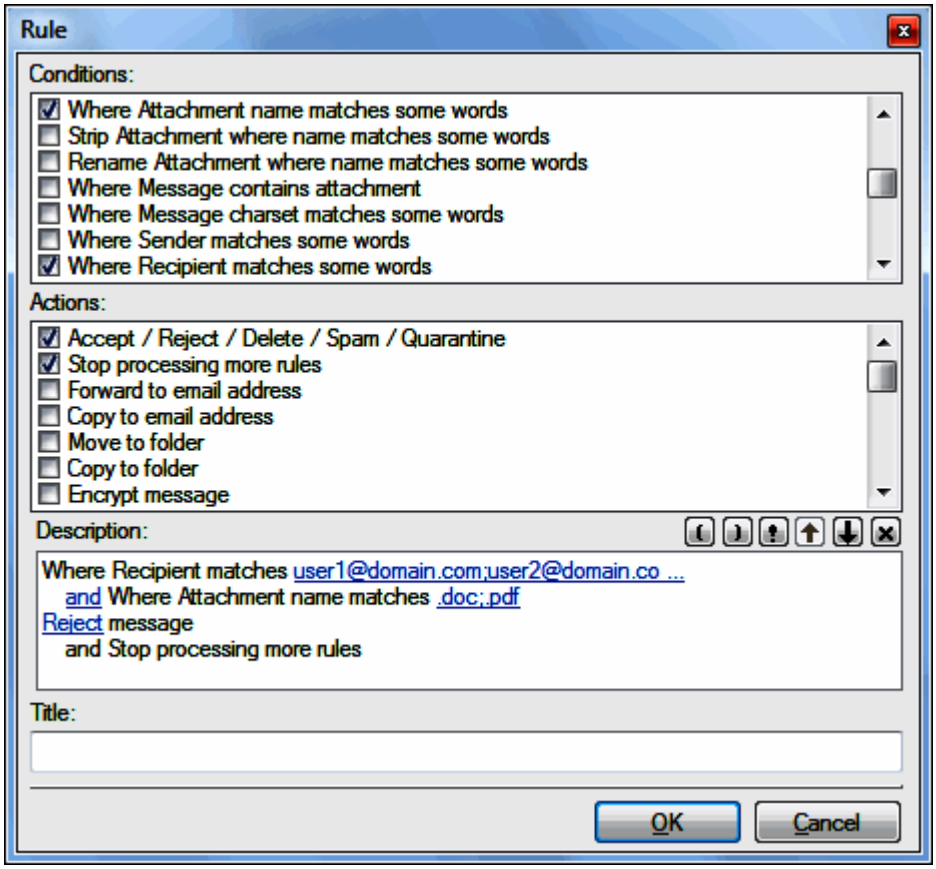
You may want to restrict some users to receiving only e. g. .doc and .pdf files.

Use these conditions:

- ***Where Recipient matches:*** user1@domain.com; user2@domain.com plus select the ***Convert to single string*** option.
- and ***Where Attachment name matches*** (plus tick the ***NOT*** box): .doc;.pdf plus select the ***At least one item matches*** option.

And use the following actions:

- Reject message
- and ***Stop processing more rules.***



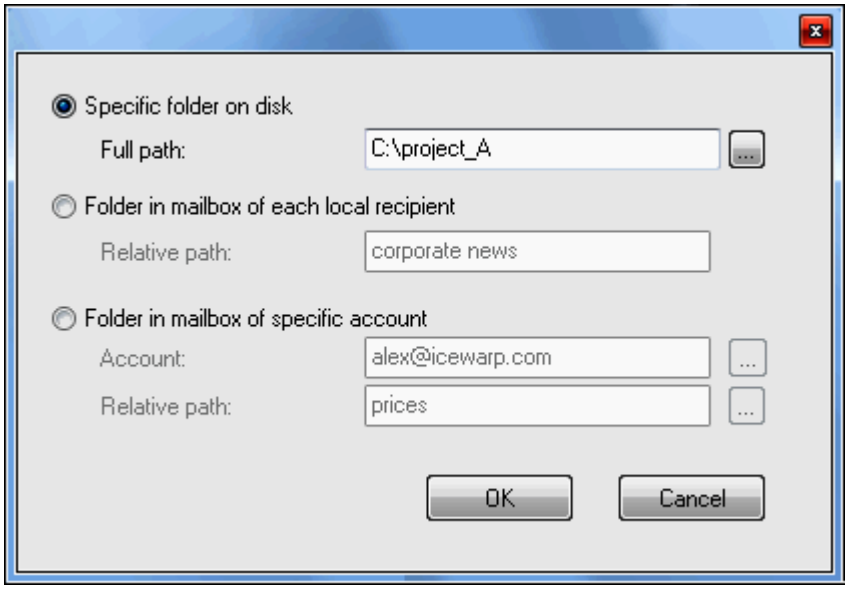
Filter Actions

When a rule is evaluated as true you have the following **actions** which you can apply to the message.

Multiple actions can be applied.

Checking an action will modify the **Rule Description** and may inset a clickable option to refine the action.

Action	**Description**
Accept/Reject/Delete/ Spam /Quarantine	Check this option to mark the message for Rejection, Acceptance or Deletion. The text **Reject** is added to the rule description. Click on Reject to open the **Message Action** dialog, where you can choose to Reject, Accept or Delete the message, or mark it as spam.
Stop processing more rules	Check this option to stop processing this message against further rules. This is useful once you have reached a decision on what to do with this message and saves any further processing power. For example - if you set up a rule to delete all messages from the domain spamcity.com you can set the action to Delete the message and Stop at this rule. The rules processing is completed and the message deleted.

Forward to email address	Check this option to forward a copy of the message to another email address. The text **email address** is added to the rule description. Click on this to open the **Email Address** dialog, allowing you to specify the address(es) to forward the message to. Multiple accounts can be specified, separated by semicolons. Use the '...' button to select accounts. *NOTE: In the Email Address field, the following syntax can be used:* ***%%Forward_local_recipients Host%%*** *This forwards an email message as it is – without any changes of headers – to other server and leaves a copy on the original server.*
Copy to email address	Check this option to have a copy of the message sent to another email address. The text **email address** is added to the rule description. Click on this to open the **Email Address** dialog, allowing you to specify the address(es) to send a message copy to. Multiple accounts can be specified, separated by semicolons. Use the '...' button to select accounts. *NOTE: There is a difference between the **Copy ...** and **Forward ...** options: The forward action forwards the messages **as-is** without any changes done by the content filter. Provided that the **Use MDA queue for internal message delivery** option (**Mail – General – Advanced**) is enabled, the copy action sends the message after all changes by the content filter have been applied.* *Lets say the content filter contains an action to change the message's header. The forward will send the message without changes and the copy will send the changed header message.*
Move to folder	Check this option to move the message to a folder. Click on ***folder*** in the rule description to open a folder-tree view dialog where you can select the folder to use. *NOTE: You can use this action also for multiple users. E. g. you can set a filter with the **Where Recipient matches some words** condition for mike@mycompany.com; alison@mycompany.com (etc.) and **Move to** Marketing **folder**. Both (all) recipients will have emails matching the defined condition moved to their specified folders provided that they have them created.* For additional information, refer to the **Rules** (on page 42) section.
Copy to folder	Check this option to copy the message to a folder. Click on ***folder*** in the rule description to open a dialog where you can select the folder to use.  ▪ ***Specific folder on disc*** – select this option and specify ***Full path*** (using the "..." button) to have

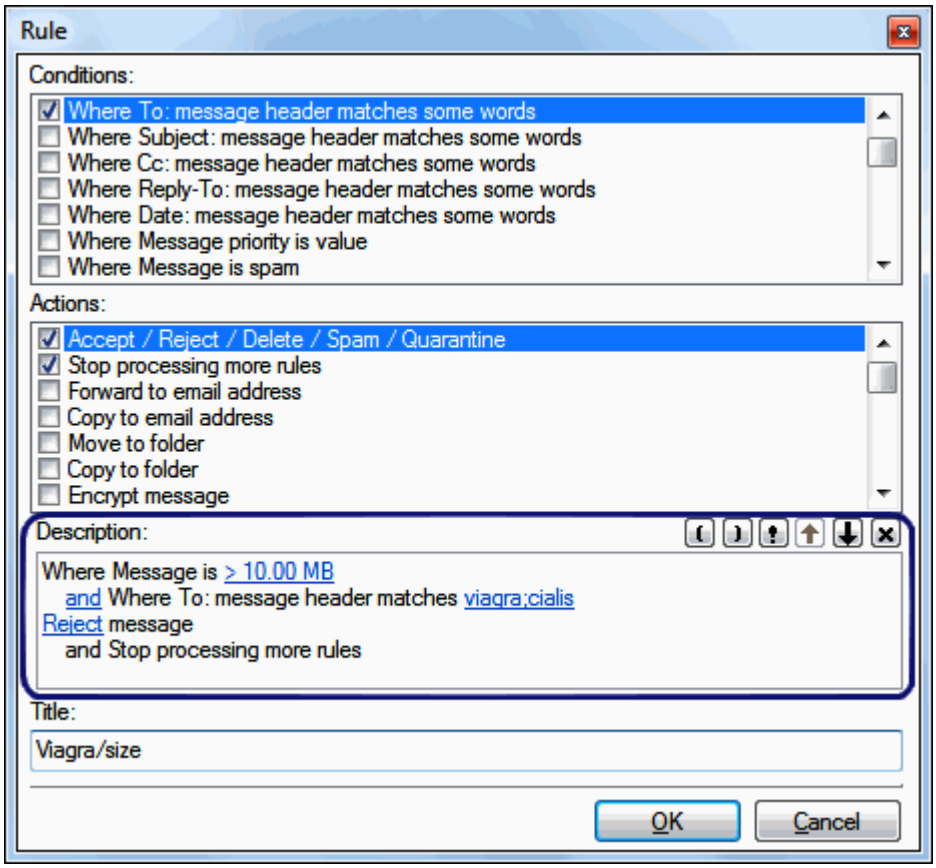
	messages copied to a folder on the server disc. Syntax for use in **WebAdmin** is <***path***>; see the example in the screenshot. ▪ ***Folder in mailbox of each local recipient*** – select this option and specify a folder name in the ***Relative path*** field to have messages copied to this folder of each local message recipient. Syntax for use in **WebAdmin** is <***folder name***>; see the example in the screenshot. ▪ ***Folder in mailbox of specific account*** – select this option to have messages copied to a specific folder of one local account. Specify this account in the ***Account*** field and the appropriate folder in the ***Relative path*** one. Syntax for **WebAdmin** is <***email_address:folder_name***>. Example: ***alex@icewarp.com:prices***. For additional information, refer to the **Rules** (on page 42) section.
Encrypt message	Check this option to have IceWarp Server encrypt the message. Only incoming messages are encrypted provided that a recipient has a certificate uploaded on the server (and the filter condition is met). Certificates can be uploaded via IceWarp WebClient (the **Tools – Options** menu items – **Security – Certificates** tabs). If you want to enforce all users to have their messages encrypted, you can do it via IceWarp WebClient (**Administrator Options – Mail – Default**), provided that all of them have their certificates uploaded.
Respond with message	Check this option to send a message back to the sender of this message. The text **message** is added to the rule description. Click on this to open the Message dialog, where you can specify the From address, the Subject, the message Text (or a file containing the message text) and whether the message Type (Email, Instant message, or both).
Send message	Check this option to send a message to any user. The **message** link is added to the rule **Description**. Click the link to open the **Message** dialog, where you can define the *To*, *From* and *Subject* fields, the *Text* of the message (or a file to retrieve the text from), the type of a message (text, HTML, or message with attachment).
Edit message header	Check this option to edit the message headers. You can add, remove or change headers. The text **header** is added to the rule description. Click this to open the Headers dialog, where you can specify the action to take, and which header to take it on. Server variables are allowed here, so for example you could modify the ***Subject:*** header to add some text: *Subject: [MyNewText] %%Subject%%* For detailed information about server variables, refer to the **Server Variables** chapter.
Set message priority to value	Check this to change the message priority. Click ***Normal*** in the ***Description*** field to select the value of ***x-priority*** message header in the **Message Priority** dialogue.
Set message flags	Check this option to set message flags. Click on flags in the rule description to select which flags to set
Add score	Check this option to add a value to the spam score of the message. Click on 1.00 in the rule description to set the value to be added. *NOTE: You can specify a negative value to have the spam score decreased.* *NOTE: When the message score is changed, the message is evaluated again whether it is OK or a spam.*
Execute application	Check this option to run an executable. The text **executable** will be added to the rule description. Click this to open the Executable dialog where you can specify the fully qualified path to the executable and it's type (Executable, StdCall, Cdecl or URL) When using the *URL* option, you can obtain the following HTTP status return codes: • ***2xx*** means TRUE

	• ***5xx*** means FALSE • ***301*** and ***302*** is processed as redirect and the status depends on the redirection target • other ***3xx*** are considered as FALSE • ***4xx*** is mostly FALSE, the exceptions are ***401*** (unauthorized) and ***407*** (proxy unauthorized), when valid username and password has been specified in URL. Then the result depends on retried request with username and password filled.
Add header/footer	Check this option to add a header and/or footer to the email. Headers and Footers are stored in files and can be plain text or HTML. The text **header/footer** is added to the rule description. Click this to open the Header/Footer dialog, which allows you to specify the fully qualified paths to the header and or footer files you want to add to the message.
Strip all attachments	Check this option to strip any attachments from the message.
Extract all attachments to directory	Check this option to store all attachments to a folder. The text **directory** is added to the rule description. Click this to open the extract attachments dialog, where you can specify the directory in which attachments should be stored. If the attachments is an IDP (IceWarp Data Packager) file you can optionally choose to have the files extracted from the package. You can also optionally choose to overwrite existing files.
Perform SmartAttach	Check the box if you want to extract attachments using SmartAttach. For detailed information about this feature, refer to the **GroupWare – SmartAttach** chapter.
Add text to a file	Check this option to add a line of text to a file. The text **text** is added to the rule description. Click this to open the Add Text dialog, where you can specify the fully qualified filename to write to and the text to be written. You can optionally choose to create a new file each time. System variables can be used within the text. This option can be useful to create your own format logs containing any information you wish to record
Respond with SMTP message text	Check this option to specify the SMTP servers response to the incoming message. The text **text** is added to the rule description. Click on this to open the SMTP Response dialog, which allows you to specify the text to send back to the originating server. The format of the text should be a numeric response code followed by your freeform text.
Fix RFC822 message	Check this option to fix messages that are not RFC822 compliant. These messages can cause problems with your server and with your user's email clients. Non-compliant messages are usually spam or hacker attacks and we recommend that you delete them with the condition "Where message violates RFC822" combined with Action "Delete" and "Stop at this filter" rather than allowing them through.
Block sender's IP address	Check this option to invoke Intrusion Prevention blocking rules to block this senders IP address for an amount of time.
Execute SQL statement value	Check this box to execute an SQL query against a database. Click value in the rule description to define the database connection parameters and the query to be run.
Skip archive	Check this box if you do not want messages matching conditions to be archived.

Filter Description

Once you have built your rule there is a description of the rule in the lower pane of the **Rule** dialog.

This section discusses the description and the ways you can use it.



All conditions are initially combined with logical ***and*** operations, these can be changed to logical ***or*** operations (and vice versa) by clicking the operator word.

Brackets can be inserted in the description field by placing a cursor where you want to have a bracket and pressing the appropriate button. "**(**" or "**)**". Using brackets, you can to change the order of condition evaluation. E.g.: condition 1 ***and*** (condition 2 ***or*** condition 3).

A condition can be negated by placing your cursor before the condition and pressing the exclamation mark "**!**" button.

Conditions can be moved up and down the list by placing your cursor within the condition and using the up and down arrows.

A condition can be deleted from the rule by placing the cursor within the condition and pressing the delete button – "**X**".

Editing a Filter

Pressing the ***Edit*** button opens the currently selected rule for editing.

The same **Rule** dialog opens as for adding a rule. The difference is that all conditions and actions will be selected as appropriate and the rule description will be populated.

Please refer to the **Adding a New Filter** chapter for full information.

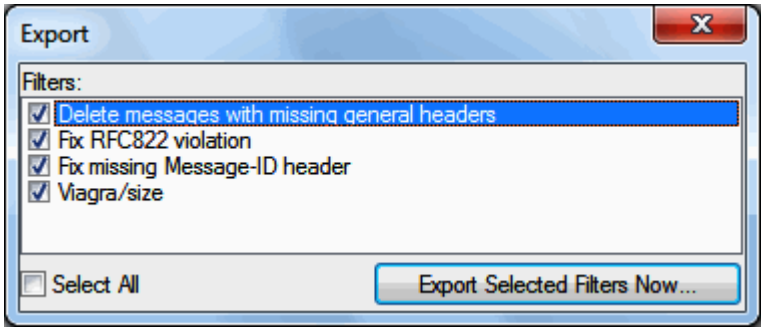
Deleting a Filter

Pressing the ***Delete*** button will delete the currently selected rule.

A confirmation dialog is presented.

Exporting Filters

The ***Export*** button opens the **Export** dialog where you can select rules to be exported to an XML file.



Check all the rules that you want to export and press the ***Export Selected Filters Now*** button.

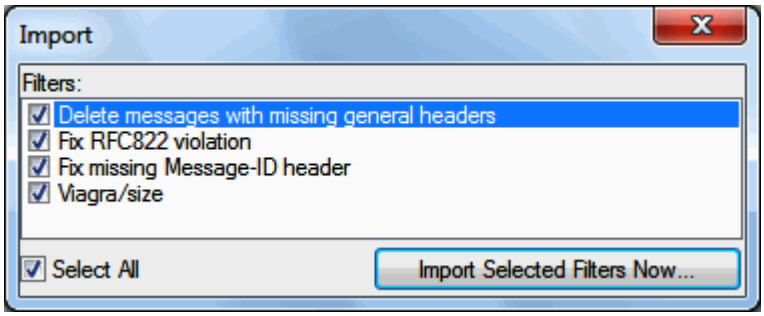
A standard file dialog allows you to save your XML file.

This can be useful as a backup copy of your filters or if you want to copy your filters from one IceWarp Server to another.

Importing Filters

The ***Import*** button opens a standard file browser dialog to locate and open your XML file of exported filters.

Once the XML file is opened, you will be presented with the **Import** dialog.



You should check the filters you wish to import and press the ***Import Selected Filters Now*** button.

Bypassing Filters

If you want to bypass existing filters, you can create/use the **IceWarp/config/cfbypass.dat** file.

For more information about its syntax, refer to the **IceWarp/examples/bypass.dat.html** file.

Understanding the SMTP Protocol and Message Headers

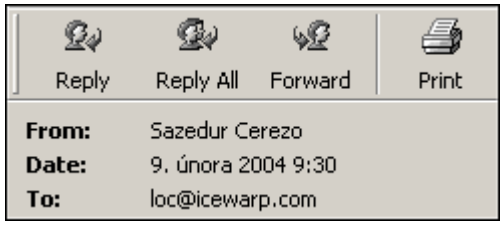
To implement Rules properly, you should understand the structure of an emails and how they are transferred via the SMTP protocol.

An email is transferred over the network using the SMTP protocol as a plain text file with a header and body part.

Instead of the term email, we will use the term **"message**". A "message" is a plain text file which contains an email and all of its attachments and other parts.

Confusion is often caused by the fact that the SMTP sender and recipient can be completely different to the From and To information displayed in an email client.

To understand the difference, look at the IceWarp Server system variables, which are related to messages.

%%From%% %%From_Email%% %%From_Alias%% %%From_Domain%% %%From_Name%%	"From:" is taken from the message header, displayed in the recipient client. 
%%To%% %%To_Email%% %%To_Alias%% %%To_Domain%% %%To_Name%%	"To:" is also taken from the message header. Both - From and To are taken from the message header and they NEED NOT be the same as the one used in the SMTP protocol during message transmission.
%%Sender%% %%Sender_Email%% %%Sender_Alias%% %%Sender_Domain%%	The Sender is the real sender in the SMTP protocol. The "From:" in the message header can be different.
%%Recipient%% %%Recipient_Email%% %%Recipient_Alias%% %%Recipient_Domain%%	This is the real recipient in the SMTP protocol. The message will be delivered to this recipient regardless of the message "To:" header.

An email client displays the information from the message header, while the delivery of the message is given by the information in the SMTP protocol.

Example:

The following is an extract from the SMTP log:

The message delivered from xxx@icewarpdemo.com to the admin@icewarpdemo.com - SMTP protocol:

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 Connected

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 220 mail.icewarpdemo.com ESMTP Merak 7.2.4; Wed, 10 Mar 2004 21:41:16 +0100

*127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< MAIL From:**xxx@icewarpdemo.com***

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.1.0 <xxx@icewarpdemo.com>... Sender ok

*127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< RCPT To:**admin@icewarpdemo.com***

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.1.5 <admin@icewarpdemo.com>... Recipient ok

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< DATA

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 354 Enter mail, end with "." on a line by itself

*127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 *** <xxx@icewarpdemo.com> <admin@icewarpdemo.com> 1 1605 00:00:00 OK*

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.6.0 1605 bytes received in 00:00:00; Message accepted for delivery

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< QUIT

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 221 2.0.0 mail.icewarpdemo.com closing connection

SYSTEM [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 Disconnected

It shows that the message is from xxx@icewarpdemo.com and should be delivered to admin@icewarpdemo.com.

The following shows the actual headers of the message

Received: from servcom2.DOMAINE.local ([213.223.244.1])

by mail.icewarp.com (Merak 7.2.1) with ESMTP id CRA73883

for <loc@icewarp.com>; Mon, 09 Feb 2004 09:28:40 +0100

Received: from metallography ([219.95.18.216]) by servcom2.DOMAINE.local with Microsoft SMTPSVC(5.0.2195.5329);

Mon, 9 Feb 2004 09:30:12 +0100

From: "Sazedur Cerezo"<locloc@YAHOO.COM>

To: loc@icewarp.com

*Subject: loc: H*G*H-Lo0k Younger Whl1e L0slnq We19ht*

Mime-Version: 1.0

Content-Type: text/html; charset=us-ascii

Content-Transfer-Encoding: 7bit

Return-Path: locloc@YAHOO.COM

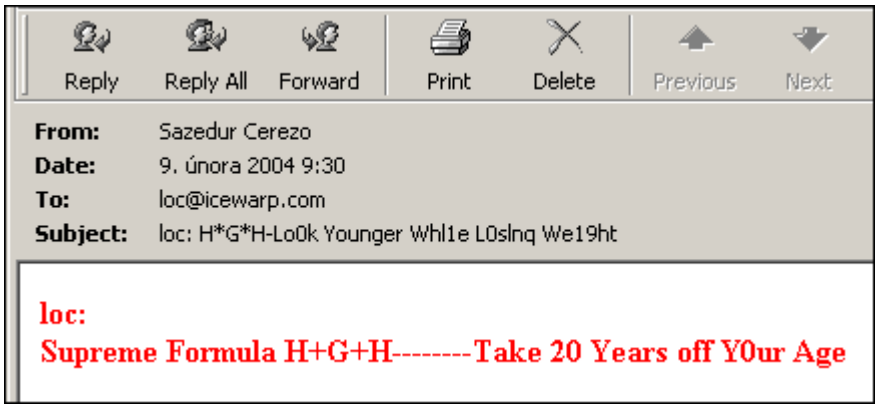
Message-ID: <SERVCOM2QFgkASNplKc000165d3@servcom2.DOMAINE.local>

X-OriginalArrivalTime: 09 Feb 2004 08:30:15.0039 (UTC) FILETIME=[F10A78F0:01C3EEE6]

Date: 9 Feb 2004 09:30:15 +0100

This shows that the headers say that the message is from "Sazedur Cerezo" and is sent to loc@icewarp.com.

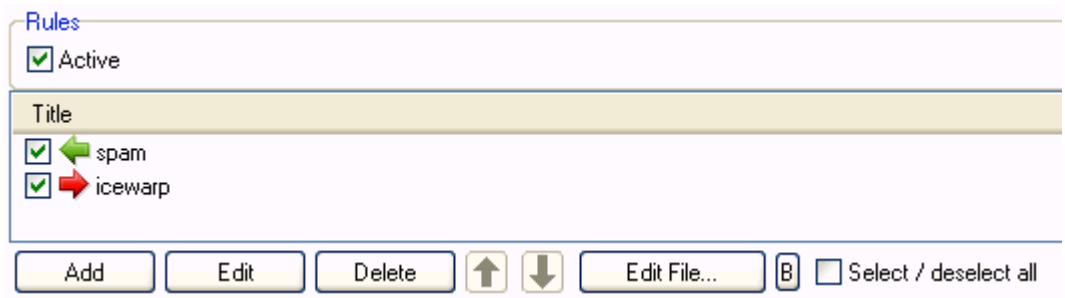
This is the information that is displayed in the email client:



From & To used in the Content Filter Condition correspond to the From: and To: of the HEADER of the message, while the **Sender & Recipient** are taken from SMTP protocol.

Rules

Selecting **Mail – Rules** – **Rules** tab gives you access to the **Rules** list, allowing you to perform maintenance on the rules.



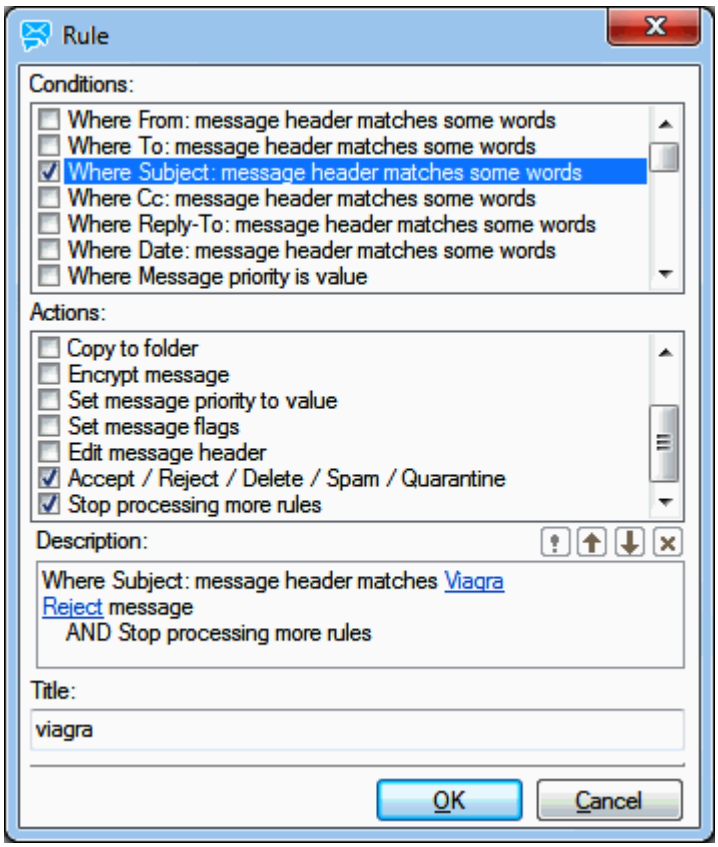
Field	Description
Active	Tick the box to activate this feature.

Add	Click the button to add a new rule. The **Rule** dialog opens.
Edit	Click the button to modify an existing rule. The **Rule** dialog opens.
Delete	Click the button to delete the selected rule.
Up/down arrows	Select a rule and click the appropriate button to move this rule up or down.
Edit File	Click the button to open the file that contains defined rules. You can edit rules here. *NOTE: The filter is a text file with a strictly defined format. The file can be edited directly using a standard text file editor but we **highly** recommend to use the **Add**, **Edit** and **Delete** buttons as even the simplest mistake can cause valid emails to be rejected.*
"B" button	Click the button to open the **Bypass** dialog where you can define items that will bypass defined rules. For more information, refer to the **Shared Items – Bypassing Rules/Filters** chapter.
Select/deselect all	Use this feature to ease operations with more rules.

Multiple rules can be selected for deletion by holding the ***CTRL*** key and clicking these rules.

A range of rules can be selected by clicking the first rule of the range and then clicking the last one while holding down the ***SHIFT*** key.

NOTE: Rules can be activated and de-activated by checking/un-checking the box to the left of the rule. This is useful for testing purposes or to disable a rule for a time without deleting it.

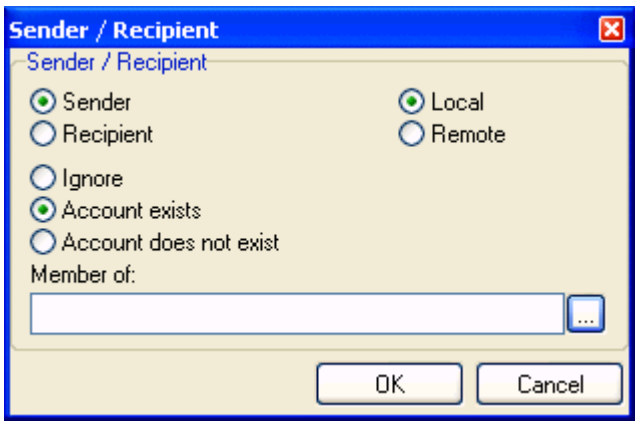


Field	**Description**
Conditions	In this area, you can select the properties of the message that you wish to perform some test on. ▪ Multiple conditions can be tested by checking multiple boxes. ▪ The same condition can be added multiple times by double clicking the condition when it is checked.

Actions	In this area, you select the action(s) that you want to perform on the message if the rule evaluates as True. ▪ Multiple actions can be selected by checking multiple boxes.
Logic buttons	The buttons below the **Actions** block are used to add logic to the rule ▪ The ***exclamation mark*** will negate (NOT) the condition you are currently modifying. ▪ The ***up*** and ***down*** arrows will move the conditions up and down within the rule. ▪ The ***X*** button will delete the current condition. We recommend experimentation with these buttons to familiarize yourself with their function.
Description	This will show the rule you are building or modifying and will change dynamically as you select or de-select conditions and actions. Areas of the rules that can be modified are highlighted in this block and clicking them opens a further dialog box to allow you to define your test.
Title	The name of the rule, for identification purposes.

The following table details individual conditions and actions.

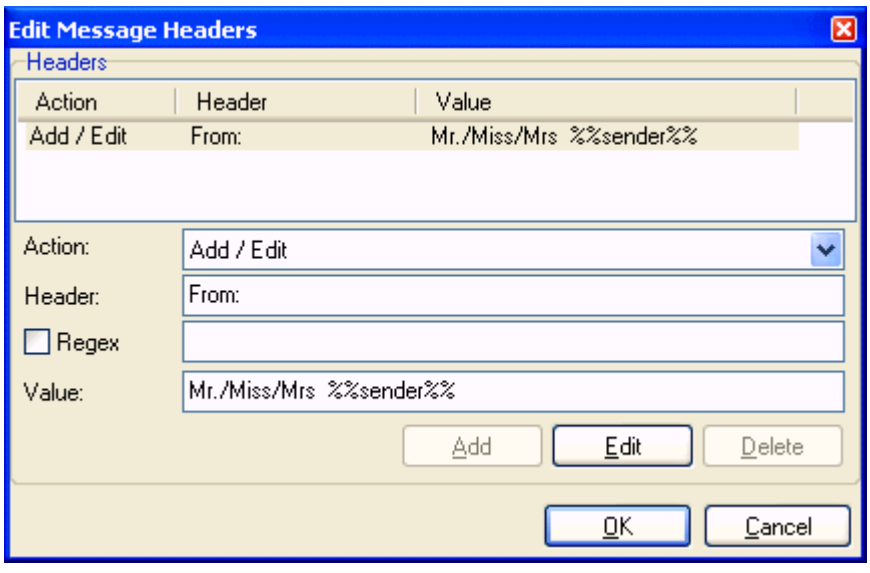
Condition	**Description**
Where From: message header matches some words	Checks the ***From:*** header for a string. In the rule description, click the **some words** to create the string (explained below).
Where To: message header matches some words	Checks the ***To:*** header for a string. In the rule description click the **some words** to create the string (explained below).
Where Subject: message header matches some words	Checks the ***Subject:*** header for a string. In the rule description click the **some words** to create the string (explained below).
Where Cc: message header matches some words	Checks the ***Cc:*** header for a string. In the rule description click the **some words** to create the string (explained below).
Where Reply-To: message header matches some words	Checks the ***Reply-To:*** header for a string. In the rule description click the **some words** to create the string (explained below).
Where Date: message header matches some words	Checks the ***Date:*** header for a string. In the rule description click the **some words** to create the string (explained below).
Where Message priority is value	Checks the priority of a message. Click the ***Normal*** in the rule description to select a priority.
Where Message is spam	Checks whether the message has been marked as spam.
Where Message is size	Checks the message size. Click the ***0 kB*** to select the message size criteria. Select ***Greater*** or ***Lower*** and specify a size (in kB, MB or GB)
Where Message body matches some words	Checks the message body for a string. In the rule description click the **some words** to create the string (explained below). *NOTE: Use this option with care as scanning the whole message body of every incoming message could seriously affect your server performance.*
Where Custom message header matches some words	Checks a custom message header for a string. In the rule description click the **some words** to create the string (explained below).

	NOTE: This rule has an unusual format for the string condition! format – ***<header>:<string condition>*** where ***<header>*** is the name of your custom header ***<string condition>*** is the string to test the header for. Example: ***MyHeader:jim;bob;john*** Would check the ***MyHeader*** header for any of the strings "jim", "bob" or "john".
Where Any message header matches some words	Checks all headers for a string. In the rule description click the **some words** to create the string (explained below).
Where Attachment name matches some words	Checks the attachment name for a string. In the rule description click the **some words** to create the string (explained below).
Where message contains attachment	Checks whether the message has an attachment.
Where Sender matches some words	Checks the sender for a string condition. In the rule description click the **some words** to create the string (explained below).
Where Recipient matches some words	Checks the recipient for a string. In the rule description click the **some words** to create the string (explained below).
Where sender/recipient is local/remote	Checks the location of the sender or recipient. In the rule description click the **local/remote** to open the following dialog:  **Sender / Recipient** Select whether you want to check the the sender or recipient address. **Local / Remote** Select whether you want whether the chosen address is a local account or a remote one. **Ignore / Account exists / Account does not exist** Select whether you want to check whether the account exists, does not exist, or ignore this check. *Only available for local accounts.* **Member of:** Checks whether the account belongs to a particular domain, group, mailing list, etc. Click the '...' button to open the standard **Select Item** dialog. *Only available for local accounts that you check the existence or non-existence of.*

Where Sender's IP address matches some words	Checks the remote IP address for a string. In the rule description click the **some words** to create the string (explained below).
Where rDNS (PTR) matches some words	Checks the rDNS (PTR) record for a string. In the rule description click the **some words** to create the string (explained below).
Where Sender's IP address is trusted	Checks whether the sender's IP address is in the trusted list.
Where Spam score is value	Click the ***0.0*** in the rule description to define a greater than or less than value to check the spam score against.
Where SMTP AUTH	Checks whether the message was delivered using an SMTP authorized connection.
All messages	A special condition that evaluates TRUE for all messages – use with care!

String Testing	**Description**
	Clicking the **some words** (in a new condition) or the string itself (in a condition already defined) will open the **String Condition** dialog. There are four options available in the dialog: The **Function** drop-down box offers seven options for the string test, the option chosen effects the content required in the **String** text-box.
Contains value from a list (semi-colon separated)	Populate the **String** box with a list of strings to test for.
Matches (Regex)	Populate the **String** box with a regular expression. For more information, refer to the **Simple RegEx Tutorial**.
Starts with	Looks for the string specified in the **String** box at the beginning of the tested text.
Ends with	Looks for the string specified in the **String** box at the end of the tested condition.
Equals	Tests whether the tested text is ***exactly*** equal to the string specified in the **String** box.
Contains a value from a file or pattern	Into the **String** box, enter the path to a text file containing a list of strings you wish to test for. Click the "..." button to open the **Open** dialog to navigate to a file where the strings are specified, one per line.
Match case	Check this box to take string case into account.
Match whole word only	Check this box to perform a standard "whole word" check against the string.

Actions	**Description**
	The following actions can be performed when a condition is evaluated TRUE. Multiple actions can be selected by checking multiple boxes. Selecting an action will add the action to the **Description** box and for some actions you are able to click the text in the description to define the action further. Details follow:
Send message	Sends a message. The **message** link is added into the **Description** area. Click this link to open the **Message** dialog, where you can specify the *From* address, *To* address, *Subject* and message *Text*.
Forward to email address	Forwards the message to an email address. Click the **email address** in the **Description** area to specify the email address. *NOTE: You can also send an instant message or an sms using this option:* *sms – use this syntax:* ***sms:<number>*** *e. g.* ***sms:0123456789***

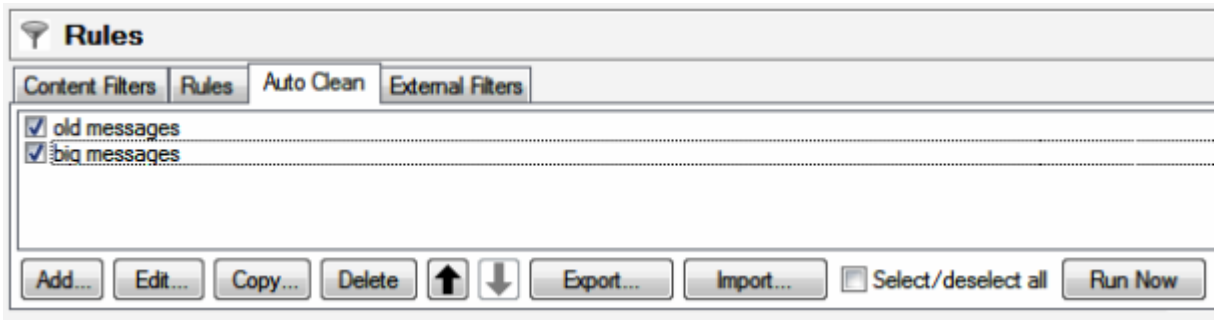
	IM – use this syntax: ***xmpp:<jabberid>*** *e. g.* ***bruce@icewarpdemo.com***
Move to folder	Moves the message to a folder. Click the **folder** in the **Description** area to select the folder to move to. *NOTE: The folder tree does not fill when you access this action within* ***Content Filters****, you have to manually specify a mailbox.* *ALSO: Although the INBOX folder may be shown in the folder tree, there is little point selecting this folder as this is the default folder that messages will come in to.* *ALSO: You can have email delivered to a specific mailbox folder by specifying* ***%%Extension%%*** *as the folder name. When this is specified, IceWarp Server will look for a folder name within the email address and store the message to that folder if it exists.* Example: A message sent to ***john:%%important%%@icewarpdemo.com*** will be stored in the folder of **important**. Note the colon used to separate the user's alias from the folder name – this can be changed to another character using the API.
Copy to Folder	Copies the message to a folder. Click the **folder** in the **Description** area to select the folder to copy to. For description of the selection dialog, refer to the **Content Filters – Filter Action** chapter. *NOTE: Although the INBOX folder may be shown in the folder tree, there is little point selecting this folder as this is the default folder that messages will come in to.*
Encrypt message	Check this option to have the message encrypted. *NOTE: For this option to work there must be a copy of the user's public certificate located in a file called* ***cert.pem*** *in the user's mailbox folder. The message will be encrypted using this certificate and then can only be decrypted by the user using his/her private key in his/her email client.*
Set message priority to value	Select this option to have the priority of the message changed. Click the ***Normal*** to select the new priority to be assigned.
Set message flags	Select this option to set a message flag. Click the **flags** to set the flag(s) you wish.
Edit message header	Select this option to ***Add, Edit*** or ***Delete*** a message header. Click the header to open the **Edit Message Headers** dialog.  Click the ***Add*** button to add a new rule.

	Select an already defined rule and click ***Edit*** or ***Delete*** to modify or remove a rule. In the ***Action*** drop-down, select whether this rule will add/edit a header or delete it. In the ***Header*** field, specify the header you want to change/add. *Remember that the last header name character has to be a colon!* You can also add your own named headers e. g. ***MyHeader:*** The first rule shown in the screenshot above modifies the ***From:*** header – it adds the string of "Mr./Miss/Mrs." to the beginning of the header. Note the use of the IceWarp Server system variable ***%%sender%%*** here, which is the value of the original ***From:*** header. Any system variable can be used.
Accept/Reject/Delete/Spam/Quarantine	Adds the ***Reject*** message (default). Click the ***Reject*** in the **Description** area to select ***Reject, Accept, Delete, Spam*** or ***Quarantine***.
Stop processing more rules	Stops any further rules from being processed, if the rule condition is evaluated as TRUE.

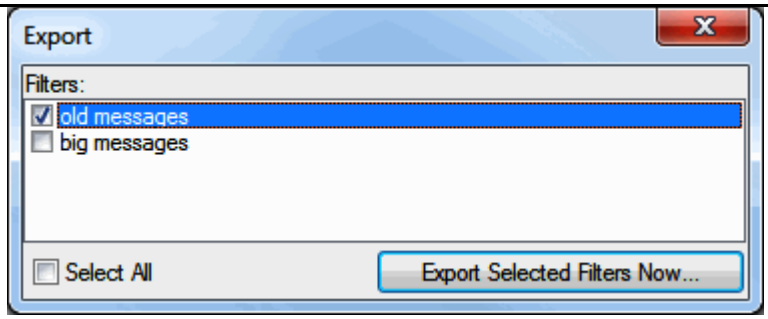
Auto Clean

This feature allows you to "clean" mailboxes. All actions defined here are performed every midnight.

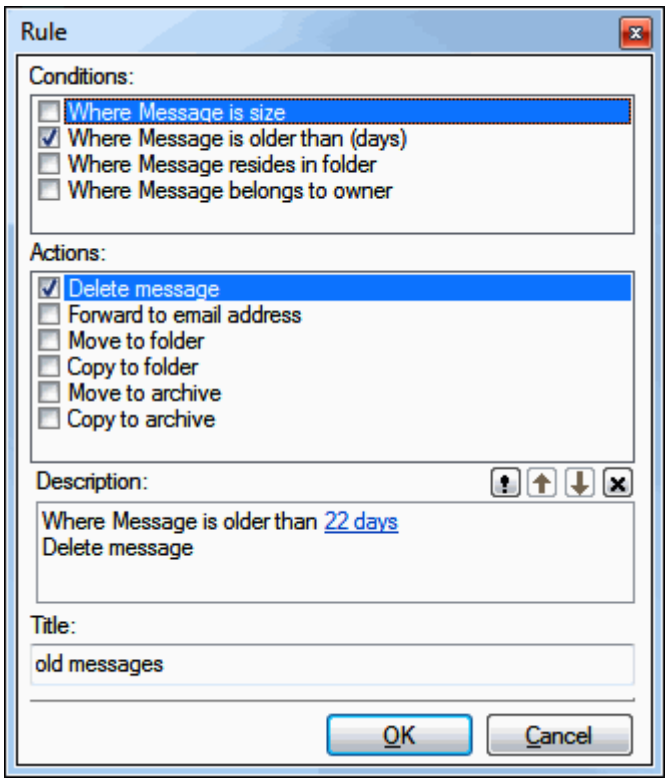
*NOTE: Auto-clean logs can be found under the **Status – Logs** node. Select the **Mail Flow** item from the **Log** list. As auto-clean is performed at midnight, you can use time as a filter criteria (**From – To**).*

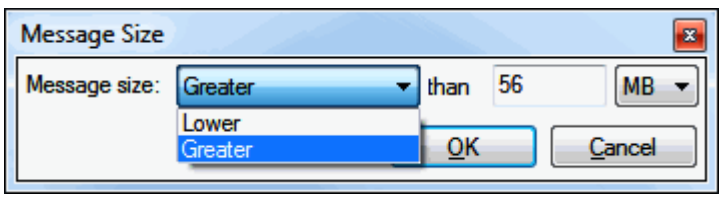


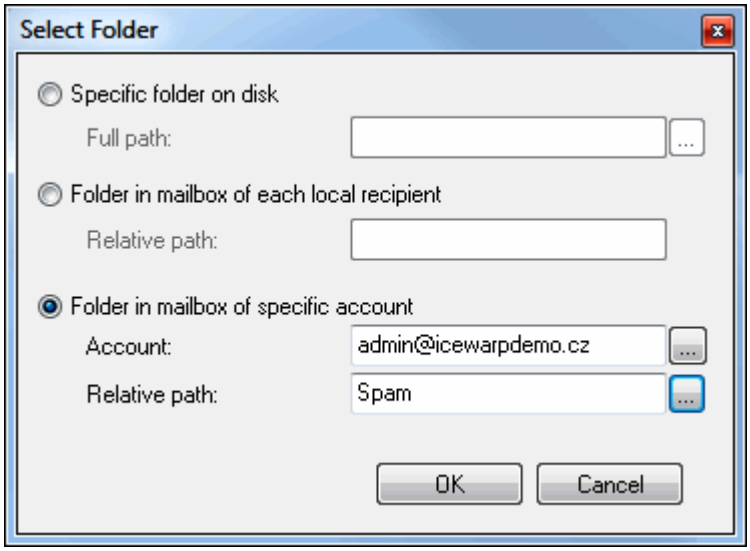
Field	Description
Active check box	Tick the box next to the rule to activate this rule.
Add	Click the button to add a new rule. The **Rule** dialog opens.
Edit	Click the button to modify an existing rule. The **Rule** dialog opens.
Copy	Select a rule and click the button to copy this rule. It is suitable when you want to perform some minor changes only. The **Rule** dialog opens.
Delete	Click the button to delete the selected rule.
Up/down arrows	Click the appropriate arrow to move the selected rule up or down.
Export	Click the button to open the **Export** dialog. Tick the rule(s) you want to export and click the ***Export Selected Filters Now*** button. Usual **Save As** dialog opens. Browse for a location where you want to save a ***xml*** file with this rule.

	
Import	Click the button to open the **Open** dialog. Browse for a ***xml*** file with the rule you want to add to the list.
Select/deselect all	Use this feature to ease operations with more rules.
Run Now	Click the button to run either all rules or only a selected one immediately.

Rule dialog



Condition	**Description**
Where Message is size	Select this condition to define a message size. Click the ***>0kB*** link in the **Description** field and in the **Message Size** dialog, define the wished size.  When this condition is met, defined actions are applied to all system users.

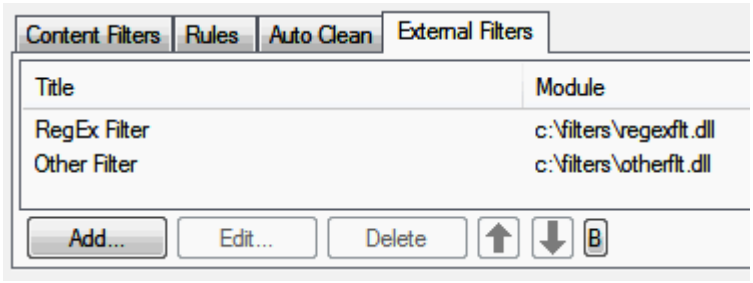
Where Message is older than (days)	Select this condition to define a message age. Click the ***days*** link in the **Description** field and in the **Message Age** dialog, define the wished time in days. When this condition is met, defined actions are applied to all system users.
Where Message resides in folder	Select this condition if you want to perform actions with messages in specific folders. Click the ***folder*** link in the **Description** field to open the **Select Folder** dialog.  Select one of the options: ▪ ***Specific folder on the disk*** – not too appropriate here (this dialog is shared). ▪ ***Folder in mailbox of each recipient*** – for example Trash. ▪ ***Folder in mailbox of specific account*** – use the "..." button to select the appropriate account and another "..." button to select the appropriate folder. If the fields are not filled in, defined actions are applied to all system users. It is useful to combine this condition with other ones.
Where Message belongs to owner	Select this condition to define a message owner (the account where the message resides). Click the ***owner*** link in the **Description** field to open the **Message Owner** dialog. Select the appropriate owner using the "..." button. *NOTE: Domain can be used too.*
Action	**Description**
Delete message	Select this action to have the messages that match the condition deleted.
Forward to email address	Select this action to have the messages that match the condition forwarded to the defined address. Click the ***email address*** link in the **Description** field to open the **Email Address** dialog. Click the "..." button here to select the appropriate address.
Move to folder	Select this action to have the messages that match the condition moved to the defined folder. Click the ***folder*** link in the **Description** field to open the **Select Folder** dialog (see the figure above). Select one of the options: ▪ ***Specific folder on the disk*** – use the "..." button to select the appropriate folder on the server disk. ▪ ***Folder in mailbox of each recipient*** – for example Trash. ▪ ***Folder in mailbox of specific account*** – use the "..." button to select the appropriate

	account and another "..." button to select the appropriate folder.
Copy to folder	Select this action to have the messages that match the condition copied to the defined folder. For other details, see the ***Move to folder*** option.
Move to archive	Select this action to have the messages that match the condition moved to the archive. *NOTE: It performs the archiving based on the date in the Date: header and based on the owner of the email. Important settings of the general archive are preserved (Archive to directory, Directory trailer path, Forward archived messages to). On the other hand Active, Do not archive spam, Do not archive RSS, Archive Messages: are ignored – i.e. archiving is performed also if those settings would prohibit it.*
Copy to archive	Select this action to have the messages that match the condition copied to the archive. See the NOTE within the *Move to archive* feature description. *NOTE: Use the Copy to archive action with special care. It should be used only in "manual" processing of autoclean rules – i.e. when you want to run them only once. Otherwise it copies the matching mail to the archive each time when the rule is executed.*
Title	Enter a short descriptive name. In the case the field is left blank, this name is generated automatically.

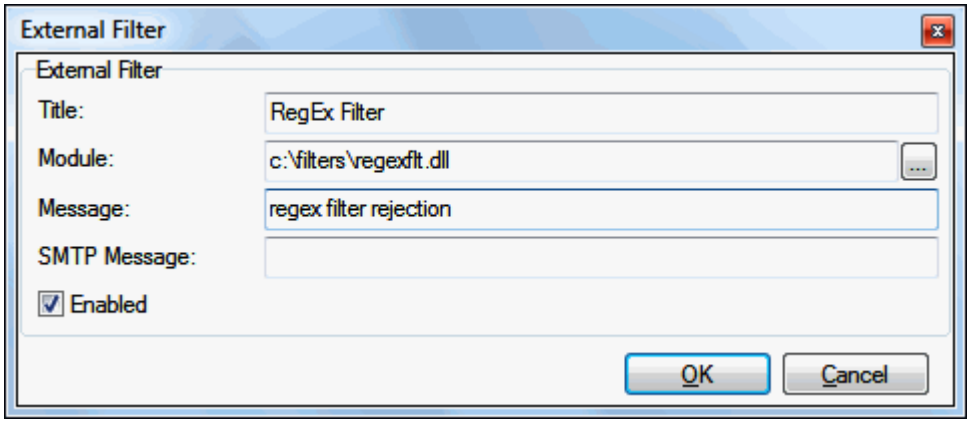
External Filters

External filters are DLL modules that are loaded in memory and invoked each time a message is received.

The filter should return a result if it wants IceWarp Server to mark the message in some way.



Button	**Description**
Add	Click the button to create a new external filter. The **External Filter** dialog opens. See bellow.
Edit	Select an existing external filter and click the button to edit this filter. The **External Filter** dialog opens. See bellow.
Delete	Select an existing external filter and click the button to remove this filter.
Arrows	Select an existing external filter and use the arrows to move this filter up or down in the list i. e. to change the order in which the filters are applied (top first).
"B" button	Click the button to specify senders, recipients, domains and IP address ranges that will not have these filters applied. For more details about bypassing filters, refer to the **Bypassing Rules/Filters** section.



Field	Description
Title	Fill in some descriptive text.
Module	Browse for the DLL library which is to be called to evaluate messages.
Message	If no SMTP message is defined, this one is used plus it has pre-defined prefix.
SMTP Message	This message is used in SMTP connections as a response when the message was caught by this filter.
Enabled	Activates/deactivates the filter.

Archive

The archiving capabilities are very rich and allow the administrator to bring archiving features directly to end users via IMAP. SMS messages are also archived automatically.

Technically all archived emails are always stored as **.imap** files which makes it possible to link the whole archive with a public folder. They also contain the ***Seen*** flag so they appear as read/unread in email clients.

New ***Directory trailer path*** option works as an appendix to directory path so you can create e. g. this: ***C:\Archive\domain.com\john\Sent\2014-Jun***.

It is also possible to store all messages in the root of the user's folder or keep them in folders (**Inbox**, **Sent**).

Native integration with IMAP allows all users of WebClient and any other IMAP client to see a new **Archive** folder by default (or however named by the administrator). Users can then browse through their archive, but access to the archive folder is read-only so they cannot delete, flag or change the read status of messages.

Examples of time-based archive structure:

<Archive>\Inbox\2014-04

<Archive>\Sent\2014-05

or simply

<Archive>\2014

with all messages included.

Archivist User Role

You have large variety of possibilities by using public folders in combination with archive:

You can grant persons access to:

- the whole server archive
- the archive folder(s) of one or more domains
- archive folders of the selected users or groups.

To grant access, do the following:

1. Create a group (e. g. *archive@icewarpdemo.com*) with a public folder (**Management – <domain> – Groups**). In the file system, go to the folder which belongs to this group and create a symlink (junction in Windows) to the directory with the archive.

   *NOTE: It is necessary to remove the **<install_dir>/mail/<domain>/<group_folder>** folder before the symlink/junction creation.*

   Junction.exe example:

   junction.exe <junction directory> <junction target>

   junction.exe c:\Program files\Icewarp\mail\domain.com\user c:\Program files\Icewarp\archive

   (For more info about symlinks, refer to this website:

   http://technet.microsoft.com/en-us/sysinternals/bb896768.aspx.

   For Linux it is: ***ln -s [existing_folder] [symlink]*** (symlink folder must not exist).

   E.g. ***ln -s /opt/icewarp/archive /opt/icewarp/mail/domain.com/user***.)

   After the junction link is created, refresh the directory cache to see available permissions for the *Archive* group.

2. Within the **<group> – Group** tab **– Permissions – Folders** dialog, grant archivist(s) access to the appropriate archive folder (which appears in the folder structure).

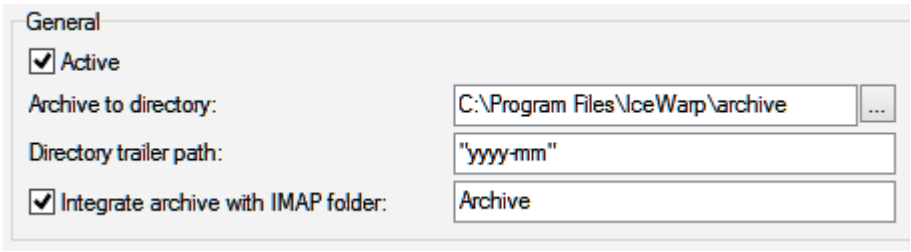
   NOTE: It is not necessary the archivist to be a member of the group.

Compatibility

Compatibility with the old archive is preserved. However **.tmp** (POP3) files will not be available in the new IMAP-based archive. Only newly received messages will be properly converted. Old structures created in the mail folders will be visible but messages will have not the ***Seen*** flag so it will appear they have not been read.

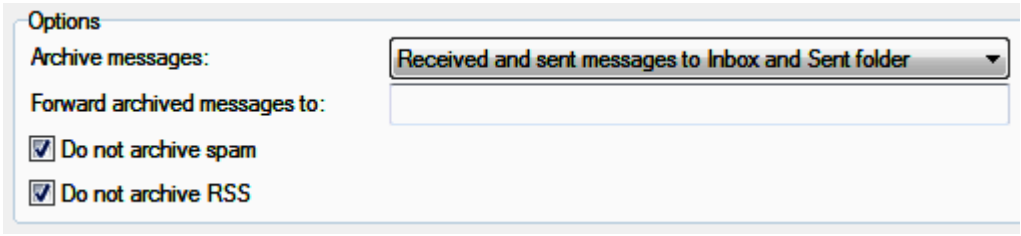
Mail Archive

The **Archive** sub-node allows you to specify mail archive and pruning options:

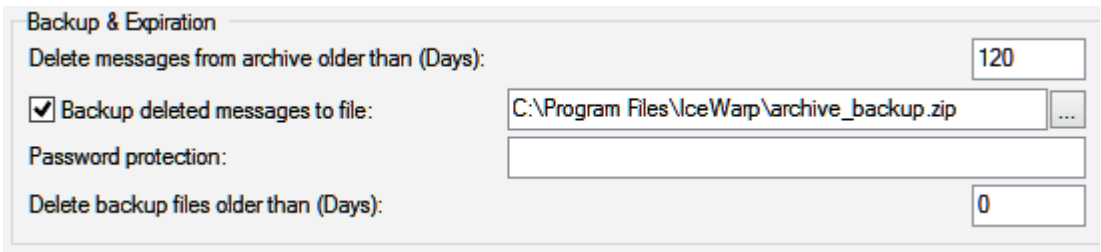


Field	Description
Active	Check this option to activate mail archiving.
Archive to directory	Select or fill in the path to the directory where mails should be archived. *NOTE: Be careful when specifying a mail archive path. It has to be a fast drive, preferable directly attached to the server or high end storage such as iSCSI/SAN. Pointing to a slow path such as SMB on the network can affect server performance as backups get written to disk during SMTP processing. Another alternative, if backing up to a drive via UNC is really necessary, is to enable MDA, since then IceWarp Server will first receive the message and afterwords archive it. For more information about MDA, refer to the **General – Advanced** chapter.* *NOTE: The archive directory path must be specified in UNC format. Do not use drive mapping letters.*
Directory trailer path	Directory that precedes the user's ***inbox/sent*** items folder.

	This field can either: ▪ be left blank ▪ or contain the date time variables to have folders (and mails) sorted chronologically.
Integrate archive with IMAP folder	If ticked, the **Archive** folder will appear in the IMAP folder list and users will have access to their received/sent messages in read-only mode. This folder automatically appears in WebClient and has to be signed up to in other email clients.



Field	Description
Archive messages	Select from four options: **Received and sent messages to Inbox and Sent folder** Archives both incoming and outgoing messages into separate folders. **Received messages to Inbox folder** Archives incoming messages into the appropriate folder. **Received and sent messages to root folder** Archives all messages into the root folder. **Received messages to root folder** Archives incoming messages into the root folder. **Deleted messages** Archives deleted messages. *NOTE: Root folder here means the root of the user's mailbox – so there will not be **Inbox/Sent** folders.*
Forward archived messages to	Fill in an email address where you want to have all messages forwarded to. You can enter more addresses separated by semicolons. This can be a way how to backup your (server/domain/user) email correspondence. It can be also any outside address.
Do not archive spam	Tick this box and messages which are marked as spam will be excluded from the archive process.
Do not archive RSS	Tick this box to have RSS feeds excluded from archive process.



Field	Description
Delete messages from	Enter a number here and emails older than this number of days will be deleted.

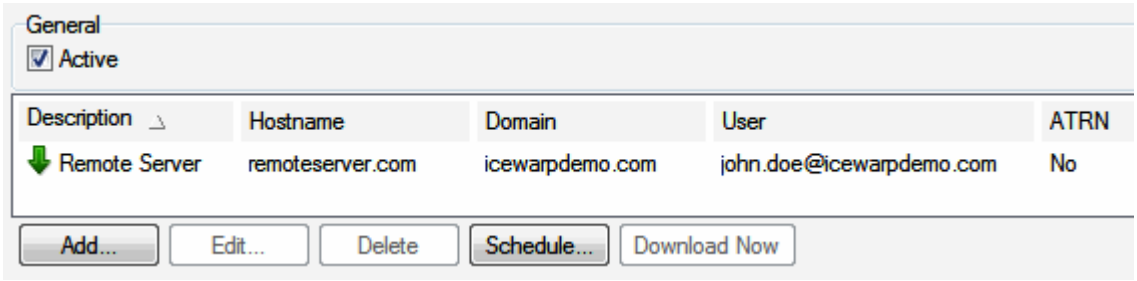
archive older than (Days)	
Backup deleted messages to file	Check this option and enter a directory name to have deleted emails backed up to the specified file. The file name can contain "yyyymmdd", which will create a separate file for each day. *These backup files are in standard ZIP format and files are stored with relative path information, so to restore a particular file you should extract the contents to your top-level mail directory with the extract option to "use folder names".*
Password protection	Optionally specify a password here to have the backup file password protected.
Delete Backup files older than (Days)	Enter a number here and backups older than this number of days will be deleted. Zero means that backup files are not deleted – they are kept forever. *NOTE: This function deletes all files with the same extension based on the system file time stamp. It is **highly** recommended that, if you use this function, you specify a directory that **only** contains these backup files.*

ETRN Download

Short for Extended Turn, ETRN is an extension to the SMTP mail delivery protocol that allows an SMTP server to request from another SMTP server any email messages it has for a specific domain. ETRN is typically used by a mail server that does not have a dedicated connection to the Internet.

The ETRN download node lets you to define ETRN or ATRN (Authenticated TURN) client requests to remote mail servers, allowing you to have IceWarp Server pick up messages held on other servers.

Multiple downloads can be defined and message collection(s) can be scheduled.



Button	Description
Active	Tick the box to enable this feature.
Add	Click the button to add a download definition. The **ETRN/ATRN Item** dialog opens. See bellow.
Edit	Select a download definition and click the button to edit this definition. The **ETRN/ATRN Item** dialog opens. See bellow.
Delete	Select a download definition and click the button to remove this definition.
Schedule	Click the button to define a schedule for downloads.
Download Now	Click the button to start a manual connection and collection of mail.



Field	**Description**
Description	A description of this download so you can identify it.
Hostname	Specifies the full hostname or IP address of the remote mail server including the port if required.
Domain	If this is an ETRN connection, specify the domain name here.
User	If this is an ETRN connection, specify the user name for authentication here.
Password	If this is an ETRN connection, specify the account password here for authentication.
ATRN	The default mode for collecting messages is ETRN. If the server you are collecting from requires ATRN (Authenticated Turn), check this box and specify the ***Domain***, ***User*** and ***Password*** to be used for authentication as described above.

SMTP Errors

This chapter lists possible SMTP errors. Text strings are self-explanatory.

For additional information on 5xx errors, refer to the **Status Node – Logs – Interpretation of 5xx Errors in IceWarp SMTP** chapter, or to this page:

http://esupport.icewarp.com/index.php?/default_import/Knowledgebase/Article/View/12/4/interpretation-of-5xx-errors-in-icewarp-smtp

stSMTPReadyToTLS = '220 ' + stEnhancedStatusCode200 + cSpace + stReadyToTLS;

stSMTPReturnDisconnected = '221 ' + stEnhancedStatusCode200 + ' %s closing connection';

stSMTPAuthOk = '235 ' + stEnhancedStatusCode200 + ' Authentication successful';

stSMTPNoopOK = '250 ' + stEnhancedStatusCode200 + ' OK';

stSMTPSenderOK = '250 ' + stEnhancedStatusCode210 + ' %s... Sender ok';

stSMTPRecipientOK = '250 ' + stEnhancedStatusCode215 + ' %s... %s';

stSMTPVrfyOk = '250 ' + stEnhancedStatusCode210 + ' %s <%s@%s>';

stSMTPExpnOk = '250-' + stEnhancedStatusCode210 + ' %s <%s@%s>';

stSMTPRsetOk = '250 ' + stEnhancedStatusCode200 + ' Reset state';

stSMTPOkReverse = '250 ' + stEnhancedStatusCode200 + ' OK now reversing connection';

stSMTPReceivedMessage = '250 ' + stEnhancedStatusCode260 + ' %s bytes received in %s; Message id %s accepted for delivery';

stSMTPBDATReceivedMessage = '250 ' + stEnhancedStatusCode260 + ' %s bytes received in %s';

stSMTPQueryStarted = '250 ' + stEnhancedStatusCode200 + ' Query for node %s started';

stSMTPTooBadCommandsSMTP = '421 ' + stEnhancedStatusCode400 + cSpace + stTooBadCommands;

stSMTPTarpitSMTP = '421 ' + stEnhancedStatusCode471 + stTarpitted;

stSMTPNoMail = '453 ' + stEnhancedStatusCode400 + ' You have no mail';

stSMTPATRNRefused = '450 ' + stEnhancedStatusCode400 + ' ATRN request refused';

stSMTPLocalError = '451 ' + stEnhancedStatusCode435 + ' Requested action aborted: local error processing';

stSMTPQuarantineError = '451 ' + stEnhancedStatusCode435 + ' Requested action aborted: quarantine error processing';

stSMTPTryAgainLater = '451 ' + stEnhancedStatusCode471 + ' Please try again later';

stSMTPGreyListing = '451 ' + stEnhancedStatusCode471 + cSpace;

stSMTPETRNIncorrectPassword = '459 ' + stEnhancedStatusCode459 + ' Node %s not allowed: Incorrect password';

stSMTPETRNNotFound = '459 ' + stEnhancedStatusCode459 + ' Node %s not allowed: Node not found';

stSMTPETRNNotAllowed = '459 ' + stEnhancedStatusCode459 + ' Node %s not allowed: ETRN is not available for this node';

stSMTPCommandUnrecognized = '500 ' + stEnhancedStatusCode551 + ' Command unrecognized: "%s"';

stSMTPDomainRequired = '501 ' + stEnhancedStatusCode552 + ' %s... Domain name required';

stSMTPUnbalanced = '501 ' + stEnhancedStatusCode552 + ' %s... Unbalanced "%s"';

stSMTPSyntaxError = '501 ' + stEnhancedStatusCode554 + ' Syntax error in parameters scanning';

stSMTPRequireDomain = '501 ' + stEnhancedStatusCode551 + ' HELO/EHLO requires domain address';

stSMTPAuthCancelled = '501 ' + stEnhancedStatusCode500 + ' Authentication cancelled';

stSMTPAuthFailed = '535 ' + stEnhancedStatusCode578 + ' Authentication credentials invalid';

stSMTPNotAllowedSender = '501 ' + stEnhancedStatusCode571 + ' %s... %s';

stSMTPTmpNotAllowedSender = '421 ' + stEnhancedStatusCode471 + ' %s... %s';

stSMTPSorryNoSupport = '502 ' + stEnhancedStatusCode551 + ' Sorry, we do not support this operation';

```
stSMTPSequenceReturn = '503 ' + stEnhancedStatusCode551 + ' Incorrect command sequence';
stSMTPAlreadyAuth = '503 ' + stEnhancedStatusCode551 + ' Authentication already done';
stSMTPGreetingError = '503 ' + stEnhancedStatusCode551 + ' HELO/EHLO command required';
stSMTPInvalidAuth = '504 ' + stEnhancedStatusCode576 + ' Unrecognized authentication type';
stSMTPHeloAgain = '503 ' + stEnhancedStatusCode551 + ' HELO/EHLO already specified';
stSMTPAuthRequired = '530 ' + stEnhancedStatusCode571 + ' Authentication required [AUTH]';
stSMTPWeDoNotRelay = '550 ' + stEnhancedStatusCode571 + ' %s' + stWeDoNotRelay + '%s';
stSMTPAccountLimits = '550 ' + stEnhancedStatusCode571 + ' %s' + stWeDoNotRelay + '%s, account limits apply';
stSMTPOnlyDomainUser = '550 ' + stEnhancedStatusCode571 + ' You have rights to send mail to local domains only';
stSMTPUnknownUserLocal = '550 ' + stEnhancedStatusCode511 + ' %s ' + stUnknownUserLocal;
stSMTPRectUser = '550 ' + stEnhancedStatusCode511 + ' %s User unknown; rejecting';
stSMTPInvalidRemoteAddr = '550 ' + stEnhancedStatusCode511 + ' %s User remote address unknown; rejecting';
stSMTPNoReplyRec = '550 ' + stEnhancedStatusCode511 + ' No replies to %s are accepted; rejecting';
stSMTPInvalidForwardAddr = '550 ' + stEnhancedStatusCode511 + ' User %s has invalid forward set and no mailbox; rejecting';
stSMTPNotAllowedTo = '550 ' + stEnhancedStatusCode571 + ' %s Access to %s not allowed';
stSMTPSRSNotAllowed = '550 ' + stEnhancedStatusCode571 + ' %s Access to %s not allowed [SPF-SRS]';
stSMTPNotAllowedToByRules = '550 ' + stEnhancedStatusCode571 + ' %s Access to %s not allowed by rules';
stSMTPNotAllowedToByRule = '550 ' + stEnhancedStatusCode571 + ' %s Access to %s not allowed by rule %s';
stSMTPPermissionDenied = '550 ' + stEnhancedStatusCode571 + cSpace + stPermissionDenied;
stSMTPSessionPermissionDenied = '554 ' + stEnhancedStatusCode571 + cSpace + stPermissionDenied;
stSMTPUserNotLocal = '551 ' + stEnhancedStatusCode511 + ' No such user found';
stSMTPMailingListNotLocal = '551 ' + stEnhancedStatusCode511 + ' No such mailing list found';
stSMTPTooRecipients = '452 ' + stEnhancedStatusCode453 + ' Too many recipients';
stSMTPTooData = '554 ' + stEnhancedStatusCode534 + ' Message size exceeds fixed maximum message size';
stSMTPMessageSizeExceedFragment = AnsiString('552 message size exceeds');
stSMTPVirusFound = '554 ' + stEnhancedStatusCode571 + ' Message cannot be accepted, virus found %s';
stSMTPFilterContent = '554 ' + stEnhancedStatusCode571 + ' Message cannot be accepted, content filter rejection';
stSMTPSpamFilterContent = '554 ' + stEnhancedStatusCode571 + ' Message cannot be accepted, rules rejection';
stSMTPSpamEngineContent = '554 ' + stEnhancedStatusCode571 + ' Message cannot be accepted, spam rejection';
stSMTPFilterDeleted = AnsiString('Message deleted by %s: %s');
stSMTPMessageNotDelivered = AnsiString('Message for %s not delivered. Reasons:%s, Action:%s');
stFilterReject = AnsiString('Message cannot be accepted, filter rejection');
stSMTPFilterReject = '554 ' + stEnhancedStatusCode571;
// According to http://tools.ietf.org/html/rfc3463
{
   X.2.2 Mailbox full
         The mailbox is full because the user has exceeded a per-mailbox
         administrative quota or physical capacity. The general
         semantics implies that the recipient can delete messages to
         make more space available. This code should be used as a
         persistent transient failure.
}
```

stSMTPMailboxSize = '452 ' + stEnhancedStatusCode422 + ' %s Mailbox has exceeded the limit';

stSMTPPermanentMailboxSize = '552 ' + stEnhancedStatusCode522 + ' %s Mailbox has exceeded the limit';

stSMTPInboxCount = '452 ' + stEnhancedStatusCode422 + ' %s Inbox has exceeded the limit of messages';

stSMTPPermanentFailure554 = '554';

stPOPFilterReject = AnsiString('Warning: message cannot be accepted, message rejected');

stSMTPLocalDelError = AnsiString('Local delivery error, check your settings, disk space and directory permissions - recipients: ');