IceWarp Unified Communications

Status Node Reference

Version 11.3

Published on 2/3/2015

Contents

Status

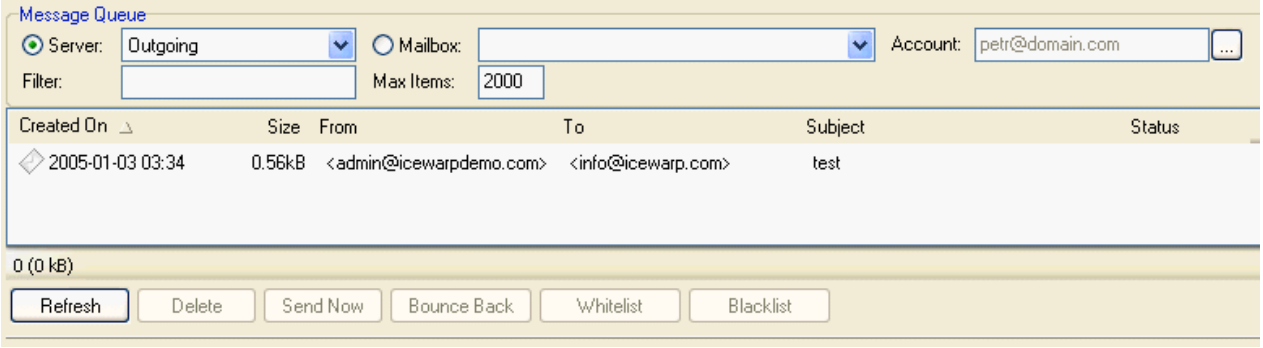
The **Status** node allows access to various queues, logs and statistics areas of IceWarp Server.

This node can be extremely helpful in diagnosing problems, seeing what has happened historically, and seeing what is happening right now.

Using these records can increase your understanding of how your IceWarp Server is being used.

Message Queue

The **Message Queue** node allows you to view both ***Incoming*** and ***Outgoing*** queues or you can show the messages from user's mailbox.



You can choose either user's regular inbox or his/her spam folder. It lists all the messages from chosen destination and moreover, you can double-click the message in the list and it opens the message in a text editor.

Field	**Description**
Server	Select the type of the server queues: ***Outgoing***, ***Incoming***, ***MDA***, ***SMS***, ***Retry***. If the ***Outgoing*** item is selected, the *Status* column displays the priority of the queue where the message is located.
Mailbox	Select the appropriate folder of the selected account.
Account	Use the "***...***" button to select the appropriate account of which you want to view queues.
Filter	You can filter message queue using expressions from the ***From***, ***To*** and ***Subject*** fields.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list will be to populate.* *NOTE: There is maximum of items set to 2000. Loading more items could break up your server.*

Button	**Description**
Refresh	Refreshes the queue or mailbox so you see current list of messages.
Delete	Deletes chosen message – you can use ***Ctrl*** and ***Shift*** keys to choose more messages.
Send Now	Forces an attempt to deliver the messages.
Bounce Back	Finishes the attempts to deliver the message in queue and returns the messages back to sender as undeliverable.
Whitelist	Click the button to whitelist the sender of the selected message.
Blacklist	Click the button to blacklist the sender of the selected message.

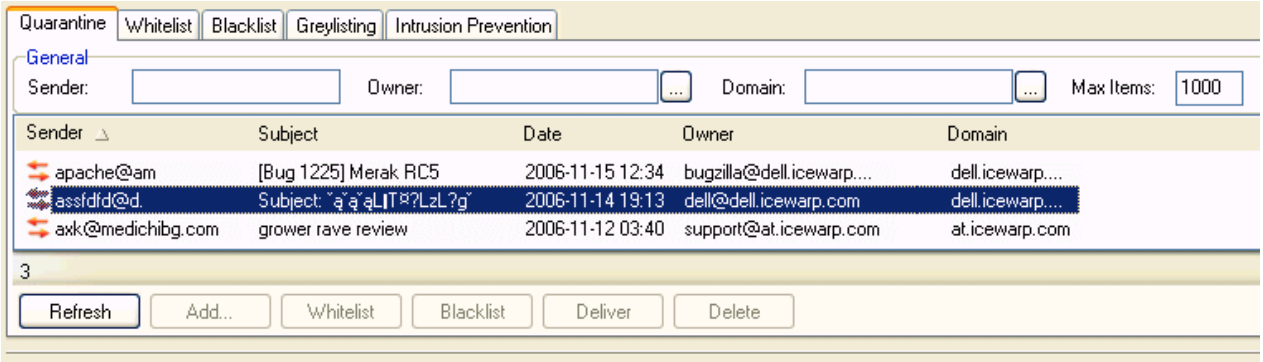
Spam Queues

The **Spam Queues** node allows you to administer spam queues.

Quarantine

Selecting the **Quarantine** tab presents you with a list of messages awaiting action.

For each message in the queue, you are shown the ***Sender***, ***Subject***, ***Date/Time*** sent, ***Owner*** (recipient) and recipient ***Domain***:

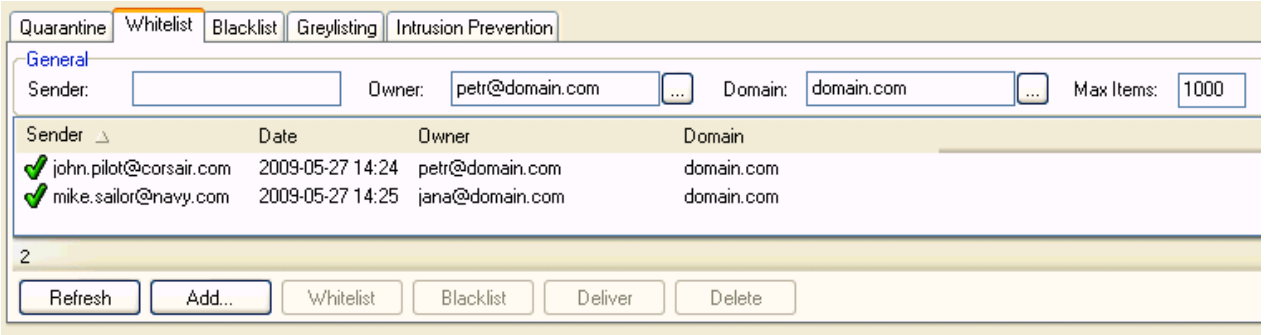


Field	Description
Sender	Specify a sender address here to show only messages from that sender. Click the ***Refresh*** button after entering the information.
Owner	Specify an owner's (recipient's) address here to only show messages destined for a particular address. Click the ***Refresh*** button after entering the information.
Domain	Specify a domain name here to show only messages from a particular domain. Click the ***Refresh*** button after entering the information.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list is populated.*
Number between the list and buttons	This figure indicates number of the list items. (In this case, it is 3.)
Refresh	Click this button to refresh the list, taking into account any filters you have entered.
Add	Non-functional here.
Whitelist	Click this button to have the senders of selected messages added to the **Whitelist**.
Blacklist	Click this button to have the senders of selected messages added to the **Blacklist**.
Deliver	Click this button to have selected messages delivered without having their sender(s) added to **Whitelist** or **Blacklist**.
Delete	Click this button to have selected messages deleted without any further action.

Whitelist

Selecting the **Whitelist** tab presents you with a list of whitelisted senders.

For each message in the queue, you are shown the ***Sender***, ***Date/Time*** added, ***Owner*** (recipient) and recipient's ***Domain***:



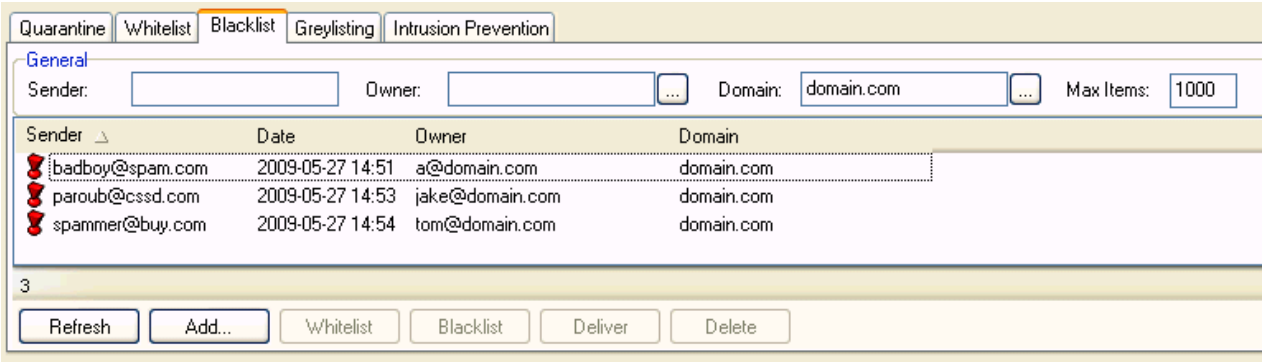
Field	**Description**
Sender	Specify a sender's address here to show only messages from that sender. Click the ***Refresh*** button after entering the information.
Owner	Specify an owner's (recipient's) address here to show only messages destined for a particular address. Click the ***Refresh*** button after entering the information.
Domain	Specify a domain name here to show only messages for a particular domain. Click the ***Refresh*** button after entering the information.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list is populated.*
Refresh	Click this button to refresh the list, taking into account any filters you have entered.
Add	Click this button to add a user to **Whitelist**. The **Whitelist** dialog will open, enter the ***Sender*** and ***Owner*** details:  ***Sender*** – the address to be whitelisted. *NOTE: The email **From** header is to be used here.* ***Owner*** – the owner of the rule. You can specify: ▪ a user address to whitelist the sender for a single user ▪ a domain to whitelist the sender for a domain ▪ an asterisk to whitelist the sender for all domains on the server Use the '...' button to open the standard **Select Item** dialog.

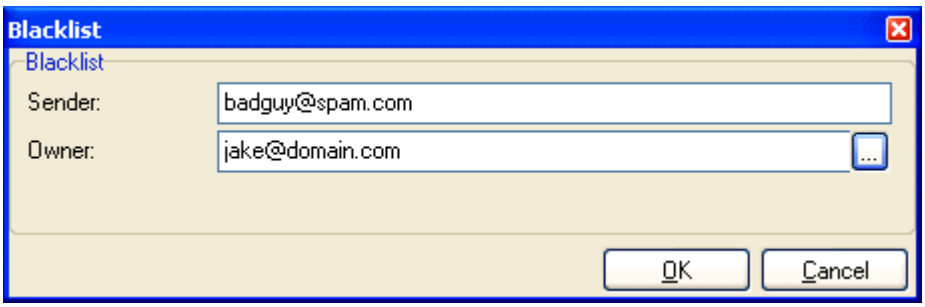
Whitelist	Click this button to have the selected sender(s) moved to **Whitelist** – useless here.
Blacklist	Click this button to have the selected sender(s) moved to **Blacklist**.
Deliver	Non-functional button here.
Delete	Click this button to have selected sender(s) deleted from **Whitelist**.

BlackList

Selecting the **Blacklist** tab presents you with a list of blacklisted senders.

For each message in the queue, you are shown the ***Sender***, ***Date/Time*** added, ***Owner*** (recipient) and recipient's ***Domain***:



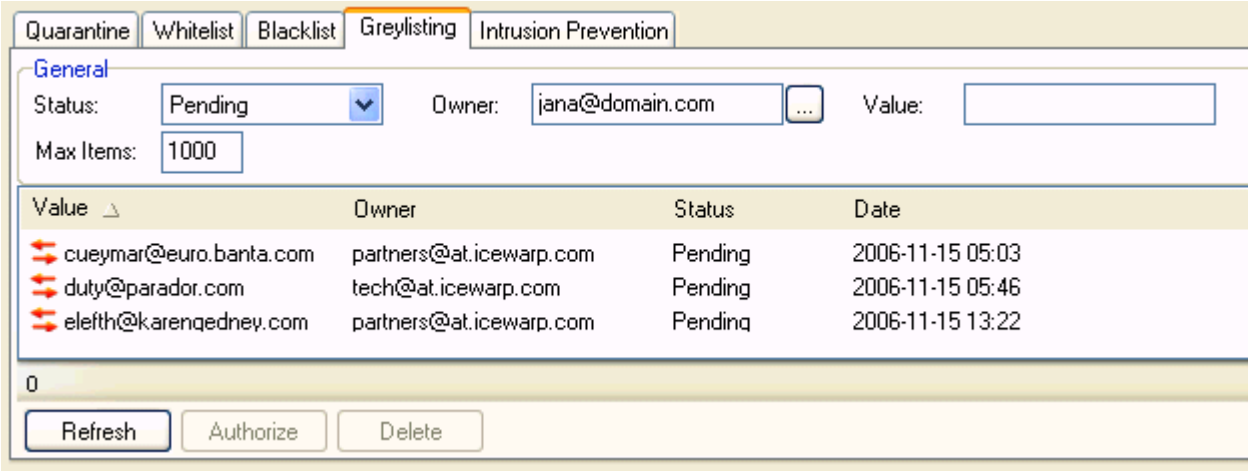
Field	**Description**
Sender	Specify a sender address here to show only messages from that sender. Click the ***Refresh*** button after entering the information.
Owner	Specify an owner's (recipient's) address here to show only messages destined for a particular address. Click the ***Refresh*** button after entering the information.
Domain	Specify a domain name here to show only messages for a particular domain. Click the ***Refresh*** button after entering the information.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list is populated.*
Refresh	Click this button to refresh the list, taking into account any filters you have entered.
Add	Click this button to add a user to the blacklist. The **Blacklist** dialog opens, specify the ***Sender*** and ***Owner*** information here:  ***Sender*** – the address to be blacklisted.

	*NOTE: The email **From** header is to be used here.* ***Owner*** – the owner of the rule. You can specify: ▪ a user address to blacklist the sender for a single user ▪ a domain to blacklist the sender for a domain ▪ an asterisk to blacklist the sender for all domains on the server. Use the '...' button to open the standard **SelectItem** dialog.
Whitelist	Click this button to have the selected senders moved to **Whitelist**.
Blacklist	Click this button to have the selected senders moved to **Blacklist** – useless here.
Deliver	Non-functional button here.
Delete	Click this button to have the selected sender deleted from **Blacklist**.

Greylisting

Selecting the **Greylisting** tab presents you with a list of connections that have been made to IceWarp Server, and their greylisting ***Status*** – ***Pending***, ***Authorized***, ***Expired***.

For each message in the queue, you are shown the ***Sender***, ***Owner*** (recipient), ***Status*** and ***Date/Time*** of first connection attempt:

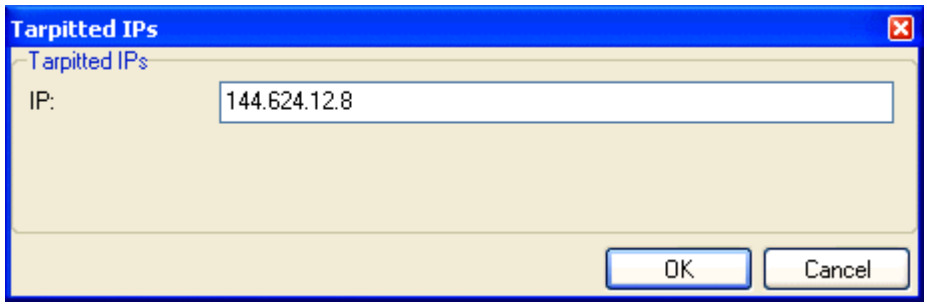


Field	**Description**
Status	Select status from the dropdown to show only entries with that status. Click the ***Refresh*** button after entering the information.
Owner	Specify owner's (recipient's) address here to show only messages destined for a particular address. Click the ***Refresh*** button after entering the information.
Value	Specify the sender's address here to show only messages from that sender. Click the ***Refresh*** button after entering the information.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list is populated.*
Refresh	Click this button to refresh the list, taking into account any filters you have entered.

Authorize	Click this button to authorize the selected connection. *NOTE: Clicking the button does not mean the message is delivered. It means the message will be accepted WHEN the remote server will try to send it again (if the remote server will do so).*
Delete	Click this button to delete the selected connection from the queue.

Intrusion Prevention

Selecting the **Intrusion Prevention** tab presents you with a list of ***IP*** addresses that have been blocked by the Intrusion Prevention function, along with the ***Expires*** (date/time) that the block will expire.

Field	Description
Refresh	Click this button to refresh the list.
Add	Click this button to add an IP address to the list. The **Tarpitted IPs** dialog is shown. Specify the IP address here. CIDR notation/ranges can be used.  *NOTE: The expiration time will be calculated according to your Anti-Spam settings.*
Remove	Click this button to remove the selected IP address(es).
Remove All Expired	Click this button to have all expired IP addresses deleted from the queue.
Remove All	Click this button to have all IP addresses removed from the queue.

Intrusion Prevention Reason Codes

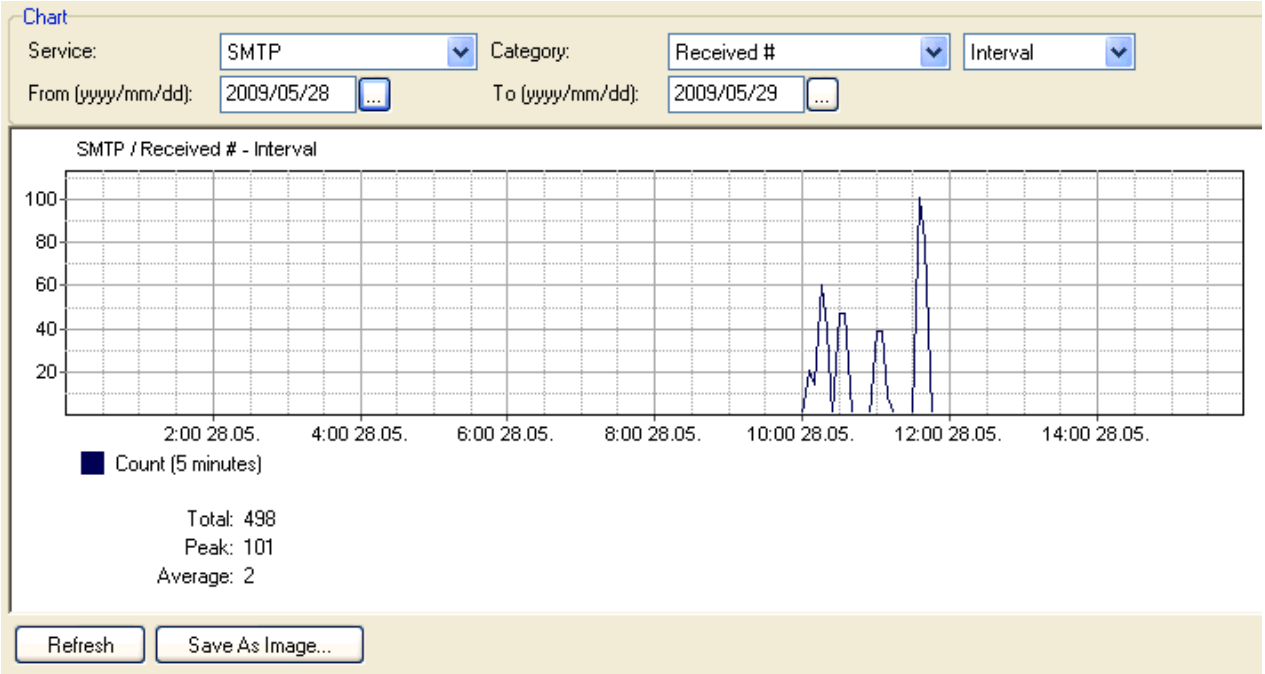
Reason Code	Explanation
C	Tarpitting invoked via Content Filters
I	IP blocked for exceeding connections in one minute
M	IP blocked for delivering oversized message
R	IP blocked for exceeding RSET command count
D	IP blocked for being listed on DNSBL

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 console
L	IP blocked for too many failed login attempts

Traffic Charts

On this tab you can see charts of traffic on your server. You can choose not only particular services to be shown but different types of messages can be shown as well – e.g. ***Received*** or ***Sent*** etc. Of course, you can adjust the time period to be shown so you can see charts per day, per week or per month.

Traffic charts data is stored within the **<install_dir>/status** folder.

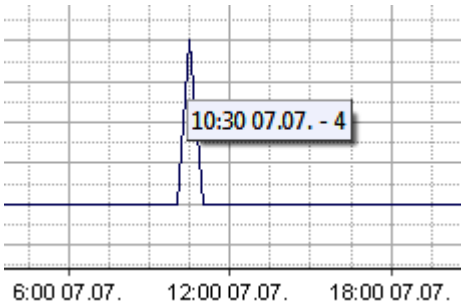


Field	Description
Service	Select the service you wish to display.
Category	Select the category of the shown data. E.g.: ***SMTP – Spam Refused #***.
<Interval>	Select the interval for data revealing. (1 Day, 1 Week, 1 Month, specified interval)
From/To	Available only when ***Interval*** chosen.
Refresh	Click this button to reveal relevant data.
Save As Image	Click the button to save data currently shown.

*NOTE: You can zoom in into a selected area. Just mark this (rectangle) area using the left mouse button. To zoom out, click the **Refresh** button.*

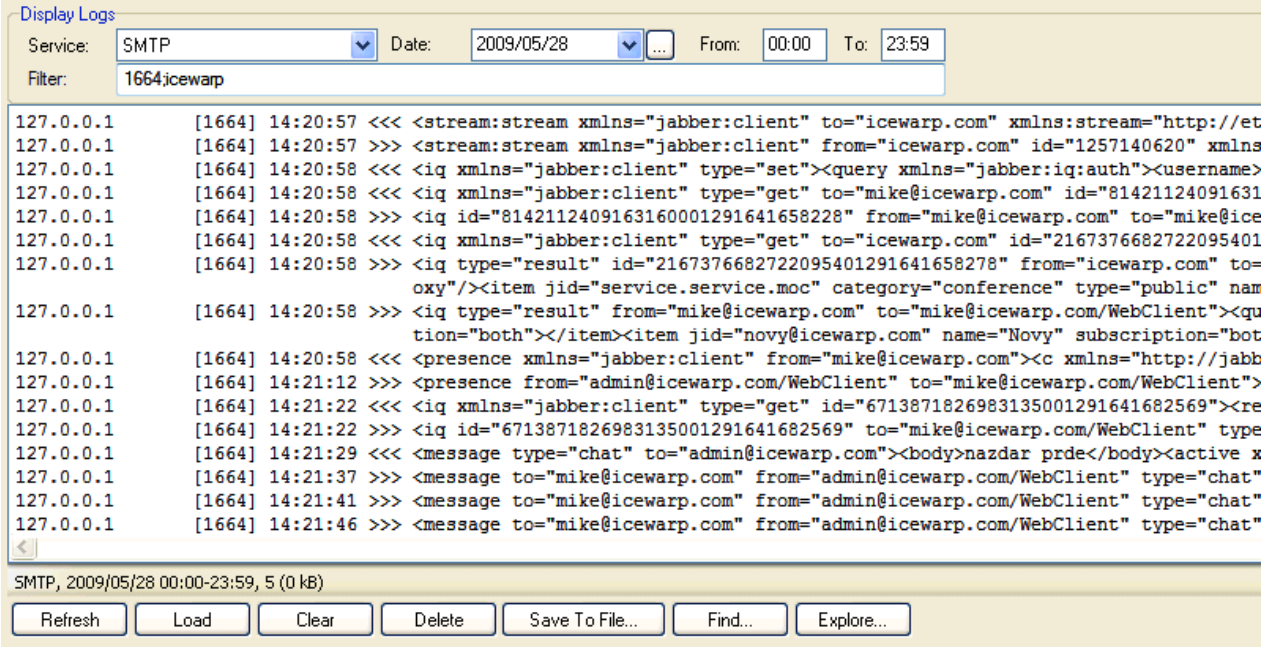
Tooltip

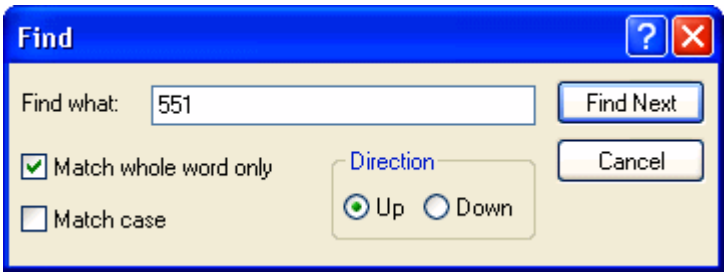
When hovering over a traffic chart, a tooltip is shown. It displays the current graph value at the place where a cursor is placed.


10:30 07.07. - 4
6:00 07.07.
12:00 07.07.
18:00 07.07.

Logs

The **Logs** tab allows you to show any part of server logs. You can choose the type of logs (even ***Error*** logs and ***Instant Messaging Archive*** can be shown), the ***Date*** and exact period of that date to be shown.



Field	Description
Service	Select the service that you want to view logs for.
Date	Select the day.
From/To	Specify time period. Usage of the ***hh:mm:ss*** format is possible.
Filter	Enter searched string. It can be any part of a log – IP, time, thread ID, user, etc. Multiple filter can be used – separate strings by ";" (semicolon) that works as a boolean AND. Click the ***Load*** button to filter.
Refresh	Click the button to reveal fresh data.
Load	Click the button to show logs for selected service, day, etc.
Clear	Click the button to clear log display.
Delete	Click the button to delete revealed logs.
Save To File	Click the button to save the selection you made to a new file.
Find	Opens a find dialog, where you can search through the current log file. This may come extremely handy for the quick visual log analysis. 

Explore	Opens the log directory (as defined in **Tools – Storage – Directories**).

NOTE: Log filtering is disabled for the following types of logs:

- Instant Messaging Archive

- Instant Messaging Presence

- VoIP (SIP)

- LDAP

- ActiveSync

- SyncML

- WebDAV

- Anti-Spam Reports

- PHP Error

- WCS logs (conferencing)

Example – Mailing List Logs

This example shows logs of a message sent to a mailing list and logs of messages sent to mailing list recipients.

```
...
189.60.216.50 [1044] 13:01:22 *** <test@luca.br> <testlist2@luca.br> 1 1356 00:00:01 OK VYQ98320
189.60.216.50 [1044] 13:01:22 >>> 250 2.6.0 1356 bytes received in 00:00:01; Message id VYQ98320 accepted for delivery
189.60.216.50 [1044] 13:01:22 <<< QUIT
189.60.216.50 [1044] 13:01:22 >>> 221 2.0.0 reverse.luca.br closing connection
189.60.216.50 [1044] 13:01:22 Disconnected
SYSTEM [0FC8] 13:01:22 Client session Message id VYQ07722 item 02200808151301225491.tm$ original VYQ98320
SYSTEM [0FC8] 13:01:22 Client session DNS query 'gmail.com' 0 (5) [OK - 3]
SYSTEM [0FC8] 13:01:22 Client session Connecting to 'gmail-smtp-in.l.google.com'
SYSTEM [03B8] 13:01:22 Client session Message id VYQ07722 item 02200808151301225495.tm$ original VYQ98320
SYSTEM [0CDC] 13:01:22 Client session Message id VYQ07722 item 02200808151301225493.tm$ original VYQ98320
SYSTEM [12AC] 13:01:22 Client session Message id VYQ07722 item 02200808151301225496.tm$ original VYQ98320
SYSTEM [0F8C] 13:01:22 Client session Message id VYQ07722 item 02200808151301225494.tm$ original VYQ98320
SYSTEM [12AC] 13:01:22 Client session DNS query 'gmail.com' 0 (5) [OK - 3]
...
```

In the mailing list scenario, one message arrives to a mailing list account. Its ID is called original ID. Because it is a mailing list, the message is resent to mailing list recipients. The resent emails have another ID, but you can find the ID of the original message in the log file.

Example – Anti-Spam Report Log

This section explains Anti-Spam report logs.

Challenge [0001] 11:24:42 0.648605 1 0 23 0

Log Part	Description
11:24:42	time
0.648605	duration of report script running (in seconds)
1	number of active accounts (= they have access to Anti-Spam or Quarantine)
0	number of active spam administrators
23	total number of spam items (= sum of all spam messages in active domains/accounts)
0	total number of quarantine items (= sum of all quarantine messages in active domains/accounts)

Example – Forwarding Logs

This example shows SMTP logs as they are created when the ***Forward mail older than (Days)*** option is used. (This option is available within **IceWarp WebClient – Tools – Mail – Forwarder** or can be set using the ***u_forwardolderdays*** console API). To search for these logs, check ones created just after midnight.

SYSTEM [0000] 00:03:52 Forwarded mails older than 20 days from 'vendas@testdomain.com.br' to 'test@gmail.com'

SYSTEM [0000] 00:03:58 Forwarded mails older than 30 days from 'sergio@tester.com.br' to 'test2@gmail.com'

Example – SMTP Logs

The following logs show the situation when IceWarp Server connects to some host (e. g. host of remote account, backup domain, etc.) and cannot resolve the host's IP.

SYSTEM [1ABC] 11:24:33 Client session Connecting to 'mail.hsps.com.br'

SYSTEM [1ABC] 11:24:36 Client session Could not connect to 'mail.hsps.com.br(0.0.0.0)'

SYSTEM [1ABC] 11:24:36 Client session Disconnected

Solution

Understand why the DNS cannot resolve this name (**System – Connection – DNS Server**), or allocate a free DNS temporarily (***openDNS***).

Example – Mail Flow Logs

When you are trying to find out the reason of some problem – e.g. certain SMTP session is taking too long – it is very helpful to search for the same thread in other kinds of logs.

Example:

SMTP log: *201.63.122.98* **[2770]** *15:40:58 Start of mail processing*

Search for that same thread in Mail Flow logs:

SYSTEM [2770] 15:40:58 HandleLocalMail Begin

SYSTEM [2770] 15:41:28 HandleLocalMail End

In this case, it does not help too much.

But when searching within Performance logs:

SYSTEM [2770] 15:40:58 SMTP: :25 s. waiting for ThreadLock(3) UserStatisticsUnit_61, waited for 486 instances

This is the reason – the delay is in the *User Statistics* option (it can be disabled in **Status – Account Statistics**).

Interpretation of 5xx Errors in Icewarp SMTP

SMTP delivery errors can occur in SMTP session log and the category of "5" indicates that a message was not delivered. The table below lists the most common SMTP errors with a short description to help you understand their cause, and provides brief remedy instructions. Consult further documentation before you modify any security settings.

Code	En. Code	Error Phrase	Description	Remedy Instructions
500	5.5.1	Command unrecognized	The SMTP command currently used was unrecognized or is not supported by the SMTP service.	Review the syntax of the last command and try again. Another possibility is that you are trying to use telnet and the telnet connection to your server is not allowed. Check the settings in administration console: **Mail Service – Security – Advanced**.
501	5.5.2	Domain name required	Sender has no domain specified (usually in MAIL FROM).	Specify the sender's domain name and try again. The problem will be with user's email client, not your server. The email client configuration is probably not supplied with a domain name.
501	5.5.2	Unbalanced	SMTP session syntax invalid (usually unbalanced brackets).	Check the syntax of the last command and the configuration of corresponding .dat files.
501	5.5.4	Syntax error in parameters scanning	Common syntax error. You probably mis-typed last command or last string is invalid.	Check the syntax of the last command.
501	5.5.1	HELO/EHLO requires domain address	Usually when there was blank or invalid string sequence after HELO/EHLO command.	Retry the SMTP greeting with correct HELO/ELHO command.
501	5.0.0	Authentication canceled	The process of authentication was canceled for any reason.	Restart the authentication process by using proper command.
501	5.7.1	Message is too long	Exceeded message size limit	Review settings of limits on server/domain/user levels.
501	5.7.1	Permission denied	1) Username given in AUTH differs from sender in mail FROM 2) Message submission is active and not used by local sender, or unauthenticated access to submission port 3) Milter filter returns error in ***envfrom*** stage	1) Disable this – check in administration console: ***Mail – Security – Advanced – Reject if SMTP AUTH different from sende***r. 2) Local senders has to use submission port or disable this setting using the **C_Mail_SMTP_Delivery_MessageSubmission** API variable. 3) Check used filter.
501	5.7.1	Sender domain must exist	MX record of sender's domain was not found	Disable this – check in administration console: ***Mail – Security – DNS – Reject if originator's domain doesn't exist*** or disable the **C_Mail_Security_Protection_RejectMX** API variable.
501	5.7.1	Sender IP must resolve	Reverse DNS query on sender's IP failed	Disable this – check in administration console: ***Mail – Security – DNS – Reject***

				if originator's IP has no rDNS or disable the **C_Mail_Security_Protection_RejectrDNS** API variable.
501	5.7.1	Sender refused by the DNSBL	Sender's domain was blacklisted by DNSBL server	Check used DNSBL server or you can disable this feature in administration console: ***Mail – Security – DNS – Use DNSBL*** or by the **C_Mail_Security_Protection_DNSBL** API variable.
502	5.5.1	Sorry, we do not support this operation	This operation is not allowed.	You can allow/disable particular operations and commands from the administration console: **Mail Service – Security – Advanced**.
503	5.5.1	Incorrect command sequence	A supported command was used in invalid order. For example command RCPT TO used before MAIL FROM or DATA command used when RCPT TO command was not accepted.	Solution depends on the context in which this error occurred. Check the last few commands sequence.
503	5.5.1	Authentication already done	Error occurs by re-authentication.	
503	5.5.1	HELO/EHLO command required	Greeting error. HELO/EHLO command is required by the server.	You have to use HELO or EHLO command. You can deactivate this option in administration console, or create a Bypass: **Mail Service – Security – Advanced**.
503	5.5.1	HELO/EHLO already specified	Greeting used again.	
504	5.7.6	Unrecognized authentication type	Invalid authentication type. Incorrect or none type of AUTH specified.	Use the command AUTH with proper authentication type.
530	5.7.1	Authentication required [AUTH]	Authentication with command AUTH is required.	Use AUTH command (SMTP Server requires authentication) or disable this authentication type in administration console.
535	5.7.1	Authentication credentials invalid	1) The username/password combination provided during authentication was invalid. 2) Milter filter ***auth*** action	1) Re-enter both the username and password and authenticate again. 2) Check used filter.
550	5.1.1	User unknown; rejecting	1) Recipient's domain is set to reject unknown accounts 2) User was not found on other servers in a distributed domain	1) Review setting of Domain – Options – Unknown accounts – Action. 2) Check other servers in your distributed domain for given account.
550	5.1.1	User %s has invalid forward set and no mailbox; rejecting	It is returned, when somebody is trying to send a mail to a user, who has NULL mailbox and non of their forwards is valid. (Then the mail is undeliverable).	
550	5.7.1	Access to recipient not allowed [SPF-SRS]	SRS hash check failed for received NDR	You can disable this security check in ***Mail – Security – DNS – Use SRS NDR Validation*** or via the **C_Mail_SMTP_Other_SPFSRSNDRVerify** API variable.

550	5.7.1	We do not relay	Server is not open for relay.	Refer to this FAQ.
550	5.7.1	We do not relay, account limits apply		Check the account limits for the particular user account, its domain and on the server level.
550	5.7.1	You have rights to send mail to local domains only	The user who gets this error is allowed to send mail only to local domains.	Disable this option in the administration console: **Management – <User> – Options – User** can send mail to local domains only.

550	5.7.1	Access not allowed	1) Server blocked access by a blacklist filter, or 2) Reject if originator's domain is local and not authorized option turned on.	1) Review server black list filter settings or set a bypass file. 2) Local users have to authorize themselves so if they do not have this set up in their e-mail clients and you turned this on they are not allowed to send.
550	5.7.1	Access to not allowed by rules	1) Server blocked user access by a blacklist filter/rule, or 2) Server blocked access from the originating server by HELO/EHLO Filter.	1) Review server black list filters and user rules or set a bypass item. 2) Whitelist the originating server in HELO/EHLO filter, or remove it from blacklist, or create a Bypass.
550	5.7.1	Permission denied		
550	5.1.1	Unknown local user		
550	5.1.1	Unknown user; rejecting	Unknown user account. The recipient is not local, thus reject the message.	Behavior and the treatment of messages coming to unknown user accounts can be set from administration console: **Management –<Domain> – Options – Unknown Accounts**.
551	5.1.1	No such user found	User account is not local.	
551	5.1.1	No such mailing list found	Mailing list is not local.	
552	5.2.2	Mailbox has exceeded the limit	Recipient's mailbox is full and ***C_Mail_SMTP_Other_FullMailboxPermanentError*** has been set.	Check recipient's quota on server/domain/user levels.
554	5.3.4	Message size exceeds fixed maximum message size	Too many data was sent by the user. User account has an amount limitation.	You can increase or disable amount limit from administration console – **Management – <User> – Limits** tab. Make sure all 3 levels (server, domain and user) are set to 0 (stands for unlimited).
554	5.7.1	Permission denied	1) Access restriction to all services is enabled and sender's IP address was found in denied list. 2) User sent some data before greeting from server was sent. 3) Milter filter returns error in ***connect*** stage.	1) Check service's access list in ***System – Services – <Service> – Properties – Access*** or disable the **C_System_Services_Firewall** API variable
554	5.7.1	Message cannot be accepted, rules rejection	1) Sender is blacklisted. 2) External filter rejects the message.	1) Check system and recipient's blacklist. 2) Check used external filters. 3) Check used external filters.

			3) Milter filter returns error in ***eom*** stage.	
554	5.7.1	Message cannot be accepted, virus found	Virus was found in the message body or in the message attachment.	If you think the attachment is not harmless (false positive), try to alter the configuration of the anti-virus engine (Quarantine instead of Reject), or create a Bypass entry.
554	5.7.1	Message cannot be accepted, content filter rejection	Content filter applied and the message was rejected.	Review the content filter settings in administration console.
554	5.7.1	Message cannot be accepted, spam filter rejection	Message is probably spam.	If you think this message is spam (false positive), try to alter the configuration of the anti-spam engine, index the message by Bayesian or create a blacklist entry.
554	5.7.1	Message cannot be accepted, spam rejection	Message is probably spam.	If you think this message is not spam (false positive), try to alter the configuration of the anti-spam engine, index the message by Bayesian or create a whitelist entry.
		Message deleted by filter		Alter your content filters configuration.
554	5.7.1	Message cannot be accepted, filter rejection	The message was rejected.	Check your filter settings and configuration.
554		Could not connect and send the mail to recipient	Client session – target server not responding	Check target server.
554		Could not verify SSL connection	Client session – target server SSL certificate cannot be verified	Check target server.
554		Permanent problems with the remote server	Client session – server returned 4xx or 0xx status	Try again later.
554		... while issuing MX query	Client session – cannot obtain MX for target server	Check DNS
554		Could not resolve target DNS	Client session – cannot contact DNS	Check DNS
554		Too many hops	Message was redirected by more than **C_Mail_SMTP_Other_MaxHopCount SMTP** servers	Check mail delivery path recorded in the ***Received*** headers.

Log Analyzer

The IceWarp Server Log Analyzer is a statistical and logical analysis tool for log files generated by the server engine.

Its functionality can be divided into two major areas:

- Importing the logs generated by the server as plain-text files into a database.
- Running pre-set or creating custom queries against the database to produce statistical graphs or reports for viewing or sending via email.

Each functional area is covered by its own interface with corresponding executables:

1. Built-in Log Importer (**mlaimp.exe**) configured from within Administration GUI of IceWarp Server.

   This processes raw log data from log text files and organizes this information into structured records stored in an SQL database in a form suitable for the external log Viewer application.

2. External log Viewer (ILA.exe).

   This standalone application does the analysis of the data using preset and/or custom SQL statements.

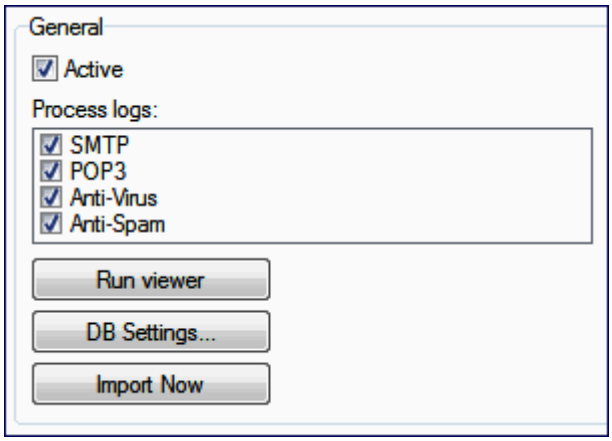
The advantage of this approach is that you can do all the configuration to collect data in the familiar Administration GUI, allowing IceWarp Server to import log files into the database automatically each night, while the external log Viewer can be run on any external machine (such as your desktop) and connect either to a local copy of the database or to a remote database (when provided with the connection details).

IceWarp Server Log Analyzer allows you to analyze your server activity quickly and efficiently over your morning cup of coffee from the convenience of your laptop.

Currently only the SMTP, POP3, IceWarp Anti-Virus and IceWarp Anti-Spam logs are supported.

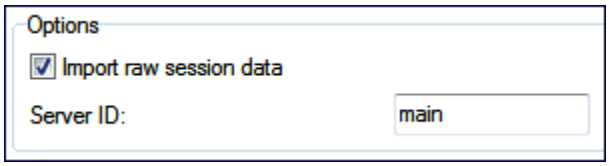
Other log types, and more detailed types of analysis will follow in the next release, along with enhanced charting, rich-text HTML statistics and other improvements to statistics reports.

General

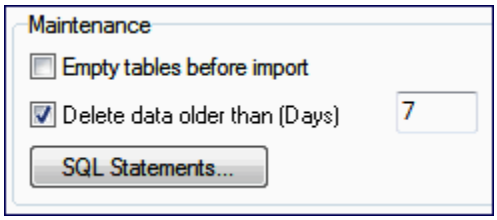


Field	Description
Active	Check this option to enable the log file import process.
Process logs	Specify which logs you want to import.

	*NOTE: Logging must be enabled and and selected for each log type that you want to import. See **System – Services – General – <service> – Logging** tab.*
Run Viewer	Click this button to launch the Viewer application which allows you to see your log data in a user-friendly format.
DB Settings	Clicking the button opens the standard **Database Settings** dialog allowing you to define which database Log Analyzer will be using and how to access it. Enter ***Syntax*** (type of database), server on which is established, username and password if required to access it.
Import Now	Click this button to import your log data immediately. It may take a while to complete, depending on the size of log files to process. You would not normally need to do this as the import is performed automatically every day at 01:00. The background process will only import logs generated until its launch. To view logs for the current day or a day in the past, use ***Import Now*** and select the day you wish to import from the **Select date** dialog. *NOTE: If a single SMTP session that spans two days occurs (e.g. starts at 11:58 PM and finishes at 00:03 AM the next day), ILA will not show it as one single session. Only the part of log from the respective day will be shown.* *Do not close the IceWarp Server console during import – the import would stop.*

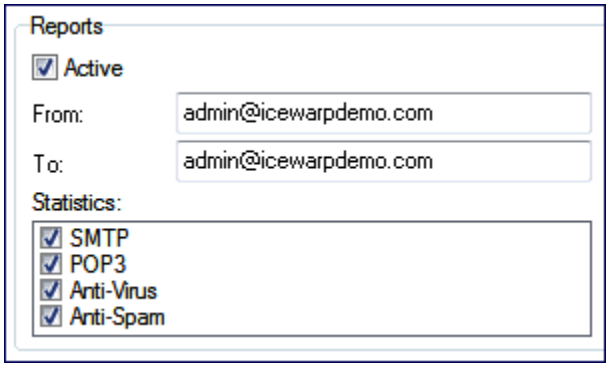


Field	**Description**
Import raw session data	Check this option to import raw log data into the database. This allows you to see the data as it was originally written, from within the viewer. Otherwise the importer will only transfer session data that is capable of using for the statistics. This option is deprecated and should be used carefully. See the ***Session log without Raw Data Import*** chapter for more information. *NOTE: This option will not give you any extra statistical information, just the ability to see the complete session from the log, and the possibility to use the records in custom queries.* *Checking this option will result in your database size increasing.*
Server ID	Optional way to "tag" data with a server name. This is useful where you have multiple servers and you import data to the same database as it allows you to query data for a particular server.



Field	Description
Empty tables before import	Checking this option will delete all data from the tables before importing, thus you will only have one day's worth of data at any one time (yesterday's).
Delete data older than (Days)	Check this box and enter an amount to have old data deleted before an import. This is useful to limit the size of your database and making sure the analyzer always has the last **n** days worth of data.
SQL Statements	You can specify a set of SQL statements to be executed before data is deleted. This could be used to, for example, archive a summarized view of data. Click the button to open a simple edit dialog where you can specify your SQL statements. *NOTE: The SQL is only run if you are using the **Delete data older than (Days)** option.*

Statistics



Field	Description
Active	Check this box to have Log Analyzer overview reports sent by email.
From:	Enter the email address that should be used as the ***Sender*** of the report.
To:	Enter the email address to receive the report. Multiple addresses can be specified, separated by commas.
Statistics:	Check the box against each set of statistics you wish to have included in the report.

Log Analyzer does not connects to a localhost to send report messages, the report message is put into the outgoing queue then the SMTP process will deliver it.

By default, Log Analyzer connects to 127.0.0.1.

If your SMTP is not binded to 127.0.0.1 in **System – Services**, you can bind it or change the IP using the ***HOST*** keyword in the **[STATS]** section of the **[install_dir]\config\mla.dat** file.

Example

To use 1.2.3.4 as your SMTP, you have to modify **mla.dat**:

[GENERAL]

.

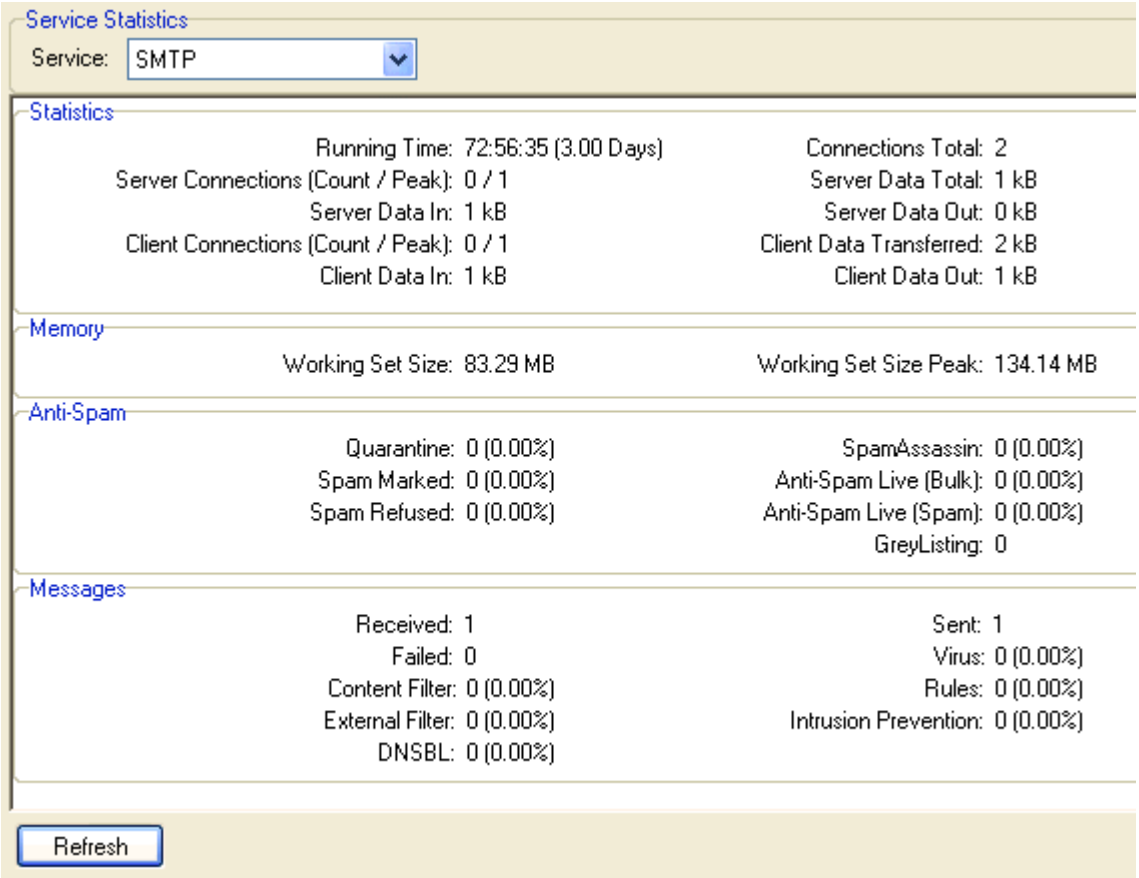
.

[STATS]

HOST=1.2.3.4

Statistics

This tab shows complete statistics about the services – you choose them from the dropdown on the top – the amount of data they transferred, the number of connections, etc. Most of the items are self-explanatory.



Item	Description
Server Connections	The connections, when IceWarp Server acts really as the server side in the Client/Server architecture. E.g. when a user connects to SMTP server and send a message.
Client Connections	The connections, when IceWarp Server acts as the client side in the Client/Server architecture. E.g. when the message is already received from a user and it is addressed to external user, IceWarp Server establishes a connection to another server and sends the message (in this case, IceWarp Server acts as client).
Server Data Transferred	Data transferred within ***Server Connections***.
Client Data Transferred	Data transferred within ***Client Connections***.
Anti-Spam/Messages	Numbers of messages positively evaluated or caught by appropriate feature (such as Content Filters, Anti-Spam System, etc.)

snmp-mib.txt File

The current version of this file is available in **<InstallationRoot>\doc\snmp-mib.txt**.

Counter Increase

Counter for one filter is increased once per session – i. e. multiple recipients (within one session) filtered by one type of a filter do not cause multiple counting.

But, multiple recipients filtered by different filters cause counter increase of all applied filters.

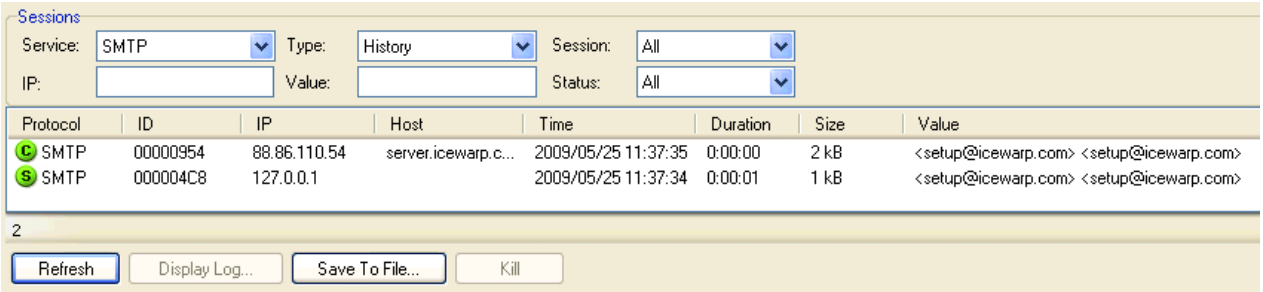
E.g. we have two recipients, for one recipient, the message is evaluated as spam, for the second one, it is rejected. After this session, two counters are increased.

SpamAssassin

This counter counts number of messages where SpamAssassin got score different from zero. It does not count "spam messages", because almost all messages get non zero score. This counter in fact means how many times SpamAssassin was applied.

Sessions

New and very powerful session monitoring and session history engine lets you perform various operations with services sessions including killing, viewing of logs, history, etc.



The Active sessions type lets you monitor the active connections and sessions to the all server services (including VoIP, GW, IM, FTP, Control, etc.)

Icons in Active Session

Within the ***Active*** sessions monitor, the icons can have one of two letters and one of three colors:

S denotes a **Server session** (IceWarp Server acts as receiver)

C denotes a **Client session** (IceWarp Server acts as sender)

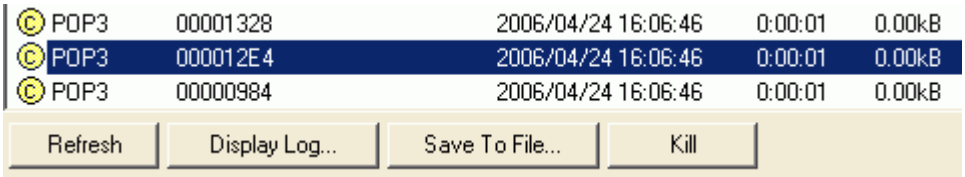
Yellow denotes an **Active session**

Green denotes a **Success**

Red denotes a **Failed Session**

You can view the commands being sent to the server and also the responses. If you have the service logging on, you can double click on the particular session and the whole history of the session protocol (log) will be displayed or can be saved into a file.

Every session can be killed. Various statistics, such as volume of transferred data for SMTP,POP3 and IMAP, current URL for Control, number of connections for user and volume of data FTP are shown.



History works for every service separately. The session ***History*** type displays all history events up to the maximum history value.

Icons in Session History

There are three colors and two letters which can be shown in **icons** in the **Session History**.

S denotes a **Server session** (IceWarp Server acts as receiver)

C denotes a **Client session** (IceWarp Server acts as sender)

Red denotes an **Fatal Error**

Green denotes a **Success**

Brown denotes a **Disconnected session**

If you double-click the circle, the log of the appropriate session will appear.

Server session

This type of session means that IceWarp Server acts as a server in the client/server model. In other words, IceWarp Server is the receiver of a message in this case. It can occur when:

- a client wants to send a message through the IceWarp Server
- another server sends a message to IceWarp Server because it is e.g. for users on IceWarp Server

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 Connected

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 >>> 220-195.122.222.29 ESMTP to je gol; Thu, 22 Apr 2004 22:01:42 +0200

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 <<< HELO localhost

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 >>> 250 195.122.222.29 Hello localhost [127.0.0.1], pleased to meet you.

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 <<< MAIL From:<admin@icewarpdemo.com>

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 >>> 250 2.1.0 <admin@icewarpdemo.com>... Sender ok

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 <<< RCPT To:<test-icewarp-001@yahoo.com>

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 >>> 250 2.1.5 <test-icewarp-001@yahoo.com>... Recipient ok; will forward

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 <<< DATA

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:42 +0200 >>> 354 Enter mail, end with '.' on a line by itself

*127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:43 +0200 *** <admin@icewarpdemo.com> <test-icewarp-001@yahoo.com> 1 348 00:00:00 OK*

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:43 +0200 >>> 250 2.6.0 348 bytes received in 00:00:00; Message accepted for delivery

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:43 +0200 <<< QUIT

127.0.0.1 [00000A1C] Thu, 22 Apr 2006 22:01:43 +0200 >>> 221 2.0.0 195.122.222.29 closing connection

SYSTEM [00000A1C] Thu, 22 Apr 2006 22:01:43 +0200 Disconnected

This is a session when client on the server sends a message from a mail client to the IceWarp Server – it was received by IceWarp Server.

Client session

This type of session occurs only when IceWarp Server sends along an already received message to another mail server.

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session Connected

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session <<< 220 mail.yahoo.com - Yahoo, Inc. ESMTP

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session >>> EHLO 195.122.222.29

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session <<< 250 8BITMIME

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session >>> MAIL From:<admin@icewarpdemo.com>

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session <<< 250 ok

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session >>> RCPT To:<test-icewarp-001@yahoo.com>

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session <<< 250 ok

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session >>> DATA

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:50 +0200 Client session <<< 354 go ahead

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:51 +0200 Client session <<< 250 ok 1082664147 qp 10068

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:51 +0200 Client session *** <admin@icewarpdemo.com> <test-icewarp-001@yahoo.com> 1 521 00:00:00 OK

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:51 +0200 Client session >>> QUIT

212.80.76.44 [00000F6C] Thu, 22 Apr 2006 22:01:51 +0200 Client session <<< 221 mail.yahoo.com - Yahoo, Inc.

SYSTEM [00000F6C] Thu, 22 Apr 2006 22:01:51 +0200 Client session Disconnected

This is a session where IceWarp Server sends along the message which was received in the previous server session.

Session history is stored just in the service memory. Only last 100 sessions are stored in the memory, this memory is cleared with every single restart – this applies for all the services except for WebClient. WebClient runs PHP sessions and only the ones which are not active anymore are visible in the history.

For WebClient, the history shows all sessions which were not properly closed with a logout – so the session file exists in ***php\temp*** *and because of this file, the entry shows up in history.*

Also note that if you close WebClient by closing the browser, the corresponding session remains active for 15 minutes after browser shutdown and then shifts into history.

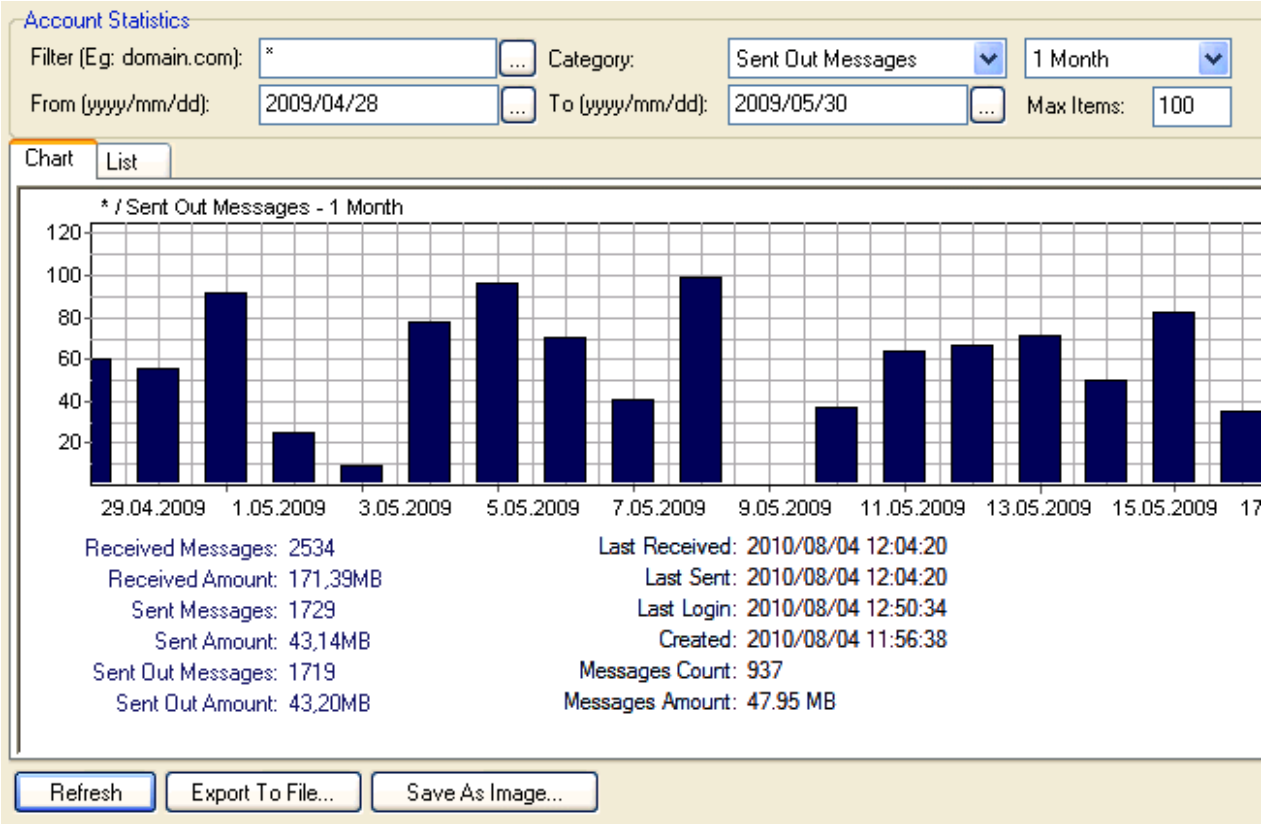
Account Statistics

This feature allows you to monitor the email usage of your users. This feature keeps a log of all sent and received messages statistics along with some other information. If you require the server to perform account statistics, enable the feature on the **System node – Logging – Services** tab. Alternatively, you can enable account statistics via API by:

tool set system C_Accounts_Global_Accounts_UserStat 1

Only then IceWarp Server will record the statistics.

The **Chart** tab offers you information in a graphical format:



The user statistics logs can be exported to file using the usual **Save As** dialog.

Field	**Description**
Filter	The filter field specifies account and domain filters for which the logs are required. Multiple filters can be specified separated by semicolon(s).
Category	Determines which item should be shown in the graph.
From/To	These fields indicate the time scale over which to obtain the log entries. It is considered only when the ***Selection*** item is chosen instead of particular time period in pull-down menu.
Max Items	Specify a non-zero value here to limit the number of messages displayed. Click the ***Refresh*** button after entering the value. *NOTE: The higher the value, the slower the list will be to populate.*
Refresh	Refresh the graph according to the chosen information in the fields.

Export To File	Queries the server to retrieve the logs and saves them to a file.
Save As Image	Click the button to save data currently shown.

Log structure

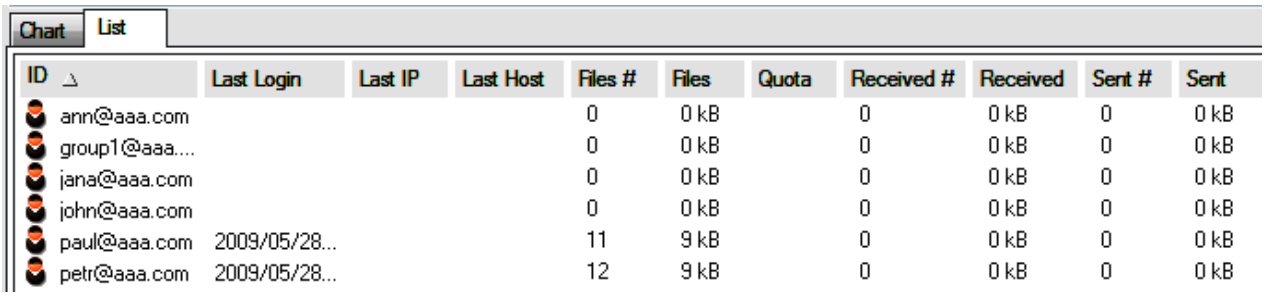
The log file structure consists of multiple lines. The first line contains the list of headers. The next lines display all the users' records matching the filter criteria. The last two lines are special.

Field	**Description**
Received Messages	The number of messages delivered to user's mailbox.
Received Amount	The total amount of data delivered to user's mailbox.
Sent Messages	The number of messages sent by the user to IceWarp Server. *NOTE: Message sent to multiple recipients will be counted as one message for each copy, i.e. a message sent to 20 users counts as 20 messages.*
Sent Amount	The total amount of data sent by the user to IceWarp Server.
Sent Out Messages	The number of messages sent from IceWarp Server whose originator is the user. Local email sent by the user is not considered. The number of recipients is considered because each recipient can be on a different server and it means that IceWarp Server has to send mail out additional times.
Sent Out Amount	The total amount of data sent from IceWarp Server whose originator is the user.
Last Sent	When the user sent their last message.
Last Received	When the last message delivered to user's mailbox arrived.
Last Login	When the user logged on IceWarp Server for the last time.
Created	This field shows when the user's mailbox was physically created (the first login or first received mail). *NOTE: This date can differ from the day when the account was created in GUI if it was not used the same day.*
Messages Count	The current number of messages in user's mailbox.
Messages Amount	The total size of messages in user's mailbox.

The line before the last line specifies all unknown senders. This record is present only if the filter criteria is empty. This information includes the relayed messages for unknown senders and delivered messages from unknown senders.

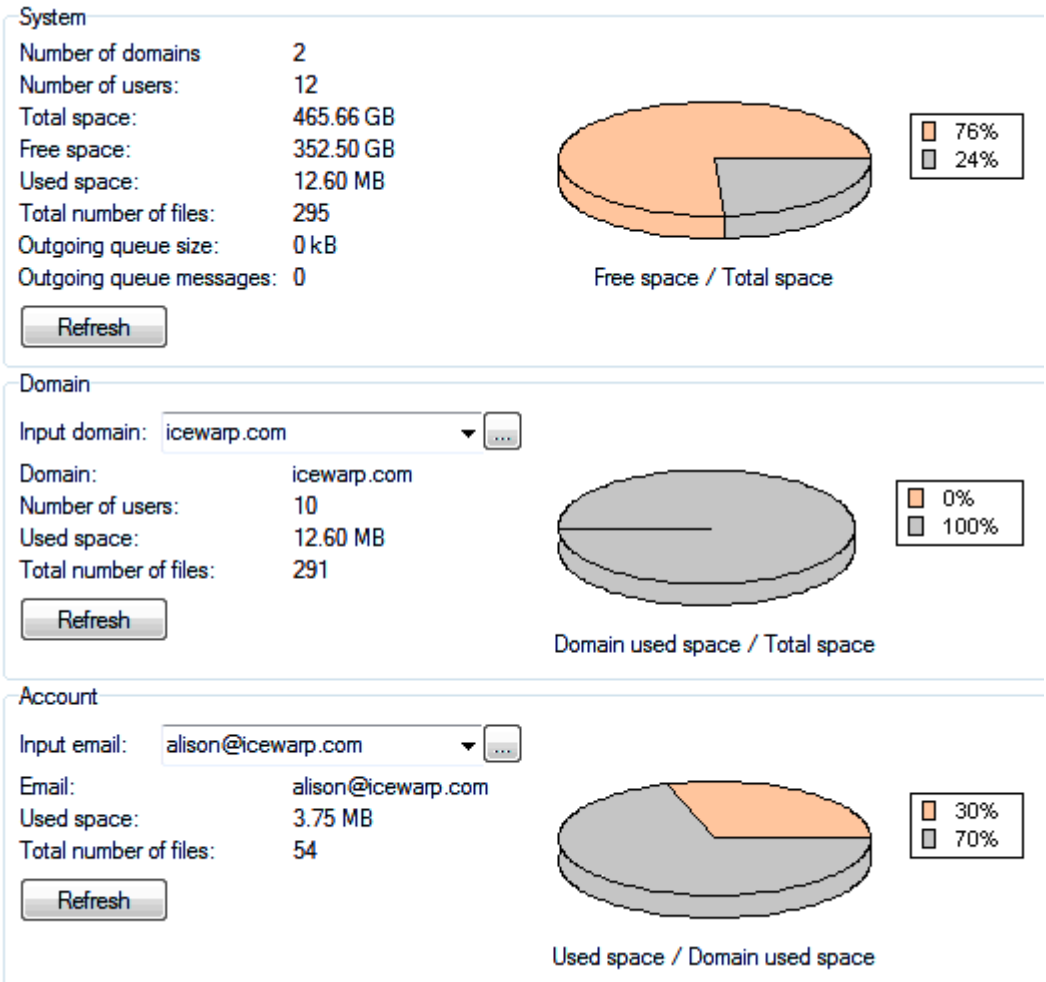
The last line specifies the total information of the filter excluding the unknown line (last but one).

The **List** tab offers you the same information in a tabular format:



Field	**Description**
ID	Account email address.
Last Login	When the user logged on IceWarp Server for the last time.
Last IP	IP address of the last server used to connect to IceWarp Server.
Last Host	Host name of the last server used to connect to IceWarp Server. Only applies when the ***Main Menu – Options – Resolve address in current view*** option is checked.
Files #	Number of files within the account folder.
Files	Size of files within the account folder.
Quota	In the case the account has any size limit set, used percentage of this limit is shown.
Received #	Number of received messages.
Received	Size of received messages.
Sent #	See ***Sent Messages*** above.
Sent	Total size of sent messages.
Sent Out #	See ***Sent Out Messages*** above.
Sent Out	Total size of sent out messages.
Created	The date of account creation.

Volume



The **Volume** tab lets you watch the current server volume statistics. To calculate the volume information click the ***Refresh*** button. Every section calculates also the previous volume counter. You can directly type in an email address or domain of the interest but better way is to select the object in the **Domains & Accounts – Management** section, right-click and select ***Display volume***. Or you can select the ***Accounts – Display volume*** menu item.

Another possibility is to select an account, group or domain with '...' button through the **Select Item** dialog.

IceWarp Server calculates the current volume by browsing all files and objects of the IceWarp Server directory. That means it is basically dependent on the file system. If you have too many files, this can take a while so be sure you use it properly.