IceWarp Unified Communications

Domains and Accounts Reference

Version 11.4



Published on 2/8/2016

Contents

Domains & Accounts 5

Management 5
Domains 6
Domain 6
Limits 7
Policies 10
Devices 11
Options 12
Aliases 18
Templates 19
DKIM 20
DKIM – How it Works 21
Directory Service 21
The syncad.dat File 26
Hierarchical Address Book (HAB) 26
Synchronizing Users with LDAP / Active Directory 27
vCard Map Feature 37
Troubleshooting 38
Best Practices 39
Rules 40
Information 41
User Accounts 42
User 42
Groups 44
Card 44
Limits 45
Policies 47
Options 51
Mail 56
VoIP 58
Rules 59
Groups 60
Group 60
Folders Dialog 62
External Contacts in GAL 63

Hierarchical Address Book (HAB) 63
Members 63
Message 65
Options 66
Rules 67
Resources 68
Resource 68
Users 69
Card 69
Rules 69
Mailing Lists 70
Mailing List 70
Members 72
Message 74
Security 76
Anti-Spam and Quarantine for Mailing lists 77
Options 77
Remove Dead Emails – Soft Failure Counter 79
Rules 79
List Servers 80
List Server 80
Lists 83
Options 83
Rules 84
Example 84
Executables 85
Executable 85
Rules 86
Remote Accounts 87
Remote Account 87
Options 89
Domain POP 90
Rules 91
Static Routes 92
Static Route 92
Rules 93
Notifications 94
Notification 94

Options 94
Rules 96
Catalogs 97
Catalog 97
Maintenance 97
Options 99
Multiple Commands 100
Rules 100
Global Settings 101
Domains 101
Templates 104
Creating Template 104
Applying Templates to New Accounts 106
Template Scenario 107
Domain Clusters 107
Advanced 110
Preserving Hierarchy of Entries 111
Welcome message 111
Policies 114
Login Policy 114
Password Policy 115
Limits – Explanation 118
Limits – Which One Is Used? 119
Limits – Max Message Size 119
Simple RegEx Tutorial 121
^' and '$' 121
'*', '+', and '?' 121
Braces { } 121
'|' OR operator 121
('.') 122
Bracket expressions 122

Domains & Accounts

This node includes the **Management**, **Global Settings** and **Policies** subnodes, which are discussed in detail in this manual.

Legend

Icon	Description
	Warning – very important!
	*Note or tip – good to know.*
NOTE: Areas...	*Note within a table.*
▸ Figure 4	Figure link – click the link to reveal the figure. Click it again to close it. (Works only in the ***CHM*** format.)

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.

Management

Selecting the **Management** node causes the right hand pane to split into a tree hierarchy view of domains on the left and the settings for the selected domain (or account) on the right. (See the **Administrative Console** section.)

Within the **Management** node you can administer all your domains and accounts, modifying any settings as required.

Right-clicking in the middle pane will open the **Accounts** menu where you can add a new domain or account, make the selected domain the primary one and import and export account, amongst others.

Domains are expandable to a list of account types, which are in turn expandable if any of that type of account are defined within the domain. Items are expandable/collapsible by clicking the (+) or (-) symbol next to them, or by double-clicking.

Selecting a domain or account will effect the right hand pane to display settings for this item. You can modify these settings here.

You can use ***SHIFT/CTRL + click*** to multi-select accounts and change a certain setting for all at once (this setting shows highlighted yellow when doing so).

You can also create a group account, define members and use the **Templates** feature within the **Options** tab of a group account to do mass changes. For example, one can add all domains as members of a temporary group account and apply a template to set all accounts of all domains to the IMAP type instead of POP3.

Another way how to perform mass changes is to use **tool.exe/tool.sh**.

The easiest way how to move users from one domain to another one is to cut and paste them. Use with care – big numbers of cut/pasted users (say hundreds and more) can cause long waiting without seeing any progress.

Domains

To create a new domain you can either:

- Select the **Accounts – Create new – Domain** menu item.
- **Right-click** the middle pane when you have the **Domains and Account – Management** node selected and select **Create new – Domain**.
- Press **CTRL+D**

To modify the settings of an existing domain you should select the **Domains and Account – Management** node, then select the domain you wish to modify.

Whether you are creating a new domain or modifying an existing one you will be presented with the settings panels for the domain in the right-hand pane.

Be aware that one of your domains must be assigned as the primary domain. The primary domain administrator is also regarded as the server administrator and any system messages (license warnings, system reports, etc.) will be sent to this account.

You can change the primary domain by selecting a domain and selecting the **Accounts – *Set as primary domain*** menu item.

The primary domain is always listed first in the domain list. Other domains are listed in alphabetical order, see the example below where the primary domain is *icewarpdemo.com*.



Functionally, there is no difference between the primary and secondary domains. You can, however, send messages to the primary domain without specifying the domain name.

For example: sending a message (internally, of course) to ***Someuser***, given the above example, would route the message to ***Someuser@icewarpdemo.com***.



BE AWARE: In the case there is a user with the same user name in another domain on the server, the message goes to a wrong person. To avoid it, consider creating a dummy primary domain without users just with an administrator set. He/she receives important system emails – the *unknown user – rejecting* message in this case.

A domain name is NOT the same as a host name. If you have a secondary domain that you want your users to connect to, you must have both A and MX DNS records set up.

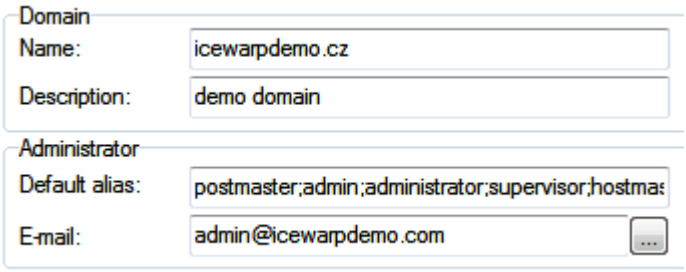


*Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Clicking the ***Domain information*** button (within the very low part of GUI) brings you to the **Information** tab that summarizes domain settings.

Domain

The **Domain** section of the **Domain** tab shows basic information about the domain:



Field	Description
Name	This is the name of the domain. Messages can be only delivered to created domains. If a message arrives for a domain that does not exist, the message will be forwarded (relayed) outside your server. *NOTE: It is possible to rename a domain. To keep all account data, it is necessary to have all services (e.g. GroupWare, AntiSpam, etc.) running when renaming!* *BE AWARE: The **Username** field of some accounts might have a full email typed in. In those cases, such usernames are NOT renamed, they remain as they were.* *To find out whether it is the case, try this query:* ***SELECT * FROM users WHERE u_mailbox LIKE '%domain.com'*** *To change the **Username** fields they to contain just usernames, use this command:* ***UPDATE Users SET U_MailBox = replace(U_MailBox,'@domain.com','') WHERE U_Domain LIKE '%domain.com';*** *BE CAREFUL – backup your database before any changes!*
Description	A short informational description of the domain.
Default alias	Specifies the administrator aliases for the email address specified in the ***E-mail*** field. Multiple aliases can be separated by semi-colons, without spaces. Any aliases you specify here do not need to have accounts created for them.
E-mail	Specifies the account that messages to a postmaster alias should be delivered to. Multiple accounts can be specified (separated by semicolons). Remote email addresses can be used. The primary domain must have an administrator email defined. It is used by the system for notification emails and system reports. Use the '...' button to select accounts and/or groups. Read more about the **Select Accounts** dialog.

For more information about personal data synchronization with AD/LDAP, refer to the **Domain – Directory Service – Personal Data Synchronization** chapter.

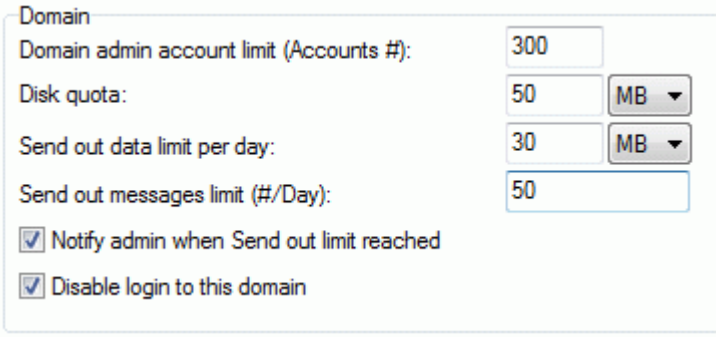
Limits



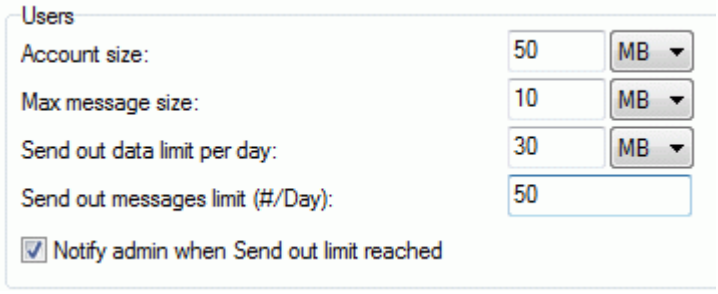
BE AWARE: In most options, value of 0 means unlimited.

The following domain limits are checked regardless of any user-level limits you have set. For example, if you have a domain ***Disk quota*** limit set to 100MB and set a user mailbox size to 500MB it will be capped at 100MB (assuming no other mailboxes are using part of the 100MB for the domain).

*NOTE: Most of fields are active only if the appropriate domain, user or expiration limits are enabled upon the **Global Settings – Domains** tab.*



Field	**Description**
Domain admin account limit	Limits the number of user accounts that can be defined in this domain by a domain administrator. This number does ***not*** include other account types (mailing lists, catalogs, etc.).
Disk quota	Limits the amount of disk space that this domain will use. Input a value and select Kilobytes, Megabytes or Gigabytes from the dropdown box. Once this amount is exceeded no further messages will be accepted by the domain, a ***4xx*** temporary error is issued and the sending server should retry after a period of time. Temporary errors showing can be changed via API. The appropriate variable is ***c_mail_smtp_other_fullmailboxpermanenterror***. *NOTE: Until version 11.2, the disk quota was limited to a maximum of 4,095GB, the next versions have no limit of disk quota.*
Send out data limit per day	Select an amount of data this domain can send out in one day.
Send out messages limit (#/Day)	Specify a maximum number of messages that this domain can send in one day.
Notify admin when Send out limit reached	Notification will be sent to administrator email defined on **Domain tab** of a domain..
Disable login to this domain	Stops all users from logging in to this domain. This option is only available if the **Use domain limits** option in **Global Settings – Domains** is checked.



Field	**Description**
NOTE	*The following limits for users in a domain are only accessible if the **Use domain limits** option is checked in **Global Settings – Domains**.* *These limits are only checked if the corresponding limit in **<user> – Limits** is set to zero or not enabled – this applies for the **<user> – Limits – Account size** feature.* *In the case some user has set a different value (differing form 0), this setting (i. e. user*

	level) is used as it has higher priority.
Account size	Limits the size of a user's mailbox. Input a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. Once exceeded no further messages will be accepted for that user.
Max message size	Limits the size of ANY message SENT by a user. Input a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. It is also possible to enable checking of user size limits of incoming messages using API and setting C_Mail_SMTP_Other_IncomingMessageLimits to 1. If this option is enabled and the message violates limits of any of the recipients, the whole message is rejected with a SMTP permanent error. By default, messages are temporarily rejected, so users can take time to get a bounce back about a delivery to a user over quota. You can change errors for mailbox full to fatal SMTP 5xx errors. Search File/API console for "fullmailboxpermanent" (without quotes) and set to True. Variable is c_mail_smtp_other_fullmailboxpermanenterror Be aware that all attachments are Base64 Encoded, which adds a size overhead of around one third, so if you wish to limit your users to a message size of 1MB you should set the limit to 1.3MB.
Send out data limit per day	Limits the amount of data that any single user can send out in one day. Input a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. Once a user exceeds the limit no further messages will be accepted from that user. Note that a message sent to multiple recipients will be counted for each recipient, i.e. a 1MB message sent to 10 recipients will be counted as 10MB towards the limit. *NOTE: Local emails are not included.*
Send out messages limit (#/Day)	Limits the number of messages that a single user can send out in one day. Once exceeded no further messages will be accepted from that user. It should be noted that a 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 towards the limit. *NOTE: Local emails are not included.* *NOTE: This feature can be used as an anti-spam security measure. Defining a reasonable day message limit (say hundreds) can prevent account abuse for sending spam.*
Notify admin when Send out limit reached	Notification will be sent to administrator email defined on **Domain tab** of a domain..



The ***Expiration*** feature allows you to define an expiration date for the domain. When a domain expires, only the login to the domain is disabled, you can still perform other actions on the domain.

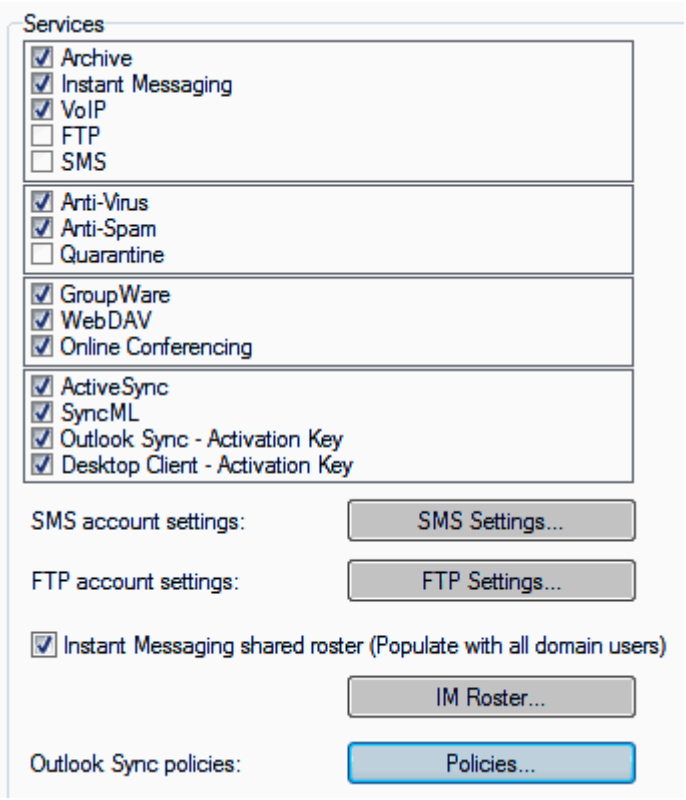
Field	**Description**
Expiration on	Specifies the date on which the domain will expire.
Notify before expiration (Days)	You have the option to notify the domain administrator before the actual expiration – specify the number of days before expiration that the message is to be sent. *NOTE: If no domain administrator email is specified (**<domain> – Domain –***

	***Administrator – E-mail**), then the server administrator (the same field of your primary domain) will be notified. The notification email will contain the domain name and the number of days until expiration.*
Delete domain when expired	If this box is checked the domain will be deleted at midnight at the end of the day it expires. *All accounts and settings will be lost at this time, so use with extreme care!*

Policies

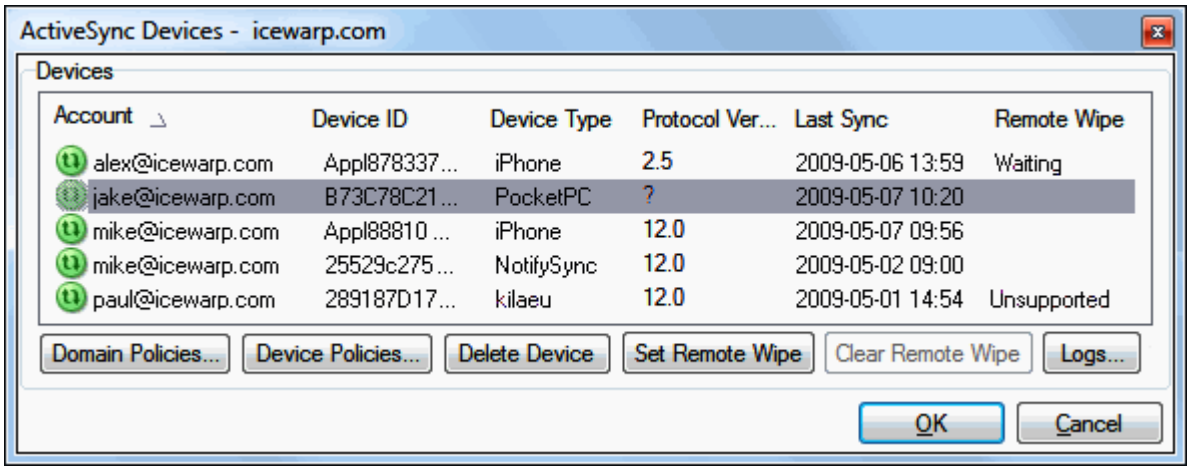
This tab lets you enable or disable selected services for the whole domain.

NOTE: You can select multiple users from the middle pane in Management using Shift+click and Ctrl+click mouse operations to perform a bulk modification.



Field	**Description**
Services	Tick the services you want to enable on the domain level. For more details about ***Activation Keys***, refer to the **User – Services** section. *NOTE: To enable activation keys for IceWarp Outlook Sync and/or Desktop Client, it is necessary to tick check boxes here and under the **<user> – Services** tab too.*
SMS account settings	Click the ***SMS Settings*** button to open the **SMS Account** dialog where you can set SMS account options. For more information about this dialog, refer to the **User Accounts – Policies** chapter – **SMS Account Dialog** section.

FTP account settings	Click the ***FTP Settings*** button to reveal the **User** dialog, where you can define settings for all system accounts. For more information about this dialog, refer to the **User Accounts – Policies** chapter – **User Dialog** section.
Instant Messaging shared roster (Populate with all domain users)	Tick the box if you want all domain users to be added into their instant messaging rosters. (Click the ***Save*** button to have this change reflected in the **roster.dat** file immediately – see further.) By default, this option is enabled. If the box is ticked, the **roster.dat** file (**<install_dir>/config/<domain>**) is edited, so users included here need not to authorize each other. *NOTE: It is possible to add a group (or more) to this file. Use the following syntax: **[group_name]**. Use a single line for each group. You can even delete the domain from the **roster.dat** file.* For more information, refer to the **Instant Messaging – Auto-populate IM roster** chapter.
IM Roster	Click the button to open the domain **roster.dat** file where you can enter any groups, domains or users that should be present for this domain users. Regarding the file syntax, see the note above. Single users are to be added without brackets.
Outlook Sync policies	Click the *Policies* button to open the **Policies** dialog. Here, you can set provisions for Outlook Sync users of the appropriate domain. It is possible to *Force settings* (not possible to change by users) or to *Set as default* (users can change these recommended values). For detail description of these options, refer to the **IceWarp Server Outlook Sync User Guide – IceWarp Options – Settings** section.



NOTE: The caption of the very left button is variable according to the level we are accessing the dialog from.

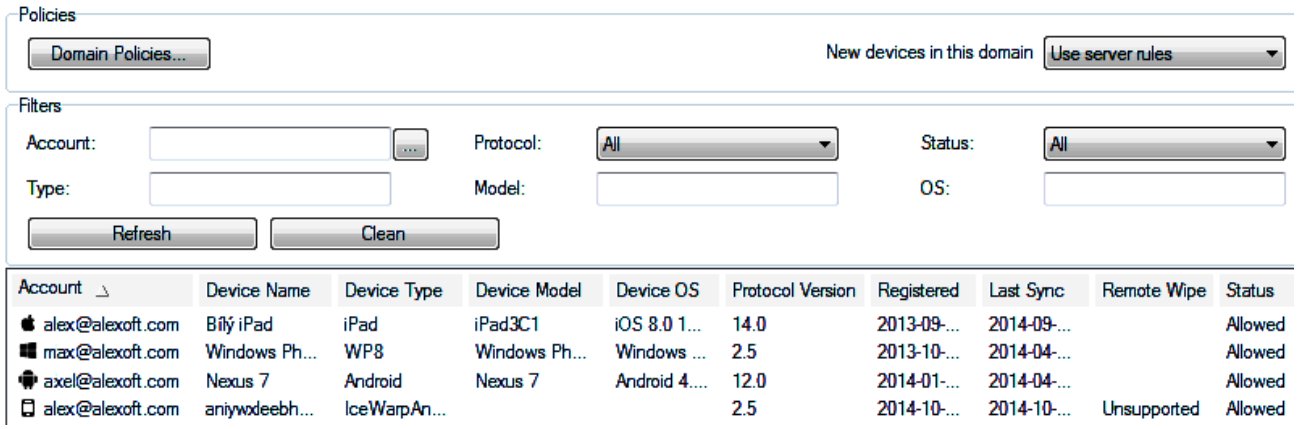
There are following (self-explanatory) possibilities:

- Global Policies (**GroupWare – ActiveSync – Device Management**)
- Domain Policies (**Domains and Accounts – Management –<domain> – Policies – ActiveSync Devices**)
- User Policies (**Domains and Accounts – Management –<user> – Policies – ActiveSync Devices**)

For more details about security policies, refer to the **ActiveSync Guide – Security Policies** section.

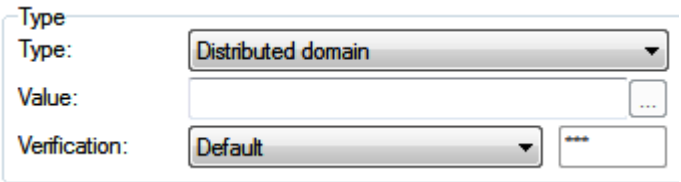
Devices

This tab lets you manage mobile devices of the domain users.



Field	Description
Domain Policies	Click the button to open the **Policies** dialog. Policies set here will be applied for all devices of this domain, unless changed within the **Device Settings** dialog (double-click the device – *Device Policies* button) for an individual device. For details about the **Policies** dialog, refer to the **ActiveSync Guide – Security Policies – Default Policies** chapter.
New devices of this domain	Select policies for new devices from the list: • *Use server rules* – new devices will be treated as defined on the server level (**GroupWare – ActiveSync – ActiveSync – Rules**) • *Allow* – new devices will be allowed • *Block* – new devices will be blocked • *Quarantine* – new devices will be quarantined
Filters	Use self-explanatory filters to ease your work with extensive device lists. Set a filter and click the *Refresh* button. Click the *Clean* button to show all list items.
Manage Device	Select a device and click this button to manage the device settings. For detailed description of this dialog, refer to the **ActiveSync Guide – Device Management** chapter.
Allow Device	Select a device and click this button to enable synchronization for this device.
Block Device	Select a device and click this button to block synchronization for this device.
Delete Device	Select a device and click this button to remove this device from the list. *NOTE: This action does not prevent the device from synchronization when it contact the server next time. Use the Block Device button to set it.*
Rule for similar devices	Select a device and click this button to create a similar rule. See the **ActiveSync Guide – ABQ Management** chapter.

Options

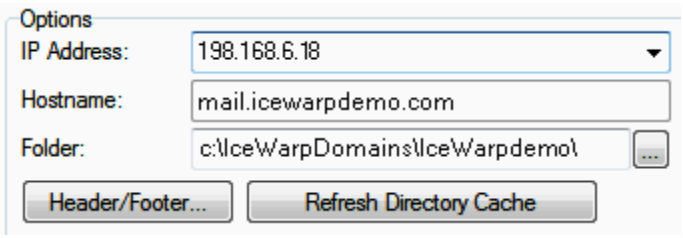


Field	Description
Type	The type of domain – there are five domain ***Types***:
Standard	This specifies a standard domain with users who have separate mailboxes. This is the default domain type and probably the most commonly used.
Domain alias	The ***Domain alias*** type is used to immediately forward any received messages to another domain. The domain to be forwarded to must be specified in the ***Value*** box. Forwarding can only be done to local domains (i.e. on the same IceWarp Server). This domain is useful where you have registered multiple combinations of a domain name but want all messages to be collected from one point. For example, if you own MyShop.com MyShop.net MyShop.org and you want all messages to go to MyShop.com. You should set up a standard domain for ***.com***, and alias domains for ***.net*** and ***.org***. Both the ***.net*** and ***.org*** domains should specify MyShop.com in the ***Value*** field. Standard MX and A records should be set up for all three domains. All messages received to the ***.net*** and ***.org*** domains will be immediately forwarded to the ***.com*** domain. *NOTE: This type of domain does NOT need to have an account defined within it (actually, it is **not recommended** to create accounts within this domain type). However, if an account is defined, any mail sent to that account will NOT be forwarded!* *NOTE: For backwards compatibility reasons and for having possibility to define different rules for a domain alias, this option is still retained. To find additional information, go to the **Domain – Aliases** section.*
Backup domain	The basic function of a backup domain is to accept messages and forward them immediately to another server. If the other server cannot be contacted then the messages are queued for delivery when the server is back online. This can be useful in three suggested scenarios: **Backup Server** This is a backup to ensure no messages are lost if your primary server is offline. ▪ You have your main server and a backup domain on different servers. Note that both servers should have the same domain name (e.g. mail.mydomain.com). ▪ MX records are defined for both servers but the backup domain server's MX has a lower priority. For example, 2 MX records are created for mydomain.com, one points to mail.MainServer.com and has priority 5 and the second points to mail.BackupServer.com and has priority 10. ▪ The backup domain is set to forward all messages to your main server. Now, if your main server is down for any reason, any remote connections should contact your backup server to deliver messages. When your main server is running correctly again, the backup one will deliver all messages collected during the down-time. **Domain Gateway** This allows you to have a server between your "real" server and the Internet. ▪ You have a backup domain server connected to the Internet and your main server is internal to your company. ▪ An MX record exists for the backup domain server only. ▪ The ***Value*** field should contain the internal IP address of your main server.

	▪ The backup domain is set to forward messages to your main server. Now, all messages sent to your company will be initially processed by your backup domain server. The backup domain server can do all the IceWarp Anti-Virus and AntiSpam processing and only deliver messages that you really want to your internal server. For this scenario, quarantine is the only option. There are no accounts, so no spam folders. There is no need to do any further forwarding of spam reports providing that you ensure that spam reports are not caught by antispam (this can be done e.g. through bypassing 127.0.0.1 from antispam/quarantine). **Migration Scenario** The third scenario where the backup server can be implemented is to help implement a phased migration of users from one email server to IceWarp Server. ▪ Set the system up the same as a domain gateway (see above) with the backup domain set up on the IceWarp Server you are migrating to. ▪ Create user accounts in the backup domain for the users you want to migrate to the new server. Any messages for defined accounts will NOT be forwarded to the old server. When a user account is not defined (i.e. not migrated) the message will be forwarded as normally. So now, as you define user accounts, they will effectively migrate to the new server. *NOTE: An important difference between the distributed domain and the backup domain is how they respond when they cannot connect to the receiving server:* *A backup domain will save the message and deliver it when the server is back online.* *A distributed domain will issue a 4xx warning to the originating server, effectively telling it to try again later.* *NOTE: If you define a user on a backup domain then any messages for this user will **not** be forwarded, but will be stored in that domain.* *NOTE: Domain aliases can be used. This can cause inconsistence between the address used for verification and address used for delivery.* *Use the **c_system_services_smtp_rewrite_backup_recipients** API variable. When set to **false**, domain aliases (used within email addresses) are not rewritten; when set to **true**, domain aliases are changed to a domain name.*
Distributed domain	The distributed domain is designed to be used where a business is spread across multiple locations and you wish to distribute your IceWarp email servers around your locations, each with a subset of your users. ▪ At each location you should set up IceWarp Server. ▪ On each server, you should set up a distributed domain, each with the same name (i.e. all called ***mydomain.com***) ▪ An MX record should be set up for each server in the distributed domain. ▪ The ***Value*** field should contain the internal IP addresses of all related distributed domains separated by semicolons. When a message is delivered to the receiving server, it will: ▪ Use the SMTP VRFY or RCPT command (see the ***Verification*** option further down) on all the other servers in the distributed domain to locate the recipient of the message (unless the user is a local one to this instance). ▪ If the user is not found, the message is rejected and a 5xx permanent error is reported to the sending server. ▪ If any of servers in the distributed system cannot be contacted and none of the other servers (that can be contacted) has the appropriate recipient, then a 4xx temporary error is reported to the sending server, which should retry after a period of time. ▪ If the user is found then any IceWarp Anti-Virus and AntiSpam processing is performed (if enabled) and the message is delivered to the user. This processing is usually done on the

	machine where the user is defined. *NOTE: Important difference between a distributed domain and a backup domain is how they respond when they cannot connect to the receiving server:* *A backup domain will save the message and deliver it when the server is back online.* *A distributed domain will issue a 4xx warning to the originating server, effectively telling it to try again later.* *NOTE: Distributed domains REQUIRE recipient real time verification. If one of the destination servers defined in the **Value** field is inaccessible, the email will NOT be sent out and the user will get the "4xx – try again later" error, until the destination server (where the appropriate account is) is available. For WebClient, there is a work-around – use **Bounce back messages for failed recipients** (**Administrator Options – Mail – General**). Other option is to use backup domains, however you lose the IM/VoIP functionality of the distributed scenario.* *NOTE: Anti-Spam is not performed for external recipients of distributed domains, this can be disabled by API variable **C_AS_BypassDistributedDomain** (set to 0). If disabled, Anti-Spam is performed provided that it is set for **outgoing messages**.* *SEE the NOTE to domain aliases and verification within the **Backup domain** field.*
ETRN/ATRN queue	This type of domain is used to hold all messages to be collected by another mail server using the ETRN or ATRN SMTP Client commands. This type would usually be used by ISPs. One user account must be created to allow the collecting server to log in and collect mail. This user account MUST have the ETRN/ATRN account option selected in the **User – Options** tab. If a password is set for this account, the collecting server must specify the password in the ATRN command.
Value	This option is valid for all domains except the standard one. Multiple values can be specified in this field, separated by semicolons. Port values can also be specified by adding a colon and the port at the end of the host name. This can be useful if your ISP blocks standard ports. Syntax: ***<domain><:port>;<domain><:port>*** Example: ***mydomain.com:81;194.148.0.1*** *NOTE: When you put more IPs separated by semicolon into the backup domain Value field, IceWarp Server will try to connect these IPs in the entered order. When the first IP fails, it will try to connect to second one etc. However, there will be a delay caused by timeout when waiting for the first IP response. Connections are done in queue, not in parallel. When the first IP succeeds, IceWarp Server will not try to connect the second one in any case.* *After some time of the first IP outage, there is no way how IceWarp Server could send emails to this IP when it comes back alive.* *NOTE: It is recommended to use host names here. Using of IP addresses could cause problems in the case it is changed.* **ETRN/ATRN queue** If the ***collecting*** server has a static IP address, then this field should contain the IP address. If the IP address is dynamic, the ***Value*** field should be left blank. **Domain alias** The field must contain the domain name of the server that you are aliasing. **Backup domain** Field can contain the host name or IP address of the server that email is to be forwarded to. If the field is left blank, then an MX lookup is performed. *NOTE: You can use the authentication as described in the **Use relay server** field (**Mail**

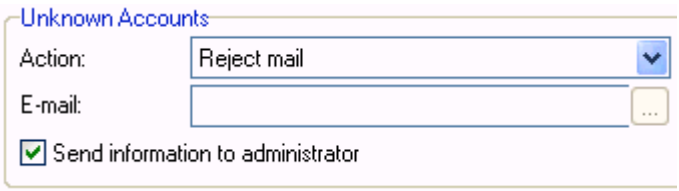
	***Service – General – Delivery** section).* **Distributed domain** Field should contain the IP addresses of the other servers in the distributed domain or can be left blank if MX DNS records are defined for all domains in the distributed system. *NOTE:In the case the desired value is too long, use defined patterns (**System – Advanced – Patterns**) in this field. Use a pattern name in brackets: **[pattern_name]**.* *NOTE: This field is disabled for standard type domains. Although it is possible to access and edit it in WebAdmin, it is meaningless for this type.*
Verification	Applies only to the ***Distributed domain*** and ***Backup domain*** types. ▪ **Distributed domain** – initially the ***Default*** verification is assigned to it. This means that the ***VRFY*** command is used. This domain uses the ***VRFY*** command or RCPT one to locate the server where the user is defined. It is recommended to use the VRFY command. The RCPT command should be used on servers that do not support the VRFY command (very rare nowadays). Selecting of ***Use Minger with password*** for ***Distributed domain*** enables the password field and lets you to set it. For more information about Minger server, refer to the **System – Services – SOCKS and Minger Server – Minger Server** section. ▪ **Backup domain** – initially the **Default** verification is assigned to it. For this type of domain it means that **NO** verification is used. Selecting of ***Use Minger with password*** for this domain type is senseless. *NOTE: For both domain types you can use the response cache. Result of a performed query is cached and the next query can be answered without necessity of another connection to a remote server.* *Use the following API variables:* ***c_accounts_global_distributed_accounts_cache_enabled** – bool – true/false* ***c_accounts_global_distributed_accounts_cache_max** – integer – maximal number of cached items (zero means no limit)* ***c_accounts_global_distributed_accounts_cacheexpire** – integer – cache expiration in seconds* *Set values are used for both **Distributed** and **Backup** domains.* *NOTE: Older MS Exchange versions (2000, 2003) do not support the **VRFY** command by default. This command can be disabled on newer versions, as **VRFY*** could be used for email harvesting. In this case, use the **RCPT** command instead.*



Field	Description
IP Address	Enter an IP address here to bind this domain to that IP. The IP address is also used for authentication, if this is not set correctly then none of your users will be able to authenticate. *NOTE: For binding of the IP address for outgoing connections, you have to enable the **Use domain IP address for outgoing connections** option. See the **Domains and***

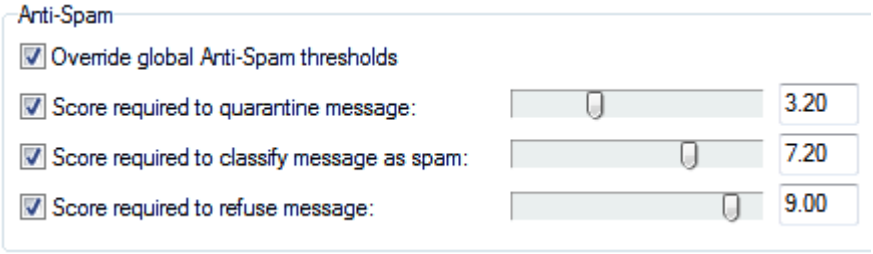
	***Accounts – Global Settings – Domains** tab.* *NOTE: For binding of the IP address for logging in, the **C_Accounts_Policies_Login_DisableDomainIPLogin** property has to be set to **0** using API.* *This applies only for logging in when user names are used. When logging in with whole email addresses, setting to 0 is not necessary as IP address binding is ignored.*
Hostname	Enter a domain hostname to be used for outgoing connections. This setting can be essential for domain identification by various AntiSpam technologies, including Greylisting, SPF and Intrusion Prevention. If defined here, the hostname defined under **System – Services – Smart Discover – SMTP** is bypassed. *NOTE: This option can be used just in the case the **Use domain hostname for outgoing connections** option (**Domains & Accounts - Global Settings – Domains – Other**) is enabled.*
Folder	Domain folder, used for all domain settings and user accounts directories. (By default, the path defined under **System – Storage – Directories – Mail path** is used.) This acts as a prefix and is added to the mailbox path for all ***newly*** created accounts (within this domain). *NOTE: In the case you have mailboxes with non-standard mailbox paths in a domain, create the **externaldirs.dat** file with these paths and put it into the **IceWarp/config** directory.* *E. g. you have most of users in a standard path but others are on a different disk (for example **e**) in the **other_accounts** folder. Add the **e:\other_accounts** path to the **externaldirs.dat** file.*
Header / Footer	You have the option to specify a domain header and a footer. Enable the global ***Header/Footer*** option (**Mail – General – Advanced** tab – even if you do not use it globally) and open the domain **Header/Footer** dialog to specify your footer and header information. If the domain header and footer are not defined, the global ones will be used. You can see more in the global **Header/Footer** settings.
Refresh Directory Cache	Files/folders copied into mailboxes will not appear to users unless the directory cache is updated. Click this button to do it. *NOTE: If you copy files/folders via the internal (console) File manager, this action is not necessary.*

The ***Unknown Accounts*** section of the **Options** tab specifies how to handle messages that arrive for delivery to undefined accounts:



Field	**Description**
Action	Specifies the action to take with any message that is destined for an account that is not defined on the server: **Reject mail** The message is rejected and returned to the sender. This is the recommended setting. **Forward to email address (catch-all)**

	The message is forwarded to the specified account. This can be useful if you wish to monitor these incoming messages but you could end up monitoring a lot of spam messages. This is also a way an ISP can offer unlimited email aliases since messages can be sent to ***anything***@domain.com and it will be delivered to the this catch-all account. When using a catch-all account, it is suggested to switch on the ***Add X-Envelope-To*** option for that account (**<account> – Options** tab). Enter the email address to use. Multiple addresses can be entered, separated by semicolons. You can also use the '...' button to select accounts or groups with a dialog (see the **Select Accounts** section for more information). **Delete mail** The message is deleted, the sender will NOT be notified.
E-mail	Specifies the email address that messages should be delivered to if the ***Forward to email address*** action is selected. Separate addresses by semicolons.
Send information to administrator	If this box is checked, the administrator's account will receive a copy of any message sent to any account that does not exist. *NOTE: This applies only in the case the **Reject mail** option or **Delete mail** is selected in the **Action** field.*



Field	Description
Override global Anti-Spam thresholds	Tick the box if you want to use individual limits for this domain.
Score required to quarantine message	Check this option to have a message quarantined if its spam score equals to or is higher than the value selected. Move the slider to change the value. *NOTE: The Quarantine function must be enabled for this control to work.*
Score required to classify message as spam	Check this option to have a message classified as spam if its spam score equals to or is higher than the value selected. Move the slider to change the value.
Score required to refuse message	Check this option to have a message deleted/rejected (see the **Anti-Spam** – **Reference** – **Action** – *Refuse message action* section for more details) if its spam score equals to or is higher than the value selected. Move the slider to change the value.

Aliases

The **Aliases** tab lets you define multiple domain aliases for existing domains on the IceWarp Server. In the screenshot bellow, you can see aliases defined for ***mycompany.com***. Email messages sent e. g. to ***joe.@mycompany.org*** will be delivered to ***joe.@mycompany.com***. (Provided that this account exists.)

NOTE: For domain aliases defined here you cannot set different rules than for the original domain. If

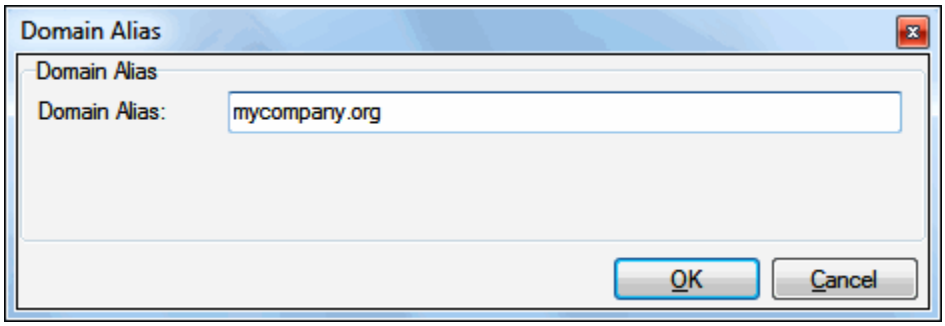
*you want to, create a new domain and on the **Options** tab select the **Domain alias** Type.*

*NOTE: Using domain aliases can cause inconsistence between the address used for verification and address used for delivery. (For more details, see the **Options** tab – **Backup domain** field.)*

*Use the **c_system_services_smtp_rewrite_backup_recipients** API variable. When set to false, domain aliases (used within email addresses) are not rewritten; when set to true, domain aliases are changed to a domain name.*



Field	Description
Add	Click the button to add a new domain alias. The **Domain Alias** dialog opens.
Edit	Select a domain alias and click the button to edit this alias. The **Domain Alias** dialog opens.
Delete	Select a domain alias and click the button to remove this alias.
Arrows	Use these buttons to move an alias up or down in the list.



Field	Description
Domain Alias	Fill in a domain alias of the current domain.

Templates

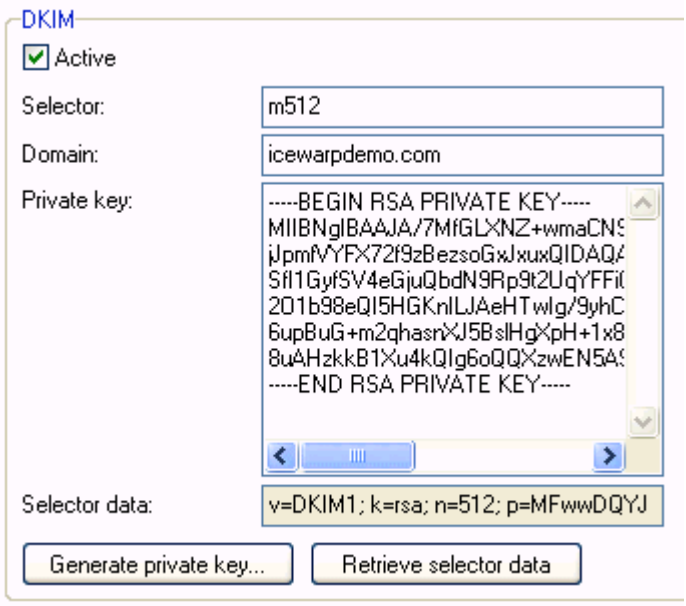
Templates are discussed in the **Global Settings – Templates** section.

NOTE: Templates created within a domain can only be used for new accounts within that domain.

DKIM

"DKIM" stands for DomainKeys Identified Mail. DKIM creates a domain-level authentication framework for email by using public-key technology and DNS record to prove the source and content of a message.

You can find general information about DKIM at ***http://dkim.org/*** and the DKIM FAQs at ***http://dkim.org/info/dkim-faq.html***.



Field	Description
Active	Check this box to enable DomainKeys technology for sending messages from the domain you are defining. *NOTE: The **Enable DKIM** feature in **Global Settings – Domains** must be checked for this option to be available.*
Selector	Specifies the domain key used to sign an outgoing email. There can be only one valid selector at a time.
Domain	Specifies the domain or subdomain for the DomainKeys technology to use. Leave this blank and the actual domain will be used.
Private key	The ***Private key*** that is used by DomainKeys. You can use the **Generate private key** button to create a file containing your private key.
Selector Data	Contains the selector data which contains your public key. Use the **Retrieve selector data** button to populate this field. This field contains the string that should be included in your DNS TXT record. The format of the DNS TXT record is: *<Selector>._domainkey.<domainname> <Selector data>*
Generate private key	Use the button to compute your private key.
Retrieve selector data	Use to generate the ***Selector data*** based on the private key and key length. The selector data contains your public key.

DKIM – How it Works

Sending Servers

There are two steps to signing an email with DKIM:

1. The domain owner generates a public/private key pair to be used for signing outgoing messages (multiple key pairs are allowed).

   The public key is published in a DNS TXT record, and the private key is made available to the DKIM-enabled outbound email server.

2. When an email is sent by an authorized user of the email server, the server uses the stored private key to generate a digital signature of the message, which is inserted in the message as a header, and the email is sent as normal

Receiving Servers

1. The DKIM-enabled receiving email server extracts the signature and claimed ***From:*** domain from the email headers.
2. The public key is retrieved from the DNS system for the claimed ***From:*** domain.
3. The public key is used by the receiving mail system to verify that the signature was generated by the matching private key. A match effectively proves that the email was truly sent from, and with the permission of, the claimed domain and that the message headers and content have not been altered during transit.
4. The receiving email system applies local policies based on the results of the signature test. For example, the message might be deleted if the signature does not match.

Directory Service

This option allows you to have IceWarp Server synchronized with directory service via LDAP protocol. Active Directory or other kinds of LDAP servers are supported. However, we recommend using LDAP server that supports operational attributes *modifyTimestamp* and *entryUUID* such as OpenLDAP. IceWarp Server uses those attributes to identify entity even after email address is changed and to detect change of user data. Without these two attributes only email is left to be used as unique identifier of entity and all user data is processed on each synchronization which can cause serious performance problems. In such cases, synchronization of groupware (user) data should be disabled by setting the *c_system_adsyncdisablevcardsync* API variable to *true*.

IceWarp Server will synchronize on a regular basis and any changes to users within the directory server will be reflected within IceWarp Server. There is a limitation however, IceWarp Server stores most of user properties into its *vCard* handled by groupware, once change is done in *vCard* on IceWarp Server side, the change is preserved during synchronization (attributes in LDIF are not stored in IceWarp Server for the changed entity).

Synchronization schedule is set to every five minutes by default, but can be altered by changing numeric value of the *c_accounts_global_activedirectorysyncinterval* API variable.

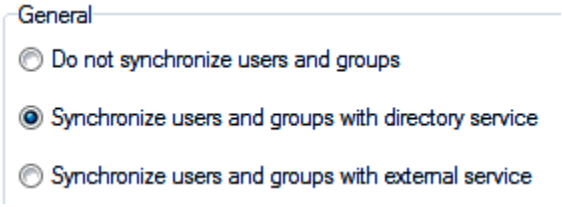


NOTE: This is a one-way synchronization only, directory server to IceWarp Server. If you change user data within IceWarp Server, this change will NOT be reflected on the directory server and IceWarp Server will revert this change to match the state on the directory server. You can still define users within the domain who do NOT exist on your directory server. Such users will not be affected by the synchronization engine.

Exception: There is a way how users synchronized against a directory server can change their passwords via IceWarp WebClient. This option is available for AD and IceWarp Server version since 10.3.0, for generic LDAP servers since version 11.2.0. For more information, refer to the ***Changing Password via IceWarp WebClient*** *chapter.*

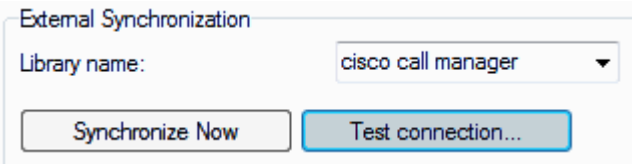
User template will be applied on newly created IceWarp accounts since version 11.3.0

Following options are appeared for Cisco Integration enabled products only. Also when external synchronization library is presented in dedicated folder – *{install_path}/externalsync*. If none from the previous options is your case, **Synchronize users and groups with directory service** check box is available instead of these options. Its functionality is the same as radio button from the picture below - synchronization of users and groups with an AD or other LDAP server.

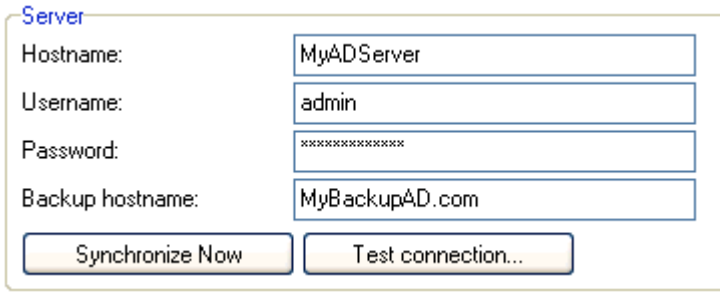


Field	Description
Do not synchronize users and groups	Select this choice if you do not want to synchronize users/groups from a directory server into this domain.
Synchronize users and groups with directory service	Select this choice if you want to synchronize users and groups with an AD or other LDAP server.
Synchronize users and groups with external service	Select this choice if you want to synchronize users and groups from an external source. This choice is available only if there is some external source available. It can be: • You have a license for CISCO integration – this external source is CISCO CUCM in this case • You have installed some ***dll*** allowing the external synchronization

If **Synchronize users and groups with external service** option is selected from the very first set of options, following drop-down list of external sync libraries is shown.

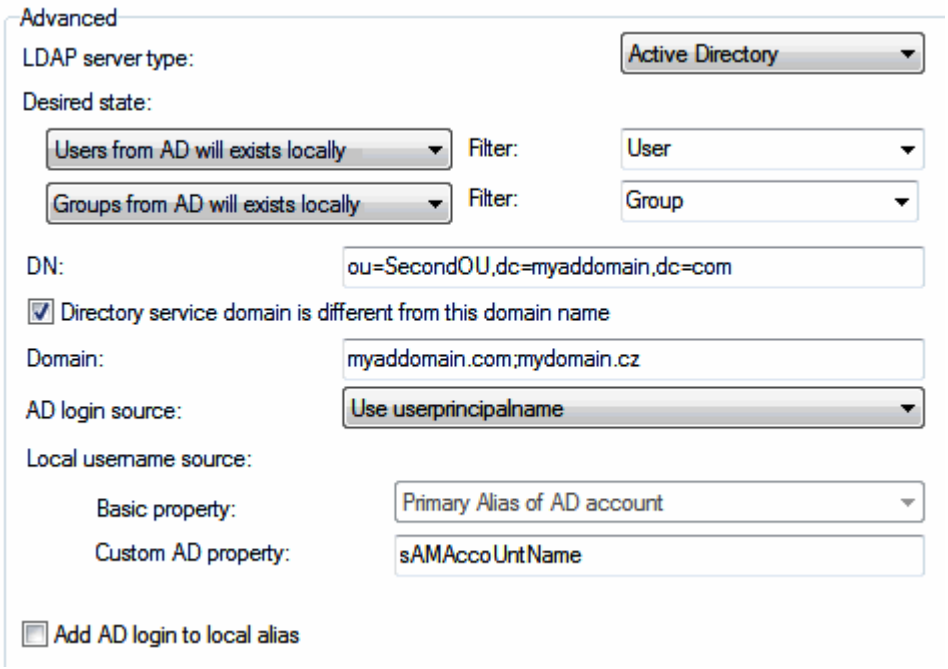


Field	Description
Library name	Select an installed *synchronizaton library* from the dropdown. See the *Synchronize users and groups with external service* feature above.
Synchronize Now	Click the button to synchronize IceWarp Server immedialtely with the specified external server.
Test connection	Click the button to check whether IceWarp Server can access the defined external server. This test will reveal what is returned from your external server to IceWarp Server. Basically, you can check your synchronization settings.



Field	Description
Hostname	Specify the ***Hostname*** or IP address of the directory server. To use LDAP over SSL in combination with ***windows.dll*** and AD, you should use FQDN of the directory server (the same value must be used in CN in certificate of that server).

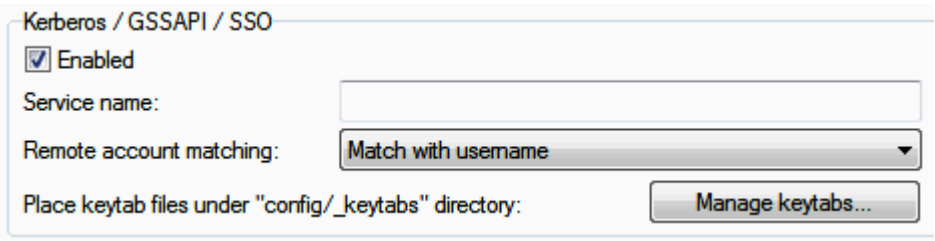
	NOTE: You can force secure communication with the LDAP server by specifying: *ldaps://<your_ldap_server> (port can be specified using the **:port** suffix).* *Example: **ldaps://ldap.icewarp.com:636*** *or **ldaps://182.164.6.24***
Username	Specify a user with access rights to user information on the directory server. User with-read only rights can synchronize itself, however change password functionality require this user to have write allowed rights too.
Password	Specify the password for the user above.
Backup hostname	Specify a backup directory server, if you have one. *NOTE: This setting may cause a problem with user login as IceWarp. It is not capable to store authentication string (user API variable **u_authmodevalue**) longer than 116 characters. Fix scheduled to version 11.5.0.*
Synchronize Now	Click this button IceWarp Server to synchronize the domain immediately with the specified directory server.
Test connection	Click this button to check that IceWarp Server can access the LDAP server. This test will reveal what is returned from your directory server to IceWarp Server. Basically, you can check your synchronization settings.



Field	**Description**
LDAP server type	Select from the list: • *Active Directory* – choose this option for Microsoft Active Directory. • *Generic LDAP* – choose this option for other LDAP servers – e. g. OpenLDAP.
Desired state *(for both users and groups)*	Select from the list: • *Users/Groups will exist locally* – users/groups will be synchronized from a remote server to the local one. • *Users/Groups will NOT exist locally* – users/groups will not be synchronized from a remote server to the local one.

	BE AWARE: If the users/groups were previously synchronized (option was set to *will exist locally*), changing settings to this option would delete them! So the name of this option describes what will happen.
Filter ***(for both users and groups)***	In this field, you can specify the full LDAP filter for users (groups respectively) to be synchronized. The syntax of the filter can be either simple or complex. For simple syntax, just enter the *objectClass* which represents a user (group respectively) on your directory service. E.g. *User* (*Group* respectively) For complex syntax enter the full filter in the syntax supported by your directory service enclosed in brackets. E.g.: *(&(objectClass=inetOrgPerson)(mail=*domain.com*))* E. g.: *(userAccountControl=66048)* – synchronizes users with the given *userAccountControl*. Generally, use the right syntax expression that the directory service (OpenLDAP, AD, atc.) uses for the desired category. See the appropriate RFC. Most typical objects types: *User* – typically used by AD. *Group* – typically used by AD. *inetOrgPerson* – objects typically used by LDAP. (For more information, refer to RFC 2798 – http://www.faqs.org/rfcs/rfc2798.html or to RFC 2254 – http://www.faqs.org/rfcs/rfc2254.html – the later one describes LDAP search filter syntax.) (For more information about this topic, refer to **More Complex Scenario** node, chapter **Sync Accounts from Multiple Email Domains**.)
DN:	This field is intended to be used for more precise control over the domain you access. DN can serve as an additional filter; it defines the scope of what is going to be read from directory server. If you do need to enter anything here then it should be a complete DN, e.g. cn=Users,dc=icewarp,dc=com or dc=icewarp,dc=com for all accounts in all sub nodes. Your directory server administrator should be able to help you with this. BE AWARE: If a large scope needs to be searched, but only a little part of returned objects match sync configuration (usually have desired mail attribute value), then should be appropriate to limit the query results with filter. For more information about this topic, refer to **More Complex Scenario** node, chapter **Sync Accounts from Multiple Email Domains**.
Directory service domain is different from this domain name	Check this option if the domain names in IceWarp Server and your directory server do not match or when the domain used in mail attribute in the directory server does not match domain in IceWarp Server or when both of the former is true. See the **AD Domain Different from IceWarp Server Domain** and **Email Domain of AD Accounts is Different from IceWarp Server Domain** chapters.
Domain	If your LDAP domain name is different from your IceWarp Server domain name, you should specify it here. You can also specify a second AD domain name here, separated with a semi-colon, if required (this is an unusual case, your AD administrator will know whether it is necessary or not). Example 1 IceWarp Server domain = icewarpdemo.com AD server domain = ADDomain email addresses in ADDomain are *@icewarpdemo.com you should enter ADDomain

	Example 2 IceWarp Server domain = icewarpdemo.com AD server domain = ADDomain email addresses in ADDomain are *@mydomain.com you should enter ADDomain;mydomain.com Example 3 IceWarp Server domain = icewarpdemo.com AD server domain = ADDomain email addresses in ADDomain are *@mydomain.com and *@corp.mydomain.com you should enter ADDomain;* See the **AD Domain Different from IceWarp Server Domain** and **Email Domain of AD Accounts is Different from IceWarp Server Domain** chapters.
AD login source	Selects which property is used as a source of login by IceWarp Server onto your directory server. This setting controls what is put into the *u_authmodevalue* variable of a synchronized user:: ▪ **Use userprincipalname** – the authentication value should end with *user@domain*. ▪ **Use samaccountname** – the authentication value should end just with NT user name. ▪ **Use DN** – the authentication string should end with something like CN=TheOne,CN=Users,DC=example,DC=com.
Local username source, Basic property	This setting determines which LDIF attribute will be used by the IceWarp Server as username for IceWarp provided services: ▪ **Primary Alias of AD Account** – alias taken from mail attribute is used ▪ **Login of AD Account** – the selected ***AD login source*** (see above) is used ▪ **CN of AD account** – the common name of directory server object is used
Local username source, Custom AD property	Set a custom LDIF attribute that you want to use as a source for username of accounts in IceWarp Server. Setting a value into this field will override and disable what you set in the *Basic property* dropdown. This field displays content of the *USERNAMEFROMSPECIALFIELD* element of the **syncad.dat** config file. For instance, if you wish to use LDIF attribute description as username in IceWarp Server, type description into this input.
Add AD login to local alias	Tick this box if you want the user's AD login name (only alias – not whole email address if used) to be added to the ***Alias*** field within the **Management – <domain> – <user> – User** tab.



Field	**Description**
Enabled	Tick the box if you want to use ***Single Sign-On*** (SSO).
Service name	Fill in the service name. Its syntax is: ***<site_name>@<ACTIVE_DIRECTORY_SERVER_DOMAIN>*** Example: ***server.icewarp.com@AD.ICEWARPDEMO.COM*** (May be, but need not to be the FQDN or domain of your IceWarp Server instance.)

Remote account matching	Select the way how IceWarp Server users will be matched with accounts in your directory server. ▪ **Match with username** – user's IceWarp Server ***Username*** will be used. ▪ **Match with alias** – user's IceWarp Server ***Alias*** will be used. ▪ **Match with AD user's connection string** – the ***Authentication*** field (when ***LDAP / Active Directory*** selected) will be used. See the **<user> – Options** tab – **Account** department.
Place keytab files under "config/_keytabs" directory	Click the ***Manage keytabs*** button to open a file manager. Into the **<install_directory>/config/_keytabs/** folder, place files with keys generated by Active Directory for individual principals (SMTP, IMAP, POP, XMPP, HTTP) using the ***ktpass*** command. Each file name has this format: ***<principal>#<server_name>@<ACTIVE_DIRECTORY_SERVER_DOMAIN>*** Examples: *xmpp#server.icewarp.com@AD.ICEWARPDEMO.COM* *HTTP#server.icewarp.com@AD.ICEWARPDEMO.COM*

The syncad.dat File

Besides of tags with self-explanatory names, this file (**<install_directory> – config**) includes ones that are not so clear:

<USERNAMEFROMADUSERNAME>1</USERNAMEFROMADUSERNAME> – if enabled (1), account name is imported from attributes ***givenname*** and ***sn***, but only in the case both are not empty and Vcard synchronization is disabled, otherwise the name is determined in a common manner – for more information refer to the **How AD Sync Determines...** section.

<ALLDATADELETION>0</ALLDATADELETION> – if enabled (1), emails and all other account bound data stored on mail storage are deleted when sync mechanism removes an account from IceWarp Server. This setting prevents accidental data loss (not all of them). On the other hand, it comes at a price as the mail storage has to be purged manually.

<VCARDMAP> – feature that allows control over import of LDIF attributes to IceWarp groupware – for more information refer to the **vCard Map Feature** section.

<GROUPSUPPORTREMOTEMEMBERS>0</GROUPSUPPORTREMOTEMEMBERS> – if enabled (1), groups can contain even members whose mail attribute value does not match sync settings (such members would not be accepted as users due to an email address from a different domain). If you want to synchronize a distribution group with email addresses that do not belong to any user synced to IceWarp, this is the option to allow it.

Hierarchical Address Book (HAB)

Synchronization can be configured to convert organization units on the directory server into IceWarp Server groups. These groups can then be a part of HAB. This functionality has to be set manually in the **syncad.dat** file (**<install_directory>/config/**).

There are three nodes to configure:

1. ***<CREATEGROUPSFOROUS>1</CREATEGROUPSFOROUS>***

   This makes the AD/LDAP sync to create groups for all relevant organization units.

   E.g. when the following user is imported into IceWarp:

   dn: CN=Lukas Novak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in – four groups are created automatically: Client, Webmail, Devel and Contacts. Lukas is a member of the Client group. Client group is a member of the Webmail group etc. The Contacts group is the automatically created as the root group.

   NOTE: The alias of the group has to be plain ASCII and unique. In the order to follow this rule, group aliases are constructed as ou=<name>_<id>.

2. ***<GROUPSFOROUSROOT>OU=some unit</GROUPSFOROUSROOT>***

   This option allows skipping of some organization units from being converted into groups. You can specify which organization unit (must be in scope of DN) to use as the root one. Only units belonging under that unit will be converted into groups.

On the contrary to the previous example, setting the root group like as follows:

<GROUPSFOROUSROOT>OU=Webmail,OU=Devel</GROUPSFOROUSROOT>

synchronization of the same user object:

dn: CN=Lukas Novak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in

would cause creation of only two groups – Client and Webmail. The default root folder of Contacts is not created, because we can determine the name of the root from ***<GROUPSFOROUSROOT>***.

3. ***<GROUPSFOROUSROOTNAME>Some name</GROUPSFOROUSROOTNAME>***

This option can override the default name of the root folder.

Examples (all cases require having CREATEGROUPSFOROUS set to 1):

Settings:

<GROUPSFOROUSROOT>OU=Webmail,OU=Devel</GROUPSFOROUSROOT>

<GROUPSFOROUSROOTNAME>Units</GROUPSFOROUSROOTNAME>

User:

dn: CN=Lukas Dvorak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in

Created groups: Units, Client

Settings:

<GROUPSFOROUSROOT></GROUPSFOROUSROOT>

<GROUPSFOROUSROOTNAME>Units</GROUPSFOROUSROOTNAME>

User:

dn: CN=Lukas Dvorak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in

Created groups: Units, Devel, Webmail, Client.

Settings:

<GROUPSFOROUSROOT></GROUPSFOROUSROOT>

<GROUPSFOROUSROOTNAME></GROUPSFOROUSROOTNAME>

User:

dn: CN=Lukas Dvorak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in

Created groups: Contacts, Devel, Webmail, Client.

Settings:

<GROUPSFOROUSROOT>OU=Devel</GROUPSFOROUSROOT>

<GROUPSFOROUSROOTNAME>Units</GROUPSFOROUSROOTNAME>

User:

dn: CN=Lukas Dvorak,OU=Client,OU=Webmail,OU=Devel,DC=icewarp,DC=in

Created groups: Units, Webmail, Client.

Synchronizing Users with LDAP / Active Directory

See also the introductory text within the **Directory Service** chapter.

Paged AD Synchronization

When user AD synchronization is enabled, synchronization is done by pages of 500 users (default value), instead of fetching whole query result content at once.

This is necessary because since Windows 2008 AD does not provide more than 5000 objects a time. It is also better not to deal with huge blocks of data.

- To use this feature on Windows, *Windows LDAP API dll* has to be used – the *c_accounts_global_ldap_usewindowsdll* API variable has to be set to ***true***.
- This feature is also available on Linux, but not on RHEL5 (or CentOS5). All other supported distributions use this algorithm.
- There is no possibility to switch it off directly or set the size of the page.

Who Is Synchronized

Entity which matches a filter is located under defined DN and has its mail attribute in an expected domain filled in. IceWarp Server reads email aliases from these LDIF properties: *mail, otherMailbox, proxyAddresses*.

Values in these attributes with the *SMTP* type defined (prefix SMTP:)are accepted as additional aliases. In the case there is no type specified (no colon char found), synchronization considers whole value as an email.

Example:

otherMailbox: SMTP:john.doe@example.com

otherMailbox: j.doe@example.com

otherMailbox: X509: john@example.com

mail: john@example.com

Parsing LDIF containing such attribute values will result in *john.doe* and *j.doe* as additional aliases of the account with primary alias *john*.

Account can be skipped from synchronization by checking **Exclude from Directory Service Synchronization** check box on user's **Options** tab. With this box checked the account will not be deleted by sync mechanism even if it ceases to match settings or is removed from directory server.

Impact of Filter on Synchronized Entities

Filter value determines which entities will be included in directory server reply, thus changing it will most probably lead to a loss of current accounts/groups and possibly to emerging of new ones. Also deleting the filter, unchecking the *Synchronize users/groups* check box in IceWarp Server older than 11.2.0 or setting *Users/Group from AD will not exist locally* in IceWarp Server 11.2.0 and newer will certainly lead to a loss of all accounts/groups.

If you want to be safe from accidental account data loss while tuning the filter, use *c_system_adsyncmaxdeletethreshold* API variable set to 1 It prevents losing more than one account after filter update. If the change would cause removal of more than one account none is removed instead, if it would cause removal of exactly one account it will be done.

How Entities Are Identified

IceWarp Server recognizes entities via *objectGUID* or *entryUUID* by default. Administrators can even customize this behavior in the **syncad.dat** file. Just add the required alternative property name into the <*guidsource*>node. When no unique id is found, IceWarp Server has no other option left than consider the email address (attribute *mail*)as a unique identifier. In this mode, any change of the email address results in deleting current account in IceWarp Server and creating a new one with a new alias. For more information, refer to the **Personal Data Synchronization** chapter.

How Account Update Is Detected

IceWarp Server uses the *whenChanged* or *modifyTimestamp* attribute to identify updates. The value returned in LDIF is compared to value stored in **adsyncrec.dat** during previous synchronization. If the value is different, a user update is detected and groupware data are read, parsed according to vCard mapping and stored.

Again, administrators can customize which property is used for this in the **syncad.dat** file – the *WHENCHANGEDSOURCE* tag.

If there is no such a property, update cannot be recognized thus vCard data are synchronized every time for every account. This can lead to a serious performance issue with groupware service. In such scenarios, we recommend to turn vCard data synchronization off. It is still possible to enable it for instance once a day. This can be easily scripted as CLI utility **tool.exe** or **tool.sh** can do this for you.

Example

Tool set system c_system_adsyncdisablevcardsync 1



This feature works only if synchronization can recognizes objects with unique identifier other than mail property. For more information, refer to the **How Entities Are Identified** (above) and **Personal Data Synchronization** chapters.

Where Synchronization Keeps its Metadata

The **adsyncrec.dat** file located under configuration directory is used for this. This file serves as a database of *objectGUIDs*, *timestamps* of last modifications, account types etc. IceWarp Server is able to delete orphaned records from this file. If you want to reset synchronization for a particular user, just delete its record from this file (the same applies for a whole domain).

The more accounts, the slower synchronization mechanism you can expect as this file grows up. IceWarp Server was tested with 22.000 accounts successfully, so there is some spare space.

How passwords are managed

IceWarp Server does not know user password until user is successfully authenticated against LDAP server. We support only plain (not hashed) password formats for this action. Once authentication is made, IceWarp caches the password on its side, but any further authentication is still made against LDAP server. Cached copy is a must for IceWarp to be able to handle hashed passwords (sent via mechanisms like CRAM-MD5). Cached copy is stored on server permanently. Such behavior brings a few problems; password can be retrieved on IceWarp side and no service that uses hashed password is working for LDAP authenticated user unless password is known to IceWarp. So let's have a look on how to handle those problems.

To protect passwords from being read, set the *c_accounts_policies_pass_denyexport* API variable to true.

To overcome limitation for hashed password authentication methods is possible only by using plain one first. Note that VoIP service does not support plain authentication method up to current release (11.4.0). VoIP will not authenticate LDAP synced user unless password is known to IceWarp. OutlookSync plugin is capable to overcome this limitation if secure connection to incoming server (**Settings/Login credentials** tab) is configured - since version 11.3.1.5. We plan to implement support for hashed passwords used to authenticate on directory server in future.

Which Library to Use

We recommend using the **windows.dll** library on Windows system. It is not possible to do otherwise on 64-bit builds. But a 32-bit build (especially existing installations) can use the **openldap.dll** one. This library does not support paged results and sometimes is not performing well (broken charsets, 500 objects limit). Switch to the **windows.dll** library can be done by setting the *c_accounts_global_ldap_usewindowsdll* API variable to *true*(restart of control module afterward is required).

How AD Sync Determines User Full Name

Imagine that AD/LDAP sync mechanism uses the following variables:

- *IW_FN*
- *IW_NAME*
- *IW_SURNAME*
- *IW_GIVEN_NAME*

At first, sync mechanism generates vCard according to mapping defined in the ***<vcardmap>*** node of a domain. Sync settings are located in the configuration file – **syncad.dat**. Then, the *IW_FN* variable is filled with the *vCard FN* value, which is, by default,

{displayName}

or

{fn}

retrieved by LDAP. When both are present, the latter one in LDIF wins. If neither of them is defined, FN is empty. Default behavior comes from definition of *FN:$*

{displayName,fn}

in default vcard map. Altering the definition in **syncad.dat** will change the behavior (*displayName* and *fn* are exact names of attributes in LDIF).

IW_NAME is a copy of the

{name}

attribute from LDIF. If it is not present, it remains undefined.

IW_SURNAME is the first semicolon separated item in the *N* attribute of the vCard generated by vCard mapping procedure. By default, this is the LDIF attribute of

{sn}.

IW_GIVEN_NAME is the second semicolon separated item in the *N* attribute of the vCard generated by vCard mapping (the LDIF attribute of

{givenName}

is used by default).

Then *IW_GIVEN_NAME* is checked whether it contains comma. If so, sync check that *N* contains less than four semicolons. If both of the former is true, *IW_GIVEN_NAME* is stripped to be the string before comma (does apply for default vCard map).

Now, when we have these four variables set, let us see the real *U_Name* generation algorithm. It works in two steps.

First step:

- If *DisplayNameFromADGivenName* is set and *IW_GIVEN_NAME* and *IW_SURNAME* are not empty,

  U_Name := IW_GIVEN_NAME + ' '+ IW_SURNAME

- otherwise, if *IW_FN* is not empty

  U_Name := IW_FN

- otherwise, if *IW_NAME* is defined

  U_Name := IW_NAME

Second step:

- If *U_Name* was not filled or is empty string and at least one of *IW_GIVEN_NAME* and *IW_SURNAME* is not empty
  - if *IW_SURNAME* is empty

    U_Name := IW_GIVEN_NAME

  - else if *IW_GIVEN_NAME* is empty

    U_Name := IW_SURNAME

  - else if both are not empty

    U_Name := IW_GIVEN_NAME + ' '+ IW_SURNAME

Basic Scenario

It is assumed in most cases that:

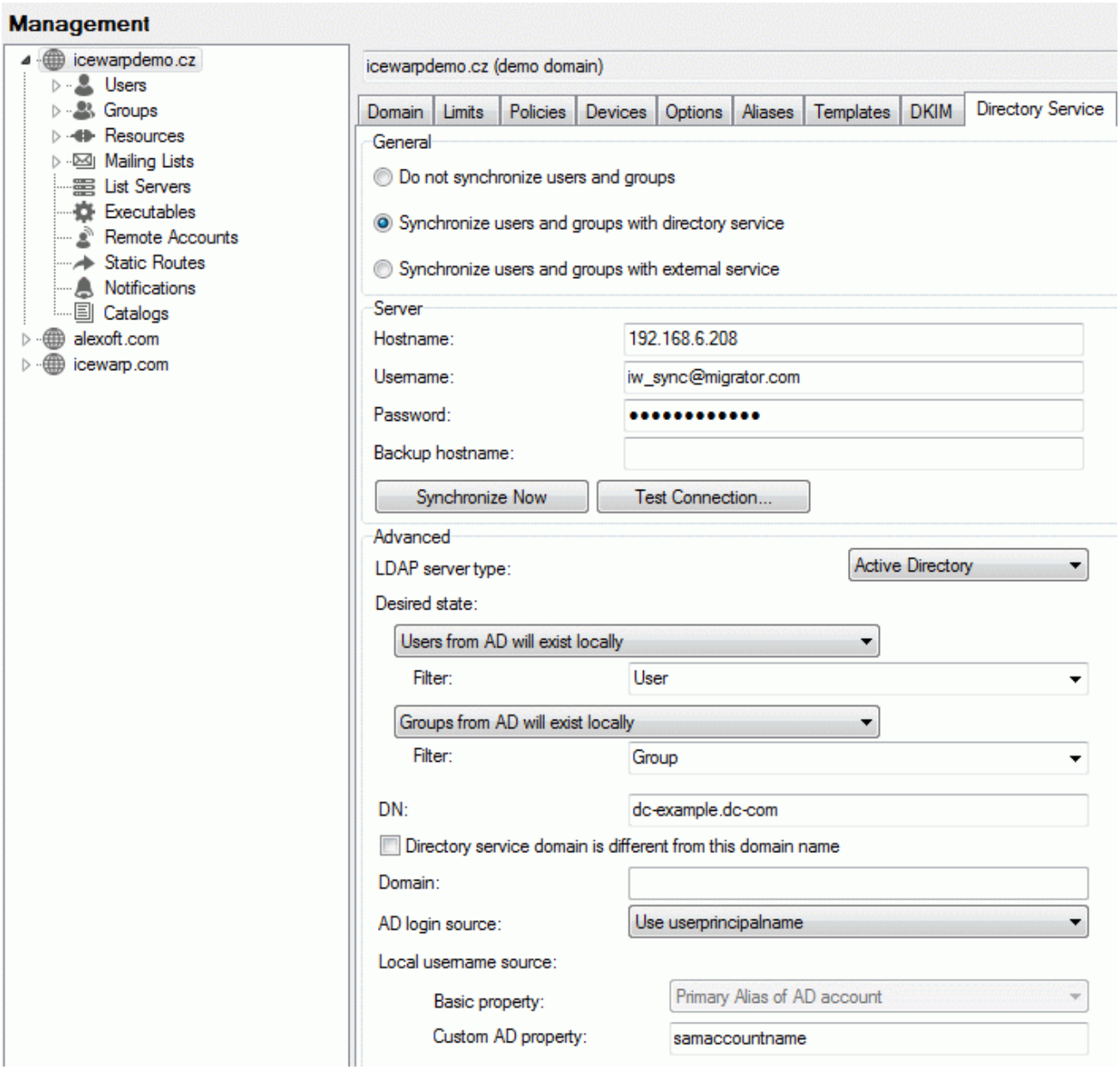
- the domain name in AD matches the domain name in IceWarp Server (not aplicable to generic LDAP servers)
- DN is constructed from domain components (dc) representing a domain existing in both directory server and IceWarp Server; **example.com => dc=example, dc=com**
- objects to synchronize are located in the default location within directory server; that means objects with common name of *Users* in domain components defined in DN in AD or objects located just in DN positioned in generic LDAP server
- objects to synchronize have their mail attributes containing domain part matching the very same domain as hosted by IceWarp Server (mail:john@example.com while there is example.com hosted by IceWarp)
- directory server supports default operational attributes. AD always provide these attributes, but not every LDAP server does

In these cases you only need to setup:

- hostname or IP of your directory server
- credentials of a user who has privileges to at least read entities
- optionally, fill in the backup AD hostname or IP – if there is one – which will be used if the primary connection fails
- LDAP server type according to the one you have
- desire state after sync - whether account and/or groups should exist (be created) after sync one of basic filters from the drop-down list, for basic scenarios the options would be either User (Group respectively) for AD or inetOrgPerson for generic LDAP
- simple DN constructed as was already described above

User accounts created during synchronization have their authetication method (API property *u_authmode*) set to **LDAP / Active Directory** automatically and will be always authenticated against the directory server. IceWarp allows administrator to change this behavior through **user – Options – Authentication**drop-down menu.

Example configuration (use case with AD)



Secure Connection

If you want to connect to your directory server using SSL connection you should use following syntax for the ***Hostname*** specification:

<protocol>://<hostname or ip><:port>

Example:

ldaps://ad.icewarpdemo.com

ldaps://182.164.6.24:636

Connection to the directory server via TLS (*STARTTLS* command) is not supported up to current build (11.4.0.0)

OpenLDAP library (Linux builds)

To establish secure connection when OpenLDAP library (*openldap.dll*) is used, do the following:

1. Modify the LDAP client **config** file (**IceWarp\ldap\ldap.conf**) – append a line containing *TLS_REQCERT never*.

   (This directive forces IceWarp Server to accept SSL certificate even if it is not signed by a trusted certificate authority.)

2. Tell the **OpenLDAP** library where to find this modified **ldap.conf** file.

   IceWarp Server uses **OpenLDAP** libraries. They expect the **ldap.conf** file in a specific path. It is searched for this file in the current working directory of the process that calls it and in the location defined by *LDAPCONF* environment variable.

   The easiest way how to make configuration file available is the environmental variable pointed to default location already mentioned above. In Windows, open **Control Panel/System/Advanced System Settings/Advanced/Environment Variables** and add a new system variable named *LDAPCONF*. Fill in the path and file name as a value of this variable e. g. **c:\Program Files\IceWarp\ldap\ldap.conf** (without quotation marks).

   You need to reload the IceWarp server administration console and restart all modules as well to apply changes.

Windows library (Windows builds)

This library requires AD certificate to be trusted on the machine where IceWarp Server is installed. To establish secure connection with this synchronization library follow these steps:

1. Get a copy of certificate used by AD server. This can be easily done with any third party LDAP browser. If the certificate is not trusted already (no security alert will pop-up) you need to make it trusted. Most probably the issuer will be unknown. You need to get either AD server certificate if self-signed or issuer CA root certificate if certificate was issued elsewhere than on AD itself. Be aware that certificate can appear trustedas it can be imported to the certificate storage of current user, but this is not sufficient for services - see next step.
2. Import the certificate to *Trusted Root Certification Authorities* storage into the scope of *Computer account* on machine running IceWarp Server so even service started under local system account can access it. The way of import slightly differs between server and workstation version of Microsoft Windows. On Windows Server platforms you have to run mmc console (mmc.exe) and add certificate manager to it - you will be able to choose the scope duríng the process.
3. Make sure certificate attribute *cn* and *Hostname* used within IceWarp Server domain directory service match. This is absolutely essential.

.



BE AWARE: 64-bit server builds for Windows cannot use two-way password AD synchronization with the ***openldap.dll*** library. To avoid issues on 32-bit builds for Windows, use the Windows library too. In fact, this library is recommended in all cases, as it can handle more users and performs better in general.

Set the ***c_accounts_global_ldap_usewindowsdll*** API variable to true to use the recommended library. Since version 11.3.0, IceWarp Server use windows library automatically on Windows platforms.

Changing Password via IceWarp WebClient

Users can change their passwords via WebClient (click the avatar in the right-hand top corner – *Options* – *Accounts* – *Change Password*). Since release of IceWarp Server version 10.3.0, the action can be performed although passwords could be stored on an Active Directory server only. Support for generic LDAP servers has been added since version 11.2.0. IceWarp Server sends password value in userPassword attribute and in plain variant only. Therefore despite secure connection (ldaps) is not usually required by generic LDAP. It is a good practice to have it enabled to protect passwords from sniffing as well as restricting access to LDAP server itself as passwords can be easily retrieved from there too.

The way how passwords are sent to directory server is determined from value set in LDAP server type drop-down list.

For password changes, ActiveDirectory requires SSL secured connection (*ldaps://*) by default.

Possible use case scenarios are:

1. IceWarp Server on Windows with *c_accounts_global_ldap_usewindowsdll* set to false – deprecated option.
2. IceWarp Server on Windows with *c_accounts_global_ldap_usewindowsdll* set to true – recommended option for all builds, the only option for 64-bit builds.
3. IceWarp Server on Linux with *c_accounts_global_ldap_usewindowsdll* set to false – the only option.

To allow password update to work for the use cases # 1 and 3, follow these steps:

1. Establish secure connection as described in the previous chapter (**Secure Connection/OpenLDAP library**).
2. Set the secured connection to AD server using the following syntax: ***ldaps://{your_AD_FQDN}:636***, where *{your_AD_FQDN}* is a placeholder for FQDN (must be resolvable on IceWarp Server side) or IP of AD server *636* (sometimes *3269*) – is the default port for secured LDAP communication – may differ on your system.

To allow password update to work for the use case # 2, follow these steps:

1. Establish secure connection as decribed in the previous chapter (**Secure Connection/OpenLDAP library**).
2. Configure *Hostname* in *Directory synchronization* to match AD certificate property *cn* (common name).

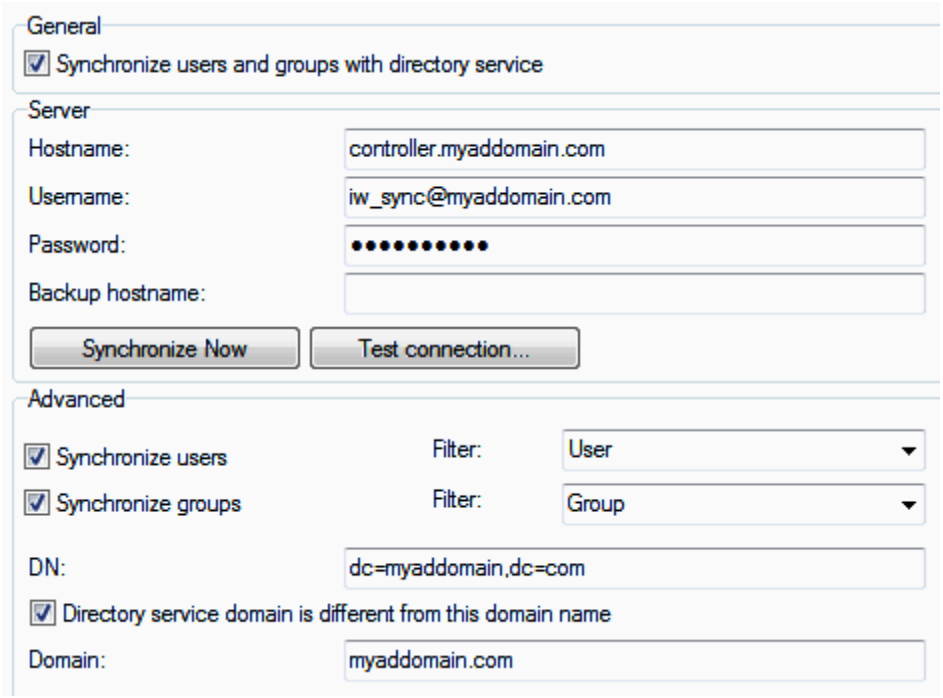
BE AWARE: 64-bit server builds cannot use the **openldap.dll** library. To avoid issues with synchronization, use the Windows library instead – even on 32-bit IceWarp Windows builds as this library can handle more users and performs better in general.

Set the ***c_accounts_global_ldap_usewindowsdll*** API variable to true to use this library. Since version 11.3.0 IceWarp Server use windows library automatically on Windows platforms.

AD Domain Different from IceWarp Server Domain

When the IceWarp Server domain is different from the AD domain (but email domain of AD users is the same as IceWarp Server domain), to set directory services of the IceWarp Server domain, enter the AD domain name into the *Domain* field.

E.g.: In IceWarp Server, you have ***mydomain.com,*** your AD domain is ***myaddomain.com***. Into the ***Domain*** field, specify:

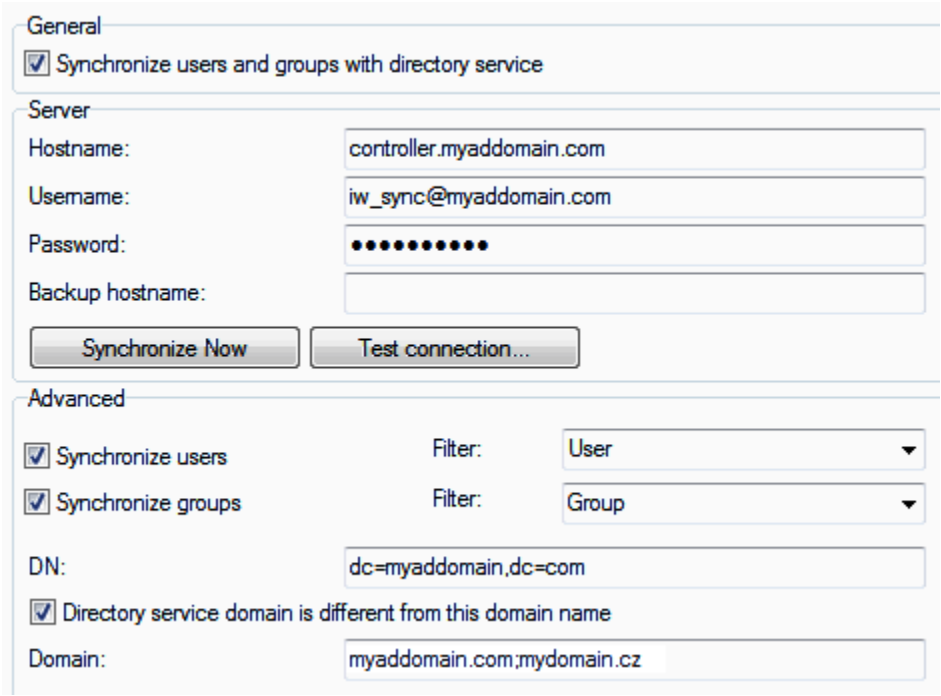


*NOTE: Valuesusedin the fields are to be specified according to your needs – this is an example only. For more details, refer to the **Domain – Directory Service** section.*

Email Domain of AD Accounts Is Different fromIceWarp Server Domain

When the user email in AD has a different email domain, to set up directory services of mydomain.com, you have to use a second parameter in the ***Domain*** field delimited by **;** (semicolon). This setting tells the server from which domain to accept emails during synchronization (only the alias part is taken and used in IW). This type of difference is between domain used in mail attribute and domain in IceWarp Server. The second value in the *Domain* field defines a mapping rule between the domain returned in the LDIF attribute of *mail* and IceWarp domain. This mapping is also applied to any other LDIF attributes IW reads aliases from (currently otherMailbox and proxyAddresses).

E.g.: In IceWarp Server, you have ***mydomain.com,*** your AD domain is ***myaddomain.com*** and user email domain is ***mydomain.cz*** (john.doe@mydomain.cz). Into the ***Domain*** field, specify:



Another example:

In IceWarp Server, you have ***company.com***, your AD domain is also ***company.com*** and user email domain is ***corp.company.com*** (john.doe@corp.company.com). Into the ***Domain*** field, specify: ***;corp.company.com***

*NOTE: The **DN** and **Objects** fields are to be specified according to your needs – these are examples only. For more details, refer to the **Domain – Directory Service** section.*

Email domain conversion feature was improved in version 11.4.0 so it affects all email addresses stored in groupware too.

Another improvements include also possibility to convert all email domains recieved in LDIFs to IW domain. To do this, you have to fill in * instead of particular domain into the Domain input.In this configuration scenario, complex LDAP query (filter) might come in handy. Such use case is covered in **More Complex Scenarios** chapter - **Sync Accounts from Multiple Email Domains** article.

More Complex Scenarios

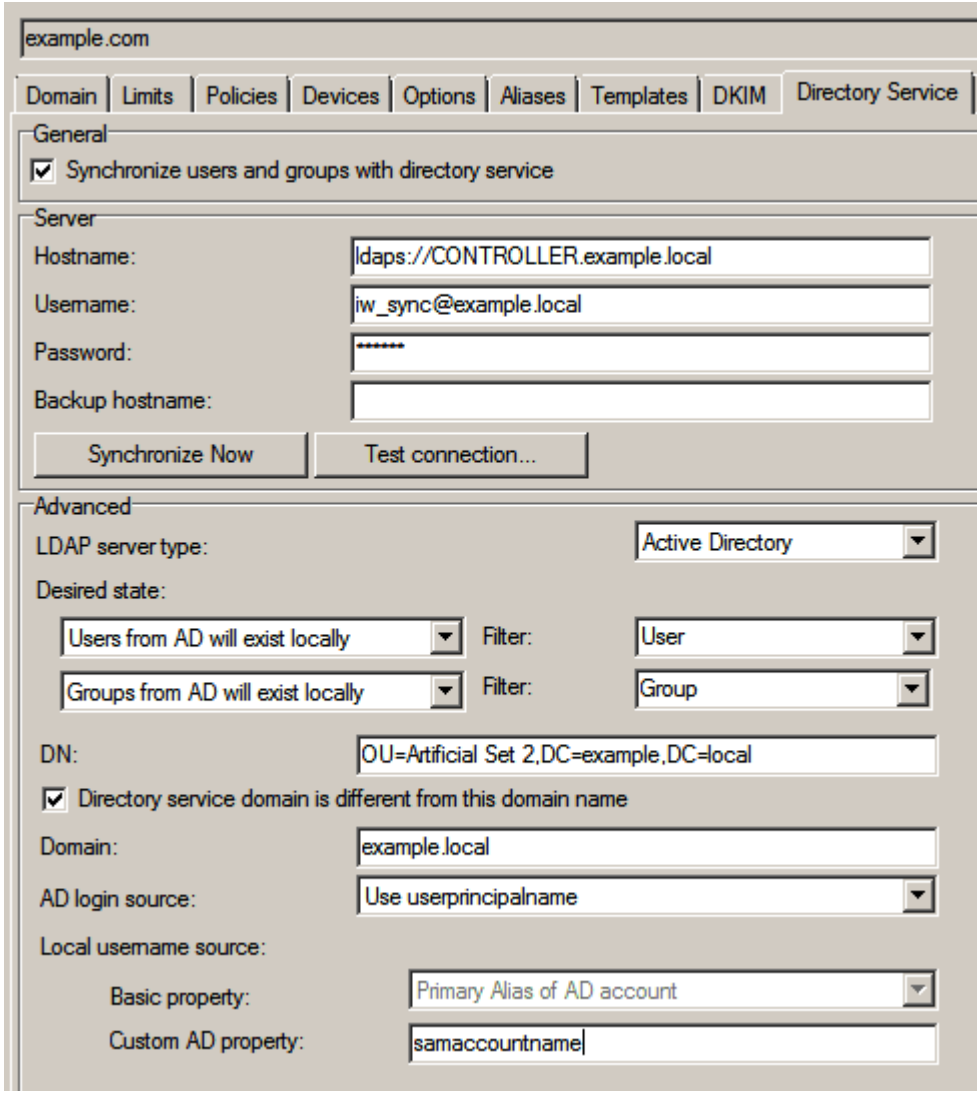
Directory server can of course contain data in more complex structures than assumed in the **Basic Scenario** chapter. When it comes to more complex scenario DN input as well as other options in configuration come handy. Let us have a look on some more complex configuration use cases.

Sync particular DN

It is pretty common that users meant to be synced to IceWarp Server (IW) are located in a special organizational unit (OU) on the domain controller (DC) or directory server. If that is the case, DN of the location must be filled in DN input in configuration. IceWarp Server will synchronize all object included in the OU (and other nested OUs) matching other configuration settings. If objects should be pulled from more OUs on the same level in the directory hierarchy DN must be set that it would allow reading both of those OUs. Usually that means that more than just desired OUs is sent to IceWarp, if that is the case filter can be used to filter out unwanted objects. However setting filter might not be necessary as missing or unsuitable mail attribute can do the same job. Please, check out example configuration for further information.

Example Configuration

Enclosed example describes a configuration for setup where the DC domain is *example.local*, IW domain is *example.com* and users/groups are located in the *Artificial Set 2* OU. IW will log on to DC using the *userPrincipalName* attribute while users will use their sAMAccountName to log on to IW services:



Sync One Account to Multiple IceWarp Domains

Synchronization mechanism can handle uncommon use cases where same object is required to be synced to multiple IceWarp domains (usually two of them). This is easy to achieve as configuration of each domain would fit into scenarios described in the **AD Domain Different from IceWarp Server Domain** and/or **Email Domain of AD Accounts Is Different from IceWarp Server Domain**.

Excluding Accounts Disabled on AD from Synchronization

IceWarp does not reflect disabling of an account in ActiveDirectory as even disabled account is returned in basic LDAP search query response. That is obvious as disabled account basically remains the same – only disabled flag bit of the *userAccountControl* attribute is toggled. Synchronization mechanism itself does not parse or understand this attribute. It means that disabling an account in AD will not disable the account on the IceWarp side. However, a filter can be effectively used to exclude disabled accounts from LDAP search query response. Accounts present in IceWarp that cease to be returned from AD (due to filter update), will be deleted (mail storage is preserved by default, this behavior is controlled by the ALLDATADELETION node in the ***config/syncad.dat*** file). In order to query individual bits of the *userAccountControl* attribute we can bitmask it – there are special matching rules to do that (to learn more about these see https://msdn.microsoft.com/en-us/library/aa746475%28v=vs.85%29.aspx). In our particular case, we want to bitmask *userAccountControl* on two which would be written in the filter query syntax as: *userAccountControl:1.2.840.113556.1.4.803:=2*.

Of course, this must be negated as we want to exclude all disabled entities that match this statement.

In practice, filtering out disabled accounts can be written as follows:

(&(objectCategory=person)(!userAccountControl:1.2.840.113556.1.4.803:=2))

Unfortunately some Linux platforms may consider filter with id matching rule as invalid, therefore it will not work. You will have to find a suitable solution.

Sync Accounts from Multiple Domains

Synchronization configuration offers possibility to use * to accept any object that have mail related attribute defined regardless the domain part value. This is handy when there are various email domains used inside the organization, but everyone should have public email address in single IceWarp Server domain. Such use case has usually **2 typical scenarios**:

1) All objects are located in the same container like one OU so scope of DN limits results by itself. In this case, simple filter can work (as DN is already restrictive enough). However it may be required to synchronize only several email domains instead of all of them. This would require limiting LDAP search query results with a more complex filter based on mail attribute value.

2) It may be required to sync object from multiple containers so DN scope itself is not enough to limit search query results. In this case query response usually contains many objects that are not relevant or desired for sync. The only option left to remove unwanted objects from response is more precise query defined in filter input.

Shortening response by filter positively affects performance too as sync mechanism does not have to handle objects with incorrect mail attribute value, also size of AD synchronization logs gets reduced.

Example:

Case 1:

Single OU (ou=mail users.dc=corp.dc=example.dc=local) contains user accounts with email address from different domains (corp.example.local.example.com, example.net), but we want to have objects using only 1 of the domains (example.com) in mail attribute.

DN: ou=mail users.dc=corp.dc=example.dc=local

AD: (&(objectClass=inetOrgPerson)(mail=*@example.com))

Case 2:

Multiple OUs (ou=icewarp.dc=example.dc=local) should serve as a source of objects to sync. User accounts with mail attributes with domain part from particular domains (example.com or example.net) are desired.

DN: dc=example.dc=local

AD: (&(objectClass=Person)((|mail=*@example.com)(mail=*@example.net)))

Personal Data Synchronization

Personal data (phone numbers, addresses, images, emails, etc.) are involved into synchronization with a directory server. These data areobtained from directory server during the first synchronization and (after it) every time change is detected on AD/LDAP side (explained inSee "Synchronizing Users with LDAP / Active Directory" on page 27chapter, **How Account Update Is Detected** article). These data are stored into groupware in a way that is by vcard map defined (explained in **vCard Map Feature** chapter). When a users changes their personal data (after the first synchronization) on the IceWarp Server side, their data are no longer synchronized. This is because a local change would get overridden by data from the directory server. As already mentioned, IceWarp Server does not propagate the change to LDAP/AD. For more information refer to the **Limitations** article.

To restore data synchronization, delete the appropriate user row in the **config/adsyncrec.dat** file.

Example:

jdoe@space.com;SQECoeoqbEShnKME2rdJrg==;20110616110044.0Z;20110620T134034Z

Synchronization consists in replacement of data on the IceWarp Server side with those from AD/LDAP.

Where aliases are taken from

Sync mechanism recognizes **3 attributes** as a source of alias:

1) Mail

2) otherMailbox

3) proxyAddresses

Of course, if **Add AD login to local alias** is enabled, alias is also taken from attribute which serves as AD login source (usually userPrincipalName).

If one of three default attributes carrying suitable value (domain part) is found, processed object is added or synced to IceWarp Server domain. One may not like this as even objects with empty mail attribute can be accepted by IceWarp. If this is the case, define filter that would require non-empty mail attribute **– e.g.** *mail*=*@*.

Removing alias source from object on directory server will lead to removal on IceWarp Server's side as well. Manually added aliases are untouched by sync mechanism.

Limitations

Full functionality requires that operational attributes are included in object's LDIF provided by directory server – particularly *objectGUID* or *entryUUID* (both are default ones and can be customized) is necessary for proper identification of object and enables further functionality. That is a possibility to detect object update made on directory server. Default operational attributes used to read modification time from is *whenChanged* (AD) or *modifyTimestamp* (generic LDAP).

For customization and more information refer to theSee "Synchronizing Users with LDAP / Active Directory" on page 27 chapter, articles **How Entities Are Identified** and **How Account Update Is Detected**.

When there is no unique identifier (other than mail attribute) provided personal data get always (each sync processing) synced overriding local (IceWarp side) changes. When there is a way to identify object, while attribute to detect change is missing local change is preserved, but each sync process even groupware data (which is not recommended, explained in**How Account Update Is Detected** article).



*NOTE: To ensure this works properly, you have to check existence of the **objectGUID** and **whenChanged** attributes within the LDIF export from AD or **entryUUID** and **modifyTimestamp** for LDAP.*

*NOTE: To disable personal data synchronization, use the **C_System_ADSyncDisableVCardSync** API variable. If set to 0 (zero), only basic account properties are synchronized. This action is recommended to solve groupware service performance issues when synchronizing against directory servers with no equivalent of whenChanged and/or objectGUID.*

For information on synchronization of users' photos, refer to the **User Accounts – User** – ***Photo*** field.

vCard Map Feature

This directory service synchronization feature allows administrators to define mapping of LDIF attributes to groupware ones.

The **config/syncad.dat** xml file includes the ***<VCARDMAP>*** element that contains mapping description. When an administrator sets directory service for some domain, this element is filled with the default mapping. Lines in the definition MUST be terminated with CRLF. If this conditions is not fulfilled, the sync mechanism will not work properly and can delete users as they will seem to be missing email address.

However, it is possible to edit this file manually to change the default behaviour and specify own synchronization rules. This can be done on domain basis, because the ***<VCARDMAP>*** element exists for each domain. Should the configuration parsing error occur, it is logged to the error log and default synchronization rules apply. You can revert back to the default by deleting the whole ***<VCARDMAP>*** element and saving the synchronized domain again.

The content of the ***<VCARDMAP>*** element is in versit-like format, each line contains a rule in the following form:

VersitItem:LDIFAttribute

A versit for each user is created using these rules and then stored in groupware using the *SetMyvCard* method call.

LDIFAttribute can contain either text, which is directly used, or variables. The form of variables is in general:

${VARIABLE_NAME}

- In the simplest form, *VARIABLE_NAME* just equals to LDIF name, so it can be for example:

  ${title} or ${wwwhomepage}

  Names are case insensitive. As an example, the whole line can be:

  URL:${wwwhomepage}

  This will place *wwwhomepage* read from AD to URL item in user's versit.

- If no *wwwhomepage* exists in AD, previous example results in:

  URL:

  This can be prevented by adding an exclamation mark after opening curly bracket:

  URL:${!wwwhomepage}

  This will expand to nothing, in the case no *wwwhomepage* (for this user) exists in AD and it will behave like before when it is there.

- More variables can be used on one line mixed with strings. In this case exclamation marks apply to whole line. For example:

  N:${!sn};${givenName}

  - will expand to *N:sn;givenname*, when there are both *sn* and *givenname* in AD
  - will expand to *N:sn;*, when there is no *givenname* in AD
  - will expand to nothing, when there is no *sn* in AD, regardless of *givenname* existence

- When the item is in LDAP form, like:

  manager: CN=John Doe,CN=Users,DC=icewarp,DC=com

  and you need just *cn* to be used, you can extract LDAP attribute from the value using this syntax:

  X-MS-MANAGER:${manager[cn]}

  Of course you can use any LDAP attribute in solid brackets.

- Sometimes there is a situation, when more LDAP items apply to one GW item. You can specify alternatives by separating them by comma within the *VARIABLE_NAME* part. Example:

  FN:${displayName,fn}

  - will expand to *FN:displayName*, when there is only *displayName* in AD
  - will expand to *FN:fn*, when there is only *fn* in AD
  - will expand to two lines:

  FN:displayName

  FN:fn

  when both *displayName* and *fn* exist (see the next paragraph to know, what to do with that)

  - will expand to *FN:*, when there is neither *displayName* nor *fn* in AD. You can of course use exclamation mark to skip this line in this case:

  FN:${!displayName,fn}

- Sometimes you do not want to expand each alternative in the list, you just want to expand one. For this behaviour, you should use | symbol to separate items in the list. The first item has highest priority in this case. For example:

  FN:${!displayName|fn}

  - will expand to *FN:displayName*, when there is only *displayName* in AD
  - will expand to *FN:fn*, when there is only *fn* in AD
  - will expand to *FN:displayName*, when there are both *diasplayName* and *fn* in AD
  - will expand to nothing (will be skipped), when there is neither *displayName* nor *fn* in AD (because of the exclamation mark)

NOTE: When you use more alternative lists separated by commas in one line, it will expand to all possible combinations.

For example:

ADR;TYPE=WORK:;;${streetAddress,street};${location,l}

will expand to four lines, when there are all four properties in AD.

If you want to have the ***$*** literal in some item, you have to write it twice in the map, i.e

MONEY:100$$

See the default ***<VACRDMAP>*** content in the **syncad.dat** file for more examples.

Troubleshooting

Connection

In the order to test that connection is working on Windows, you can use tthe **ldp.exe** tool which can be downloaded free from Microsoft.

If the above is not applicable, use Wireshark. It could be also useful to try the connection with some kind of LDAP browser.

Response from Directory Server

It is possible to learn what is returned from the directory server by pressing the *Test connection* button in the IceWarp Administration console. If there is no result or the result is not what you intended, than your configuration is not correct. Check DN.

Users Are Not Synchronized

This issue is most probably caused by the value in the *mail* attribute. Again, use the *Test connection* button to check what is returned from the directory server and how IceWarp Server handled entities from the response. The domain used in the *mail* attribute must either match IW domain or mapping must be set in the *Domain* field (for more info see the **Email Domain of AD Accounts Is Different from IceWarp Server Domain** chapter).

Another reason can be that the domain on the directory server is not the same as the one in your IceWarp Server. In such a case mapping must be defined in the *Domain* field (see **AD Domain Different from IceWarp Server Domain** chapter).

After synchronization is performed, you have to refresh Administration console by pressing F5, otherwise results will not be visible (users and/or groups added by the synchronization will not be visible).

Starting from Scratch

If something went wrong and you wish to revert to the initial state, do the following:

- stop the **Control** service, erase/move the **adsyncrec.dat** file
- clear settings within the ***Directory Service*** tab for the domain
- start the **Control** service

Account Disappeared

The **config/syncad.dat** xml file includes the ***<VCARDMAP>*** element that contains mapping description. When an administrator sets directory service for some domain, this element is filled with the default mapping. IceWarp Server prior release of 11.3.0. required lines in the definition terminated with CRLF. If this condition is not fulfilled, the sync mechanism will not work properly and can delete users as they will seem to be missing email address.

Best Practices

Which Library to Use

We recommend using the **windows.dll** library on Windows system. It is not possible to do otherwise on 64-bit builds and/or releases since 11.3.0. But older 32-bit builds (especially existing installations) can use the **openldap.dll** one. This library does not support paged results and sometimes is not performing well (broken charsets, 500 accounts limit). Switching to the **windows.dll** library can be done by setting the *c_accounts_global_ldap_usewindowsdll* API variable to *true*. You have to restart the ***Control*** service after the API variable change to apply changes!

AD Login Source Is Set to DN or Is a Longer String

Such a case can cause a problem of endlessly detected update of users with login longer than what can be stored in a user file (the *u_authmodevalue* property has 116 characters limit), thus we encourage administrators to migrate users into a database which can contain much longer strings than binary structure in the user config file.

General Upgrade Recommendations

In order to prevent loss of account(s), set the *c_system_adsyncmaxdeletethreshold* API variable to ***1***. This will prevent AD synchronization mechanism from deleting anything in the case more than one account would be erased after synchronization.

Even though accounts would disappear from IceWarp Server Administration console (due to deletion), their mail storage remains unaffected unless the ***<ALLDATADELETION>*** node is set to ***1*** in the **syncad.dat** config file. Thus it is wise to set this node to ***0*** before the upgrade procedure.

Upgrade from Version Older than 11.1.0

It is recommended to review directory service configuration settings as there were improvements made – especially, to check how users/groups are recognized and filtered (LDAP query). IceWarp Server will attempt to parse your current configuration into a new style automatically. However, manual correction may be needed.

Upgrade to Version 11.3 and newer

There are some changes regarding our integrated OpenLDAP server and client:

Client

Untill now, 64-bit Windows IceWarp Server used the Windows LDAP library, but on 32-bit administrators could set the *C_Accounts_Global_LDAP_UseWindowsDLL* variable to ***false*** and then the OpenLDAP client library was used.

Since version 11.3, the *C_Accounts_Global_LDAP_UseWindowsDLL* variable has no effect. Windows LDAP library is always used on Windows (and OpenLDAP on Linux).

Server

New V 11.3 installations:

- OpenLDAP 2.4.38 will be installed
- When LDAP server logs are enabled, they will go to the IceWarp Server log directory (the ***slapd.conf*** file). It is not rotated/marked with timestamp as of now.

Servers that were upgraded to V 11.3 from older versions:

- Ancient OpenLDAP server 2.2.29 will be left there
- LDAP tools that crashed will be replaced with newer versions

It is not possible to perform a simple upgrade, because the LDAP database changed its binary format between these two versions (there is a 10 year gap). It would be dangerous to upgrade user's LDAP servers automatically – there can be some peculiar configuration.

Find details of needed upgrade steps further:

1. It is a good idea to stop all IceWarp Server services and *config* before performing the migration. As the absolute minimum, stop the LDAP server and check that Windows LDAP dll is used – not OpenLDAP.
2. Export the database content to *ldif* running this command in the *ldap* directory

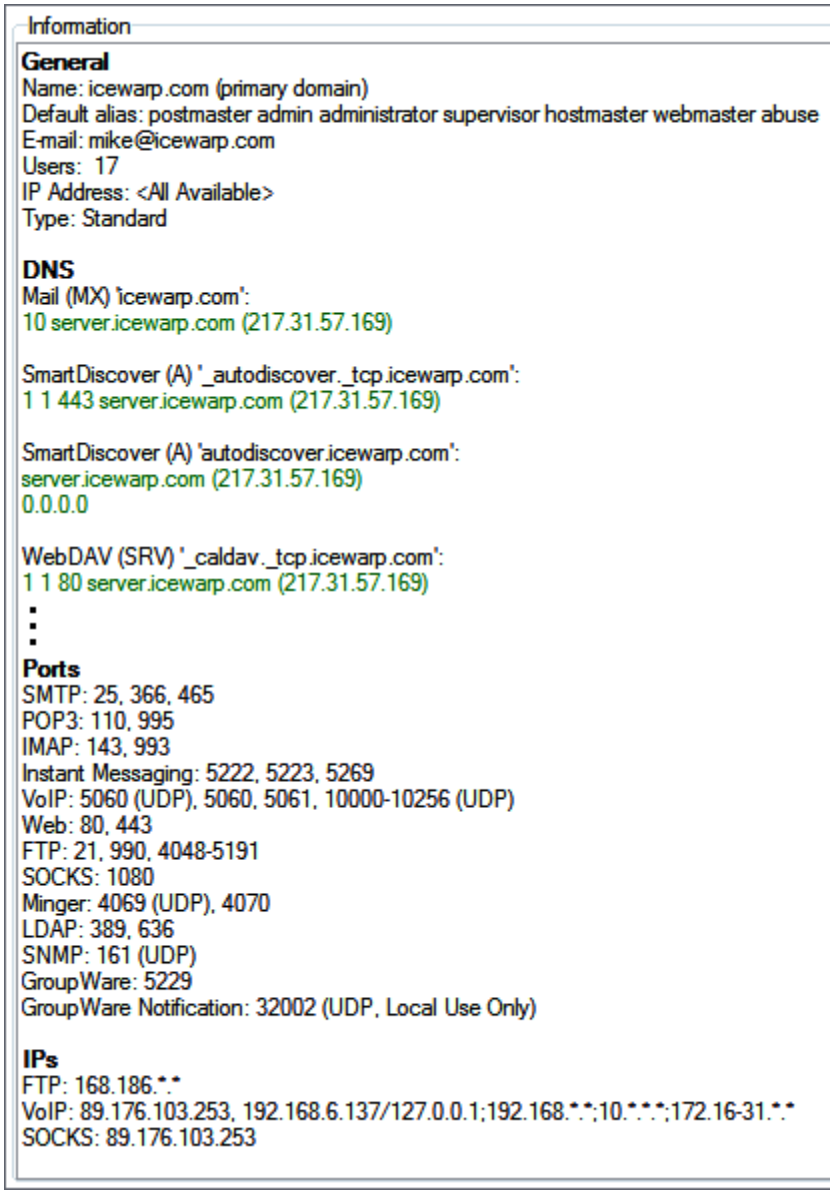
   slapcat.exe -l backup.ldif -f slapd.conf
3. Then copy the *backup.ldif* file to some safe place.
4. If you did some modifications in the *slapd.conf* file, copy it to the some safe place.
5. Delete the *ldap* subdirectory from IceWarp Server installation directory.
6. Run the IceWarp Server installer. It need not to be an upgrade one, the same version like the already installed will suffice. Note that this will stop IceWarp Server services temporarily.
7. After installation, copy *backup.ldif* to the newly created *ldap* subdirectory.
8. If you backed up also the *slapd.conf* file, merge it with the current *slapd.conf*. The merge would not be difficult, there were not so many changes, most of them are just comments.
9. Delete the *ldap*\ directory data.
10. Run the following command:

    slapadd.exe -l backup.ldif -f slapd.conf
11. Start the LDAP server.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Information



The **Information** tab displays summary of general information about the selected domain, as well as information about its DNS records and running services ports (both TCP and UDP ones plus port ranges). NOTE: When using a remote console to connect to other IceWarp Server, it uses the remote console's DNSes (specified in IceWarp Server) to show information within the **Information** tab of a domain. It also considers your outgoing IP address to be the one of the machine running this remote console.

This tab can help you to configure all settings needed for smooth server running.

The information shown is self-explanatory. Green lines represent properly set records, while red ones announce missing configuration.



NOTE: The number of accounts shown here includes only user accounts.

*For more information about service ports, refer to the **System Node – Services – Service Ports** chapter.*

User Accounts

User accounts are the most common accounts on the IceWarp Server.

All accounts are defined within a domain and an email address consists of a user name and domain one – ***[user]@[domain_name]***.

Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.

User



Field	Description
Alias	A unique identifier for the account within this domain. This alias becomes part of the user's email address. Example: Entering an alias of Support into domain of MyDomain.com would give this user an email address of Support@MyDomain.com ***Multiple aliases*** can be used by separating them with semi-colons: e. g. ***support;help;bugs;info*** – meaning that messages to any of these accounts will be delivered to this one mailbox. *NOTE: Maximal length of this field is limited to 255 characters. If you want to use more aliases, you can use a pattern.* *Syntax:* ***Alias: <primary_alias>; <[pattern_name]>*** *E.g.:* ***Alias: support; [support_aliases]*** *For more information, refer to the* ***System Node Reference – Advanced – Patterns*** *chapter.*
Phone #	Here you can enter the number for the user's unique SIP phone, if he/she has one. Multiple phone numbers are supported, delimited with semi-colons.
Username	This is the IceWarp Server identification name of the mailbox, which is used for authenticating access to IceWarp Server services unless authentication is set to the ***Users login with their email addresses*** (**Policies – Login Policy**) – in this case ***Alias*** is used (plus the appropriate domain is added). ***Username*** is usually the same as the ***Alias*** of the account, but does not have to be. *NOTE: Regardless of the previous information, EAS always uses alias (plus* ***@<domain>****)*

	as username. *NOTE: It is recommended not to use whole email addresses as usernames. In the case you want to rename a domain, you have to change domain parts of addresses manually or use SQL manager to perform mass changes.*
Name	The user's real name or an identifier of the account. This field is used by WebClient and can be changed there (**Tools – Accounts – Primary – Name**). It is the ***FROM*** header shown to users that receive emails from WebClient.
Description	Enter account description. This can also be seen/changed in WebClient (**Tools – Accounts – Primary – Description**).
Password	The password for the mailbox.
The **:** button	Press this button to let IceWarp Server generate a random password for you. IceWarp Server will generate a password according to the password policy, if you have one defined under **Domains & Accounts – Policies – Password Policy**.
Permissions	Click the button to set access rights for the account where emails are forwarded to. It is possible to set rights for either whole email account or selected folders (e.g. Inbox, Contacts, Calendar, etc.). For detailed information on permissions, refer to the **GroupWare – Reference – Public Folders – General – Permissions Tab** and also see bellow.
Photo	Click the field to reveal the **Open** dialog and insert a user's photo. *NOTE: This photo (as well as one in the IW **WebClient – My Details** dialog) can be synchronized from a directory server. In this case, the figure is expected to be stored within the LDIF attribute of **thumbnailPhoto** (AD default) in the JPEG format. (Other formats supported by AD – e.g. PNG – are not fully supported by IceWarp Server, though WebClient can display them correctly.)*

For more information about personal data synchronization with AD/LDAP, refer to the **Domain – Directory Service – Personal Data Synchronization** chapter.

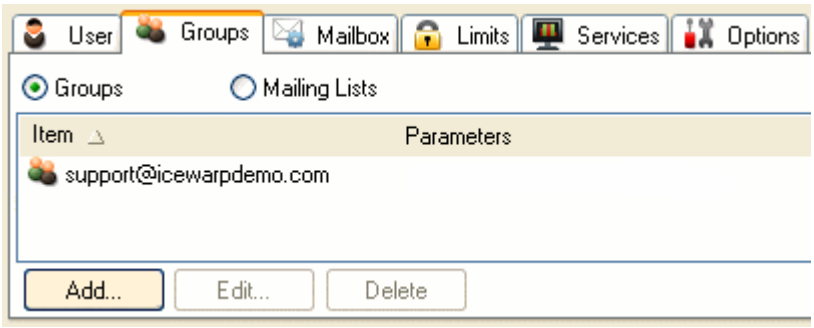
Permissions

Access Right	**Description**
Lookup	basic right just to see folders (not to see items); this allows users to open subfolders they have been given access to
Read	right only to read messages
Keep Seen Flag	right to mark messages as read
Write	right to set or clear flags other than seen and deleted
Insert	right to insert a new email message
Post	right to send an email via SMTP
Create	right to create a new mailbox
Delete	right to delete messages
Expunge	mails can be removed from a folder (Inbox, Sent, ...) and sent to **Trash** for example versus deleted at all; this right allows final deleting of mails
Delete Mailbox	right to delete a mailbox
Administer	full rights

Groups

The **Groups** tab displays a sortable list of all groups or mailing lists that this user is a member of.

Select one of the radio buttons – ***Groups*** or ***Mailing Lists*** – to see the appropriate list.

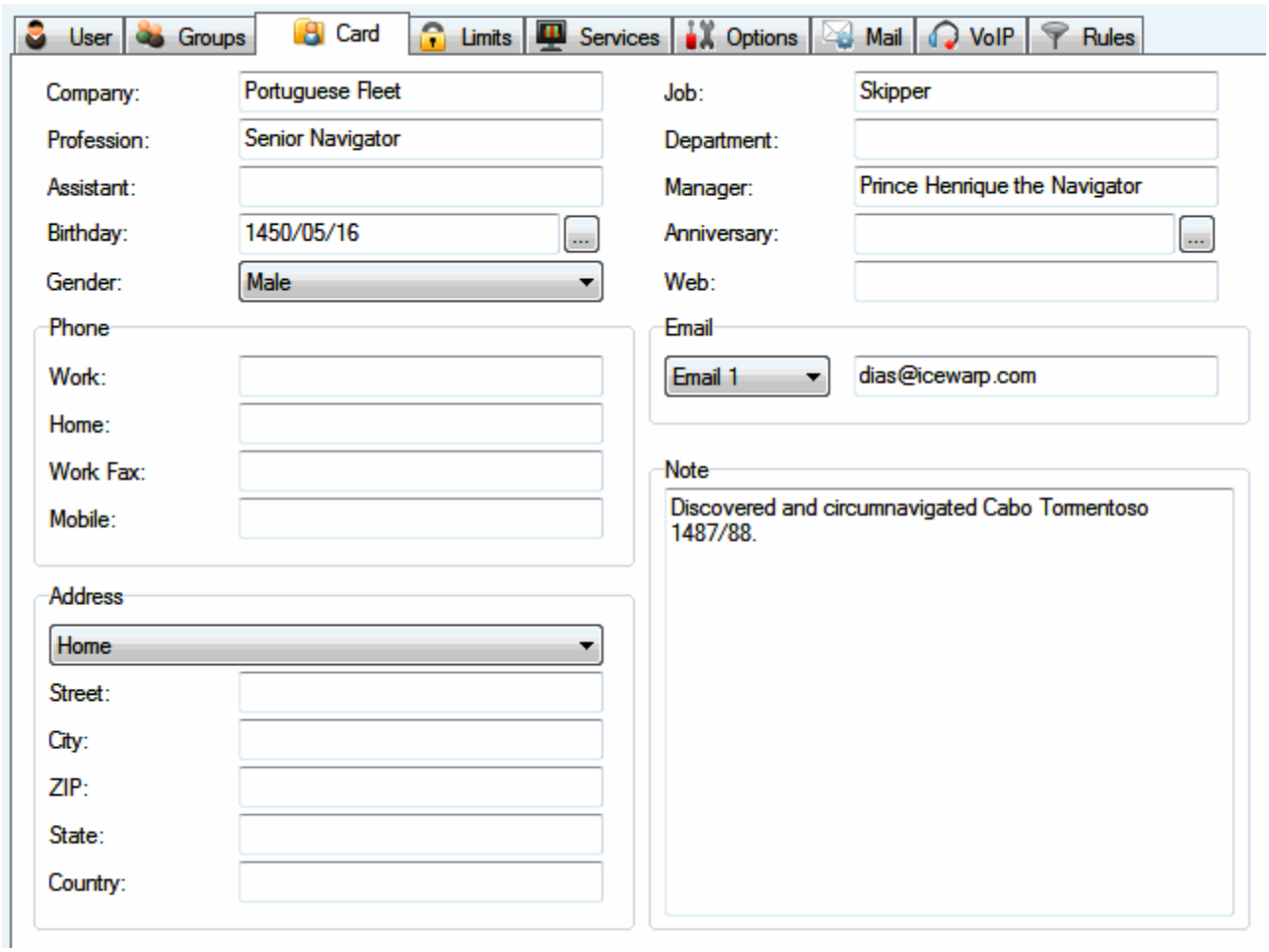


Button	Description
Add	This button allows you to add groups or mailing lists via the **Select Item** dialog.
Edit	Select a group and click the button to modify settings.
Delete	Select a group and click the button to delete this group from a list.

Card

This tab allows you to summarize user's personal information. As this feature is integrated with GAL, all data presented here will be shown also within the user's GAL contact.

If LDAP (or AD) synchronization is set, personal data from LDAP/AD are imported here. Use the ***C_System_ADSyncDisableVCardSync*** API variable to change it: 0 – all data are shown, 1 – just user name and password are synchronized.



Fill in the appropriate fields – all of them are optional ones. Their labels are self-explanatory.

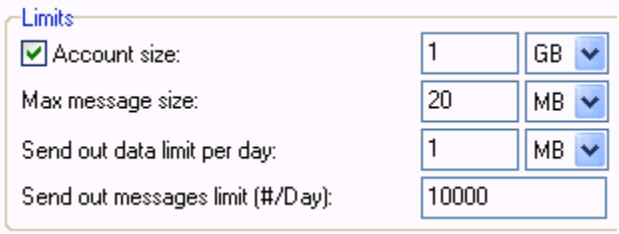
Choosing the ***Address*** type (***Home/Work***) allows you to insert, save and lately show both addresses. The same mechanism you can use for up to three email addresses.

For more information on vCards settings, refer to the **GroupWare – Sharing Concepts – Miscellaneous** chapter.

Limits

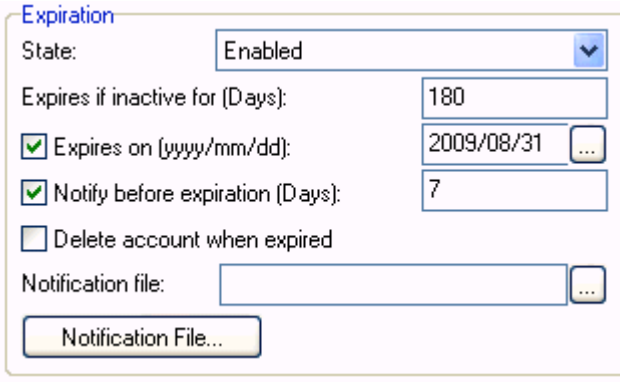
BE AWARE: The following limits do not override any domain-level limits that are set.

However, if they are set to a non-zero value, they do override any domain-user limits.



Field	Description
Account size	Limits the size of a user's account. Both email messages and groupware items are included in this limit.

	Enter a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. Once exceeded no further messages will be accepted for that user. *NOTE: If the box is ticked, zero values override domain-user limits (of account size) and mean that the account has unlimited disk space available. If not ticked, values are inherited from a domain level (**<domain> – Limits – Users – Account size**).*
Max message size	Limits the size of ANY message SENT by a user. Enter a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. It is also possible to enable checking of user size limits of incoming messages using API and setting ***C_Mail_SMTP_Other_IncomingMessageLimits*** to 1. If this option is enabled and the message violates limits of any of the recipients, the whole message is rejected with a SMTP permanent error. Be aware that attachments to messages are Base64 encoded, which adds a size overhead of around 30%, so if you wish to limit your users to attachments of 1MB you should set the limit to 1.3MB.
Send out data limit per day	Limits the amount of data that any single user can send out in one day. Enter a value and select Kilobytes, Megabytes or Gigabytes from the drop-down box. Once a user exceeds the limit no further messages will accepted from that user. *NOTE: A message sent to multiple recipients will be counted for each recipient, i.e. a 1MB message sent to 10 recipients will be counted as 10 MB towards the limit.* *NOTE: Limits smaller than 1 MB can not be saved. It means that you can use limits in kB, but values have to be higher or equal to 1024 kB.* *Also NOTE that values are rounded down. E.g. value of 3000 kB is saved as 2 MB.* *NOTE: Local emails are not included.*
Send out messages limit (#/Day)	Limits the number of messages that a single user can send out in one day. Once exceeded no further messages will be accepted from that user. *NOTE: 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.* *NOTE: This value corresponds with **Account Statistics – Sent Out**.*



Field	**Description**
State	**Enabled** Fully working account. **Disabled (Login)** Partially disabled account. Mail is received, but the user cannot log-in and access any messages.

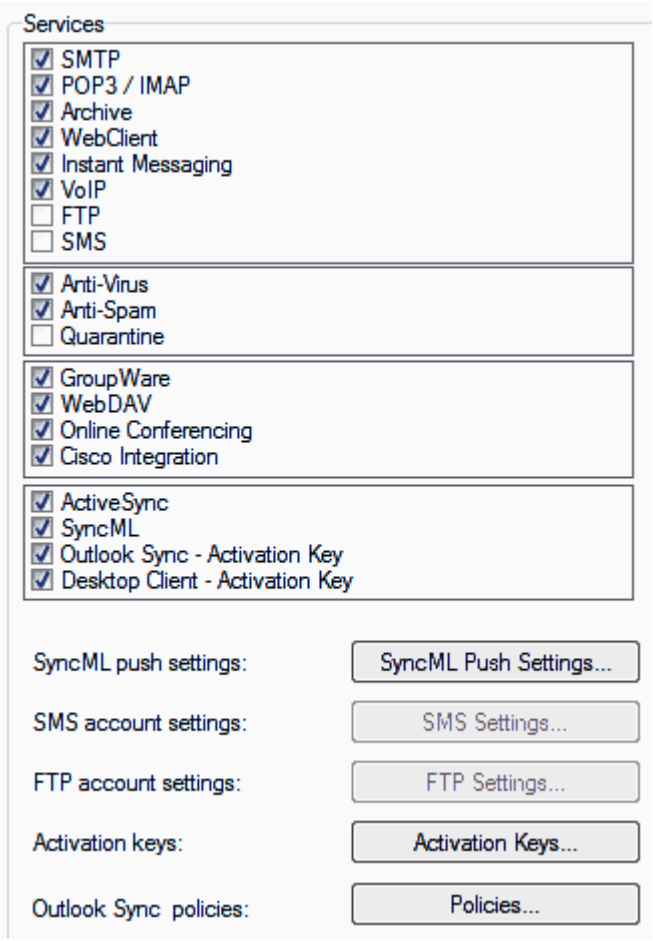
	It is very suitable for ISP providers, if they need to disable accounts temporarily. **Disabled (Login, Receive)** Completely disabled account. The user is unable to login and incoming messages are rejected. **Disabled (Spam Trap)** If email is delivered to this account, the sender is considered as an "Intruder" (see **Intrusion Prevention**) and his IP address is blocked according to the **Intrusion Prevention** settings.
Expires if inactive for [Days]	The account expires if it is not used for the specified number of days. When expired, the account is disabled after midnight at the end of the next day after expiration.
Expires on (yyyy/mm/d)	Specifies that the account will expire on the specified date. The account will be disabled at midnight at the end of the day.
Notify before expiration (Days)	If the account is set to ***Expire*** on a specific date then a notification message can be sent the specified number of days before the account expires.
Delete account when expired	Expired accounts will be deleted if this option is on. USE WITH CARE, you may not be able to retrieve account information once it is deleted.
Notification file	This specifies the full path and file name of a report that will be sent to the user informing them that their account will expire soon. If this field is blank, a standard report will be generated.

Policies

This tab lets you enable or disable selected services for the user. These settings are also considered by the licensing engine when comparing the license size with the amount of activated user seats – only user accounts are licensed.



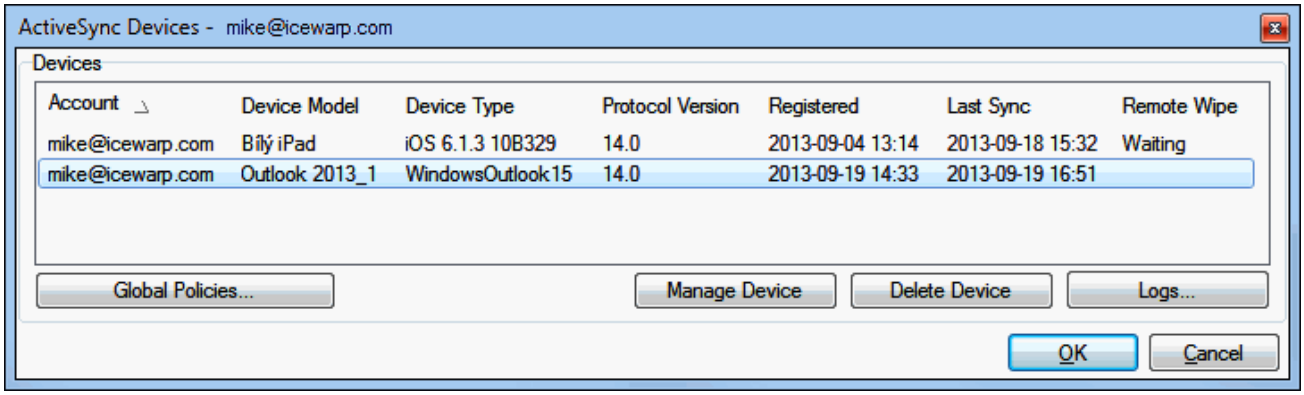
*NOTE: You can select multiple users from the middle pane in **Management** using Shift+click and Ctrl+click mouse operations to perform a bulk modification.*



Field	Description
Services	Tick the services you want to enable on the user level. *NOTE: Check boxes are enabled only if the accesses to services are granted on higher levels (domain).* *NOTE: To enable activation keys for IceWarp Outlook Sync and/or Desktop Client, it is necessary to have ticked check boxes under the **<domain> – Services** tab first.* *NOTE: After upgrade from 10.3.x to 10.4 in the case the previous access mode was **Accounts from the list**, the appropriate services appear disabled here, but settings are kept. To find out these settings, use **API Console** (global level – **File** menu) – filter variables using the filter value of **processinggroup**.* *In the case the **Advanced** mode was used, users will have their modes set to **[service_user10.3.x XNOR service_domain10.3.x]** in 10.4.* *NOTE: In the case an account is created as POP3 one, you will not be able to tick even the **Desktop Client – Activation Key** box (besides other boxes in this section). If you want to provide the DC license to the appropriate user, set his/her account to POP3/IMAP at least temporarily.*
ActiveSync Devices	Click this button to reveal the **ActiveSync Devices** dialog. This dialog lists all user's devices that use ActiveSync. See below. You can set ***User Policies*** (for all user devices), set ***Device Policies*** (for the selected user's device), remove devices from the list (***Delete Device***), set remote wipe for selected devices (***Set Remote Wipe***) and cancel remote wipe once set provided that it has not been executed yet (***Clear Remote Wipe***). *NOTE: Remote wipe is a total remote deletion of all device data. It is executed when the*

	device contacts the server first time after setting it. Within this period, it is possible to cancel it.
SyncML push settings	This button opens the **Device** dialog that lets you set the **SyncML Push** settings. For detailed information about this dialog, refer to the **SyncML Push – Server Configuration – Settings and User Accounts** section.
SMS account settings	This button opens the **SMS Account** dialog where you can set SMS account options. See below.
FTP account settings	This button opens the **User** dialog where you can define FTP Service settings. See bellow.
Activation keys	Clicking this button opens the **License** dialog (see lower) that allows you to transfer activation keys for IceWarp Outlook Sync and IceWarp Desktop Client to the user. The Activation Keys can be distributed by the following means: ▪ by email, click Activation Keys... and Send Key to User by Email ▪ available to the user from WebClient – Tools – License dialog ▪ automatically installed by SmartDiscover with no user intervention Once you have obtained a license with some amount of possible client activations (see **Help – License...**), tick **Outlook Sync – Activation Key** or **Desktop Client – Activation Key** for users that should be allowed to activate the corresponding application. This will automatically generate an Activation Key for the user and make it available by SmartDiscover and WebClient. You need to tick the Activation Key checkboxes in the **Services** tab on both the domain level and user level to have the Activation Keys generated automatically. You can still have them unticked on either level and generate activation keys manually in **Activation Keys... – Generate Key**. *NOTE: Unticking the checkbox will not unregister an already licensed application, it will only disallow the distribution of the Activation Key by SmartDiscover and WebClient.*
Outlook Sync policies	Click the *Policies* button to open the **Policies** dialog. Here, you can set provisions for the appropriate Outlook Sync user. It is possible to *Force settings* (not possible to change by users) or to *Set as default* (users can change these recommended values). For detail description of these options, refer to the **IceWarp Server Outlook Sync User Guide – IceWarp Options – Settings** section.

ActiveSync Devices Dialog



NOTE: The caption of the very left button is variable according to the level we are accessing the dialog from.

There are following (self-explanatory) possibilities:

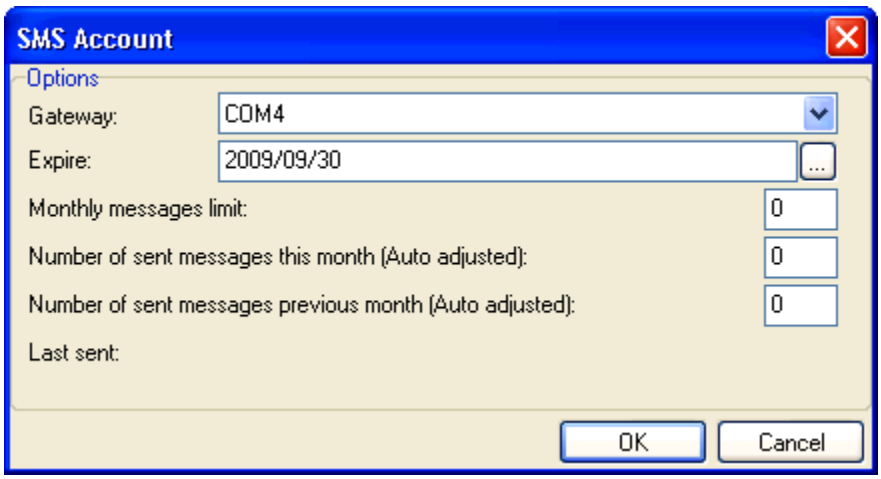
- Global Policies (**GroupWare – ActiveSync – Device Management**)

- Domain Policies (**Domains and Accounts – Management –<domain> – Services – ActiveSync Devices**)
- User Policies (**Domains and Accounts – Management –<user> – Services – ActiveSync Devices**)

For more details about security policies, refer to the **ActiveSync Guide – Security Policies** section.

SMS Account Dialog

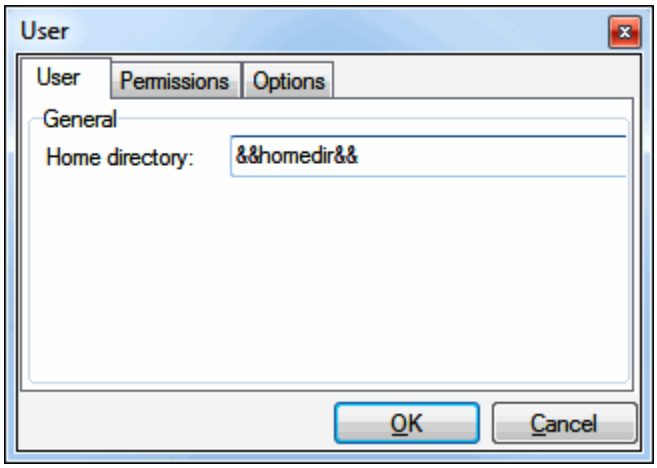
These settings are used in the case the SMS service on the domain level (**[domain] – Policies**) is enabled.



Field	**Description**
Gateway	Select from the list. (Gateways defined under the **SMS – General** tab.)
Expire	Select the date of the account expiration.
Monthly message limit	Enter the maximum number of messages that can be sent per month; if "0" (zero) is left, there is no limit set. For example, evaluation accounts can be created by limiting a number of sent messages to 10 and/or setting a 7 day expiration. *NOTE: Even if set on the domain level, this limit is applied per user. E.g. if set to 1000 on the domain level, each domain user can send 1000 messages per month (unless he/she has set this limit individually).*
Number of sent messages this month (Auto adjusted)	The use is two-fold: 1. Message counter.The value shown here tells you how many messages have been sent this month by users or groups within this account. It is automatically reset to 0 at each month's end. 2. Counter reset. Type 0 or any other value and click OK to reset the monthly counter.
Number of sent messages previous month (Auto adjusted)	1. The value shown here tells you how many messages have been sent in the previous month by users or groups within this account. If there has been no activity in that month, it is automatically reset to 0 at each calendar month's end. 2. Counter reset. Type 0 or any other value and click OK to reset the monthly counter. (May be meaningful for invoicing.)
Last sent	Shows the date and time when the last message was sent through this SMS account.

User Dialog

The **User** tab lets you set the directory the system users will have granted access to.

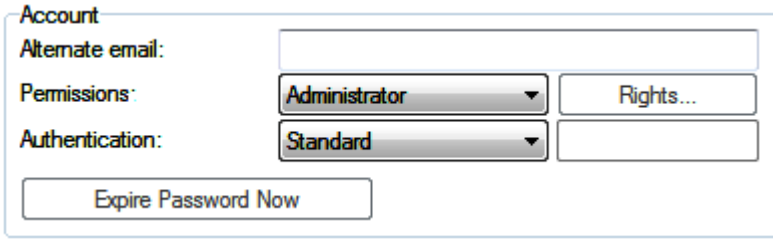


Field	Description
Home directory	You have the following possibilities: ▪ leave the field blank – same as the next option ▪ use the ***&&homedir&&*** variable – users are directed to their email folders (**<InstallDirectory>/mail/<domain>/<user>**) ▪ use the ***&&sitedir&&*** variable – users have access to the whole site, by default they have the ***read, write*** and ***delete*** rights ▪ enter some path – users are directed to this directory regardless of the site(s) defined lower

For description of the **Permissions** tab, refer to the **FTP Service – General Tab – FTP Service Dialog – Users – Permissions** section.

For description of the **Options** tab, refer to the **FTP Service – General Tab – FTP Service Dialog – Users – Options** section.

Options



Field	Description
Alternate email	Fill in an external email address where a password will be sent in the case a user has forgotten it. Also editable in WebClient – **Tools – Accounts – Primary – Alternate Email**.

Permissions	Restricts the level of access this user has to server resources: **Standard** A standard user account can access all services and can manage his/her quarantine queue, whitelist and blacklist using the WebAdmin interface. Settings can be changed using IceWarp WebClient. **Domain Administrator** Domain administrators can also maintain accounts within the domains they administer but they cannot perform changes within IceWarp Server's Global Settings. The **Rights** button becomes active if this option is selected. **Administrator** Administrator permissions grant this user full access to the IceWarp Server without limitation.
Rights	Clicking this button opens the **Domain Admin Rights** dialog where you can specify which particular account types the administrator can modify, and also whether this account is a spam administrator account (the ***Spam queue*** option). *NOTE: This button is only active when the **Domain Administrator** permission is selected.* *NOTE: For detailed information on domain administrator rights, refer to the **F1 help – Shared Topics – Domain Admin Rights** chapter.*
Authentication	The authentication mode lets you specify how the IceWarp Server authenticates login requests for this user. **Standard** This is the default mode. The IceWarp Server uses its own authentication engine, which supports many authentication schemes such as CRAM-MD5, MD5, DIGEST-MD5, PLAIN, LOGIN, etc. **NT Domain** The NT domain mode specifies that the NT domain controller should be used to authenticate the user. IceWarp Server must have the SE_TCB_NAME privilege. By default, the local machine domain controller and user will be used. If necessary, the domain controller and user can be explicitly identified in the text box to the right, in the following format: ***NT Controller;NT username*** **LDAP / Active Directory** The Active Directory mode authenticates against an AD server. By default the localhost AD server and username of the email address is used. If the AD server name, username or domain differs, you can explicitly set it in the text box to the right, in the following format: ***ADserver;ADusername@ADdomain*** *NOTE: You can specify multiple **servers;users** here (maybe a backup server) separated by the | character (pipe character).* *E.g. **Server1;User1@domain1.com|Server2;User2@Domain2.com*** **Any Password** This mode specifies that any password will be accepted. This option is not recommended as it can lead to account abuse, but could be used for a trial account or similar.
Expire Password Now	Click the button if you want to force this user to change his/her password right now. *NOTE: This button is enabled when the **Password Expiration – Active** box is ticked*

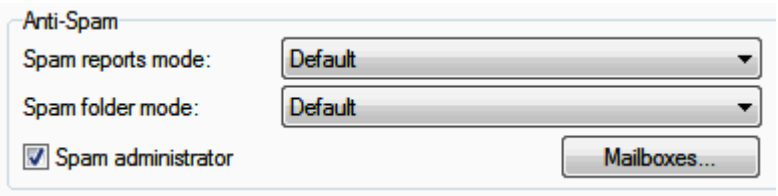
	*(**Domains and Accounts – Policies – Password Policy**).*



Field	Description
Type	Specifies the mailbox type: **POP3** Standard POP3 access to the account. BE AWARE: When accounts are set as POP3, both ActiveSync and Outlook Sync **do NOT work**! **IMAP** Standard IMAP access to the account. All folders can be accessed from an email client. **IMAP & POP3** Access via IMAP or POP3. Remember that POP3 normally deletes the messages from the **Inbox** folder unless it is configured not to do so by the user. *NOTE: If you convert POP accounts to IMAP, these accounts can lose the read/unread status in WebClient Inbox folders. All messages become UNREAD.* To resolve it, you can: ▪ run the **pop_to_imap.html** script (in **c:\icewarp\html\admin\tools**) prior to converting accounts. While running the script, select these accounts. Then change account(s) type here. ▪ or run the script (mentioned above) and do multiple changes using **Tool.exe**. E. g. ***tool modify account *@* u_accounttype 1*** – which means that accounts will become ***Type*** of POP+IMAP. *ALSO: Beware, if you use accounts that are of POP type only, the **read/unread** status is kept in the PDO database. If you start a new PDO database or drop tables, the **read/unread** status of messages will be lost. So for example, in WebClient Pro, all emails will show as UNREAD.* *If you really need to start a new PDO database or migrate to a new database type (for example from SQLite to MySQL), you can first convert all accounts to POP+IMAP (using the **pop_to_imap.html** script (**IceWarp\html\admin\tools**)).* *NOTE: When adding an "other account" within WebClient (**Tools – Accounts – Other – Add**), the account behaviour is as follows:*

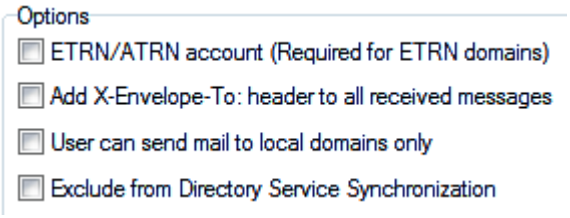
Account Type	Remote	Local
POP3	POP3	LocalPOP
IMAP	IMAP	IMAP

	IMAP&POP3 | IMAP | IMAP LocalPOP means that it does not use any service – just the file system. It also means that mail downloads are not logged in POP3 logs (you will only see get requests in IW WebClient logs – if enabled). If you use IMAP or POP3/IMAP accounts, IMAP logs are used – i.e. all logs are available.
Mailbox Path	This specifies the location of the user account's mailbox, where all files and messages related to the account will be stored. By default, the path is inherited from **System – Storage – Directories – Mailbox path** or from **Domain – Options – Folder** if enabled. IceWarp Server automatically defaults this to a path based on the domain name and user alias but you can change it to anything you wish, including a fully qualified path. *NOTE: You can specify a network location for a user mailbox, but this must be specified in UNC format.* *Example: \\ComputerName\SharedFolder\Resource* *NOTE: Shared drive letters are not supported.*
Remote Address	This specifies that mail will not be stored in the mailbox but sent on to a remote address instead. This address is to be of the following format: ***name@domain.com***. This field may contain multiple addresses separated by semi-colons.
NULL	This option specifies that this is a dummy account and any messages sent to this account will be deleted, but any forwarding and auto responder functions will work as normal.
Refresh Directory Cache	Files/folders copied into mailboxes will not appear to users unless the directory cache is updated. Use this button to update it.



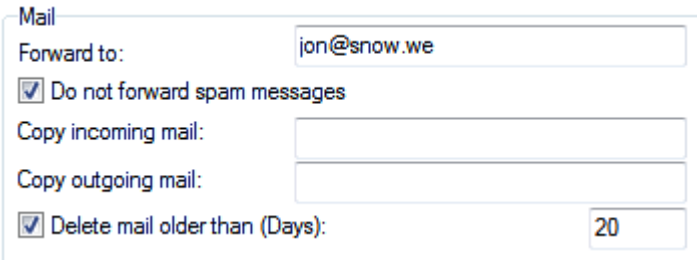
Field	**Description**
Spam reports mode	Select the ***Spam report mode*** for this user: **Disabled** The user will not receive spam reports. **Default** The user will receive spam reports with either new items only or all items listed – according to the settings specified in the **AntiSpam – Action – Reports** node – ***Report mode***. **New Items** The user will receive a listing of new spam items received since the last report was produced. **All Items** The user will receive a listing of all spam items.
Spam folder mode	See the IceWarp Server Anti-Spam section for more details about spam folders. You can choose one of three modes: **Default** The default setting set in **AntiSpam – Action** will be used.

	Do not use Spam Folder A spam folder will not be used for this account. **Use Spam Folder** A spam folder will be used for this account.
Spam administrator	This checkbox is only enabled if your anti-spam settings allow. A user can be a ***Spam Administrator***, allowing him/her to administrate spam/quarantine and approve message indexing. For more details, see also the **AntiSpam – Processing for Pending Queue** section. *NOTE: The accounts that are to be administered by this spam administer have to have AntiSpam and spam folders enabled.*
Mailboxes	Enabled only if the account is defined as a spam administrator. Pressing this button opens a dialog where you can specify additional mailboxes this user can maintain or moderate via the AntiSpam access. Examples are included in the dialog.



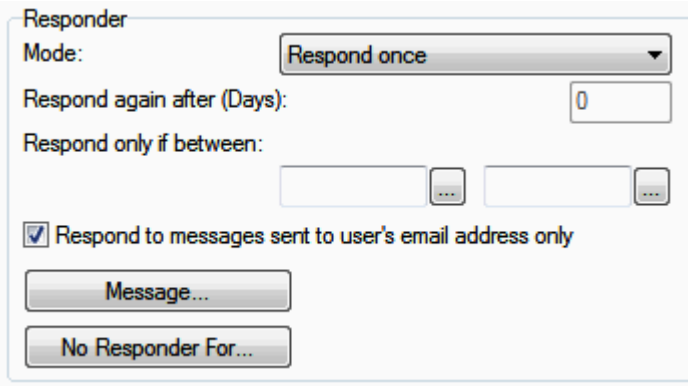
Field	Description
ETRN/ATRN account	If this domain is ETRN/ATRN one, then this option is required and this account should be the only account defined in the domain. This is the account where all incoming messages are kept for the collecting server.
Add X-Envelope-To header to all received messages	Check this option and all messages received will have the X-Envelope-To header added, containing the recipient. This option is useful for ***Catch All*** accounts so the collector of messages can see who the intended recipient was. *NOTE: Use with care as it can reveal **Bcc** recipients in the header.*
User can send mail to local domains only	Check this option to limit the user to sending messages only within the local domains. *NOTE: Do not use this option together with the **Bounce back messages for failed recipients** one (**WebClient – Administrator Options – Mail – General**). For detailed information, refer to the **WebClient Administration Guide – Administration Options – Forcing Options on Other Users** chapter – **Bounce back messages for failed recipients** option.)*
Exclude from Directory Service Synchronization	Tick the box if you want to exclude the user from directory service synchronization. If the appropriate domain has set synchronization with an AD/LDAP server (**<domain> – Directory Service**), it is possible to set IceWarp Server to ignore any changes performed on the directory service server. *NOTE: After disabling this feature, the user is synchronized again.*

Mail



NOTE: Patterns can be used within the following three fields.

Field	Description
Forward to	All incoming messages will be forwarded to any address(es) specified in this field. This provides a mechanism for automatically copying messages to other users, both remote or local. Multiple addresses can be specified with semi-colons as delimiters. *NOTE: The original message is also delivered to a local account. If you do not want a copy in a local mailbox, you should use the **User – Options – Remote Address** option.* *NOTE: This setting is also accessible via IceWarp WebClient GUI.* *NOTE: The **Sender** header is set to **noreply** to prevent forwarding the message back to the original forwarder.* *NOTE: Also the **sms:** protocol (**xmpp:** one respectively) can be used. Email header(s) and/or footer(s) – if set – are not added in this case.*
Do not forward spam messages	Tick the box if you want messages evaluated as spam not to be forwarded.
Copy incoming mail	Specifies either: • an email addresses that all incoming messages will be copied to • or a path to a directory where message copies will be stored. *NOTE: For this feature, content filters can be applied. (Set the **mailinusecf** API variable to true.)* *NOTE: Copying of incoming messages (for local users) is not logged.*
Copy outgoing mail	Specifies either: • an email addresses that all outgoing messages will be copied to • or a path to a directory where message copies will be stored.
Delete mail older than (Days)	Tick the box and specify number of days. All older email messages (in the user's Inbox) will be deleted.



Field	Description
Mode	Specifies whether an auto-response is sent or not. There are four options: **Do Not Respond** No response is sent. **Respond Always** Every message will be responded to. *NOTE: Use with care! If the original sender has an auto-responder doing the same thing, you could create a message loop. (It is also possible to misuse it for spamming.)* **Respond Once** A response will be sent once to each individual sender of a message, so the second and subsequent messages from another person will not receive a response. **Respond after a period** This option will send multiple responses to individual senders, but only the specified number of days ***after the previous response*** to the same sender. The number of days is specified in the text box to the right. For example: Assume **Respond after a period** is selected and **7** is specified in the text box. If a user sends multiple message ***every*** day he/she will receive a response after the first message, then again after the first message 7 days later, then again 7 days later and so on.
Respond again after (Days)	The minimum number of days between responses. Maximal supported period between responses is 63 days.
Respond only if between	This option lets you specify exact dates when a response will be sent. Click the "..." buttons to open a date-picker dialog.
Respond to messages sent to user's email address only	Check this option and a response will only be sent if the ***To:*** header contains the email address associated with this account.
Message...	Click this button to create the response message. The **Message** dialog is displayed – here you can specify the message properties. *NOTE: The **From** and **To** fields accept only valid mail headers, i.e. either email – **john@doe.com** or name + email – **"John Doe" <john@doe.com>** Name alone is not allowed.* *NOTE: For more information on responder settings, refer to the **manual.chm – Shared Topics – Server Variables** chapter – **Examples** section.*
No Responder For...	This button opens a file where you can specify a list of email addresses and/or domains that should not have responses sent to them. Each email address or domain must be on a separate line. Example:

	dias@icewarpdemo.com ***mydomain.net***



BE AWARE: In some cases, IceWarp Server sends out "robotic" messages back to their sender. For example auto-responder, challenge response, bounce back messages. This is OK as far as the sender is a genuine one – NOT a spammer.

There are antispam services (SpamCom, SenderBase.org) that might blacklist the mail server if is set up to send out these robotic messages.

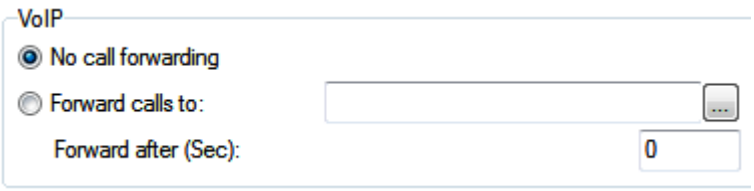
Scenario

1. Spammer sends a spam message to an IceWarp Server local account.
2. Spammer forged the sender's address.
3. Message is not recognized as spam.
4. Robotic message is generated and sent to spoofed innocent email address (because of auto/responder/challenge response/bounce back).
5. Antispam services like ***SenderBase.org*** and others once find this out, they list IceWarp server to a list of suspicions servers.
6. Because of bad "karma", SMTP communication from the IceWarp Server might be rejected by a recipient who uses the AntiSpam service like the ***SenderBase.org***.

Available solution – disable all "robotic" messages:

- ***Challenge Response*** in **AntiSpam – Quarantine –*Send Challenge response email for messages to be quarantined***.
- Any automatic respond to sender set via ***Content Filter, Rule or Responder*** in user settings under the **Domains and Accounts – Management – <domain> – <user> –Options** tab.
- Set ***Bounce backmessages*** to be sent to ***Local senders only*** (in the **Mail Service – General – Delivery – NDR** section).

VoIP



Field	Description
No call forwarding	Call forwarding is disabled.
Forward calls to	Select account(s) where to redirect calls. (Use the "..." button.) Multiple accounts are to be separated by semicolons. Users are dialed in the order they are entered here. External phone numbers can be inserted provided that there is an appropriate gateway defined.
Forward after (Sec)	Enter a time period (of ringing) after which calls are redirected.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Use rules for incoming messages, while content filters can be used for both sent and received messages.

Groups

GroupWare allows a group of people to share the following data:

- calendar information
- contact information
- email information

In conjunction with GroupWare, the ability to define group accounts provides a powerful collaboration process. A group account contains a list of member accounts, which can be user, mailing list or even other group accounts.

Groups can be given access to any shared folders defined on the system.

Individual users can share their calendar and contact information with groups, as well as individual users.

Emails can be sent to group accounts, which will be routed to all group members.

This functionality gives the ability to, for example, create a group for a corporate department and define a common data store (shared folder), common address book and common calendar. Any data changes in this common store are immediately available to all users with access to this store.

Combining this powerful functionality with the fact that GroupWare is accessible through IceWarp WebClient means that users never need to be out of touch or in possession of out-dated information.

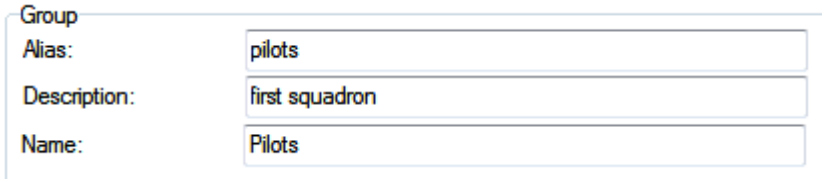
IceWarp Server also provides a plug-in for MS Outlook, the **IceWarp Outlook Sync** that allows offline GroupWare functionality directly from MS Outlook itself.

Simple administration keeps the maintenance of group accounts at minimum.



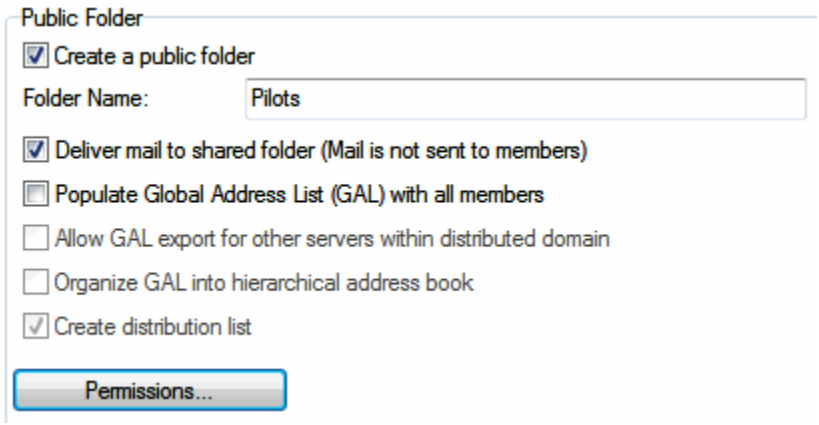
*Do not forget that templates can be set up to streamline the definition of groups, see **Account Templates**.*

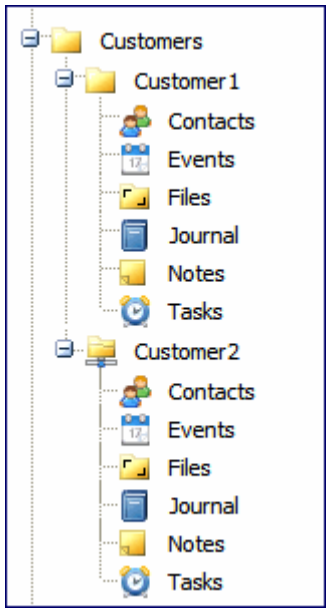
Group



Field	Description
Alias	A unique identifier for the group within the domain. ***Alias*** is the first part of the group email address. In the above screenshot, ***pilots@icewarpdemo.com*** would be the group email address. Multiple aliases can be used with semi-colons as delimiters: *pilots;airmen;aviators* *NOTE: Maximal length of this field is limited to 255 characters. If you want to use more aliases, you can use a pattern.* *Syntax: Alias: **<primary_alias>; <[pattern_name]>*** *E.g.: Alias: **support; [support_aliases]*** *For more information, refer to the **System Node Reference – Advanced – Patterns** chapter.*

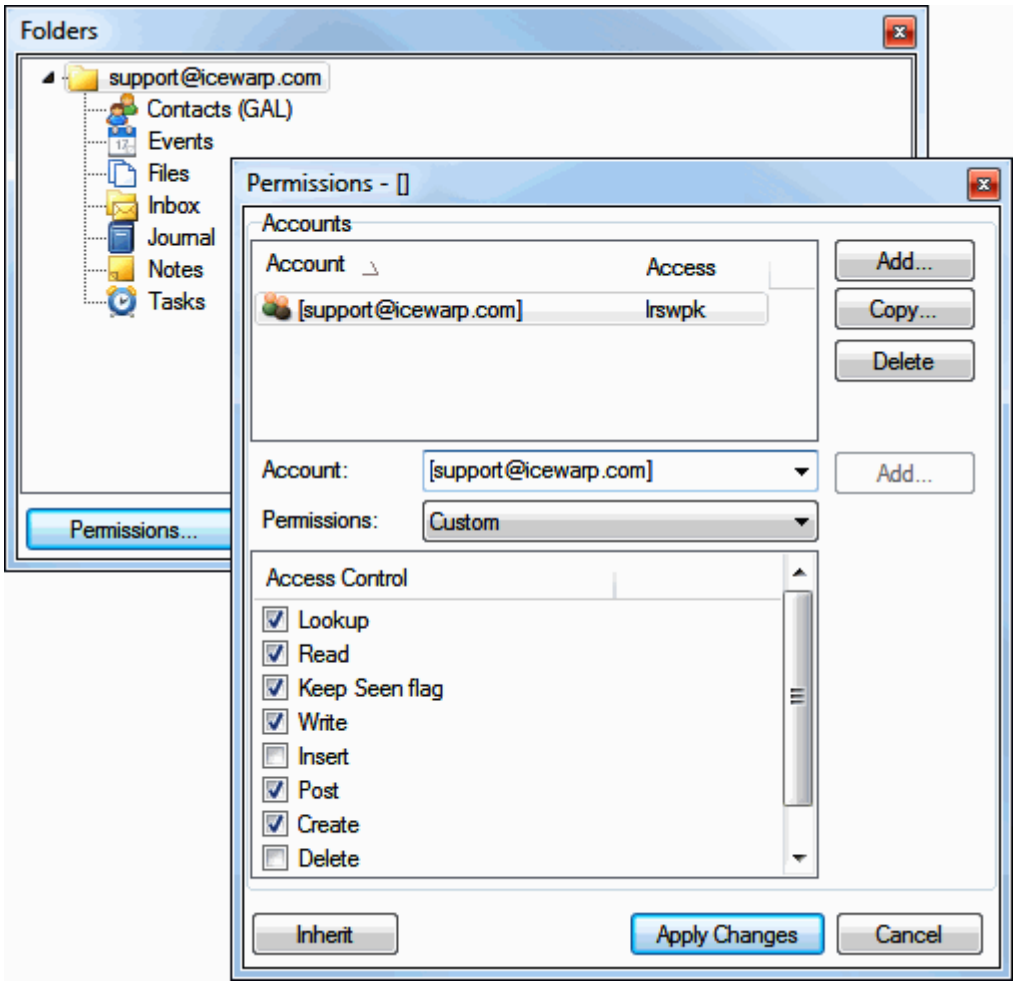
Description	A short description of the group. When using **GAL**, this description is shown as a group name. If left blank, ***Alias*** is used instead.
Name	Enter the group name as it will be shown in GAL.



Field	**Description**
Create a public folder	Check this box to create a public shared folder for this group. A shared GroupWare and IMAP folder will be created for the group members.
Folder Name	The name of the public shared folder for this group. This name is displayed in an email client. *NOTE: You may want to create large amount of similar folders for the same purpose and do not want to have all these folders in the folder tree root. You can nest folders into one created for this and placed to the root. Use backslash in the folder name.* *E.g.:* ***Customers\Customer1*** *Customers\Customer2* *etc.* 
Deliver mail to shared folder (Mail is not sent to members)	Check this option and mail sent to this group will not be delivered to individual member's mailboxes, but to the shared folder instead.
Populate GAL with all members	Check this option IceWarp Server to create GroupWare contacts for all group members. Contacts will be displayed in users' email clients. You can create members of the group in a simple text file using the ***Text File*** button on the

	members tab (see **Groups – Members**).
Allow GAL export for other servers within distributed domain	Tick the box if you want to use a remote GAL for a distributed domain. For more information, refer to the **GroupWare – GAL– Remote GAL** chapter.
Create distribution list	If the box is ticked, a distribution list with all group members is created. This list is available to all members. By default, this option is enabled.
Permissions	Click the button to set access rights for individual group members. The **Folders** dialog opens – see lower. It is possible to set rights for either whole email account or selected folders (e.g. Inbox, Contacts, Calendar, etc.). For detailed information, refer to the **GroupWare – Reference – Public Folders – General** section.
Organize GAL into hierarchical address book	When a GAL group has other groups as members, the GAL population creates a folder structure where the ***Name*** of a subgroup is used as folder name. Tick the box in the case, this is desirable behaviour. This works also with remote GALs synchronized from another instances of distributed domains. (If the box is not ticked, all users are shown on the same level.) For more details, refer to the **Hierarchical Address Book** section below.
Save	Click the button to save group settings.

Folders Dialog



Within this dialog, select either the whole account or an individual folder and click the *Permissions* button. The **Permissions** dialog opens. Click the *Add* button and within the **Select Item** dialog select either the whole group or individual members and tick the wished access levels. Click the *Apply Changes* button to save these settings.

Refer to the **GroupWare – Reference – Public Folders – General** chapter for detailed description of the **Permissions** dialog.

External Contacts in GAL

It is possible to add external contacts into both a global GAL and group one. All system (group respectively) users with at least ***Write*** rights can add external contacts manually. For more contacts this is not a smart way.

Better way:

1. Create a group, select the ***Create a public folder*** and ***Populate GAL with all members*** options.
2. Grant some member(s) at least the ***Write*** rights (use the ***Permissions*** button) for the **Contacts (GAL)** folder.
3. This member can use IceWarp WebClient to import a ***csv*** file with external contacts into the group **Contacts (GAL)** folder (***Tools – Import/Export – Import***).
4. Grant all group members who should see these external contacts at least the ***Read*** rights.

Hierarchical Address Book (HAB)

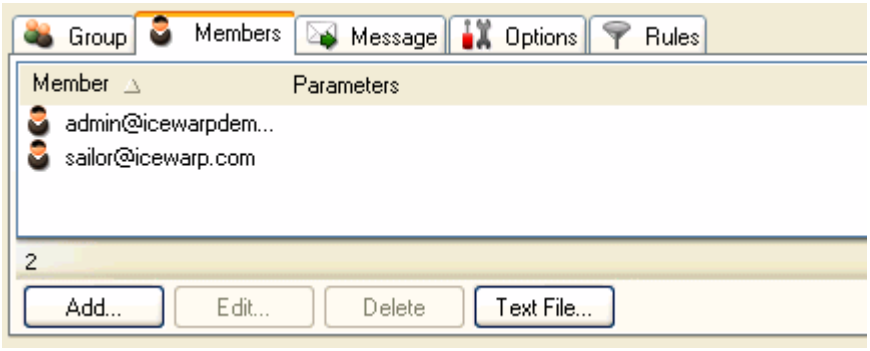
For detailed description, refer to the **Directory Service –** Hierarchical Address Book (HAB) chapter.



*NOTE: To set event and task reminders for group members, right-click the appropriate group name and select the API Console item. Filter variables – use the **gw** string. Two variables are shown: gw.dailyagenda and gw.reminders – set both to true.*

Members

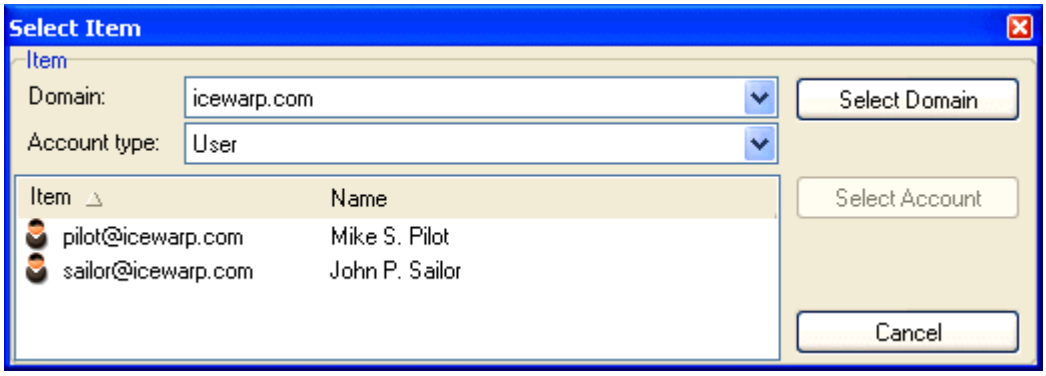
Selecting the **Members** tab displays the following pane.



The view shows a sortable list of members of the selected group. IceWarp Server auto-organizes all members in alphabetical order.

Add Button

Clicking the ***Add*** button opens the **Select Item** dialog:



You can use the **Domain** and *Account Type* drop-downs to refine your search.

Once the correct account is displayed, select it and click the *Select Account* button.

To add the whole domain, select it in the list and click the *Select Domain* button.

BE AWARE: Not all users might appear, due to 4000 user limitation for processing reasons. If so, either drag and drop the appropriate user(s) to the **Members** tab or add the group to the user(s) within the **Users – <user> – Groups** tab.

Edit Button

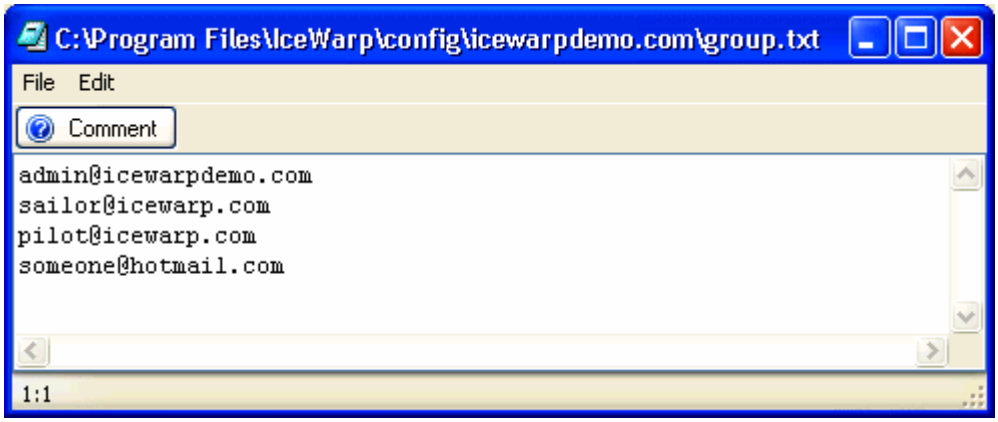
This button is not enabled here. (It is enabled only for ***Mailing lists***.)

Delete button

Select a group member and click this button to remove this member from the group. Confirm deletion in the **Question** dialog.

Text File Button

Click the ***Text File*** button to display the text file with defined group members:



The file can be edited directly in this window. To see syntax information, click the ***Comment*** button.

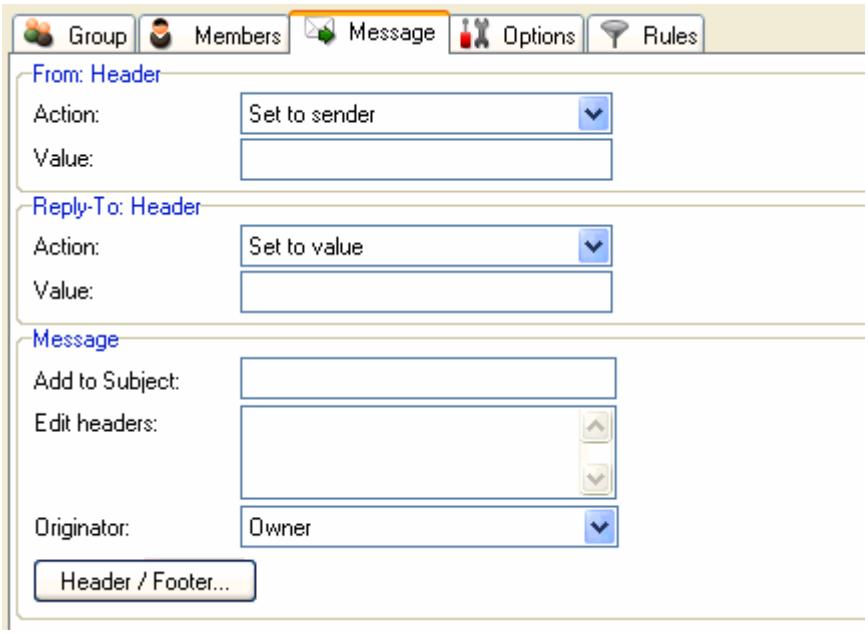
BE AWARE: To save any changes, select the ***File – Save*** menu items.

External Delivery

You may want to send messages to group members as they were sent externally. Group members can have whitelisted some other members or set rules for them. In the case such a member sends a message via a group account, these whitelistings/rules will not work.

Use the *g_deliverexternally* API variable to workaround. (Right-click the group name, select the *API console* item and search for ***externally***.) Set the value to *true*.

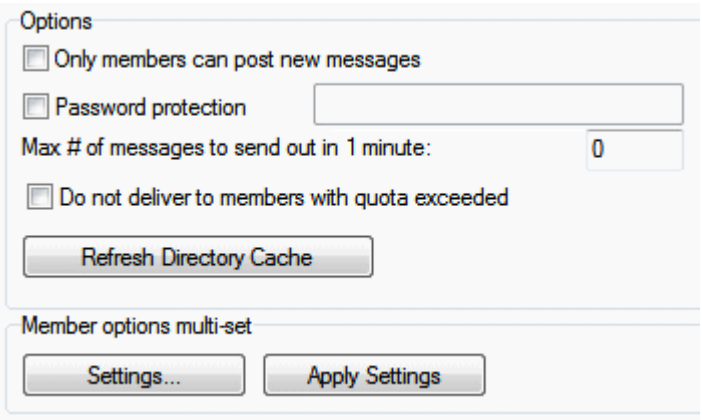
Message



Field	Description
From: Header Action	You can specify changes to the ***From:*** header of a message: ***No Change*** No change will be made. ***Set to sender*** The header will be set to the address of the message sender. **Set to Value** Set the header to the value specified in the ***Value:*** field.
Reply-To: Header Action	You can specify changes to the ***Reply-To:*** header of a message: **No Change** No change will be made. **Set to sender** The header will be set to the address of the message sender. **Set to Value** Set the header to the value specified in the ***Value:*** field.
Message Add to Subject	This prefixes the ***Subject:*** header with the specified string. If the text is already present, it does not duplicate it. If the ***Subject:*** header is not present, it is created.
Edit headers	You can add any number of custom headers to the message. System variables can be used here. Example: ***Size:%%Size%%*** This field is limited in size, so if you need to add many headers you should use a file to specify the headers to add, like this:

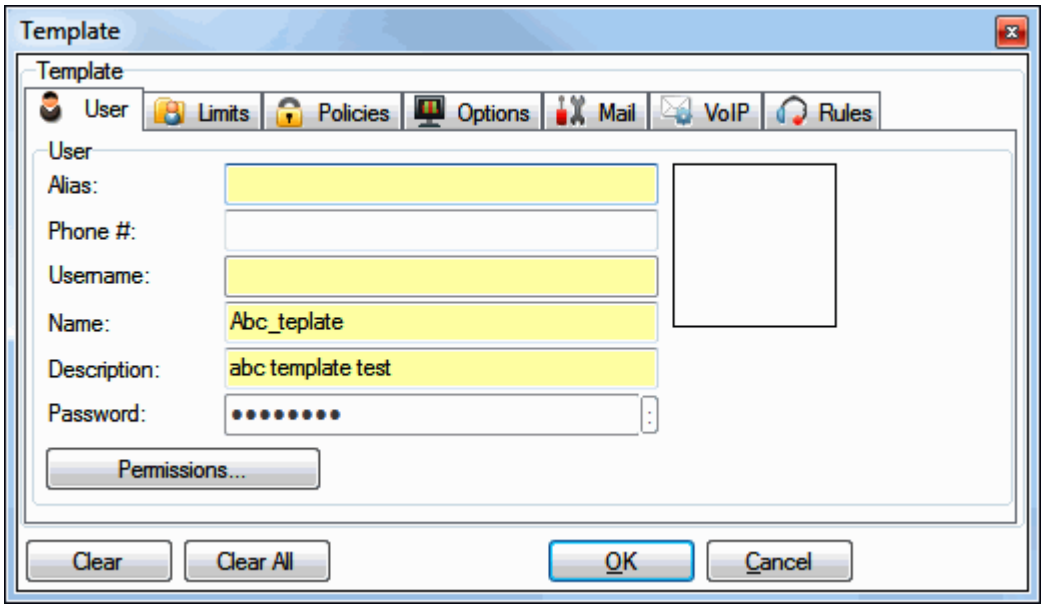
	▪ Enter ***%%include <FileName>%%*** in the ***Add headers:*** text area, where ***<FileName>*** is a fully qualified path to the file. ▪ Create the file specified, as a simple text file, and add the headers you wish to add to messages.
Originator	This is an advanced SMTP option. You can specify the exact content of the SMTP MAIL FROM command. The possible options are: **Blank** – the MAIL FROM command offers an empty field. **Sender** – the sender's address is used. **Owner** – the list owner's address is used. *NOTES:* *If the **Blank** option is selected (the default), some email servers might reject the message.* *When you choose the **Sender** or **Owner** all bounce backs of failed messages will be sent to that email address.*
Header/Footer	The **Header/Footer** dialog is opened where you can specify text and html files (for text and html messages respectively) that will be inserted at the beginning or end of all messages sent through the mailing list. Always specify a fully qualified path to the file. *NOTE: HTML files should only contain HTML BODY content (without the BODY tags).*

Options



Field	Description
Only members can post new messages	Check this option and only members of the group will be allowed to post new messages to the group.
Password protection	Check this box to have password protection switched on for this group, and specify a password in the field. To send a message to the group a user has to specify the correct password at the beginning of the subject line of the email (followed by a space and actual message subject). The password will not be shown to users that receive the message.
Max # of messages to sent out in 1 minute	Enter a non-zero number to limit the number of messages that this group account will send within a one-minute period. This allows you to implement basic flow control for outgoing messages if the group becomes

	large (say 10000 members).
Do not deliver to members with quota exceeded	Group accounts can have set mail box limits. (Size, number of delivered messages, etc.) Tick this box if you want to exclude group members with any of these limits exceeded from obtaining messages (until they "clean" their mailboxes).
Refresh Directory Cache	Files/folders copied manually into mailboxes will not appear to users unless the directory cache is updated. Use this button to update it.
Settings	Click the button to reveal the **Template** dialog (see lower) that lets you define common options for groups. After applying a template, all existing group members settings are changed accordingly. E. g. you have defined the IMAP mailbox type, but some of group members have POP3 mailboxes. They are changed to IMAP ones. For members added to this group afterwords, you have to apply the template again to change their settings. *TIP: You may want to create a group ad hoc to set some features for selected users (they can be from different domains), apply the wished changes and delete the group.* For more details, refer to the **Creating Template** (on page 104) section.
Apply Settings	Click the button if you want to use the created template for all groups created afterwords.



Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Field	Description
Active	Tick the box to enable rules executing.

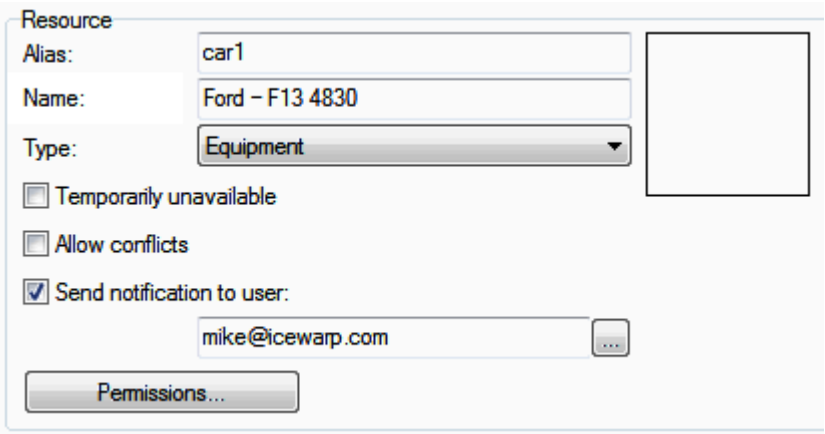
Resources

This IceWarp Server feature allows smooth and easy resource management process. This process consists in reservation of company resources and their allocation.

Resources are meeting rooms, projectors, cars, etc.

For more details, refer to the **GroupWare Reference – Scheduling and Resource Management** chapter.

Resource

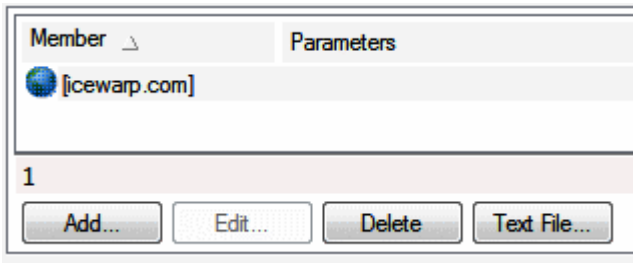


Field	Description
Alias	Fill in a resource alias.
Name	Fill in a short resource description. The entered value is checked for duplicity. It has to be unique globally (or left blank). This value is used in WebClient for ***Resources*** available to user (from all domains) to show resource folders.
Type	Select the appropriate resource type: ***Room*** – use this type for meeting rooms, conference ones, etc. ***Equipment*** – use this type for other items such as projectors, computers, etc. ***Car*** – use this type for cars.
Temporarily unavailable	Tick this box in the case of temporary unavailability of the item – e.g. the item is under repair. Ticking this box causes that organizers are not able to add the resource when sending a reservation.
Allow conflicts	Tick this box if you want to allow situations when reservation requests can overlap. The resource manager resolves eventual conflicts. If the box is not ticked, an automatic iMIP agent rejects requests that coincide with accepted ones.
Send notification to user	Tick the box if you want some user to be notified about every accepted or declined request. This user can act as a resource manager. In this case, give him/her a full rights (use the ***Permission*** button). Select this user clicking the "..." button. You can enter more accounts separated by semicolon (or multi-select them in the **Select Item** dialog using CTRL + click or SHIFT + click).

Permissions	Click the button to set access rights for individual users, groups or domains. For detailed information, refer to the **GroupWare – Reference – Public Folders – General** section. *NOTE: All resource users are added with **lookup, read, insert** and **post** rights (even system or domain administrators). In the case you want to grant someone higher permissions, do it here manually. The same applies for the user(s) selected in the **Send notification to user** field.*

Users

This tab lets you define resource users. You can choose individual accounts as well as groups and even whole domains. Under the **Resource tab – Permissions**, you can set different rights for individual users.



Button	Description
Add	Click the button to add a new organizer. Clicking reveals the usual **Select Item** dialog that allows you to add accounts, groups and domains from the server. (For the dialog description, refer to the **Group – Members** section.)
Edit	This button is not active here.
Delete	Click the button to remove the selected organizer.
Text File	Click the button to reveal a text file with all organizers. To see syntax rules and examples, click the ***Comment*** button here.

Card

This tab allows you to summarize resource's information.

Fill in the appropriate fields – all of them are optional ones. Their labels are self-explanatory.

For more details, refer to the **User Accounts – Card** chapter.

Rules

For description of this tab, refer to the **Mail Service – Rules – Content Filters – Rules** section.

Mailing Lists

This type of account enables you to define a list of email addresses that you can send to using one email address.

They can be used for discussion groups, departmental announcements, etc.

The members of a mailing list can be stored in a plain text file, a database or they can be IceWarp Server user accounts on the same server.

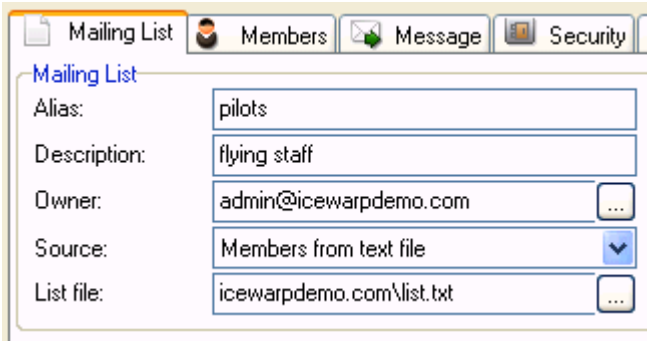
Variable names and values can be stored for each member, which can then be used within messages to customize individual messages for the receiver.

A mailing list can be a member of an another mailing list account, but care should be taken not to include a mailing list within itself as you may end up with a recursive mailing situation.



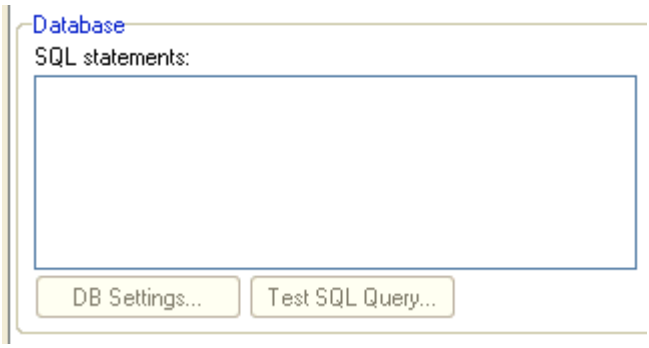
*NOTE: Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Mailing List



Field	Description
Alias	A unique identifier for the account within the domain.
Description	A short descriptive text for the account.
Owner	The email address of the mailing list owner – multiple addresses can be specified here, separated by semicolons. The account owner has special rights to this account. You can use the '...' button open the **Select Accounts** dialog.
Source	A drop-down box allowing to quickly add a pre-defined set of members: **Members from Text file** Allows you to specify, or create, a simple text file containing email addresses of members. Each address is to be specified on a single line of the file. **Members from ODBC** Select this option to have IceWarp Server interrogate a database for list members. If you choose this option you will need to supply the SQL that IceWarp Server should use to extract addresses and variables from the database. See the next section for more information. *NOTE: The commands chosen at the **Allowed Commands** section (**Management – List Servers – <list server> – List Server**), e.g. **Join (Subscribe)**, **Leave (Unsubscribe)**, etc. are not available when this option is selected.*

	All current Domain Users Messages will be sent to all users defined within this domain. **All System Users** Messages will be sent to all users defined in all domains within this IceWarp Server. **All System Domain Administrators** Messages will be sent to all domain administrators within this IceWarp Server. **All System Administrators** Messages will be sent to all system administrators within this IceWarp Server.
List file	A simple text file containing all members of the group, one per line.

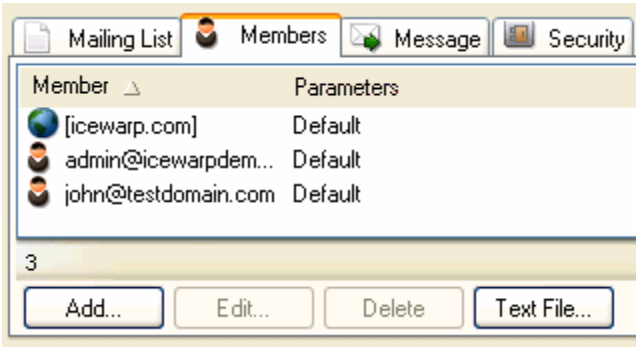


SQL statements	If you want to choose the ***Members from ODBC*** option (in the previous section), you need to supply the SQL that IceWarp Server should use to extract information from the database. For example: ***SELECT <YourData> FROM <YourTable> WHERE <YourCriteria>*** ▪ **<YourData>** should specify which columns you need data extracted from. ▪ **<YourTable>** should specify the table containing your data. ▪ **<YourCriteria>** should specify any criteria you need to apply to your data. *NOTE: Variable values can be stored within the database and extracted within this SQL to create personalized messages, but:* ▪ the first field returned **MUST** be the email address ▪ the second field returned (if at all) **MUST** be the member ***Rights*** or blank ▪ subsequent fields can be any variable values you wish to use. If you also wish to use the ***Remove dead emails*** option in the **Options** tab, you will need to specify a second SQL statement here which IceWarp Server will use to delete addresses as required. The %s system variable should be used to specify the email address. For example: ***DELETE FROM <YourTable> WHERE <YourEmailField> = '%s'*** ▪ **<YourEmailField>** should specify the column containing the email address of the member. The two statements should be separated by a single line with a semicolon. Example: ***SELECT <YourData> FROM <YourTable> WHERE <YourCriteria>*** *;* ***DELETE FROM <YourTable> WHERE <YourEmailField> = '%s'*** If your SQL is particularly long, you can specify it within a simple text file and enter the fully

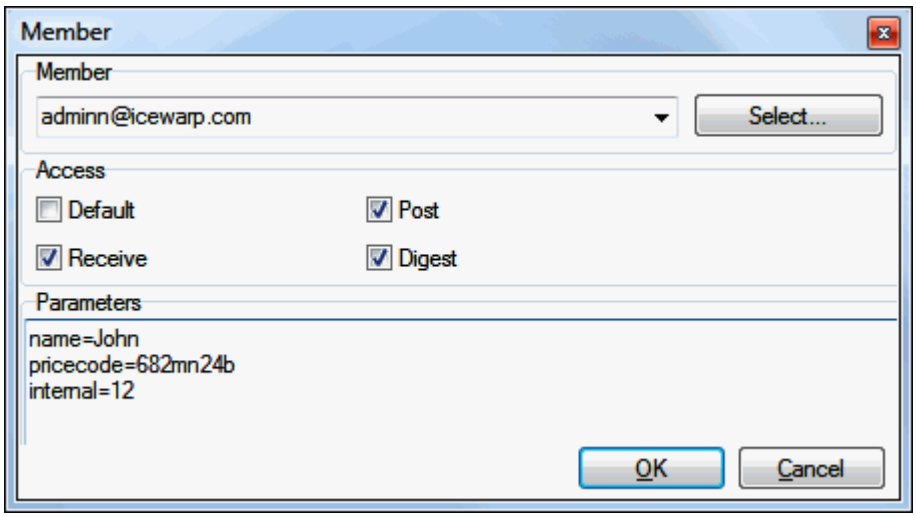
	qualified filename in this area. IceWarp Server will recognize this as a file name and read it to collect the SQL.
Test SQL query	Performs an SQL state command to see if everything has been setup properly.
ODBC settings	Sets the ODBC source for the database connection.

Members

This tab displays a sortable list of members of the selected mailing list. By default, members are listed in alphabetical order.



Button	Description
Add	Click the button to add a new mailing list member. The **Member** dialog opens.
Edit	Select a member and click the button to edit his/her settings. The **Member** dialog opens.
Delete	Select a member and click the button to delete this mailing list member.
Text File	Click the button to open and edit a plain text file listing the mailing list members. To reveal the syntax rules, click the ***Comment*** button there. *NOTE: You have to use UTF-8 format for this file, if you want to import it.*



Field	Description
Member	The email address of the member.

	It can contain the user's full name, in the following format: ***"John Doe"<john@icewarpdemo.com>*** You can use the ***Select*** button to open the **Select Account** dialogue. *NOTE: You also can send SMS messages to mailing list members. For more information, see lower.*
Access	Determines what the member can do. **Default** Member will have default rights as defined within the **Mailing List – Security** tab of mailing list settings. Or various combinations of the following can be chosen from: **Receive** Member will receive all messages sent to the list and cannot post messages to the list. **Post** Member can post message to the mailing list. **Digest** Member will receive all messages sent to the list, in a single "digest" message, and cannot post messages to the list. *NOTE: If a mailing list has a group entered as a member, then any rights defined in the mailing list for that group will override any rights defined in the group definition.*
Parameters	Defines variables which can be used within a message to create personalized messages. Variables can be included within a message by including the variable name enclosed within double braces. For example: in the above screenshot, any occurrence of ***{{name}}*** within the message is replaced with ***John*****.**

Sending SMS Messages to Mailing List Members

Besides email messages, you can set sending SMS messages to mailing list members. I this case, use the following syntax:

<sms:<number>?user=<username>&pass=<password>>

Where:

<number> – user's phone number

<username> – is a valid username for authentication (can be an account created for this purpose) – only required if SMS server authentication is active

<password> – is the valid password associated with the username – only required if SMS server authentication is active

Example:

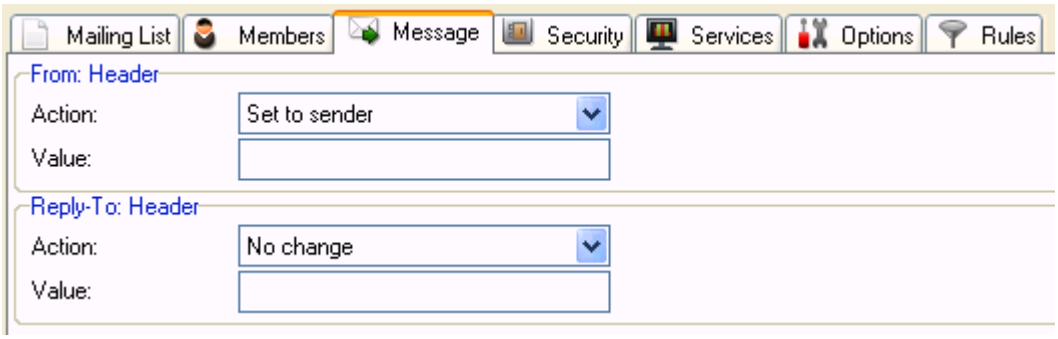
<sms:+15551234567?user=john&pass=johnspwd>

External Delivery

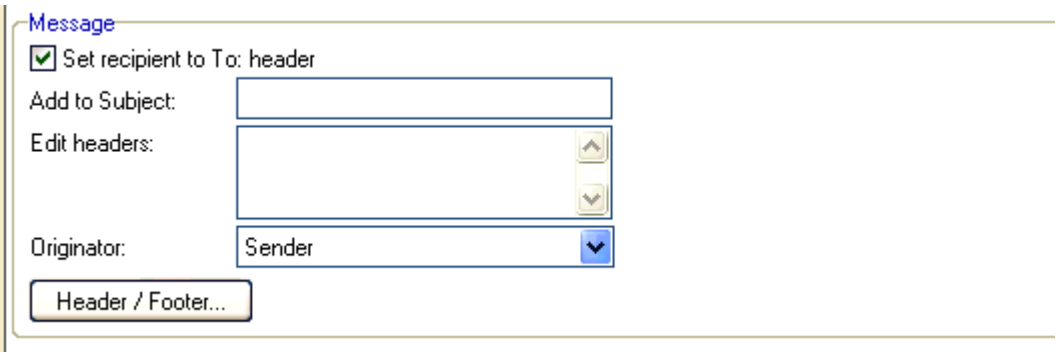
You may want to send messages to mailing list members as they were sent externally. Mailing list members can have whitelisted some other members or set rules for them. In the case such a member sends a message via a mailing list account, these whitelistings/rules will not work.

Use the *m_deliverexternally* API variable to workaround. (Right-click the mailing list name, select the *API console* item and search for ***externally***.) Set the value to *true*.

Message



Field	Description
From: Header	You can specify changes to the ***From:*** header of a message: **No Change** No change will be made. **Set to sender** The header will be set to the address of the message sender. **Set to Value** Set the header to the value specified in the ***Value*** box.
Reply-To: Header	You can specify changes to the ***Reply-To:*** header of a message: **No Change** No change will be made. **Set to sender** The header will be set to the address of the message sender. **Set to Value** Set the header to the value specified in the ***Value*** box.



Field	Description
Set recipient To: header	When a message is sent to a mailing list, the ***To:*** header will contain the address of the mailing list itself. Checking this option causes the ***To:*** header of each message is modified to contain the actual address of the recipient.
Add to Subject	This prefixes the ***Subject:*** header with the specified string.

	If the text is already present, it does not duplicate it. If the ***Subject:*** header is not present, it is created.
Edit headers	You can add any number of custom headers to the message. System variables can be used here. Example: ***Size:%%Size%%*** This field is limited in size, so if you need to add many headers you should use a file to specify the headers to add, like this: ▪ Enter **%%include <FileName>%%** in the Add headers: text area, where **<FileName>** is a fully qualified path to the file. ▪ Create the file specified, as a simple text file, and add the headers you wish to add to messages. *NOTE: Some systems (like Hotmail) dislike receiving messages from a list where the **FROM** header is one their customer's address, however, message was not sent through recipient's (Hotmail in this case) mail server's SMTP. One solution is to change the **FROM** to something static and define for example **Subject: %%subject%% - sent by %%sender_email%%** within the **Edit headers** field.* *This keeps the original subject that the user has typed and add the actual sender next to it.*
Originator	This is an advanced SMTP option. You can specify the exact content of the SMTP MAIL FROM command. The possible options are: **Blank** – the MAIL FROM command offers an empty field. **Sender** – the sender's address is used. **Owner** – the list owner's address is used. *NOTES:* *If the **Blank** option is selected (the default) some email servers might reject the message.* *When you choose the **Sender** or **Owner,** all bounce backs of failed messages will be sent to that email address.*
Header / Footer	The **Header/Footer** dialog is opened. Here you can specify text and HTML files (for text and HTML messages respectively) that will be inserted at the start and end of all messages sent through the mailing list. Always specify a fully qualified path to the file. *NOTE: HTML files should only contain HTML BODY content (without the BODY tags).*

Security



Field	Description
Only members can post new messages	Check this option to stop non-members of the mailing list from sending messages to the mailing list. *NOTE: This option does not override any member rights set in **Mailing List – Members**. A member must also have posting rights to be able to post.* *NOTE: If you do not check this option then **anyone** can send a message to the mailing list and it will be accepted (after usual rules, AntiSpam and IceWarp Anti-Virus checking).* *NOTE: One can forge the sender as being one of the list members and be able to send. To avoid it, use the **Reject if originators domain is local and not authorized** option (**Mail Service – Security – General**).* *Also, you can use the **Reject if SMTP AUTH different from sender** option (**Mail Service – Security – Advanced**) to prevent local users from mailing list misuse.*
Password protection	Select a level of password protection you require for this mailing list. **Not password protected** Users do not need to specify a password to post to the list. There are two types of moderated lists which require a password to be included either at the beginning of the ***Subject:*** header, or in the X-Approved MIME header. The difference between the two types is in the way that a message is treated when no password is given: **Server Moderated** A server moderated list will store a non-passworded message and send a copy to the list owner. If the owner wants to allow the message then he should reply to it (no password required) and the server will distribute the message. This is a way of having a list moderated by a real person. **Client Moderated** A client moderated list will send a non-passworded message back to the sender, effectively as a prompt to re-send the message with the password included. *NOTE: Some mail clients support the X-Approved MIME header which can contain the password. IceWarp Server will automatically check that header and allow the message if the password is correct.*
Password	The password which IceWarp Server will check for.

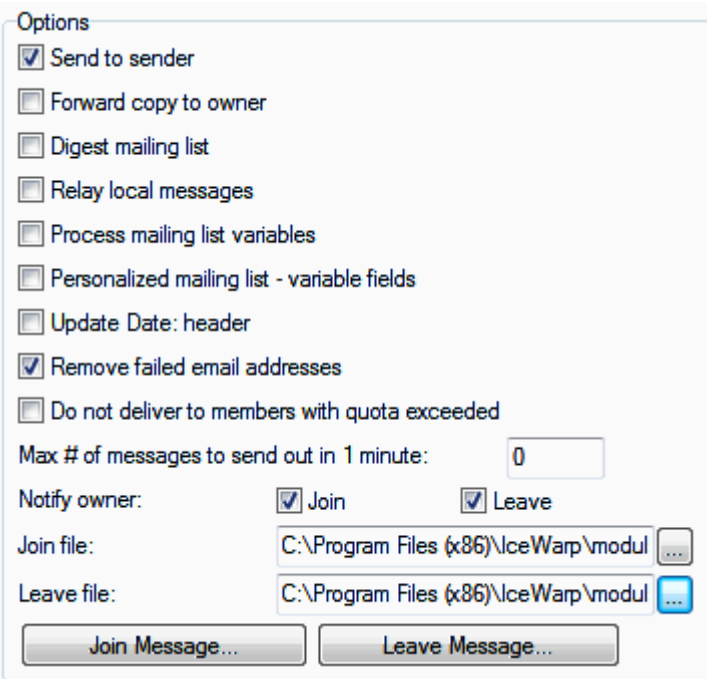
Allow subscribers	As an extra security you can specify a fully qualified path to a file of addresses which are allowed to subscribe to this list. Use a single line for each address.
Default Rights	Determines what rights a member will have if you chose ***Default*** rights for the member. Various combinations of the following options are available: **Receive** Member will receive all messages sent to the list **Post** Member can send any message to the mailing list. **Digest** Member will receive all messages sent to the list once a day (at midnight) in a package.
Max message size	Select a maximum message size that can be sent.
Max members count	Specify a maximum number of members for this mailing list. *NOTE: Limiting max members always applies to static members sources, such as all domain users or all system users.*
Deny EXPN	Normally, if a client issues the EXPN command the list members will be returned. As a security precaution you can check this option and IceWarp Server will respond with a "No such Mailing List" message.

Anti-Spam and Quarantine for Mailing lists

Up to version 10.4.x, it is possible to enable anti-spam and quarantine only for all mailing lists. Use the ***c_as_mailinglist_quarantine_disable*** and ***c_as_mailinglist_antispam_disable*** variables (**console – File – Api Console**).

For version 11.x, it is possible to enable/disable these features for individual mailing lists. Right-click the mailing list name (**Domains and Accounts – Management – <domain> – Mailing Lists**), select the *API Console* item and search for the ***m_as*** variable (for anti-spam) and ***m_cr*** one (for quarantine). Set them properly.

Options



Field	Description
Send to sender	When a list member sends a message to the list, he/she will also receive a copy if this option is checked.
Forward copy to owner	If the owner of the list is not a member of the list then checking this option will copy messages to the owner. However, it is recommended list owners to subscribe lists they own.
Digest mailing list	Checking this option will allow a user to subscribe to this mailing list as a "Digest" service. At midnight a single message containing all the messages of the day is sent to the members.
Relay local messages	Checking this option will instruct IceWarp Server to send all messages to local users via the outgoing queues and back to the local server. This means that all locally-bound messages will go through all the standard IceWarp Anti-Virus, AntiSpam, and Rules processing.
Process mailing list variables	Check this option if you want to allow variables (included in the **<install_dir>/examples/variables.dat.html** file) to be processed within messages sent to this list. *NOTE: This option has to be enabled the **Personalized mailing list...** feature to work properly.*
Personalized mailing list – variable fields	The personalized mailing list option lets you customize your messages with variables linked to the members of the list. Variables included within a message, in the format **{{VariableName}}** will be replaced with the corresponding value of the variable for each member. Variables are set when you define a member (see **Mailing List – Members**). Personalized mail example: Dear **{{name}}**, Congratulations! Your sales last month exceeded $**{{totalsales}}**. We are pleased to offer you a special price for your next purchases. Please use pricecode **{{pricecode}}** with your next order. Your Team In the above example the values for variables ***name, totalsales*** and ***pricecode*** will be replaced by the appropriate values. *NOTE: The **Process mailing list variables** option has to be enabled.*
Update Date: header	When using vast mailing lists, last messages can be significantly older than ones sent earlier. Tick this box if you want to have the time of sending updated.
Remove failed email addresses	Check this option if you want IceWarp Server to remove permanently any members from the list if it encounters a permanent error while attempting delivery. *NOTE: FULL MAILBOX at the receiving address can issue a fatal error and cause a legitimate address to be deleted – care should be taken in using this option.* To deal with this situation and enhance this feature capabilities, see the **Remove Dead Emails – Soft Failure Counter** subchapter lower. *NOTE: If you are using a database to store your lists you must also have specified the SQL to delete a user from the database – see **Mailing List – Definition**.* *NOTE: Dead email addresses are not removed immediately after the first unsuccessful delivery attempt. They are removed before the next delivery action.* *NOTE: This option does not work in the case the **Deliver messages via relay server***

	***when direct delivery fail**s option (**Mail Service – SMTP Service – General**) is enabled.*
Do not deliver to members with quota exceeded	Users can have set mail box limits. (Size, number of delivered messages, etc.) Tick this box if you want to exclude mailing list members with any of these limits exceeded from obtaining messages (until they "clean" their mailboxes).
Max # of messages to send out in 1 min.	Enter a non-zero number here to limit the number of messages that this list will send within one minute. This allows you to implement basic flow control for outgoing messages if your list becomes large (say 10000 members)
Notify owner	Check the **Join** and/or **Leave** boxes to automatically send a notification of these events to the list owner. (Applies in the case, the administrator has setup a ***listserver*** account.)
Join & Leave Files	Specify fully qualified file names to customized ***Join*** and ***Leave*** files and they will be used to create messages to new and departing members of the list. You can use the buttons bellow to edit these files once they have been specified.
Join message	Press this button to define a message that is sent to all users joining the mailing list.
Leave message	Press this button to define a message that is sent to users leaving the mailing list.

Remove Dead Emails – Soft Failure Counter

When using *Source: Members from database* (the **Mailing List** tab), you can use queries that:

- will select all mailing list members that have a "soft failure counter" less than e.g. 3,
- use (only) these users as mailing list members,
- raise the counter in the case, another fatal error occurs.

In addition, you can create a scheduled script that will check functionality of all email addresses with the counter higher than e.g. 3. It can either reset the counter (if the check is successful), increase it (if the check is not successful) or even (if the counter reaches some higher value) remove such an account.

Queries example:

table: mlist

columns: id int(11) auto_increment, email varchar(80) not null unique, rights varchar(16) default null, error int(4)

SELECT email, rights FROM mlist WHERE error<3;

UPDATE mlist SET error=error+1 WHERE email = '%s' ;

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

List Servers

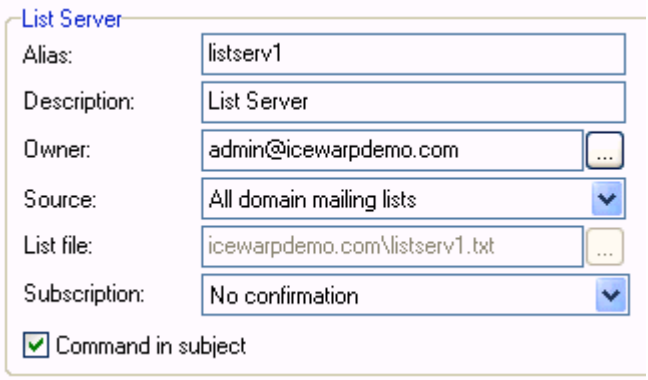
List server account is an account used to allow users to control their access to any mailing list accounts.

Various commands, such as ***Join*** and ***Leave***, can be issued via emails.

Moderated List Server option is available. It verifies all commands by means of a password.

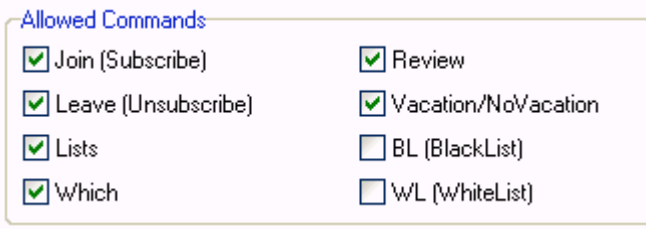
*NOTE: Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

List Server



Field	Description
Alias	A unique identifier for the account within the domain.
Description	A short description of the account.
Owner	The email address of the list server owner. Multiple addresses can be specified, separated by semi-colons. This address is used for replies from the list server and also for confirmation messages.
Source	Select whether this list server will serve all mailing lists on this server or only a sub-set: **All domain mailing lists** Select this option to have this single list server serving all mailing lists on this domain. **Mailing lists from text file** Select this option if you want to have multiple list servers serving different sub-sets of domains or you only want this list server to serve a subset of mailing lists. The text file containing the mailing list(s) to be served is selected in the next option.
List file	By default, this option is left blank, allowing all mailing lists within the domain to be administered just by this list server. If you need to have multiple list servers controlling different sets of mailing lists, you should create a list file specifying which mailing list accounts are controlled by this list server. Each mailing list address should be specified on a separate line, as shown below: ***list1@domain.com*** ***list2@domain.com***
Subscription	Select a type of subscription confirmation:

	No confirmation Subscription (or ***Join***) requests are processed without any confirmation. **User confirmed** Subscription requests will only be processed if the subscribing email came directly from the subscribing email address. This stops users from subscribing other people to the list. **Owner confirmed** Subscriptions requests must be confirmed via email by the owner of the mailing list.
Command in Subject	Checked by default, only the ***Subject*** header of an incoming message will be checked for a command. If you un-check this option, commands must be contained within the body of the message and multiple commands can be issued.



Check all the commands you wish to allow people to use on this list server.

*NOTE: **Join, Leave** and **Vacation/NoVacation** commands (only these) are not available when the **Source** feature (**Management – Mailing Lists – <mailing list> – Mailing List**) is set to **Members from database**.*

NOTE: These commands are case insensitive.

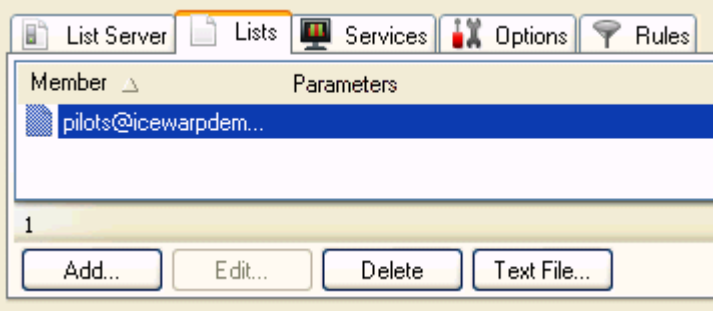
Detailed commands descriptions are given below:

Command	Description	Usage
JOIN, SUBSCRIBE, JOIN-DIGEST, SUBSCRIBE – DIGEST	The join or subscribe commands are issued by users who wish to join a mailing list. Adding ***JOIN – DIGEST*** to the command will cause the subscriber to receive one daily message containing all the messages for that day. *NOTE: This option only works if the mailing list has the **DIGEST** mailing list option set.* When the ***Owner confirmed*** subscription option is set, a confirmation message is sent to the owner of the list for approval.	JOIN|SUBSCRIBE [***password***] {list name}, [***email address***], [***full name***], [***rights]***,[***parameters***] Values in ***italics*** are optional. The action on omission of a ***password*** will depend on the **Subscription** option selected (see above). If ***email address*** is omitted, the sending address will be used. ***Rights*** are set as follows: 0 – no access at all 1 – Read only 2 – Post only 3 – Read and Post 4 – Digest only 5 – Read and Digest 6 – Post and Digest 7 – Read, Post and Digest If ***rights*** are omitted the default value of **3 – *Read and Post*** is used.

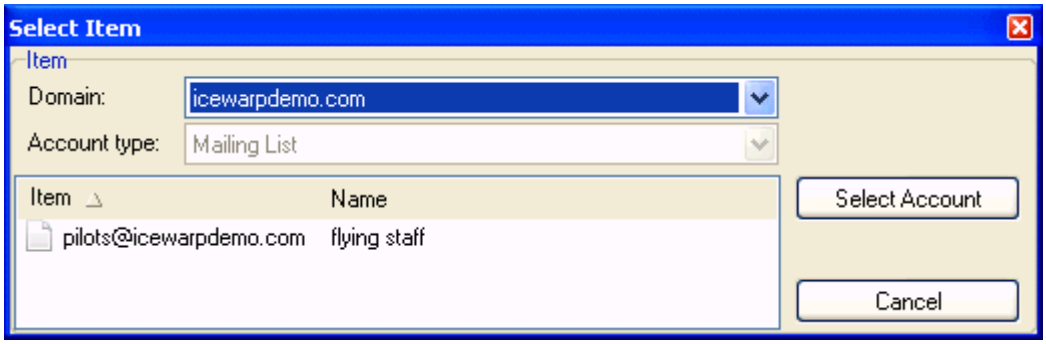
		Parameters are used for personalized mailing lists, multiple variables can be entered using & as a delimiter Example: JOIN listpass newsletter@domain.com,me@mydomain.com,My Name,7,name=John&city=London
LEAVE, UNSUBSCRIBE LEAVE-DIGEST UNSUBSCRIBE-DIGEST	Allows users to leave a mailing list.	UNSUBSCRIBE|LEAVE [***password***] {list name}, [***mail address***]
LISTS	Allows a user to obtain a list of all the mailing lists that are served by this list server.	LISTS [***password***]
WHICH	Allows a user to retrieve a list of all mailing lists which he/she has subscribed.	WHICH [***password***] [***mail address***]
REVIEW, RECIPIENTS	Allows a user to retrieve a list of subscribers to a mailing list.	REVIEW|RECIPIENTS [***password***] {list}
HELP	Allows a user to retrieve a list of all list server commands (as on this page). This response can be customized using the ***List server help*** field under the **Options** tab.	HELP [***password***]
BLACKLIST or WHITELIST (BL or WL)	Allows a user to add/remove email addresses to/from his individual Black & White List rules.	BLACKLIST [***password***] {email}, [sender], ["remove"] or WHITELIST [password],{email}, [sender], ["remove"]
VACATION or NOVACATION	Allows a user to temporarily stop receiving messages. Issue the ***VACATION*** command to stop receiving and the ***NOVACATION*** command to start receiving again. This can also be used where somebody is subscribed to a mailing list with two addresses but only wishes to receive messages to one account. He/she should issue the ***VACATION*** command from the other address.	VACATION [***password***] {list name}, ***[mail address]*** NOVACATION [***password***] {list name}, [***mail address***]

Lists

This tab allows you to select which lists are to be managed by this list server. You are presented with a list of managed lists:

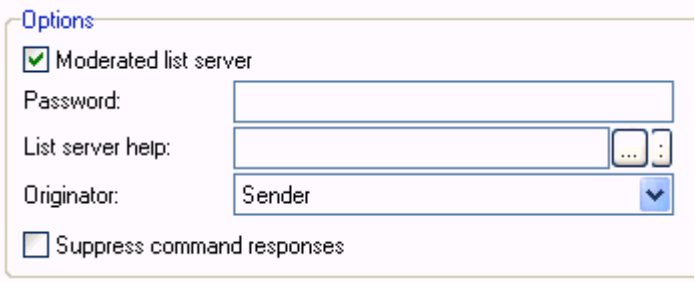


Button	Description
Add	Click the button to add a new list. The **Select Item** dialog is shown – see below.
Edit	The button is disabled here.
Delete	Select a list and click the button to remove this list.
Text File	Clicking this button opens a text file with mailing lists served by the list server. Click the **Comment** button here to reveal a help with syntax rules and examples. *NOTE: This button is enabled only if the **Source** feature (the **List Server** tab) is set to the **Mailing lists from text file** option.*



Select the list(s) and press the ***Select Account*** button to add them.

Options



Field	Description
Moderated list server	When checked all list server commands are protected by a password (see the previous section for command syntax). If the password is omitted or an incorrect password is given, the command will not be processed.
Password	Specify the password here.
List server help	If a user sends the HELP command to the list server, the server responds with a standard help message. You can customize the content of the message by specifying a text file here. A second file can be added here. It will be used as the confirmation message from the list server if confirmed subscriptions are in use. Syntax: ***helpfile;confirmationfile***
Originator	Here you can choose the content of the SMTP ***MAIL FROM*** command. The possible values are: **Blank** – some mail servers may reject a message with an empty ***MAIL FROM*** header. **Sender** – the sender's address will be used. **Owner** – the owner's address will be used. *NOTE: If you choose **Sender** or **Owner** any bounced messages will be sent to that address.*
Suppress command responses	Failure and success responses to commands are suppressed and not sent to the sender of the command. This might be useful when processing web form requests by emails.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Example

Here is an example of how to use a list server.

Assume the following for the list server:

Domain	icewarpdemo.com
List Server Alias	ls1
List server password	lspass
Command in Subject	Yes
Mailing lists served by this server	announcements tech_news general

To get a list of mailing lists send an email to ls1@icewarpdemo.com with a subject of ***LISTS***.

Executables

Executable accounts are designed to allow you to run jobs or processes on a server without using any remote access tools. A job is defined in advance on the server and it can be executed by sending an email to the executable account.

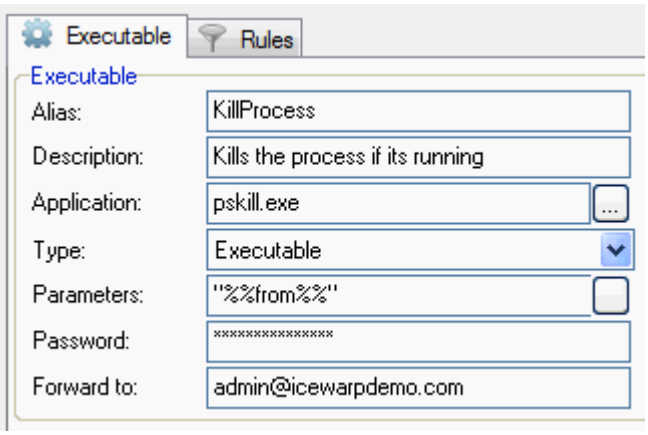
Be aware that the process must exit correctly by itself without any need for user input, so the server can complete the task correctly.

It is highly recommended that a password is set for the executable account and/or rules are set up to restrict email access to the account.



*NOTE: Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Executable



Field	Description
Alias	A name for the account within this domain.
Description	A short description of the account.
Application	Specifies the fully qualified file name (or URL) of the executable, which can be a DOS, Win32 application or a DLL. *NOTE: It **must not** be a GUI application which requires user input.*
Type	You must choose the correct type of application here for the executable to be processed correctly. Use ***Executable*** for DOS. Use ***StdCall*** or ***Cdecl*** to specify the library interface for a DLL file. Use ***URL*** when the executable is a remote script.
Parameters	If the executable requires parameters they can be specified here. You can also pass IceWarp Server system variables to the executable A complete list of variables can be found in the system variable example file (**<InstallDirectory>/examples/variables.dat.html**) Some examples are: ***%%From%%*** – who the mail was sent from ***%%To%%*** – who the mail was sent to ***%%Subject%%*** – the subject of the mail

	%%MessageFile%% – the full path and file name to the received message
Password	The executable account can be protected by a password. If this field is filled, the ***Subject*** of the message will be checked for the password. If the password is found, it is deleted from the ***Subject*** and the executable is processed. If the password is not found, the executable is not processed – an error message is not sent.
Forward to	Specifies that the message is also forwarded to the address specified here. This way you will know it was executed.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Remote Accounts

Remote accounts are used to fetch mail from accounts on external POP3 and IMAP servers.

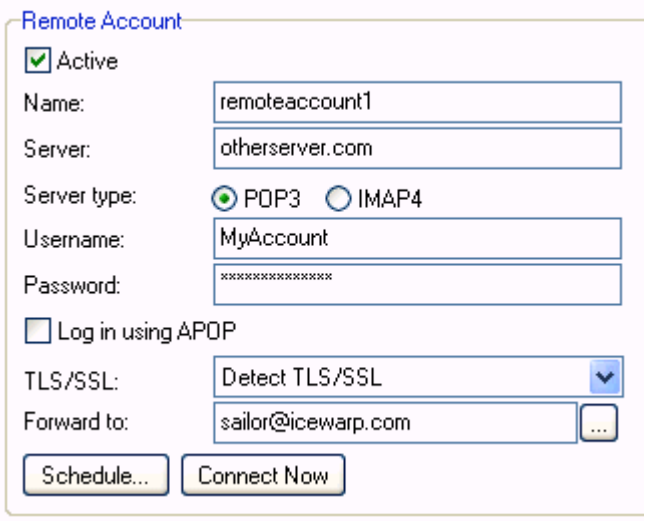
A ***Forward To*** can be set to receive messages that cannot be distributed correctly.

If the remote account is a catch-all account and you set IceWarp Server to use Domain POP processing, it will distribute the messages accordingly.

Copies of all messages can be sent to an address for audit or archive purposes.

*Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Remote Account



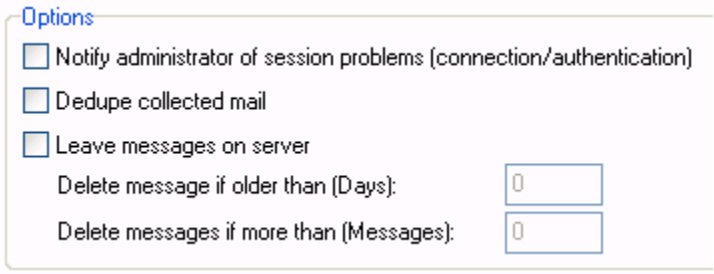
Field	Description
Active	Check this box to make this remote account active.
Name	A unique name for the account within this domain.
Server	Specify here the host name of the server that this remote account should collect messages from. Examples: ***pop3.demo.com*** ***imap.demo.com*** *NOTE: In the case POP3/IMAP run on non-standard ports, you can specify them:* ***pop3.demo.com:966*** *NOTE: By default, only messages from INBOX of the remote server are downloaded, but you can override this. Use the following syntax:* ***hostname/folder** – **folder** is either * (asterisk) or a folder name* *e.g. **imap.demo.com/*** – contents of all folders are downloaded* ***imap.demo.com/myfolder** – only content of **myfolder** is downloaded*

Server type	Specify the protocol that should be used to collect messages: ***POP3 –*** use the POP3 protocol to collect messages. ***IMAP4 –*** use the IMAP4 protocol to collect messages. *NOTE: The local account (specified in the **Forward to:** field, see below) must be an IMAP4 account.* *ALSO: When the POP3 protocol for a remote server is used, message downloads can overlap – it can cause a message dupe. If so, use POP3 with POP3 locking – enable it using API Console (the **c_system_pop3_locking** variable). In this case, only one connection at a time is realized.* *NOTE: If you do not mark to Leave messages on server (the **Options** tab), even in the case you choose IMAP, all emails will be deleted from the source folder.*
Username	You need to specify the ***Username*** that is used to access the remote server to collect mail.
Password	The password for the ***Username*** specified above.
Log in using APOP	For extra security, and if the remote server supports it, you can specify that APOP is used for the login process. APOP is a secure login method using ***md5*** encryption.
TLS/SSL	Specifies whether to use a TLS/SSL connection to access the remote account. We recommend leaving this option as the default (Detect TLS/SSL). ***Detect TLS/SSL –*** The remote connection will be checked using the CAPA command for TLS support. If supported, the connection will continue in TLS/SSL mode. ***Direct TLS/SSL –*** The connection will be made using TLS/SSL. ***Disable TLS/SSL –*** No TLS/SSL will be used – a non-secured TCP/IP connection will be established.
Forward to	An account should be specified here where messages will be forwarded if the local recipient cannot be found. In the case you use ***DOMAIN POP***, the email address specified here receives emails where IceWarp Server cannot DISCERN to whom to send mails fetched via a remote account to. *NOTE: If you specify a path to a mailbox here, the folder structure of the remote server is created within this mailbox and no filters or AntiSpam processing is applied.* *You should also be aware that original receive times are only kept for IMAP collection as POP3 does not provide this information.* *The folder structure is created according to the settings in the **Server** section. I.e. if it is set to download only messages from one folder (by default only messages from INBOX are downloaded), then, of course, only this one folder is created locally.* *Hence, full folder hierarchy is created only if you specify **hostname/*** in the **Server** section.* *The path specified here can be absolute, or relative (e.g. **icewarpdemo.com\joe**).*
Schedule	Use the ***Schedule*** button to open the standard **Schedule** dialog where you can define a schedule for mail collection. *NOTE: You can also set a global schedule (within a remote account template), allowing you to use this schedule rather than defining one for each remote account.* *NOTE: Choosing the **Every x minutes** option for email download and setting it to a short interval (say 5 or 10 minutes) can cause download overlaps.* *If this situation occurs, you can resolve it by enabling POP3 locking on the remote server (provided that it is also IceWarp Server):* ***C_System_POP3_Locking = $31E;** // Bool POP3 does not allow multiple login of one*

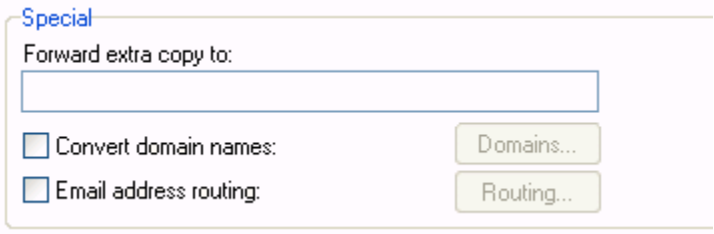
	account 0 *Use this command:* ***tool modify system C_System_POP3_Locking 1***
Connect Now	Use this button to connect to the remote server and collect mail immediately.

*NOTE: You may want/need to reset a downloaded emails index for a specific user. In the **<install_dir>/config/<domain>** directory, find the **remote.<user_name>.<alphanumeric_string>** file and delete it.*

Options



Field	Description
Notify administrator...	Check this option and the administrator will receive email messages if there are any problems connecting to the remote server.
Dedupe collected mail	IceWarp Server will store ***Message-ID*** headers and if duplicates are found only the first will be processed. Storage of headers is only for the current connection session, so the dedupe is per session. This option is recommended for ***Domain POP*** mode to avoid duplication of messages sent to multiple local recipients.
Leave messages on server	IceWarp Server will not delete messages from the remote server after collection. A log of downloaded messages and their IDs is kept so that messages are not downloaded in subsequent sessions. *NOTE: If you want to re-download all messages delete (or rename) the **remote.cfg** file (**<install_dir>/config**). This action clears indexes for ALL remote accounts!*
Delete message if older than	If the message on the remote server is older than the specified number of days it is deleted. Useful in conjunction with ***Leave messages on server*** as simple server message storage management.
Delete messages if more than	If there is more than the specified number of messages on the server, all messages are deleted.



Field	Description
Forward extra copy to	All messages received by the remote account can also be forwarded to a given email address using this option. This could be useful as an archive solution.
Convert domain names	IceWarp Server expects the domain name on the remote server to be the same as the name of this server. You can create a set of rules to convert domain names that are not defined, each rule on a separate line. Example: ***what.com=here.com*** would cause any email to ***someone@what.com*** to be re-routed to ***someone@here.com***
Email address routing	This option lets you specify routing rules for messages received by the remote account. Clicking the ***Routing*** button opens a dialog to create these rules, with examples. Examples: ***sales@icewarpdemo.com=info@business.com*** ***Mymail.com=icewarpdemo.com*** ***usa.net=info@icewarpdemo.com*** The above rules have the following affects: messages to ***sales@icewarpdemo.com*** are routed to ***info@business.com*** messages to ***Mymail.com*** are routed to ***icewarpdemo.com*** messages to ***usa.net*** are routed to ***info@icewarpdemo.com***

Domain POP



Field	Description
Domain POP	Check this option to tell IceWarp Server that this remote account is collecting email from a

	catch-all account at the remote server, i.e. the account contains all the messages for the domain. The domain should exist on the IceWarp Server. Messages are distributed according to the their headers. See the previous sections for explanations of the ***Forward to*** and ***Convert domain names*** options. *NOTE: For a catch-all account on the source (remote) server, it is recommended to tick the **Add X-Envelope ...** box (**<account> – Options**) to distinguish to what account emails should be forwarded to, even in the case the recipient is in the **Bcc** field. (Provided that this remote server supports the **Add X-Envelope ...** feature).*
Do not process Received: header	Specifies that IceWarp Server should not use the ***Received:*** header or the "for" item to evaluate the recipient. Some remote mail servers set these fields to an email address differing from the one in the ***To:*** header. This can cause severe problems. *This option is recommended.*
Stop parsing if Received: yields a local address	If IceWarp Server is set to process received headers it will always use the first received header created in the message. Checking this option tells IceWarp Server to check all of the received headers for a local email address. The first, if any, local address found will be used to deliver the message.
Parse these headers	Checking his option tells IceWarp Server to check other MIME headers for recipient information. Click the ***Headers*** button to create your list of headers to check.
Real name address matching	Checking this option instructs IceWarp Server to search for and check real names in the message headers. For example, if a message is found for "John Doe <john@doe.com>" IceWarp Server will look for "John Doe" on the server and, if found, will deliver the message to that account.
If email	Specifying an email address here limits the ***Real name address matching*** to messages addressed to this email address.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Static Routes

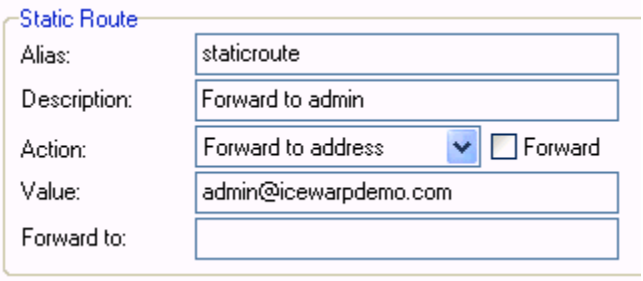
Static routes are simply aliases which are able to receive mail and perform a pre-defined action directly on the server based on whatever filter mechanisms are configured.

Most actions can be achieved using content filter actions or redirect features (SMTP routing) and these are the preferred methods.

This type of account is available for backwards compatibility of IceWarp Server versions.

*Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Static Route



Field	Description
Alias	A unique identifier of the account in the domain.
Description	A short description of the account.
Action	**Forward To Address** All messages will be forwarded to an address. The forwarding address must be specified in the ***Value*** field. **Forward To Domain** All messages will be forwarded to a domain, the alias of the recipient will be preserved. The domain must be specified in the ***Value*** field. **Forward to Host** All messages will be sent to the specified host machine. It can be a host name or IP address. The host or IP address must be specified in the ***Value*** field. **Deliver to This Domain** All messages will be delivered to a domain without any other filtering. This is useful when you want to check all messages for something (with external filters, for example) and then deliver it to the recipient. You can use external filters to do whatever you want. The domain must be specified in the ***Value*** field. **Delete** All messages will be deleted.

Forward	Checking this option instructs IceWarp Server to forward messages via the outgoing queue, even if the domain is local.
Value	Described in the ***Action*** field above.
Forward to	This option lets you save or archive all messages which meet the filter criteria. This is the email address to send messages to.

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Notifications

This is an account you can use to convert an incoming message into a format suitable for delivery to a gateway server, such as an SMS or instant messaging server.

In essence, this usually means chopping the message into notification chunks, stripping off attachments, changing the subject and defining the body of the message to be sent.

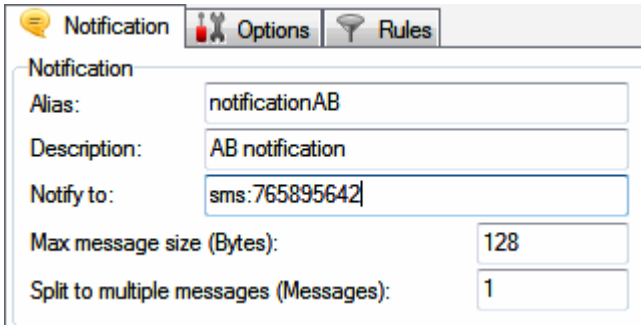
In order to use this option, you need an email gateway from your provider. (Even if you do not have one, you can use IceWarp SMS Server to deliver messages to such devices. Exchange Active Sync is another way how to deliver emails with push). This means you need to have an email address you can send messages to where they will be forwarded to your notification device. These devices can be PDAs, cell phones or any other devices capable of receiving short messages.

The same can be achieved using the content filters. This is a simplified object to be used for such requirements.



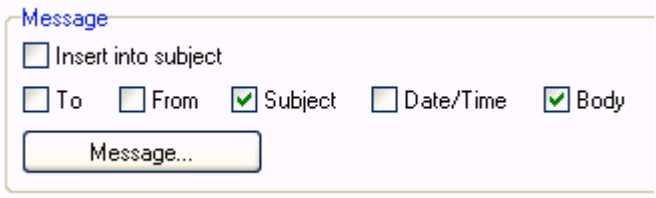
*Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

Notification

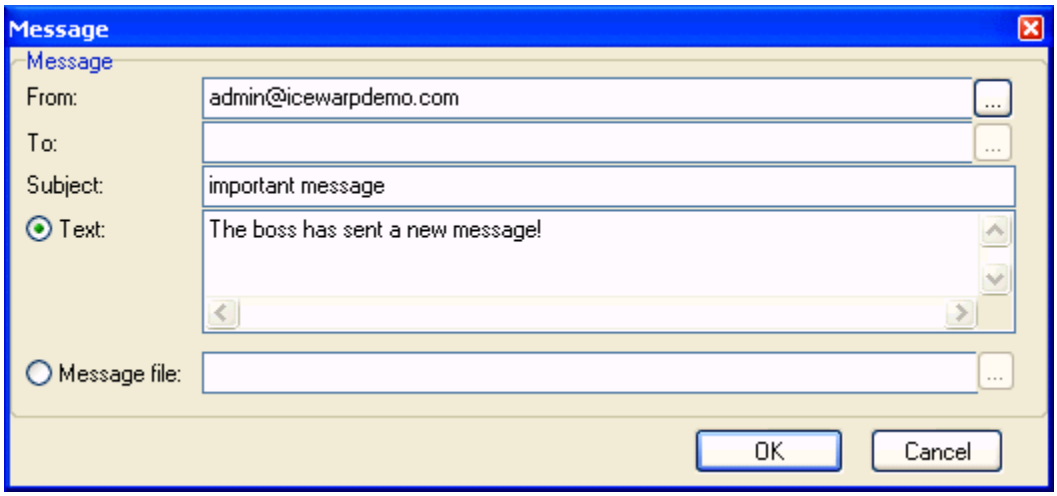


Field	Description
Alias	A unique identifier for the account within the domain.
Description	A short description of the account.
Notify to	Specifies the email address that the formatted notification message will be sent to. *NOTE: You can also send an instant message or an SMS using this option:* *sms – use **sms:<number>** e.g. sms:123456789* *IM – use **xmpp:<jabberid>** e.g. bruce@icewarpdemo.com* The example above shows how to send an SMS to the phone number of 123456789. Multiple addresses can be specified, separated by semicolons.
Max message size	This specifies the maximum number of characters that can be accepted in a single notification. This is specific to the gateway provider.
Split to multiple messages	The option specifies the number of chunks a message should be split to when the length of the notification message text exceeds the value specified in the ***Max message size*** field.

Options



Field	Description
Insert into Subject	The subject of the notification message will be compiled from the options below.
To	The original ***To*** header will be placed into the notification.
From	The original ***From*** header will be placed into the notification.
Subject	The original ***Subject*** header will be placed into the notification.
Date/Time	The original ***Date*** header will be placed into the notification.
Body	The original body content will be placed into the notification.
Message	Clicking the ***Message*** button opens the **Messag**e dialog. It allows you to specify your own content for various parts of the message, as described next.



Field	Description
From	Specify your own ***From:*** header for the notification message. System variables are allowed.
To	This field is disabled – it has no use here. (The dialog is shared.)
Subject	Specify your own ***Subject:*** header for the notification message. System variables are allowed.
Text	Select this radio button and enter some text to be used for the message body.
Message file	As an alternative to using the ***Text*** area to format your message, you can tell IceWarp Server to use a pre-formatted file. Press the '...' button to open a standard file browser to select the file you want to use.



Field	Description
Forward to	Specify an email address that the original message will be forwarded to – also ***sms:*** protocol and ***xmpp:*** one can be used. For audit or archive purposes.
Originator	This is an advanced SMTP option. You can specify the exact content of the SMTP MAIL FROM command. The possible values are: **Blank** – an empty mail ***From:*** header will be generated. **Sender** – the original sender will be used. **From** – the owner of the account will be used. *NOTES:* *If the empty mail **From** is selected (default), some email servers might reject the message.* *When you choose either **Sender** or **From** all bounce backs of failed messages will be sent to that email address.*

Rules

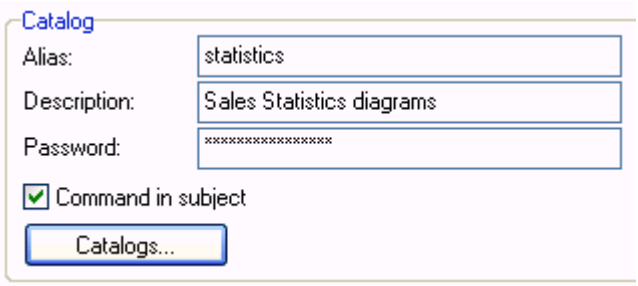
Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters – Rules** section.

Catalogs

Catalog is a type of "FTP via email", where you define catalogs that point to directories on the server drive(s) and users can send emails with commands to ***GET*** or ***LIST*** files in a catalog. If they choose to ***GET*** a file, it is sent to them as an attachment.

For syntax examples, refer to the **Options** chapter.

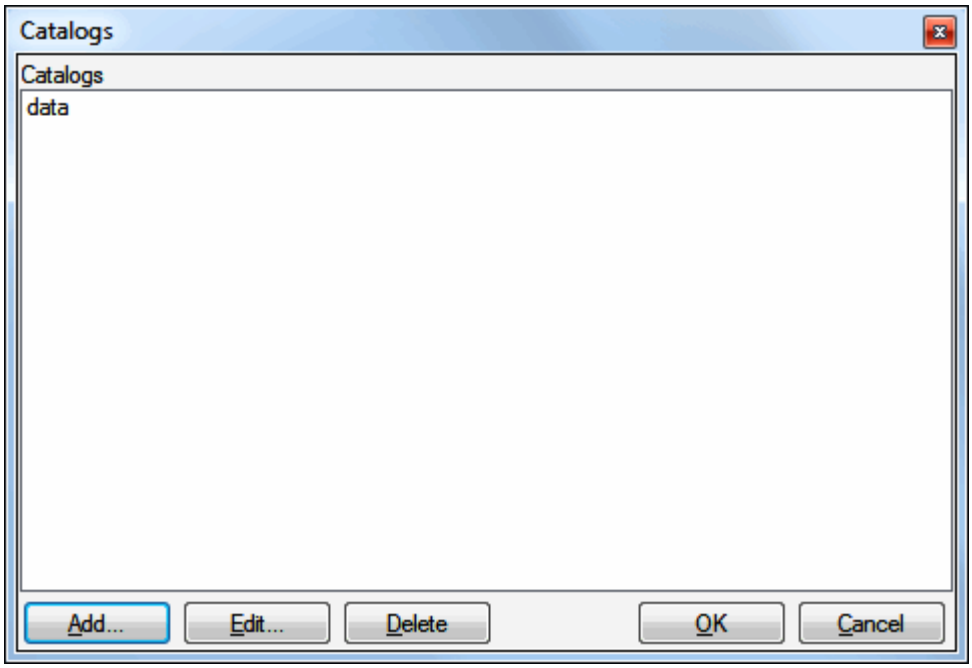
Catalog



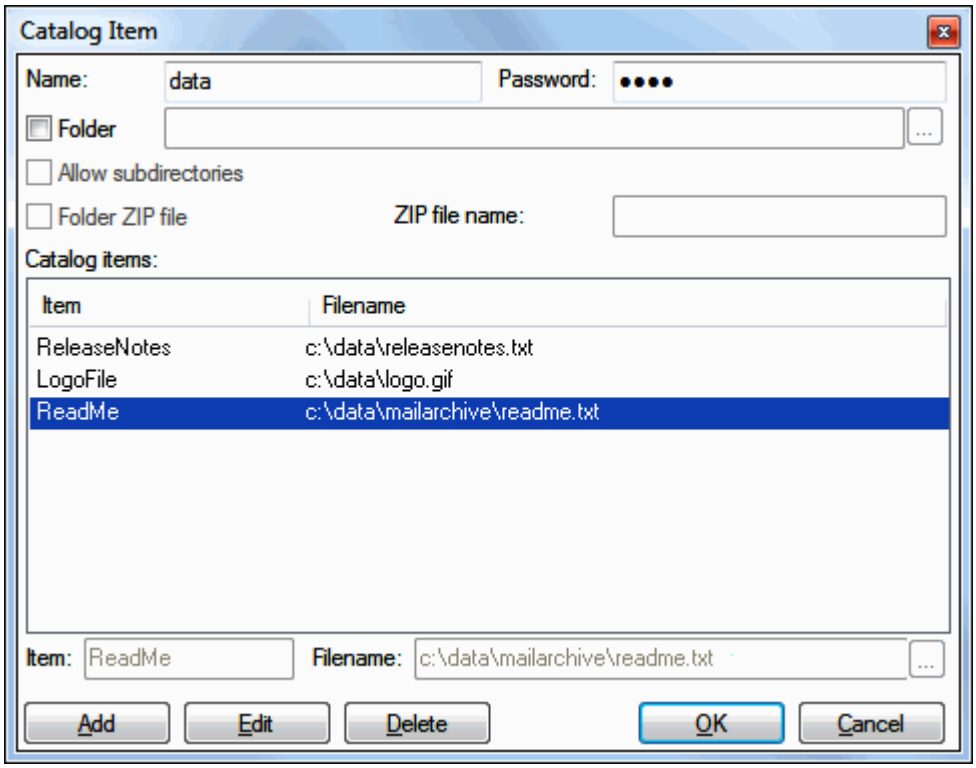
Field	Description
Alias	A unique identifier for the account within the domain.
Description	A short description of the account.
Password	You can specify a global password which must be used for all commands sent to this catalog account. We recommend to protect all your catalogs with passwords. You should also take care to protect the passwords themselves.
Command in Subject	By default, all commands are read from the ***Subject*** header. If you uncheck this option, the message body will be checked for commands. Possible command within the ***Subject*** header is ignored, in this case. This allows multiple commands to be issued within the body text.
Catalogs	This button brings up the catalog configuration dialog where you can define all the catalog stores and items. See **Catalog – Maintenance**.

Maintenance

To define/modify files and directories within the catalog account, click the **Catalogs** button.



In the **Catalogs** dialog you can add, edit and delete particular catalogs.

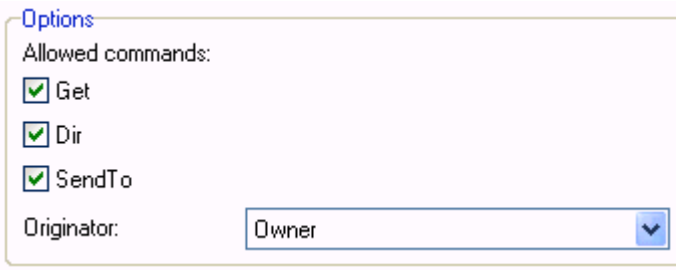


In this dialog you can configure the whole catalog.

Field	**Description**
Name	Specifies the catalog name or ID which will be used in the commands. This should be unique within the catalog accounts.
Password	Specifies the password required to GET this item (the DIR command does not require a password).
Folder	Specifies that this item is a folder. All files within the folder will be available individually within the catalog.

	You have to enter a fully qualified path in the text box.
Allow subdirectories	Only available if the item is a folder, checking this will include files within subfolders of the specified folder.
Folder ZIP file	If checked, all files in this item will be compressed using ZIP compression. You have to fill in the ***ZIP file name*** field for the file. This option is useful when you have a large amount of data within a catalog. The ZIP file, if sent as an attachment via email, can be automatically decompressed by a content filter. See the ***Actions*** list of the content filters options.
ZIP file name	The file name to which the folder will be compressed.
Item	Choose a unique identifier for the item within the catalog – available when adding or editing an item (via the ***Add*** or ***Edit*** buttons). This is the item name that is used within the ***GET*** command.
Filename	Specifies the full path to the file which is linked to this item. Use the "..." button to browse to the file.

Options



Field	Description
Get	Check this box to allow users to retrieve files from the catalog. Syntax: ***GET [Catalog_Account_Password] Catalog_Name Item [Catalog_Password]*** Example: ***GET marketing23 Prices PriceList2 Prices2010*** *NOTE: Passwords are to be included only if they are set.*
Dir	Check this box to allow users to retrieve a directory listing of the catalog contents. Syntax: ***DIR[Catalog_Account_Password] Catalog_Name*** Example: ***DIR marketing23 Samples*** *NOTE: Password is to be included only if it is set.*
SendTo	Check this box to allow users to send catalog content to another users. The ***SENDTO*** command lets users specify the receiver's email address. Syntax: ***SENDTO [Catalog_Account_Password] Email_Address*** Example:

	SENDTO j.doe@navy.org ***GET nelson Ships Sails horatio*** *NOTE: Passwords are to be included only if they are set. Not set in this example.* For information about multiple commands, see further.
Originator	Select the address that will be used as the sender field of emails sent by the catalog. Choose from: ***Blank*** – the ***Sender*** field will be left blank. ***Sender*** – the ***Sender*** field will be populated with the address of the initiator of the email. ***Owner*** – the ***Sender*** field will be populated with the address of the catalog owner.

Multiple Commands

Multiple commands are sent within an email body. In this case, any command in the ***Subject*** header is ignored. Many users use pre-defined signatures that are inserted into emails. These are ignored as well as other text.



*NOTE: For multiple commands, the **Command in subject** box (**Catalog – Definition**) has to be un-ticked.*

Example 1:

Assume, we have a catalog account and catalogs without passwords set.

DIR CATALOG1

DIR CATALOG2

GET CATALOG1 Manual.doc

This set of commands returns lists of catalogs items plus attaches the ***Manual.doc*** item to the answer mail.

Example 2:

SENDTO flying jerry@pilots.net

GET flying Plains gliders2.pdf

SENDTO flying sue@pilots.net

GET flying Plains gliders2.pdf



NOTES:

*When a catalog account password is set, it is necessary to use it also for the **SENDTO** command.*

*It is necessary to repeat the **GET** command for all recipients even if the same item is sent.*

*Catalog password is not set, hence not used for the **GET** command.*

Rules

Rules are common to all domain types and user accounts and are described in detail in the **Mail Service – Rules – Content Filters –Rules** section.

Global Settings

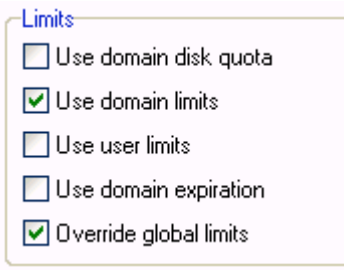
The **Global Settings** area allows you to set certain options which can affect all accounts, all domains and some console display areas.

Some of these global options affect whether further domain and account options are available for use.

Domains



*Do not forget that templates can be set up to streamline the definition of accounts, see **Account Templates**.*

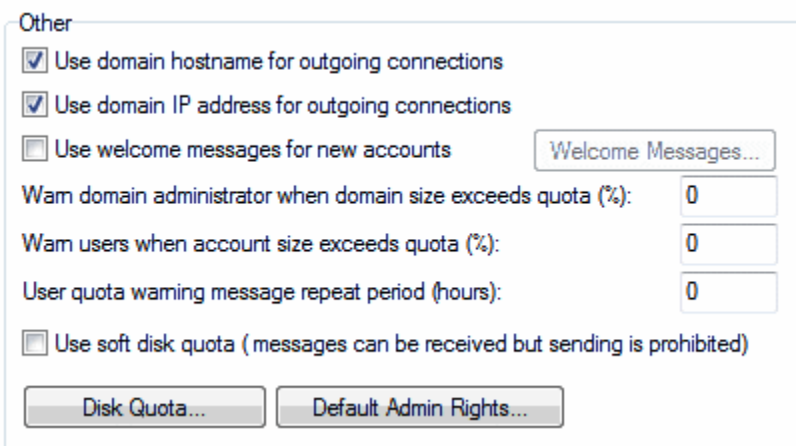


Field	Description
Use domain disk quota	Check this option IceWarp Server to check for domain disk quota information when messages are received. Domain quotas are defined in the **diskquot.dat** file, which can be edited by using the ***Disk Quota*** button (described below). Quotas can also be defined in **Domain – Limits**. *NOTE: Not all domains have to have a disk quota defined and you can specify a default disk quota for domains that have no individual quota defined.*
Use domain limits	Check this option to allow domain limits to be set and applied.
Use user limits	Check this option to allow domain-level limits for users to be set and applied.
Use domain expiration	Check this option to enable domain expiration dates.
Override global limits	Check this option to have ***non-zero*** domain-level limits override global ones. *NOTE: This option applies for **Max message size** set globally (**Mail – General – Delivery**; for both sent and received messages) versus the same feature set on the domain level (**<domain> – Limits – Users – Max message size**; for sent out messages).*



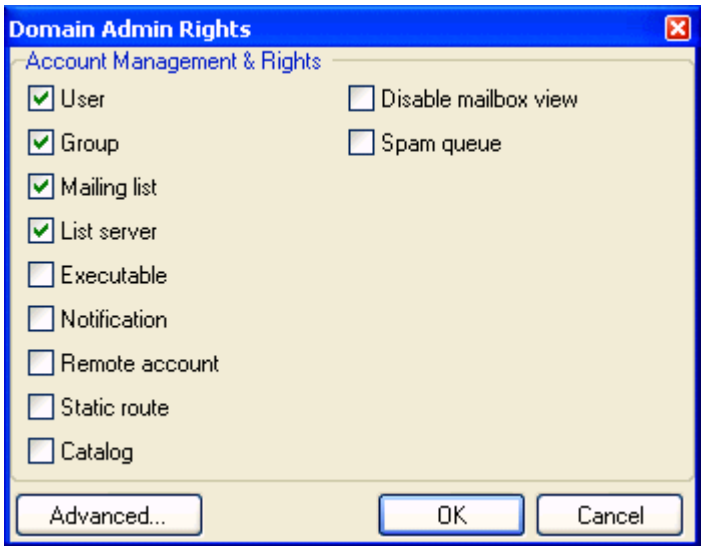
Field	Description
Enable DKIM	Enables use of DKIM AntiSpam technology within a domain (see ***Domain – DKIM***).
Enable domain literals	Checking this option virtually bind all your domain names to IP addresses. The effect of this is

	that your domain will be capable of receiving emails in the following format: user@[IP] The real IP value depends on your IP binding settings and system IP addresses. This can be useful for testing – you may want to send emails to a domain without DNS records.



Field	Description
Use domain hostname for outgoing connections	Check this option to force IceWarp Server to use the hostname defined on domain level in the SMTP HELO command. Contrary to globally defined one (**System – Services – SmartDiscover – SMTP**).
Use domain IP address for outgoing connections	Checking this option will force all emails from a domain to be defined as coming from the IP address specified for the domain in **Domain – Options**. This is helpful when trying to connect to external servers using AntiSpam technologies which check the sending server.
Warn domain administrator when domain size exceeds quota (%)	Specify a percentage value and a warning message will be sent to the domain administrator (specified on the **Domain** tab) when the domain exceeds that percentage of its quota. A value of 0 means no warning will be sent. For example, set value to 85 to have the warning message sent when the domain space reaches 85% of the quota.
Warn users when account size exceeds quota	Specify a percentage value and a warning message will be sent to the user when their account exceeds that percentage of its quota. A value of 0 means no warning will be sent. For example, set value to 85 to have the warning message sent when the domain space reaches 85% of the quota. (Plus another message is sent when the defined threshold is reached.)
User quota warning message repeat period (hours)	Define a time period after what warning messages are to be sent again. 0 (zero) means the message is never repeated. The warning message is only sent when the account recieves a new message or at midnight every day. The period defined is the minimum time between two warning messages.
Use soft disk quota...	Tick the box if you want to use the soft quota feature. When the quota is exceeded, the user still can receive mails as normally, but each attempt to send mail will fail with e.g.: ***501 5.7.1 <abc@top.com>... Soft quota applied***
Disk Quota	Click this button to edit the **diskquot.dat** file (in the **Config** subdirectory). This file contains all the domain disk quota data in a simple format that you can modify. Examples are included. The format of the file is as follows: ***domain=limit***

	Example: ***usa.net=5000*** ****=10000*** This specifies that all domains have a 10MB limit apart from ***usa.net*** which has 5MB. *The default (*) line should be the last line in the file.*
Default Admin Rights	Click this button to select the default domain administrator rights. See the **Domain Admin Rights** dialog. *NOTE: If you want to change default domain administrator rights here and you have some domain administrators already set, you have to change their rights manually. All domain administrators created after this change will obtain correct rights.* *In the case you have too many domain administrators to change rights manually, use some find and replace tool to replace all **domain.dat** files within the **IceWarp/mail** folder. The correct **domain.dat** file you can find after rights setting in the **IceWarp/config** folder.* *Another way is to set the rights here properly and delete all **domain.dat** files. Domain administrators will inherit global rights.* *For more information about the **domain.dat** file, refer to the **F1 help – Shared Topics – Domain Admin Rights** chapter.*



Field	Description
Account Management & Rights	Here you can set the default domain administrator rights for single items of the **Domains and Accounts** module. Besides the domain items explained in this manual (see the **Accounts** section), there are two other check boxes: ▪ Disable mailbox view – tick this checkbox if you want to prevent domain administrators from viewing domain users mailboxes and their emails. ▪ Spam queue – tick this checkbox if you want to allow domain administrators to administer spam queues (quarantines) of domain users.
Advanced	Click this button to edit the **domain.dat** file. For more information about the **domain.dat** file, refer to the **F1 help – Shared Topics – Domain Admin Rights** chapter.

Templates

Using templates can ease your work and make it more productive. This section is referred back to more times in the manual and it is probably worth familiarizing yourself with these ideas.

Most of the examples given further deal with account templates but other ones (group, domain, etc.) are used alike.



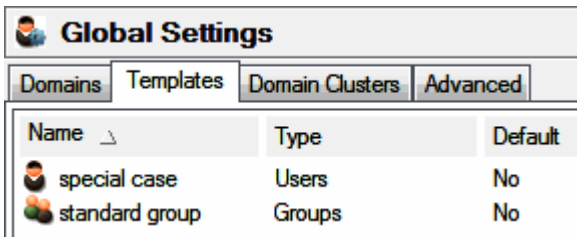
BE AWARE: Not all options can be set via templates. This applies to permissions, SMS and FTP settings and auto-responder content.

Creating Template

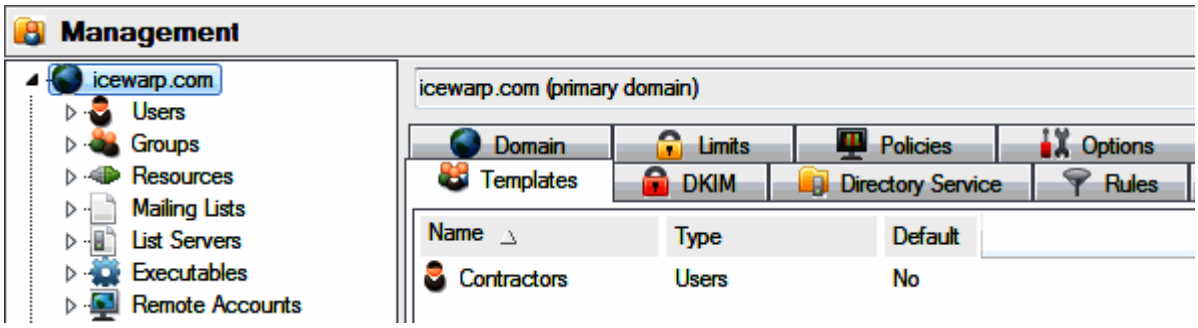
Account templates are used to define a standard set of properties that can be applied to a new account.

Account templates can be defined in two places within the IceWarp Server console:

1. The **Global Settings – Templates** tab:



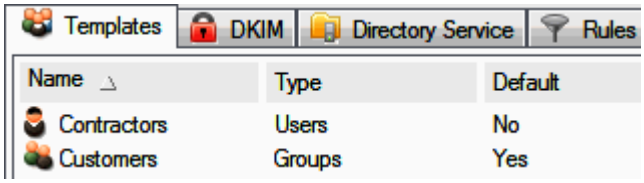
2. With a domain selected, in the **Templates** tab:



Both these areas allow you to create and edit templates via the same dialogs but you should be aware that:

- In **Global Settings**, you ***can*** create domain account templates, within the **<domain>** node, you ***cannot***.
- Each template only applies to a specific account type (user, group, etc.).
- You can create templates of the same name within **Global Settings** and also within multiple domains, and these are ***NOT*** the same templates.
- You can create a ***default*** template for account types. When an account of that type is created, this default template will be applied. There should only be one default template for each account type.

Selecting the **Templates** tab will present you with a list of all templates defined within the selected domain (or Global) as shown below:

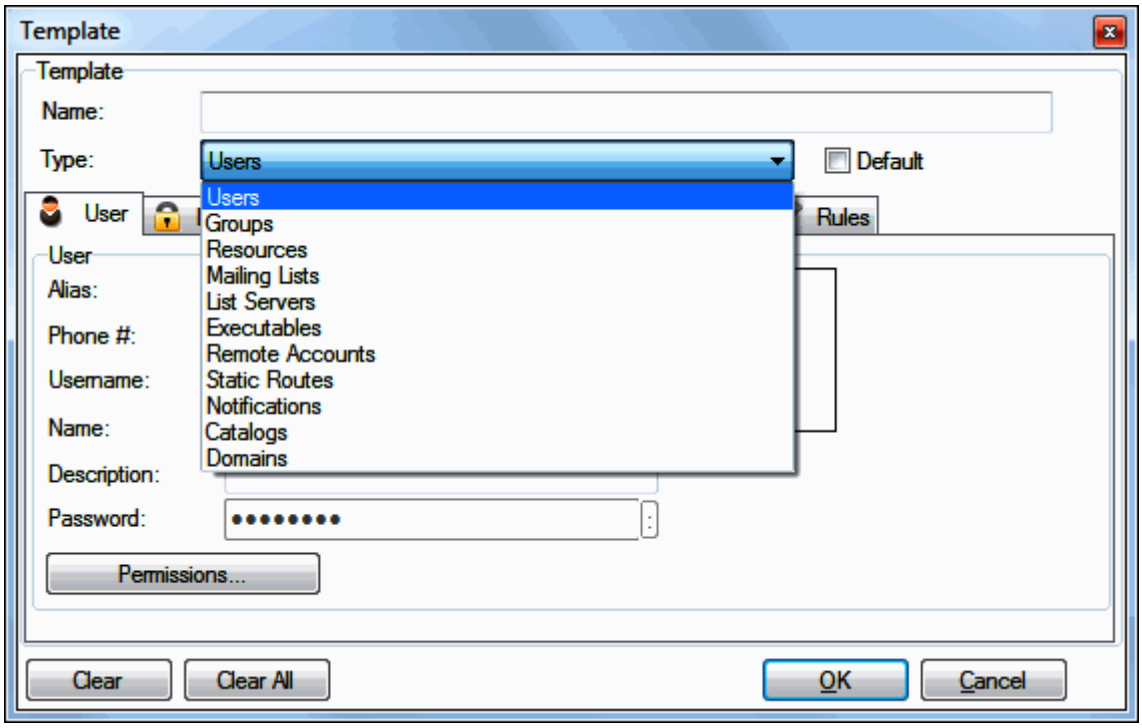


The above screenshot shows that we have two templates defined:

- Contractors – which can only be applied to user accounts, and is not a default template, so will be applied to new user accounts only if selected..
- Customers – which applies to group accounts, and is a default one, so will be applied automatically.

Selecting a template and clicking the ***Delete*** button deletes this template (or templates if more than one are selected).

Clicking the ***Add*** or ***Edit*** button will open the **Template** dialog:

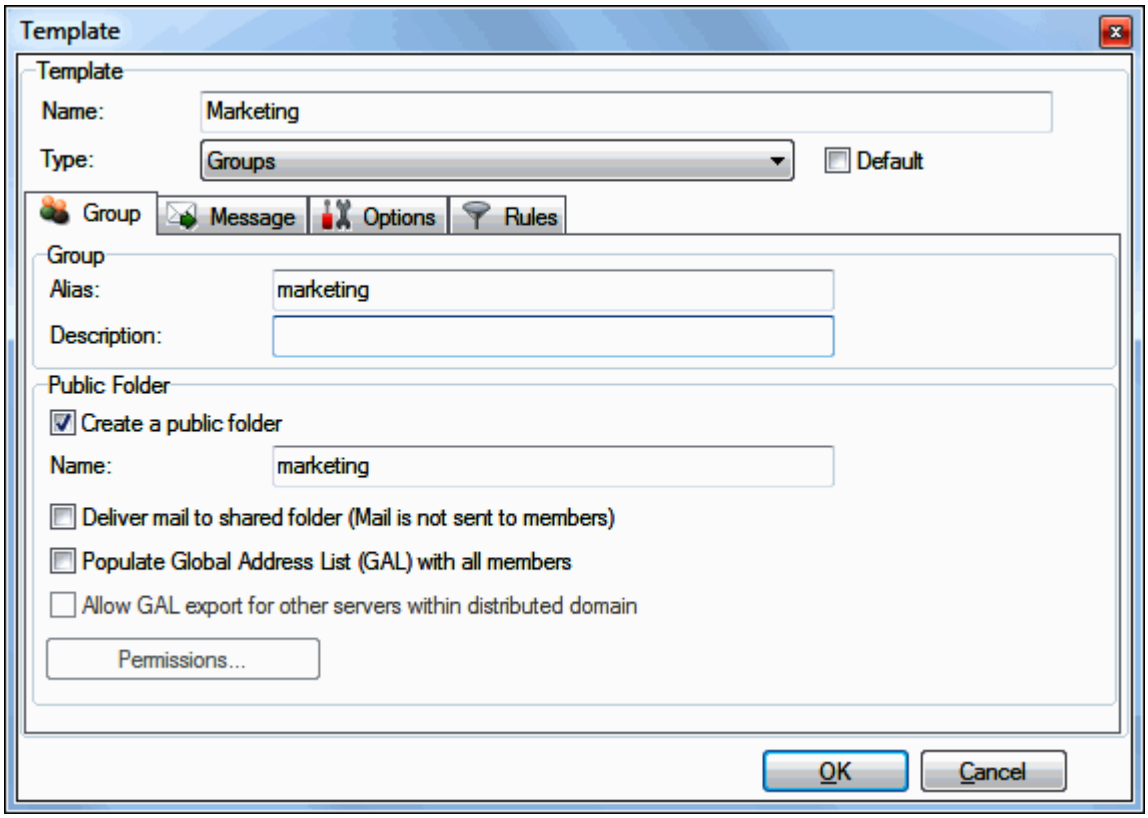


In the top area, above the tabs, you choose the ***Name*** of the template, the ***Type*** of account it can be applied to, and whether it is a ***Default*** template (i.e. automatically applied to all newly created accounts of the type selected).

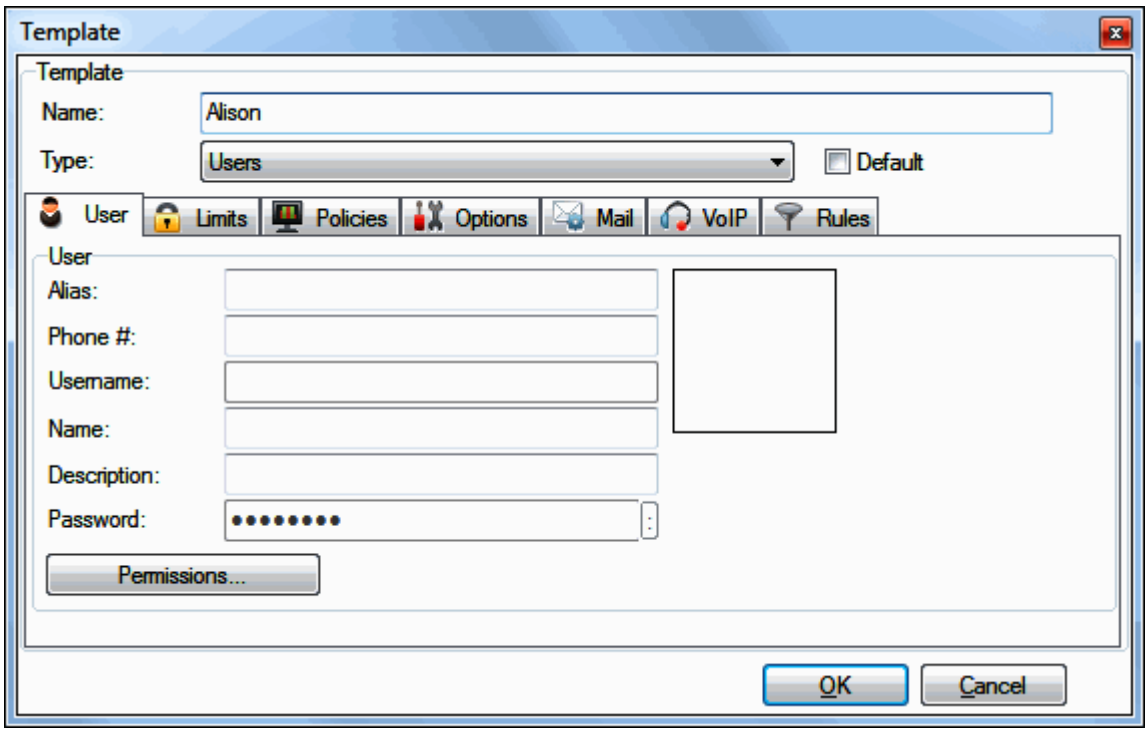
*NOTE: The above screenshot shows the **Type** drop-down expanded so you can see all the account types shown. As this dialog was accessed via the **Global Settings – Templates** tab, this list offers also the **Domain** type. When using the **Management – <domain> – Templates** tab, this type is not listed.*

The tabbed area changes according to the account type selected and reflects the options available for this account type. These options are explained in the relevant manual sections related to the appropriate account types. Note that not all options are available as it is not sensible to have them in a template.

Below, the **Template** dialog is shown, with the ***Groups*** type selected:

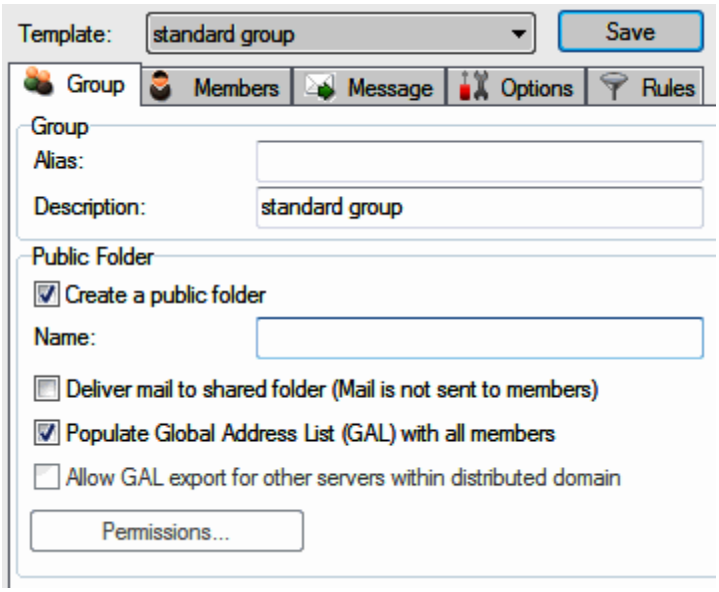


And with the ***Users*** type is selected:



Applying Templates to New Accounts

Whenever you create a new account, and if there are any templates that can be applied to that type of account, the following ***Template*** drop-down is displayed:



The drop-down box lists all global and domain-specific templates that can be applied to this account type.

To apply a template, just select it.

NOTE: Default templates are applied when you create users not only via the console, but also via WebAdmin, the API, Active Directory, etc. The API can also specify a template to use when creating an account.

Template Scenario

This example shows how careful setup of templates could dramatically reduce effort setting up new accounts:

Scenario:

Worried about disk space

You have many small domains with hundreds of users in each, and one domain (BigDomain) with a few users who want to email large files to each other. So you want to set the users in the small domains to have a mailbox size of 20MB, and the users in BigDomain to have a mailbox size of 1GB.

Solution:

Set up a template in **Global Settings** called **mailbox**, for account type of ***User***, as default and set the mailbox size to 20MB.

Set up a template in BigDomain, also called **mailbox**, for account type of ***User***, as default and set the mailbox size to 1GB.

Explanation:

Whenever you setup a new user account, IceWarp Server will see the global default template of **mailbox** and will apply it to the new user settings, ***unless*** the new account is in BigDomain, in which case the domain template of **mailbox** will override the global template of the same name.

Domain Clusters

About

This feature allows splitting a domain into logical parts with different settings by defining domain clusters. A set of domains is grouped into a cluster with one domain defined as a master domain. The master domain then serves as a "dynamic alias" for all the other domains.

The domain cluster makes sure it is not possible to create the same account in any of the domains which are parts of the cluster and works as a domain alias.

All accounts look like they are still in the master domain (login, smtp, im, sip) but in fact they are in different domains. Thus it is possible to define different limits, rules and other options on the domain level for these domains.

Example:

Let's have a cluster with three domains:

icewarpdemo.com (no users, master domain)

demo1.icewarpdemo.com (user jose)

demo2.icewarpdemo.com (user mike)

Messages for ***mike@icewarpdemo.com*** go to inbox of ***mike@demo2.icewarpdemo.com***

Key points

- Domain cluster consists of one master domain and one or more slave domains.
- All domains within the cluster have to exist and be of type "standard domain".
- Aliases within the whole cluster have to be unique.
- Nonexisting aliases in the master domain will be automatically checked in slave domains. If not found, master domain settings will be used to handle nonexisting account.
- Nonexisting aliases in a slave domain will not be checked in other slave domains, slave domain settings will be used to handle nonexisting account.

For the rest of this document we use this domain cluster as an example:

	Domain	**Account**	**User Type**	**IP**
Master	*icewarp.com*	jose	domain admin with default rights	1
Slave 1	*develop.icewarp.com*	charles	domain admin with default rights	2
Slave 2	*support.icewarp.com*	peter	domain admin with default rights	3

The following table describes handling of existing and nonexistent aliases:

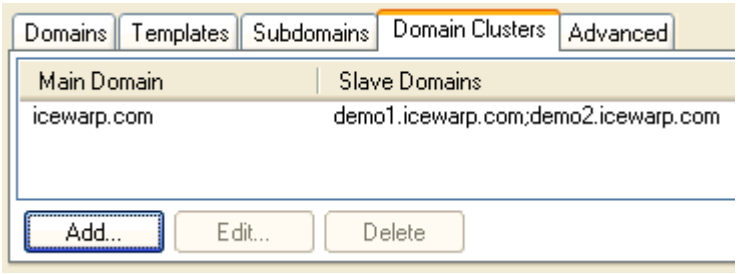
Recipient	**Action**
charles@icewarp.com	goes to ***charles@develop.icewarp.com***
peter@icewarp.com	goes to ***peter@support.icewarp.com***
charles@support.icewarp.com	handled as a nonexisting alias using ***support.icewarp.com*** settings
dan@icewarp.com	handled as a nonexisting alias using ***icewarp.com*** settings

Domain administrator has by default rights only for their real (slave) domain.

Administrator	**Rights**
jose@icewarp.com	can administer only ***icewarp.com***, not the slave domains
charles@icewarp.com	can administer only ***develop.icewarp.com***
peter@icewarp.com	can administer only ***support.icewarp.com***
peter@support.icewarp.com	can administer only ***support.icewarp.com***

- Domain IP binding should work according to the real domain:
  - * ***charles@icewarp.com*** can log only to IP 2
  - * ***jose@icewarp.com*** can log only to IP 1
  - * mail from ***peter@icewarp.com*** is initiated from IP 3
  - * mail from ***charles@develop.icewarp.com*** is initiated from IP 2
- DKIM works according to the master domain:
  - * mail from ***charles@develop.icewarp.com*** –> DKIM of ***icewarp.com*** is used
- WebClient behaves so that any slave domain user can assume he belongs to the master domain.
  - * After Charles logs in as ***charles@develop.icewarp.com***, he is presented as ***charles@icewarp.com***. Address ***charles@icewarp.com*** is also put into header of any created email and used as "sender".
- Authentication – only emails consisting of alias and master domain can be authenticated.
  - * User name ***charles@develop.icewarp.com*** is not authenticated
  - * ***charles@icewarp.com*** is authenticated
- Domain rule of the true user domain will be used.
  - * ***develop.icewarp.com*** domain rules are used for mails going to ***charles@icewarp.com***
- Changing domain type option is to be disabled for domains in cluster.

Setup



Click the ***Delete*** button to remove the selected domain cluster.

Use the ***Add...*** and ***Edit...*** buttons to open the **Domain Clusters** dialog.



Field	**Description**
Main Domain	Use the "***...***" button to select the master domain.
Slave Domains	Use the "***...***" button to select slave domains. *NOTE: These domains have to be created in advance.*

Advanced

This feature allows synchronization of IceWarp Server users to an LDAP server, which can be IceWarp Server itself (LDAP service has to be running) or a 3rd party server such as OpenLDAP.

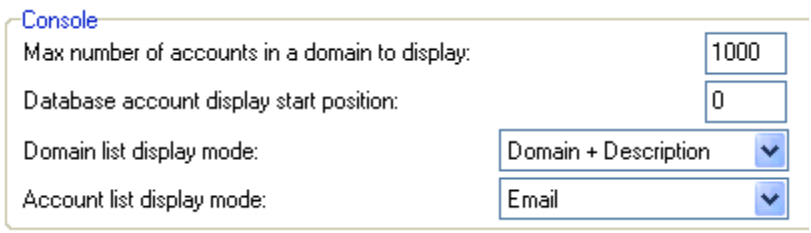
NOTE: The initial synchronization has to be done manually. Other changes within IceWarp Server (adding/deleting users etc.) are reflected into LDAP structure automatically.

Only users and GALs are synchronized.

BE AWARE: Accounts without its name (the *u_name* property) filled in will not be synchronized as this property is absolutely essential. Make sure there is this name filled in if an account is not synced to LDAP server.



Field	Description
Active	Check this box to activate ***LDAP User Synchronization***.
LDAP Host	Enter the hostname of your LDAP server. *NOTE: If the LDAP server you are accessing does not use the standard port 389, you should specify it here after the hostname, separated with a colon.* *E.g. 123.128.88.26:489 would use port 489 to access the LDAP server.*
Base DN	Enter the base DN of your LDAP server. The default setting is ***dc=root***.
User DN	Enter the user DN required to access your LDAP server.
Password	Enter the password associated with the given ***User DN***.
Synchronize All Users To LDAP Now	Click this button to have IceWarp Server immediately synchronize itself with your LDAP server.



Field	Description
Max number of	How many accounts are shown at one time within the IceWarp Server console, within a domain.

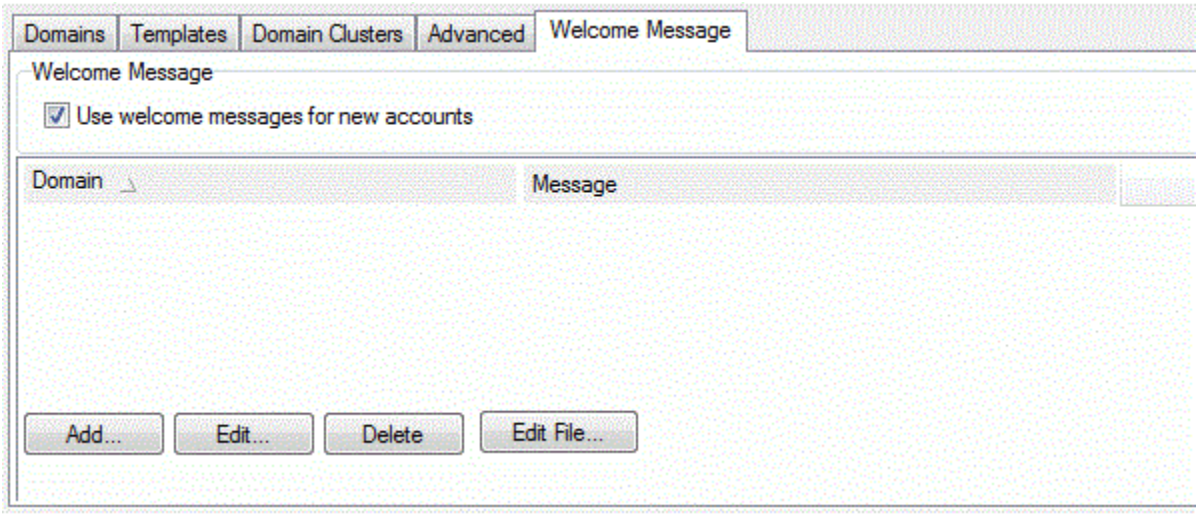
accounts in a domain to display	*NOTE: The higher the number you specify here, the longer the list will take to load and display.*
Database account display start position	The start position of the account list. Used in conjunction with the ***Max number of accounts***. Example: Assume you have ***Max number of accounts*** set to 1000 and are displaying a domain containing 3000 accounts – your display will show the accounts 1 to 1000. If you want to see the next 1000, you should set this ***start position*** to 1001 and accounts 1001 to 2000 will be displayed.
Domain list display mode	There are three ways to display domain list in the **Domains & Accounts** section – choose whichever suits you: **Domain** Only domain names are displayed. **Domain + Description** Domain names and descriptions are displayed. Example: ***doc.icewarpdemo.com (Documentation Server)*** **Description + Domain** Domain descriptions and names are displayed. Example: *(Documentation Server) doc.icewarpdemo.com* *NOTE: If the **System – Storage – Accounts** feature is set to **Database** and this display mode is set to one of options with description, processing/ high load issues may occur. This does not apply when the account storage is set to **File system**.*
Account list display mode	There are three ways to display account list in the **Domains & Accounts** section – choose whichever suits you: **Email** Email address is displayed. **Alias** User's alias as filled in to the appropriate field is displayed. **Name** User's name as filled in to the appropriate field is displayed.

Preserving Hierarchy of Entries

IceWarp Server is capable of synchronizing the hierarchy of domains and accounts as it exists on its side. You can achieve it with the server variable of ***%domain_dc%*** placed in the ***rootDN*** input. Sync mechanism will automatically create *dc* (domain component) for each domain level – in other words IceWarp domain of *my.example.com* will be parsed as *dc=my*,*dc=example*,*dc=com* and all accounts will be synced under this LDAP entry. It is also possible to store whole hierarchy under another container, i.e. if you wish to have mail server accounts stored in *dc=mailserver*, fill in ***%domain_dc%***, *dc=mailserver* into the ***rootDN*** field.

Welcome message

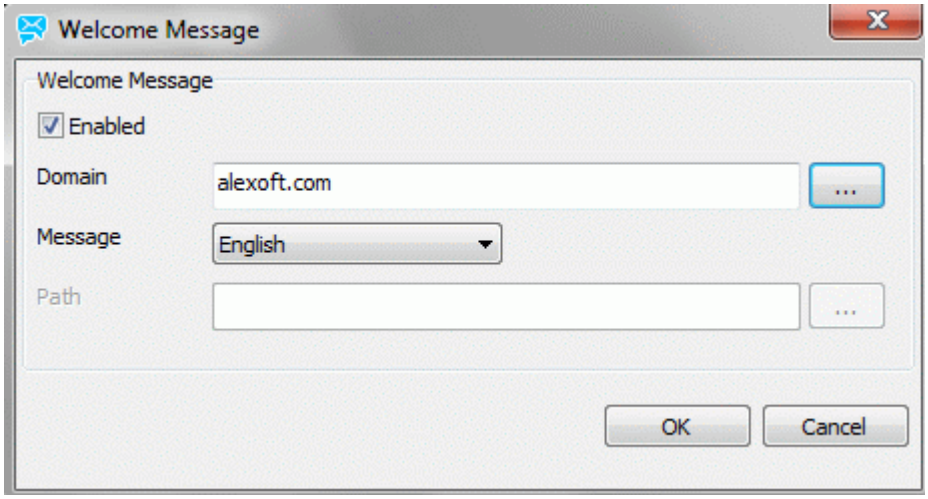
This feature allows you to have a welcome message sent to the mailbox of all newly created users.



Field	Description
Use welcome messages for new accounts	Check this option to have a welcome message sent to the mailbox of all newly created users. Message content is specified in a simple text file. Domains and text files are linked in the **messages.dat** file, which you can edit by clicking the **Welcome Messages** button. Examples are given and you can specify different welcome messages for different domains.

There is no need to edit the contents of the file - it is shown on the data grid - **add/edit/delete** options available.

Each row represents setting for one domain.



Within **Add...** button, you can set:

- **Enabled** - disable / enable welcome messages for particular domains
- **Domain** - select domain from the list. Use * for defining default behavior.
- **Message** - Either Select "Custom file", or select Language which will be used

If specific language was selected, IceWarp will generate welcome message based on icewarp predefined template.

If custom file is selected - you have to define Path to the email template.

- **Path** - path to the template. It can be either .eml file (for backward compatibility) - or it can be html file. If the htmlo file contains references to images, those images must be in the same directory as the html file.

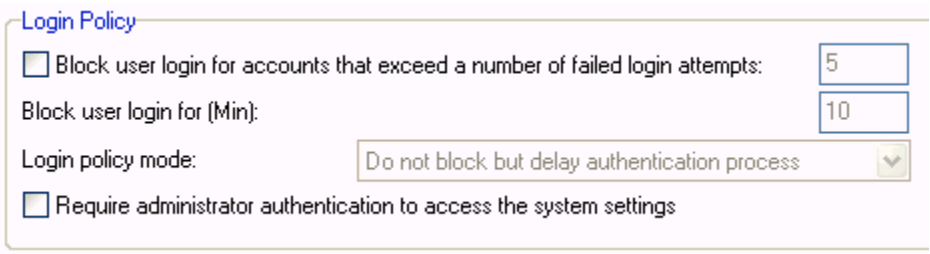
If there are no rows in the grid (e.g. the config file is empty), it means, that you should use the icewarp predefined template and use server language

It is also possible to display the dialog for particular domain from the domain/options tab.

Policies

You may need to be more restrictive to make your server more secure. There are policies to do this for you. Read particular options carefully as they offer you powerful ways to secure your users against attacks or misuse. If your policies are set incorrectly, it may take some time to find out the causes of your problems. (E.g. if you setup your login policy with the email address option chosen, and then your users try to login with their common usernames, they will no longer be able to log on until you resolve your policy settings.)

Login Policy



Field	Description
Block user login for accounts that exceed a number of failed attempts	Check this option to block users for a specified length of time, if they exceed the given number of consecutive failed login attempts. Set the value in the text box to the number of allowed attempts (5 in the above screen shot).
Block user login for (Min):	Specify how many minutes a user should be blocked for, if they exceed the failed login attempts number (10 minutes in the above screenshot). After entering the correct password, the account will be unblocked for the next attempts. I. e. only one attempt to login with correct password will be blocked.
Login policy mode	Choose one of two options: **Do not block but delay authentication process** If a user enters an incorrect password, the authentication procedure will be delayed by 20 seconds. If the user then enters the correct password, they are still delayed by 20 seconds but only for the first time. Next login attempt behaves the same way as if the account was never blocked. **Block account for specified amount of time** If a user enters an incorrect password, account access is blocked for the amount of time specified above. If a user is blocked, **login.dat** file is created in their mail folder. Also, it is shown on the **<user> – User** tab. The ***Unblock*** button is presented to unblock the user. Clicking it deletes the user's **login.dat** file. User blocking is logged in the ***Authentication*** logs (**Status – Logs**) – can be enabled in **System – Logging**. If a user enters correct password after block it will unblock the account only. The Second correct password will login to WebClient.
Require administrator authentication to access the system settings	Check this option IceWarp Server console to ask for a user/password combination when it is started. The user entered must be an administrator. *NOTE: In the case you have forgotten your administrator password (definitely very rare situation), you can use the following command to disable it:* ***tool modify system***

	c_gui_auth 0.

BE AWARE: Login Policy settings apply to all types of authentication in IceWarp Server (SMTP, POP3, IMAP, HTTP, etc.)



Field	Description
Users login with their usernames/ email addresses	▪ ***Users login with their usernames*** – selecting this option allows users to login with both usernames or email addresses. ▪ ***Users login with their email addresses*** – only email address is to be used to login. If you have a large number of domains and accounts, it is advisable to use login with email address. This will reduce mail authentication and login time as IceWarp Server will be able to locate the account more quickly. Using this option also allows you to have the same user/password combination in different domains.
Convert characters % and / to @ in usernames	Some older mail clients (Netscape and Mac) do not allow using @ in a username. If you wish to use the login with email address option, check this option so that your users have the option to login with % or / in the email address. Example: ***user%icewarpdemo.com*** will be converted to ***user@icewarpdemo.com***



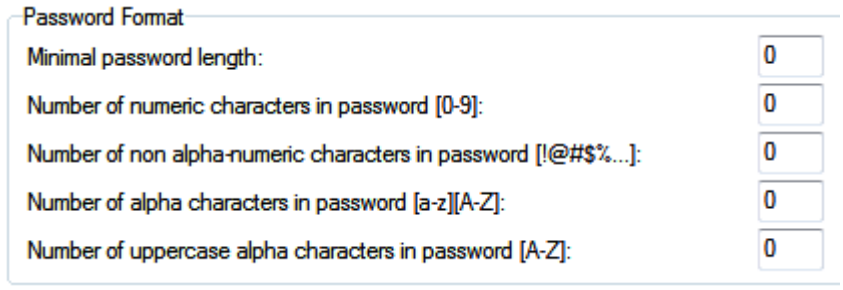
Field	Description
Use account login IP restrictions	Enabling this option offers you an IP security system to ensure that particular accounts can only access the IceWarp Server from specific IP addresses. Rules are stored in a file which can be created and edited by click the **Login Restriction** button.
Login Restriction...	Pressing this button will open a dialog where you can create or edit your IP restriction rules. This applies to all services. Examples are given within the editor dialog – click the ***Comment*** button.

Password Policy

NOTE: In the case you are trying to set a password that does not meet this password policy anywhere within the administrative console, the appropriate field is highlighted red. See the figure below.

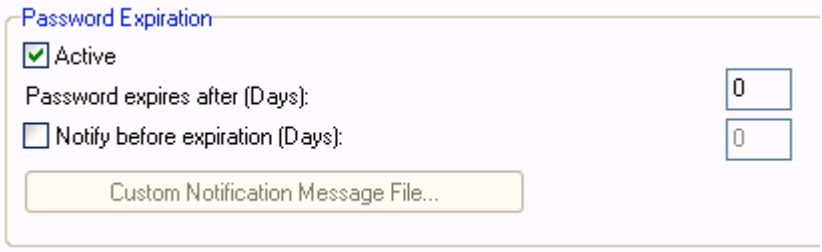


Field	Description
Active	Check this box to have password policies enforced. When not checked, the value fields are disabled.
Password can not contain Username and Alias	Checking this box stops anyone creating a password equal to their username or alias.
Enable password encryption	Check this box IceWarp Server to use encryption for passwords. This setting is applied only for newly created or modified accounts. *NOTE: Passwords are encrypted only if user accounts are stored in a database (not in a file system).* *TIP: Easy way how to apply password encryption for existing accounts is e. g. to set password expiration. This forces users to change their passwords = modify accounts.* *Or use the tool command:* ***tool modify account *@* U_SMTP 1*** *This modifies all accounts by enabling SMTP (which is already enabled).*

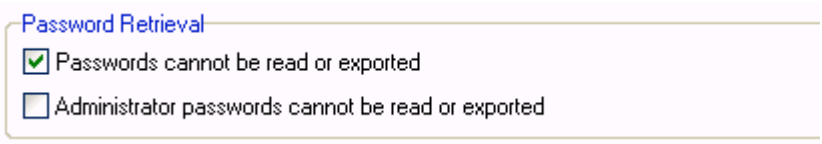


Field	Description
Minimal password length	Specify a minimum password length. A value of 0 means no minimum length is required.
Number of numeric characters in password [0-9]	Specify the minimum number of numeric characters that must be present in the password. A value of 0 means no numeric characters are required (but they can still be used).
Number of non alpha-numeric characters in password [!@#$%...]	Specify the minimum number of non alpha-numeric characters that must be present in the password. A value of 0 means no non alpha-numeric characters are required (but they can still be used).
Number of alpha characters in password [a-z] [A-Z]	Specify the minimum number of non alpha characters that must be present in the password. A value of 0 means no alpha characters are required (but they can still be used).

Number of uppercase alpha characters in password [A-Z]	Specify the minimum number of uppercase alpha characters that must be present in the password. A value of 0 means no uppercase alpha characters are required (but they can still be used).



Field	**Description**
Active	Check this option to enable password expiration. Passwords will expire after the specified number of days, forcing your users to regularly change them via IceWarp WebClient. This can increase security. *NOTE: This box has to be ticked if you want to use the **Expire Password Now** button (**Management – <Domain> – <User> – Options**). In the case, you want to have this feature active, but still want passwords not to expire, set the **Password expires after** field to 0 (zero).*
Password expires after (Days)	Specify the number of days after which the password expires. Zero means that a password does not expire even if the ***Active*** box is checked.
Notify before expiration (Days)	Check this box to have users notified of their imminent password expiration. Specify the number of days before expiration that the notification is to be sent.
Custom Notification Message File	Click this button to open a file where you can specify the content of the expiration notifications.



Field	**Description**
Passwords cannot be read or exported	Check this option to stop passwords being read or exported via the API or any other method. For example, ***tool display account account@domain.com u_password*** will reveal a star instead of the password. This is a recommended option as it can significantly increase security.
Administrator passwords cannot be read or exported	The same effect as the above option but only applies to server and domain administrators passwords. This is a recommended option as it can significantly increase security.

Limits – Explanation

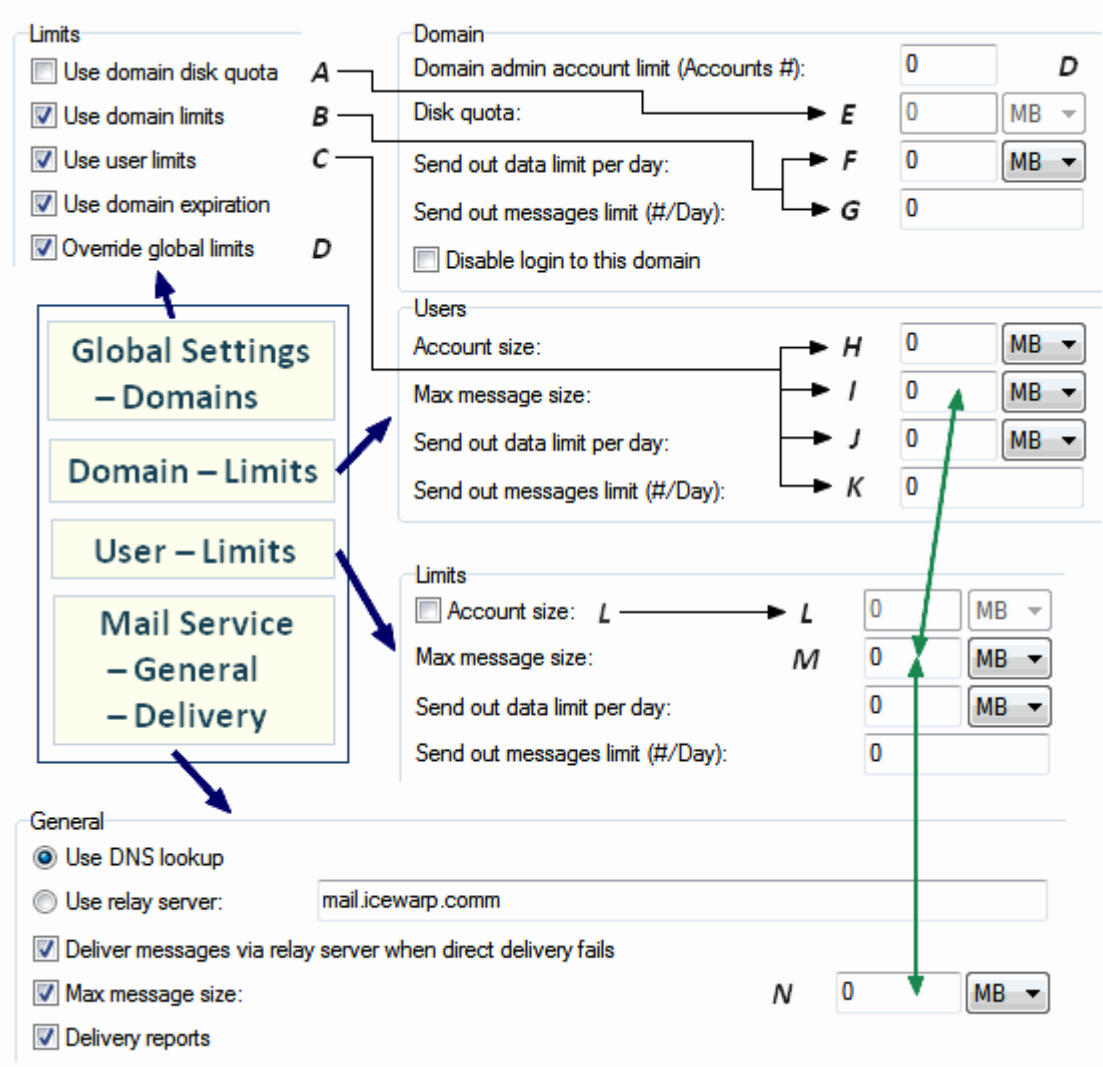
This section is designed to give you a very brief overview of how the various limits in IceWarp Server are applied, enabled, and which limit overrides which.

These limits can be set on global, domain and user levels. The only limit set on the global level is the ***Max message size*** value – for detailed description, refer to the **Limits – Max Message Size** chapter.

There are five areas where limits are enabled and/or set

- Global Settings – Domains
- <domain> – Limits – Domain
- <domain> – Limits – Users
- User – Limits
- Mail – General – Delivery – General

The following diagram clarifies how limits are enabled:



The diagram shows all the areas where limits are enabled and set. The straight arrows indicate a dependancy from one item to another, e.g. checking item of B (***Use domain limits***) will enable items of F and G (plus the ***Disable login to this domain*** box).

The two green arrows indicate the three places where a maximum message size can be set. This is the only true "global limit" that can be set at the moment.

Limits – Which One Is Used?

The following text explains how the limits are applied:

Assume that the ***Use domain limits*** and ***Use user limits*** options are ticked.

User limits are always checked.

Domain user limits are only checked if the corresponding ***user limit*** is set to zero.

Domain Limits are always checked, and you should bear in your mind that a ***domain limit*** may cause a failure even though a ***user limit*** or ***domain user limit*** has not been breached, as the ***domain limits*** consider **all** messages sent by **all** users in the domain.

Example:

a. ***Use domain limits*** is ticked.

b. ***Use user limits*** is ticked.

c. *DomainA* has domain limit of ***Send out data limit per day*** set to 500MB.

d. *DomainA* has user limit of ***Send out data limit per day*** set to 20MB.

e. *UserA* has ***Send out data limit per day*** set to 100MB.

f. *UserB* has ***Send out data limit per day*** set to zero.

If *UserA* tries to send out a message of size 200MB, it will not be sent as it breaks the ***user limit*** (e).

If *UserA* tries to send out a message of size 99MB, it will be accepted unless the ***domain limit*** of 500MB (c) has been broken (the domain limit considers the totals of all messages sent by all the domain users), the ***domain user limit*** (d) is not checked.

If *UserB* tries to send a message over 20MB in size, it will fail as it breaks the ***domain user limit*** (d).

If *UserB* tries to send a message under 20MB, it will be successful unless the ***domain limit*** (c) has been broken.

Limits – Max Message Size

The ***Max message size*** limit is a special case worth mentioning, as it can be set as a global limit as well as a domain user limit and a user limit.

If the global limit is checked and set in **Mail Service – General – Delivery – General** and ***Override Global limits*** (**Global Settings – Domains**) is not ticked then the limit set will be applied to ***all*** messages from ***all*** users in ***all*** domains on this server. Any message larger than the size set will be rejected.

If ***Override global limits*** is checked then the limits are checked in the following order until a non-zero value is found (if only zero values are found then the message is passed).

1. User limit
2. Domain user limit
3. **Mail – Delivery** limit

Example 1:

a. **Mail Service – General – Delivery** has ***Max message size*** **t**icked and set to 10MB

b. ***Override Global limits*** is **not** checked

Any message with a size greater than 10MB will be rejected.

Example 2:

a. **Mail Service – General – Delivery** has ***Max message size*** ticked and set to 10MB

b. ***Override Global limits*** is checked

c. ***Use domain limits*** (**Global Settings – Domains**) is ticked

d. ***Use user limits*** is ticked

e. *DomainA* has the domain user limit of ***Max message size*** set to 20MB

f. *UserA* has the ***user limit*** of ***Max message size*** set to 50MB

g. *DomainB* has the domain user limit of ***Max message size*** set to zero

h. *UserB* (in *DomainB*) has a user limit of ***Max message size*** set to zero.

If *UserA* tries to send a message of 40MB in size, it will be accepted as his/her ***user limit*** (f) takes priority.

If any other user in *DomainA* tries to send a message of 40MB in size, it will be rejected as it breaks the domain limit (e) of 20MB.

If *UserB* tries to send a message of 40MB in size, it will fail as it breaks the global limit (a).

Simple RegEx Tutorial

Regular expressions can be used in content filter conditions.

Regular expressions can be extremely complex but they are very flexible and powerful and can be used to perform comparisons that cannot be done using the other checks available.

Some very basic examples of regular expression usage follow. For a complete description, please visit ***http://www.regular-expressions.info/***.

^' and '$'

First of all, let's take a look at two special symbols: '^' and '$'. These symbols indicate the start and the end of a string, respectively:

"^The"	matches any string that starts with "The".
"of despair$"	matches a string that ends in with "of despair".
"^abc$"	a string that starts and ends with "abc" – effectively an exact match comparison.
"notice"	a string that has the text "notice" in it.

You can see that if you do not use either of these two characters, you are saying that the pattern may occur anywhere inside the string – you are not "hooking" it to any of the edges.

'*', '+', and '?'

In addition, the symbols '*', '+', and '?', denote the number of times a character or a sequence of characters may occur. What they mean is: "zero or more", "one or more", and "zero or one." Here are some examples:

"ab*"	matches a string that has an 'a' followed by zero or more b's ("ac", "abc", "abbc", etc.)
"ab+"	same, but there is at least one b ("abc", "abbc", etc., but not "ac")
"ab?"	there might be a single b or not ("ac", "abc" but not "abbc").
"a?b+$"	a possible 'a' followed by one or more 'b's at the end of the string: Matches any string ending with "ab", "abb", "abbb" etc. or "b", "bb", etc. but not "aab", "aabb", etc.

Braces { }

You can also use bounds, which appear inside braces and indicate ranges in the number of occurrences:

"ab{2}"	matches a string that has an a followed by exactly two b's ("abb")
"ab{2,}"	there are at least two b's ("abb", "abbbb", etc.)
"ab{3,5}"	from three to five b's ("abbb", "abbbb", or "abbbbb")

Note – you must always specify the first number of a range (i.e., "{0,2}", not "{,2}"). Also, as you might have noticed, the symbols '*', '+', and '?' have the same effect as using the bounds "{0,}", "{1,}", and "{0,1}", respectively.

Now, to quantify a sequence of characters, put them inside parentheses:

"a(bc)*"	matches a string that has an 'a' followed by zero or more copies of the sequence "bc"
"a(bc){1,5}"	one through five copies of "bc."

'|' OR operator

There is also the '|' symbol, which works as an OR operator:

"hi|hello"	matches a string that has either "hi" or "hello" in it
"(b|cd)ef"	a string that has either "bef" or "cdef"
"(a|b)*c"	a string that has a sequence of alternating 'a's and 'b's ending in a 'c'

('.')

A period ('.') stands for any single character:

"a.[0-9]"	matches a string that has an 'a' followed by one character and a digit
"^.{3}$"	a string with exactly 3 characters

Bracket expressions

Specify which characters are allowed in a single position of a string:

"[ab]"	matches a string that has either an 'a' or a 'b' (that is the same as "a|b")
"[a-d]"	a string that has lower case letters 'a' through 'd' (that is equal to "a|b|c|d" and even "[abcd]")
"^[a-zA-Z]"	a string that starts with a letter
"[0-9]%"	a string that has a single digit before a percent sign
",[a-zA-Z0- 9]$"	a string that ends in a comma followed by an alphanumeric character

You can also list which characters you DO NOT want – just use a '^' as the first symbol in a bracket expression (i.e., "%[^a- zA-Z]%" matches a string with a character that is not a letter between two percent signs).

In order to be taken literally, you must escape the characters "^.[$()|*+?{\" with a backslash ('\'), as they have special meaning. On top of that, you must escape the backslash character itself in PHP3 strings, so, for instance, the regular expression "(\$|A)[0-9]+" would have the function call: ereg("(\\$|A)[0-9]+", $str) (what string does that validate?)

Just do not forget that bracket expressions are an exception to that rule -- inside them, all special characters, including the backslash ('\'), lose their special powers (i.e., "[*\+?{}.]" matches exactly any of the characters inside the brackets). And, as the regex manual pages tell us: "To include a literal ']' in the list, make it the first character (following a possible '^'). To include a literal '-', make it the first or last character, or the second end point of a range."