IceWarp Unified Communications

System Node Reference

Version 12

Published on 3/6/2017

Contents

System Node

The **System** node contains options and settings related to overall IceWarp Server functionality.

These include:

- ***Service*** management
- ***Connection*** options
- ***Logging*** options
- ***Tools*** supplied with IceWarp Server
- ***Storage*** options
- ***Certificate*** management
- and some ***Advanced*** options.

Services

Service Ports

Each service is bound to one or more IP addresses and port number.

These can be changed if required, however, IceWarp Server's default ports conform to Internet standards which are commonly defined in client applications and may be required by your ISP.

Most installations will work correctly with the defaults.

If you are using Firewall, you must open the TCP ports for all the services you are using. This applies only for Linux, for Windows it is done automatically.

Warning: IceWarp Server's POP3 and IMAP run as one module, so if you stop this module, both services will also stop.

The same applies for IM and SIP.

You should also be aware that IceWarp WebClient and FTP run under the ***Control*** service. If you stop or restrict access to the ***Control*** service, your users may not be able to use IceWarp WebClient or FTP.

Service Ports

NOTE: All ports are TCP ones unless stated otherwise.

Service	Purpose	Basic Ports	SSL Ports
SMTP	Send mail Users send out emails, server sends and receives emails to/from other mail servers	25 2nd basic port: 587 (for more info refer to the **Mail – Security – General – Submission Port** chapter.) This port can be set also via the *c_system_services_smtp_altport* API variable. For more information on using TLS/SSL, refer to the **Mail Service – General – Advanced – Use TLS/SSL** section. *NOTE: Older installations used the port of 366 as a 2nd basic one.*	*NOTE: The port of 465 is obsolete and is not to be used anymore.*
POP3	Receive mail	110	995
IMAP	Read mail	143	993
Web (Control)	Web admin, web mail, proxy server, WebDAV, CalDAV, iSchedule	80 2nd basic: 32000	443 2nd port 32001
GroupWare	GroupWare and Calendar	5229 *NOTE: It is necessary to open this port only if some 3rd party application wants to access groupware API from the outside.*	

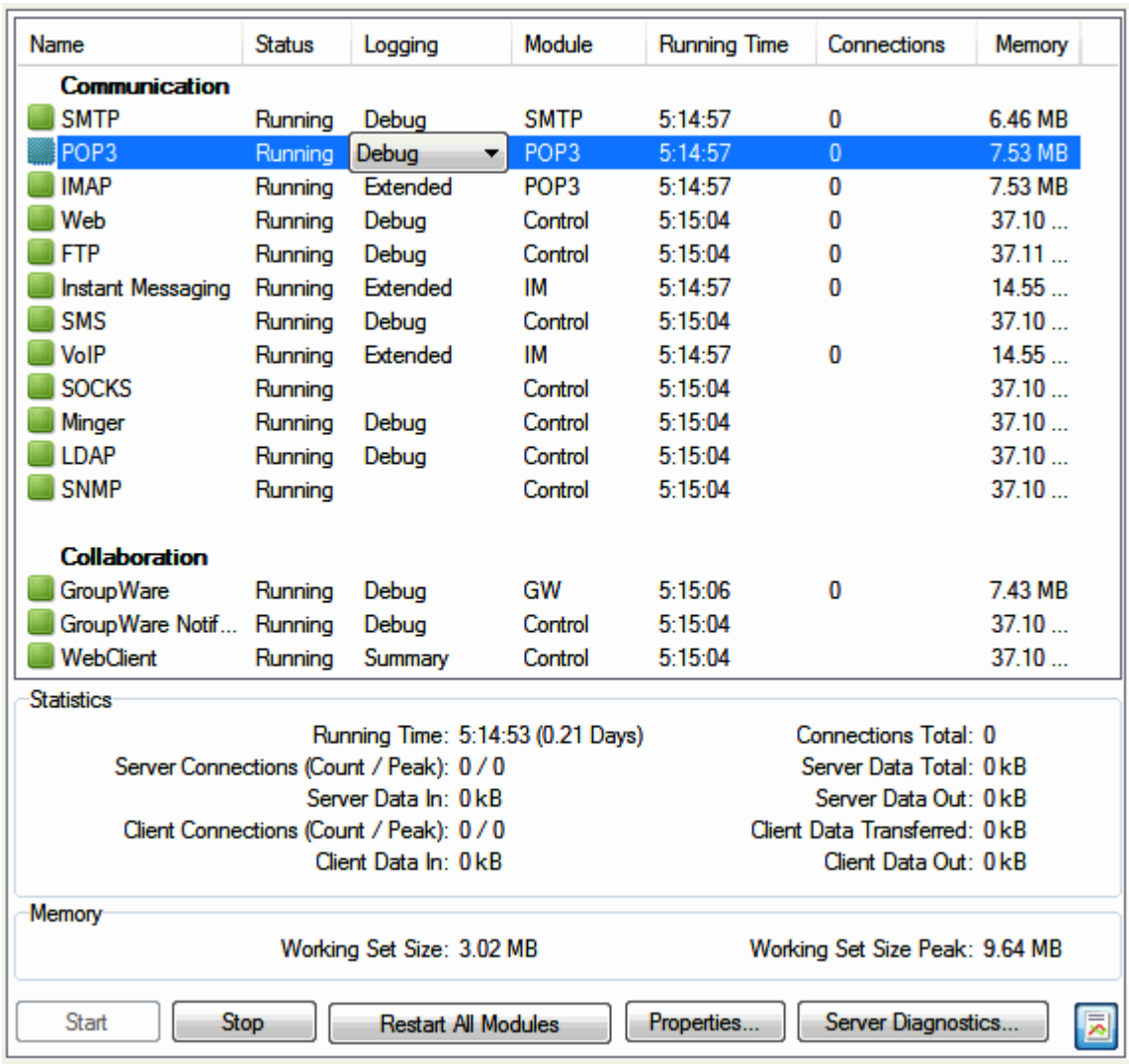
GroupWare Notification	GW push	32002	
IM	Instant Messaging Server	5222 2nd basic port: 5269	5223 *NOTE: This port is obsolete and is not to be used anymore.*
LDAP	LDAP Server (directory service)	389	636
FTP	File Transfer Protocol	21 (or 20) plus user-defined range (see **FTP Service – Options**)	990
SIP/VoIP	Session Initiation Protocol Delivery of voice communications over IP networks.	5060 plus user-defined range (see **SIP**) *NOTE: This is a UDP & TCP port.*	5061
SOCKS	Routing of network packets between client-server applications via a proxy server.	1080	
Minger	Use of domain sharing across multiple servers.	4069 *NOTE: This is a UDP port.*	4070
SNMP	Simple Network Management Protocol	161 *NOTE: This is a UDP port.*	
Time server	time server – has to be enabled in **console – System – Advanced – Protocol – *Enable Daytime server (Port)***	13	

You may also need to set specific IP binding of the machine the server is running on if that machine is running other, non-IceWarp Server services (IIS, for example) as IceWarp Server will bind to all available IP addresses. The same port/IP cannot be used by more then one server software.

*For more details about DNS SRV records, refer to the **IM – Trusted Hosts**, **GroupWare – WebDAV**, **VoIP – Advanced** sections plus to **http://en.wikipedia.org/wiki/SRV_record**.*

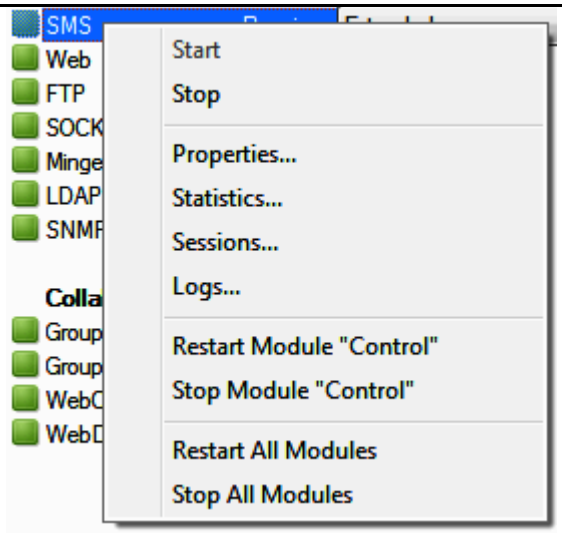
General

Selecting the **System – Services** node in the administration console brings up a screen similar to the following:



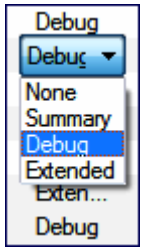
This tab shows a complete list of available services on your server and some information about their status.

Column Name	**Description**
Name	This column shows the name of the available service. To the left of the name is either a red or green box which gives you a visual indication of whether the service is running – a green box if the service is running or a red box if the service is stopped. Right-click the appropriate service name to reveal the following pop up menu:



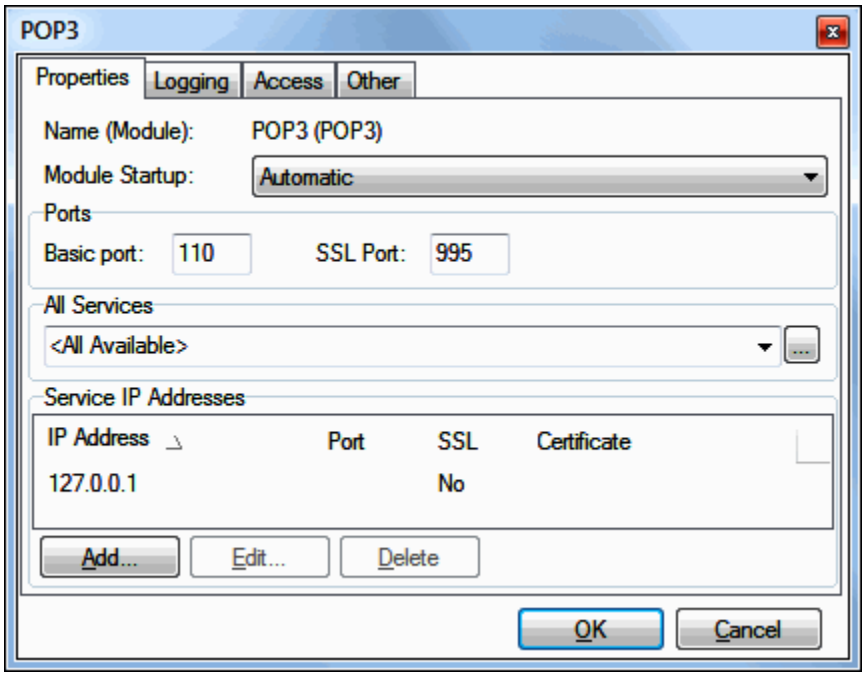
Item	Description
Start	Makes the service active, i. e. available for users.
Stop	Makes the service inactive, i. e. not available for users but the appropriate module is still running. *NOTE: Web service cannot be stopped in remote console mode, it would disconnect the console.*
Properties	Reveals the service properties dialog. See the **Service – Properties** section.
Statistics	Brings you to the **Status – Statistics** tab for the appropriate service.
Sessions	Brings you to the **Status – Sessions** tab for the appropriate service.
Logs	Brings you to the **Status – Logs** tab for the appropriate service.
Restart Module "<module>"	Restarts the module that includes the selected service(s).
Stop Module "<module>"	Stops the module that includes the selected service(s). *NOTE: The Control module cannot be stopped in the remote console mode, it would disconnect the console.* *NOTE: One module (Windows service or Linux process) can (but need not) handle more services. In the case you stop a module, all these services are stopped, as modules are **.exe** files (in Windows).*
Restart All Modules	Restarts all running modules. *NOTE: The Control service is not restarted in remote console mode.*
Stop All Modules	Stops all running modules. *NOTE: The Control service cannot be stopped in remote console mode, it would disconnect the console.*

NOTE: In the case services stop very often (say every hour), check whether your license

	is valid (not expired).
Status	Tells you whether the service is running or stopped.
Logging	Click the logging state to change it – select from the menu.  *NOTE: You can use multi select (CTRL+click, SHIFT+click), when performing the same change for more services. Logging state of all selected services can be changed en bloc.* For more information about logging, refer to the **System – Logging** chapter.
Module	Tells you what module serves the appropriate service.
Running Time	Tells you how long the service has been running.
Connections	Tells you how many current connections to the service.
Memory	Amount of virtual memory reserved for a use by the service.
Button	**Use**
Start	Makes the selected service(s) active, i. e. available for users. You can select a service group by clicking its name.
Stop	Makes the selected service(s) inactive, i. e. not available for users but still running. You can select a service group by clicking its name. *NOTE: The Control service cannot be stopped in the remote console mode, it would disconnect the console.*
Restart All Modules	Restarts all running modules. *NOTE: The Control service is not restarted in the remote console mode.*
Properties	Opens the service properties dialog for the selected service (you can also double-click the service to open properties). Discussed in detail in the following topics (**Service – Properties**).
Server Diagnostics	Performs basic diagnostics on your services. Discussed further in **Server Diagnostics**.
Show/Hide Statistics 	Select a service and click the button (in the right-hand lower corner) to reveal/hide statistics for this service. Statistics are not shown when any service is not selected. Furthermore, statistics are available only for services listed in the **Status – Statistics – Service** list.

Service – Properties

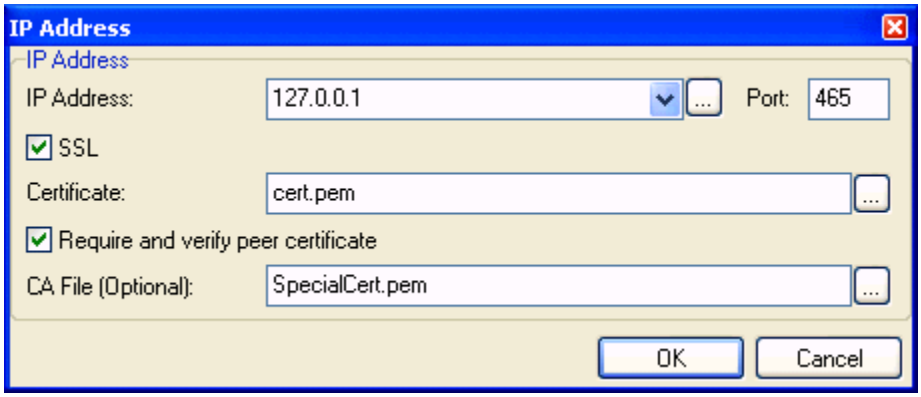
Selecting the ***Properties*** item from a pop-up menu (or double-clicking the service) opens the **<service>** dialog:



This dialog is the same for most IceWarp Server services. For some services, the dialog is reduced.

Field	**Description**
Name (Module)	This label shows you which service is being shown (not editable).
Module Startup	Choose whether this service should be started automatically when your server is booted. Choose from ***Automatic*** (recommended) and ***Manual***. *NOTE: If you choose **Manual**, you will need to put a process in place to start the services when required.* *NOTE: The automatic startup does not apply for Linux.*
All services	This is a global setting that affects all services. A combo box is presented, where you can choose between all the known IP addresses for this machine, a **<none>** option, and an **<All Available>** option. You can also type multiple IP addresses manually into the text area, separated by semi-colons. e.g. 192.168.0.32;192.168.0.57;192.168.0.145
Ports	The ports that this service listens on. The defaults are the standard Internet ports as defined by ICANN (Internet Corporation for Assigned Names and Numbers). Some services do not need an SSL port as they can convert a non-SSL connection to an SSL connection on the same port. For information about the submission port # 587, refer to the **Mail Service – Security – Genera**l section.
Service IP addresses	Here you can specify an IP address to bind this specific service to. This might be useful if you need to run a service on a non-standard port or for assigning a special certificate.
Add	Click the button to add a new IP address. The **IP Address** dialog opens.

Edit	Select an IP address and click the button to edit settings.
Delete	Select an IP address and click the button to remove this address.

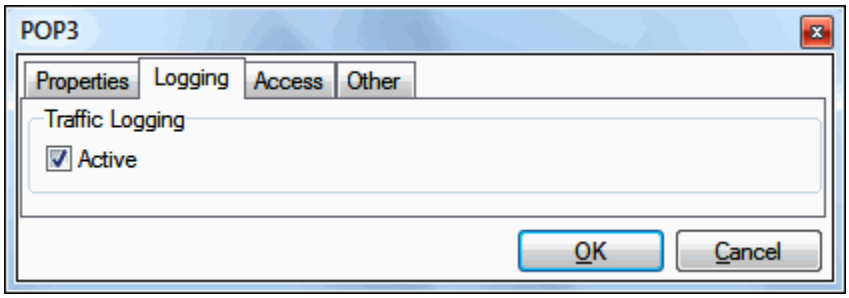


Binding is not necessary for correct multiple domain configuration.

If you do need to bind IceWarp Server on Windows XP, you will need to disable the *IP Pooling* features of the operating system first.

Field	**Description**
IP Address	Choose the IP Address to bind this service to.
Port	Enter the port that this service will use. *NOTE: This port must be open in any firewalls or routers that you server has to go through.*
SSL	Check this box to have the connection SSL encrypted.
Certificate	Enter a path to a certificate file this connection to use that certificate.
Require and verify peer certificate	Check this box to only allow connections from peers with valid certificates.
CA File (Optional)	Enter a path to an alternate certificate file if you need to. If this field is left blank, the CA File defined under **Certificates – CA** will be used.

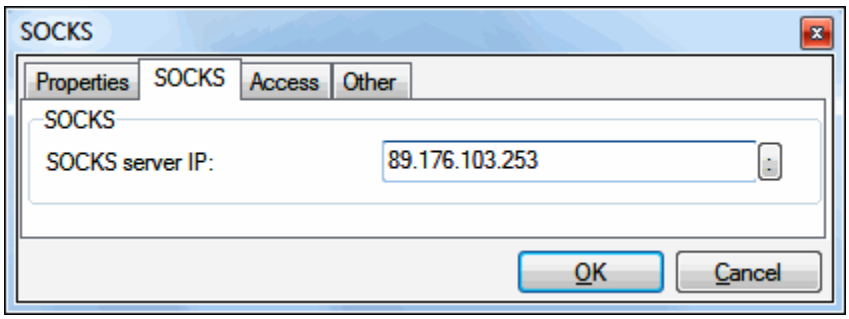
Service – Logging



Field	Description
Active	Tick the box if you want to have traffic logs available. For logs, refer to the **Status – Traffic Charts** node.

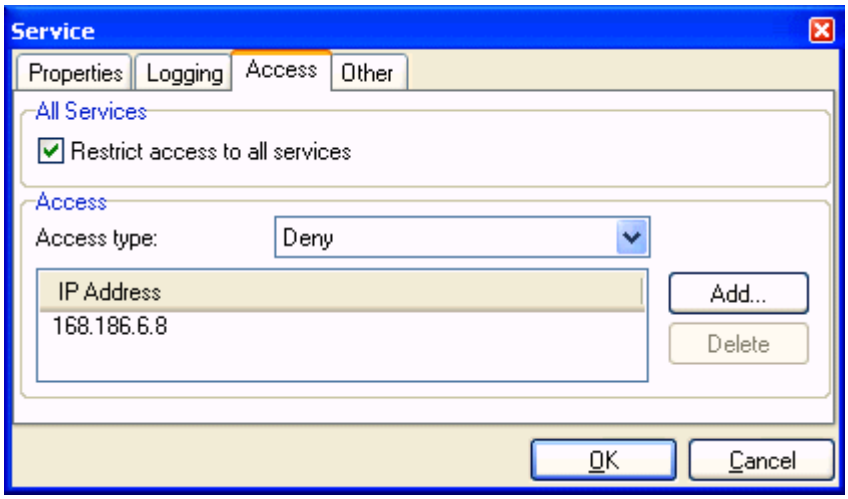
Other related options can be set in **Logging**.

NOTE: For SOCKS service, this tab is different.



Field	Description
SOCKS server IP	This field should contain the external IP address or hostname of your router or NAT device, i.e. the IP address that the Internet sees as you or your network. Click the "**:**" button to have the IP address discovered for you. *NOTE: Using a hostname can solve problems with connections from inside and outside the network (by translating the hostname to different IPs for inside and outside connections).* *Control module has to be restarted to use new setting.*

Service – Access

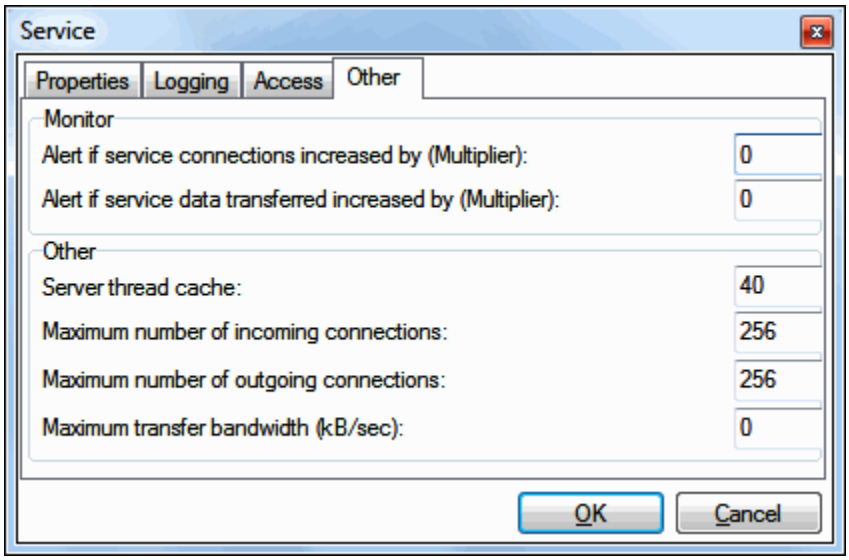


The **Access** feature acts as a basic firewall and allows you to block or grant access to specific IP addresses that try to connect to your server.

This is not an anti relaying option, and normally you would not need to use this feature.

Field	Description
Restrict access to all services	This option affects all services. Check this box to enable the feature.
Access type	**Grant** means only the listed IPs will be able to establish connections to your server. **Deny** means the listed IPs will not be allowed to connect.
IP Addresses	Specify IP addresses you wish to grant or block access to. You can specify full IP addresses here or subnets (masked IP addresses). CIDR notation/ranges can be used. Multiple entries are allowed, separated with semicolons. Example: 192.168.*.*;127.0.0.1;192-193.*.*.*;[Firewall] *NOTE: [Firewall] here is a **Pattern**. (For more information on patterns, refer to the **Advanced – Patterns** section.)*
Add	Click the button to add a new IP address. The **IP Address** dialog appears. See the **Service – Properties** chapter.
Delete	Click the button to delete the selected IP address.

Service – Other



Field	Description
Alert if service connections increased by (Multiplier)	Enables service connections monitoring by entering a multiplier. For example, a value of 2 will create an alert when the service connections increased by 200% in one minute (based on 5 min. average). The alert email message is sent to the email account specified in the **System Monitor** tool. **PLEASE BE AWARE: In a load-balanced system, these alerts do not function correctly and it is recommended that you do not use them.** *NOTE: The values are not evaluated within the first 30 minutes after the appropriate service start/restart.*
Alert if service data transfer increased by (Multiplier)	Enables service data transferred monitoring by entering a multiplier. For example, if you enter 3, you will be alerted after a 300% increase in the amount of data transferred by a particular service. (Use only integer numbers.) The alert email message is sent to the email account specified in the **System Monitor** tool. **PLEASE BE AWARE: In a load-balanced system, these alerts do not function correctly and it is recommended that you do not use them.** *NOTE: The values are not evaluated within the first 30 minutes after the appropriate service start/restart.*
Server thread cache	The thread cache specifies the maximum number of threads that can be reused for new client connections. Each new connection that is accepted by the server is given a separate execution thread. In order to improve performance, server sockets store these threads in a cache rather than freeing them when the connection is closed. New connections can then reuse threads from the cache, rather than requiring the server to create a new thread every time a connection is accepted. Optimal setting is a number of threads based on average connections. *NOTE: It is not recommended to change the defaults values unless you have a specific reason to do so.*
Maximum number of incoming connections	The maximum number of simultaneous connections from remote servers. You can limit the flow of incoming connections with this option.

Maximum number of outgoing connections	The maximum number of simultaneous connections to another mail server. You can limit the flow of outgoing connection with this option. Consider using this limit if your server's CPU usage is too high. *NOTE: This is only active for the SMTP, POP3, IMAP and FTP services.*
Maximum transfer bandwidth (kB/sec)	You can restrict the maximum speed (in kilobytes per second) which can be used for particular service. This is useful if you have a slow connection and you want to leave bandwidth available for other services. A value of "0" means no restriction is applied. *NOTE:This limit is not applied to trusted IPs.*

SOCKS and Minger Server

SOCKS

SOCKS service is required for file transfers between XMPP/Jabber clients in cases where direct transfer is not possible due to NAT problems.

SOCKS server IP

This field (described within the **Services – Logging** chapter) should contain the external IP address of your router or NAT device, i.e. the IP address that the Internet sees as you or your network.

Click the "**:**" button to have the IP address discovered for you.

BE AWARE: ***SOCKS Server*** port is set on the **Properties** tab of the **Service** dialog (**System – Services – General** tab, double-click the service). This port must be available on the machine this service will run on. The default port of ***1080*** may be already in use, if this is the case then you must locate a port that is free and enter it here.

This port must also be enabled in your firewall/router.

NOTE: When using IceWarp SOCKS service together with PSI (IM client), it is necessary to set PSI properly file transfer to work correctly behind NAT:

*The **Data transfer base port** field (**PSI – General – Options – Application**) is to be set to **0** (zero).*

*The **Data Transfer Proxy** field (**PSI – General – Account Setup –** (select account) **– Modify – Misc.** tab) has to include the **JID** value of the **PSI – Service Discovery – Bytestreams Proxy** item.*

NOTE: If you are using NAT and your server does not recognize external IPs, specify the servers NAT IP in SOCKS properties (System – Services – double click SOCKS – SOCKS tab). If you are using load balancing, specify the master server's NAT IP.

NOTE: If you need to access SOCKS server from LAN and WAN and your public IP is not usable from LAN, you can put A DNS record to SOCKS IP field instead of IP. Then configure DNS, this record (domain name) to be translated into valid and accessible server IPs for both WAN and LAN.

Note that Control and IM services need to be restarted and then a user needs to relog to WebClient to have the SOCKS IP change applied.

Minger Server

This technology allows you to use a complete domain sharing feature (including instant messaging, VoIP, etc.). You can have the same domain across multiple servers and keep different sets of accounts in each and still be able to reach the other accounts via email, instant messaging and VoIP.

There is a UDP server used for checking if a user exists on a remote server. This is protected by a domain shared (secret) password and it is processed by a smart hash mechanism (Minger Protocol RFC draft). You use the Minger functionality instead of using VRFY or RCPT domain.

Whenever a local account does not exist, remote servers (specified in the list) are checked simultaneously whether this account exists there. If yes, emails are forwarded there, IM messages are sent via S2S XMPP protocol and VoIP is also forwarded to the final destination.

*NOTE: If you want to set a password that the servers serving the distributed domain will use for mutual contact, go to the **Domains and Accounts – Management – <domain> – Options** tab – Verification field. This password has to be set on all these servers. This prevents queries from unknown servers.*

ALSO: By default, the service comes stopped – to obtain any logs, you have to start it first.

LDAP

About

LDAP is an acronym for **Lightweight Directory Access Protocol.**

LDAP, also known as a Directory System Agent (DSA), allows you to locate organizations, individuals, and other resources such as files and devices in a network, regardless if you are on the Internet or on a corporate intranet. Additionally, it does not matter whether or not you know the domain name, IP address, or geographic whereabouts.

An LDAP directory can be distributed among many servers on a network, then replicated and synchronized regularly.

LDAP was developed at the University of Michigan; it is "lightweight" in contrast to DAP, a part of the older X.500 direct protocol for networks.

IceWarp Server's implementation of the LDAP is based on the OpenLDAP Project at ***http://www.openldap.org/***, extended with SSL support. The whole LDAP server is installed and configured automatically during the IceWarp Server installation.

There many ***resources*** (see "LDAP References") about LDAP on the Internet. It is definitely good idea to study some of them…

LDAP utilizes Client-Server Architecture.

LDAP Server is installed with IceWarp Server and resides in the folder <InstallDirectory>\LDAP\

LDAP Client is usually your email client, or other application. Many current email clients, including Microsoft Outlook, Eudora, and Netscape Communicator are able to access this LDAP Server. See the **Using LDAP** section.

LDAP Server

IceWarp Server supports LDAP v3 and is based on the **OpenLDAP project** (http://www.openldap.org/). Any additional information can be found on that site. See the license agreement in the **LDAP\readme.txt** file (downloaded from the project web site – see the link above).

Once installed, you can start the LDAP server and it will be ready and working. It has its suffix already created so you can go on with creating new entries immediately.

LDAP runs under the Control service and works only on Windows NT and higher (2000,XP, 2008, Vista, 7) platforms (as well as on Linux). It does not support Windows ME,95,98.

LDAP setting files can be found in the **<InstallDirectory>\LDAP** directory and follows the OpenLDAP project.

To activate LDAP, you have to have IceWarp Server running on Windows NT (and higher) platforms. Click ***Active and Save***. LDAP server will start immediately.

When started you can see it is really running in the **System – Services – General** tab.

You can also change the LDAP ports. LDAP in IceWarp Server supports SSL so you can connect to the LDAP over a secure connection using the certificates installed on IceWarp Server. Same certificates as for HTTP and other services will be used.

Make always sure to check the LDAP running status. If any errors were created in the settings, the LDAP server will not start.

In case that LDAP fails after restart, you can follow these steps:

- Install IceWarp clean or rename LDAP folder and reinstall IceWarp (you need to be sure that LDAP is the newest version and there are no config issues).
- Make sure LDAP is not started yet after the install.
- Make sure debug logging is enabled for LDAP.
- Start LDAP and logs show its ok.
- Stop LDAP
- Start LDAP
- Logs show LDAP is stopped

  There is an error in the log: bdb_db_open: database "": unclean shutdown detected attempting recovery

  It then shows it failed.

  LDAP is not usable at this point.
- Stop LDAP service.
- Delete contents of LDAP/data folder to create new DBs.
- Start LDAP and its working.

NOTE: Use the console to start and stop LDAP during this test.

LDAP Configuration

To configure LDAP properly you have to have some prior knowledge. To learn more about LDAP search the Internet or follow the resource links. IceWarp Server's LDAP will let you immediately add, modify, delete and search records on LDAP.

The main settings are done in the **LDAP\slapd.conf** file. The file looks like this:

```
#
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
#
ucdata-path ./ucdata
include ./schema/core.schema
include ./schema/cosine.schema
include ./schema/inetorgperson.schema
# Define global ACLs to disable default read access.
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral ldap:/root.openldap.org
pidfile ./run/slapd.pid
argsfile ./run/slapd.args
# Load dynamic backend modules:
# modulepath ./libexec/openldap
# moduleload back_bdb.la
# moduleload back_ldap.la
# moduleload back_ldbm.la
# moduleload back_passwd.la
# moduleload back_shell.la
# Sample security restrictions
# Require integrity protection (prevent hijacking)
# Require 112-bit (3DES or better) encryption for updates
# Require 63-bit encryption for simple bind
# security ssf=1 update_ssf=112 simple_bind=64
# Sample access control policy:
# Root DSE: allow anyone to read it
# Subschema (sub)entry DSE: allow anyone to read it
# Other DSEs:
# Allow self write access
# Allow authenticated users read access
# Allow anonymous users to authenticate
# Directives needed to implement policy:
# access to dn.base="" by * read
# access to dn.base="cn=Subschema" by * read
# access to *
```

```
# by self write
# by users read
# by anonymous auth
#
# if no access controls are present, the default policy
# allows anyone and everyone to read anything but restricts
# updates to rootdn. (e.g., "access to * by * read")
#
# rootdn can always read and write EVERYTHING!
#######################################################################
# BDB database definitions
#######################################################################
database bdb
suffix ""
rootdn "cn=admin"
# Cleartext passwords, especially for the rootdn, should
# be avoid. See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
rootpw admin
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory ./data
# Indices to maintain
index objectClass eq
```

include

This item lets you include additional schema definitions. All schema definitions are located in the **LDAP\Schema** directory. You can create your own definitions and edit the existing. Make sure to follow the creation rules otherwise LDAP will not start. If you are a beginner use always the existing schema definitions.

suffix

This item identifies the suffix you will use the LDAP server under. All client connections will have to use this suffix. All DB records are also under this suffix so when you change the suffix you need to create the new records again under the suffix. Usually the suffix is like your domain name.

```
suffix    "dc=icewarpdemo.com,dc=com"
```

We wanted to you to be able to use the LDAP right always so we created the suffix:

```
suffix    "dc=root"
```

rootdn

This item identifies the administrator user of LDAP that does not need to exist in LDAP and still perform any actions like add, edit and delete records. It always has to contain the suffix at the end. The default is:

```
rootdn    "cn=admin,dc=root"
```

rootpw

This item contains the password for rootdn the administrator account in LDAP.

The rest of the **slapd.conf** file lets you perform additional changes. Make sure you do not change them unless you know what you are doing. Any additional information can be found at ***http://www.openldap.org/***.

access

This directive is used to define access rights (ACL) to a database. By default, only users are allowed to read (not anyone). If you want to allow access for anyone (what was default before version 11.2.0), remove or comment out access definition. Please read comment in the **.config** file for more information on this subject.

LDAP configuration - import on Windows

Get a certificate for AD server from a CA and import it.

This certificate for AD can be self-signed. It is certificate, which AD that you want to sync users from use, to the machine where you run IceWarp. Import this certificate on IceWarp Server to Trusted Root CA / local machine so even service running under system account can access it.

To get the certificate use ldap browser or some other 3rd party tool that connects to **port 636**, ldapadmin is recommended.

Than you have to import the certificate to a certificate store which is accessible to services as IceWarp runs as service by default. If you run it under particular user, obviously you can import certificate to storage accessible to that user only. Open **mmc** add certificate snap-in, select local computer as the scope.

Certificate attribute cn and AD hostname used in IceWarp Server domain directory service must match.

When you configure IceWarp Server domain sync, use the same value for hostname as there is in certificate property CN, otherwise it will not work as windows library will not trust the certificate.

Using LDAP

Adding, modifying and deleting records on LDAP can be done using different LDAP tools. We recommend using **LDAP Administrator** that can be downloaded from **Softerra** (http://www.softerra.com/).

Another good free tool you can download from ***http://ldapadmin.sourceforge.net/download/ldapadmin.html***.

All mail clients supporting LDAP allow you to search records on LDAP servers. Hardly some will help you to modify records on the server. Some mail clients have a better LDAP implementation and searching is smooth and some are cumbersome and hardly to use.

Configuring MS Outlook 2010 for LDAP

To configure MS Outlook 2010 for LDAP, use a detailed description provided on this web site:
https://kb.wisc.edu/wiscmail/page.php?id=13789.

LDAP Tools

There are some tools in the LDAP directory (**icewarp/ldap**) that help to administer LDAP DB. The tools have the same parameters as the tools of the OpenLDAP project.

slapadd

Slapadd allows you add records to LDAP DB using the LDIF format. You can see an example in the LDAP directory. The two files, create.ldif and create.bat, create the suffix in the LDAP DB using the **slapadd** tool. Similarly you can add more records by editing the create.ldif file. Syntax of the LDIF format can be found on the Internet.

schema

The LDAP schema, as with all database schemata, is the definition of what can be stored in the directory. The basic thing in an entry is an attribute, like given Name. Each attribute is associated with a syntax that determines what can be stored in that attribute (plain text, binary data, encoded data of some sort), and how searches against them work (case sensitivity, for example). An object class is a three-tuple, consisting of (must have, required, may have), saying what other attributes can or should be present.

There is a standard core of schema definitions (object classes, attributes and syntaxes), and you can define your own to suit your particular needs. Most every organization will want to do that.

LDAP References

- LDAP Zone ***http://www.ldapzone.com/***
- ldapman.org ***http://www.ldapman.org/*** has some great introductory articles.
- The LDAP Schema Repository ***http://ldap.akbkhome.com/*** is indispensable for figuring out what to stuff in there and how.
- Jeff Hodge's LDAP roadmap and faq ***http://www.kingsmountain.com/LDAPRoadmap/***
- The Yahoo! category ***http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Protocols/LDAP__Lightweight_Directory_Access_Protocol_/*** has great links.

LDAP Server Installation on Linux

To install LDAP server on Linux, do the following:

1. Stop the **Control** service (***System – Services – LDAP*** – right-click *Stop Module 'Control'*).
2. Rename folder of ***c:\Program Files\IceWarp\ldap\data*** to ***c:\Program Files\IceWarp\ldap\data.bak***.
3. Create a new folder – ***c:\Program Files\IceWarp\ldap\data***.
4. Edit the ***c:\Program Files\IceWarp\ldap\slapd.conf*** file and change the *"# ldbm database definitions"* section like this:

   database bdb

   suffix "o=testes.icewarp.com.br"

   rootdn "cn=Manager,o=testes.icewarp.com.br"

   rootpw put-your-password-here

   # The database directory MUST exist prior to running slapd AND # should only be accessible by the slapd/tools. Mode 700 recommended.

   #directory %LOCALSTATEDIR%/openldap-ldbm

   # Indices to maintain

   index objectClass eq

 # The database directory MUST exist prior to running slapd AND # should only be accessible by the slapd and slap tools.
 # Mode 700 recommended.
directory ./data

5. Within the **System – Services – LDAP** dialog – ***Properties*** tab, enter the port number for LDAP (389 by default, if 389 is used (by AD for example), choose an another port).
6. Start the **Control** service (***System – Services – LDAP*** – right-click *Start Module 'Control'*).
7. Create a new file – ***c:\Program Files\IceWarp\ldap\create-custom.ldif*** with the following content:

o=testes.icewarp.com.br
objectClass: organization
o: testes.icewarp.com.br
description: test

dn: cn=Manager, o=testes.icewarp.com.br
objectclass: organizationalRole
cn: Manager
description: Directory Manager

dn: ou=users, o=testes.icewarp.com.br
ou: users
objectClass: organizationalunit
objectClass: top

dn: ou=groupes, o=testes.icewarp.com.br
ou: groupes
objectClass: organizationalunit
objectClass: top

8. Add the nodes declared in ***custom-create.ldif***:
ldapadd -f create-custom.ldif -D "cn=manager, o=testes.icewarp.com.br" -w admin
(***ldapadd.exe*** is in the ***c:\Program Files\IceWarp\ldap*** directory.)
This command will output:
adding new entry "o=testes.icewarp.com.br"
adding new entry "cn=Manager, o=testes.icewarp.com.br"
adding new entry "ou=users, o=testes.icewarp.com.br"
adding new entry "ou=groupes, o=testes.icewarp.com.br"
9. Check contents of LDAP:
*ldapsearch -b "o=testes.icewarp.com.br" objectclass=**
—> it should list four entries.
10. Configure **Domains & Accounts – Global Settings – Advanced**:
LDAP server: <IP>:<port>
Base DN: ou=users, o=testes.icewarp.com.br
User DN: cn=Manager, o=testes.icewarp.com.br
password: <the one entered in slapd.conf>
11. On the **Domains & Accounts – Global settings – Advanced** tab, click the *Synchronize All Users...* button.
12. Check the result, use either the ***tool.exe*** file or the command line:
*ldapsearch -b "o=testes.icewarp.com.br" objectclass=**
—> it should list all 'user' accounts on the server.

SmartDiscover

About

Due to many different services and protocols used in communication software these days, end users are often in doubt how to setup their client applications (email client, mobile synchronization, VoIP client and so on). Administrators need to use various mass-configuration tools or create detailed how-tos for end users.

It is also time consuming and prone to error to configure all server's protocols in the client application. A solution to retrieve all the server's capabilities and supported protocols is required.

SmartDiscover is a mechanism which ensures that any client application once supplied email address and password (every user must know their email address and password) and authenticated by the server will receive a complete list of available protocols, ports, URLs and server addresses. User can start working immediately with zero configuration required.

Microsoft has implemented AutoDiscover in Exchange Server for Outlook and ActiveSync clients only. IceWarp goes further and extends available applications by its own email client, Outlook Sync plugin, SIP and IM clients, and the Notifier utility. Virtually any protocol settings can be configured using AutoDiscover feature, provided that the corresponding client has AutoDiscover support built-in.

MSDN Links:

http://msdn.microsoft.com/en-us/library/cc433481.aspx

http://msdn.microsoft.com/en-us/library/cc463896.aspx

Test:

https://www.testexchangeconnectivity.com/

How it Works

The client application once supplied with the user's email address will try to contact the server through a set of simple ***HTTP GET requests***, using the domain part of the email address as a basis. If the URL does not exist or failed with an error, the client retries the other URL using the same mechanism until the server's AutoDiscover service can be contacted.

Assuming that you are configuring your server for the domain of *icewarpdemo.com*, the preset URLs are:

https://autodiscover.icewarpdemo.com/autodiscover/autodiscover.xml

https://icewarpdemo.com/autodiscover/autodiscover.xml

The client will then authenticate by HTTP authentication, using the same email address and password combination and if successful, the server will return the configuration details in the form of an XML formatted plain text file. The client reads the parts corresponding to services it provides, and configures itself without any user's interaction.

Request

1. SmartDiscover domain attempt

   A client having an email address and password of the user will issue a simple HTTP GET request to:

   https://autodiscover.icewarpdemo.com/autodiscover/autodiscover.xml

   Authentication request should be returned from the server. When authenticated properly via HTTP authentication, an XML response is returned from the server.

2. Original domain attempt

   If the URL does not exist or failed with an error, the client should retry additional URL using the same mechanism:

   https://icewarpdemo.com/autodiscover/autodiscover.xml

3. MX query host attempt

   If still not successful, a client MAY issue a DNS MX query for the domain to list the records that correspond to the server's hostname. It checks all MX records in the order of preference and attempts to contact the same URL as in step #2:

   https://mxhost1/autodiscover/autodiscover.xml

   https://mxhost2/autodiscover/autodiscover.xml

NOTE: This step is specific to clients developed by IceWarp and does not follow the original Microsoft specification.

Response

Successful response consists of HTTP 200 OK and a Content-Type: text/xml file.

Configuration

1. The administrator needs to ensure that both of these DNS records exist:

   • DNS A record: ***autodiscover.icewarpdemo.com*** (normally it does not exist)

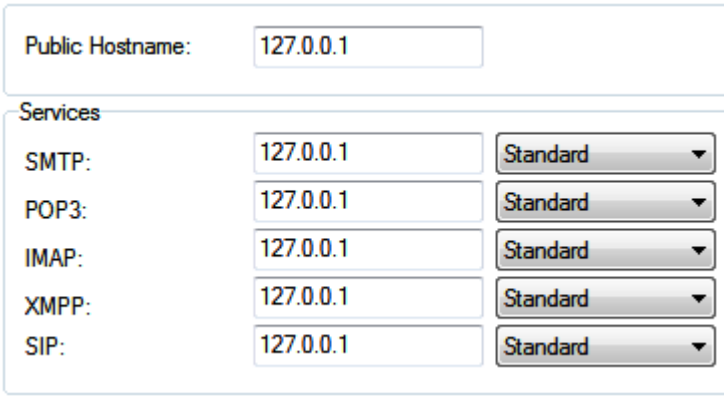
   • DNS A record: ***icewarpdemo.com*** (where the domain is the exact hostname of the server where all services are running; normally it does not exist for a plain mail server, but can be already established for web, XMPP or SIP services)

   Use the **DNS Tool** (**System – Connections – General** – ***DNS Tool*** button) to check your A records (Host address) if the AutoDiscover fails for ActiveSync clients.

   NOTE: For Notifier and other IceWarp native clients, the records do not have to be established in DNS – these clients will also check the hostname using the MX records, i.e. if the email is working, Notifier will configure itself without additional DNS changes. However for ActiveSync, one of the A records above must exist.

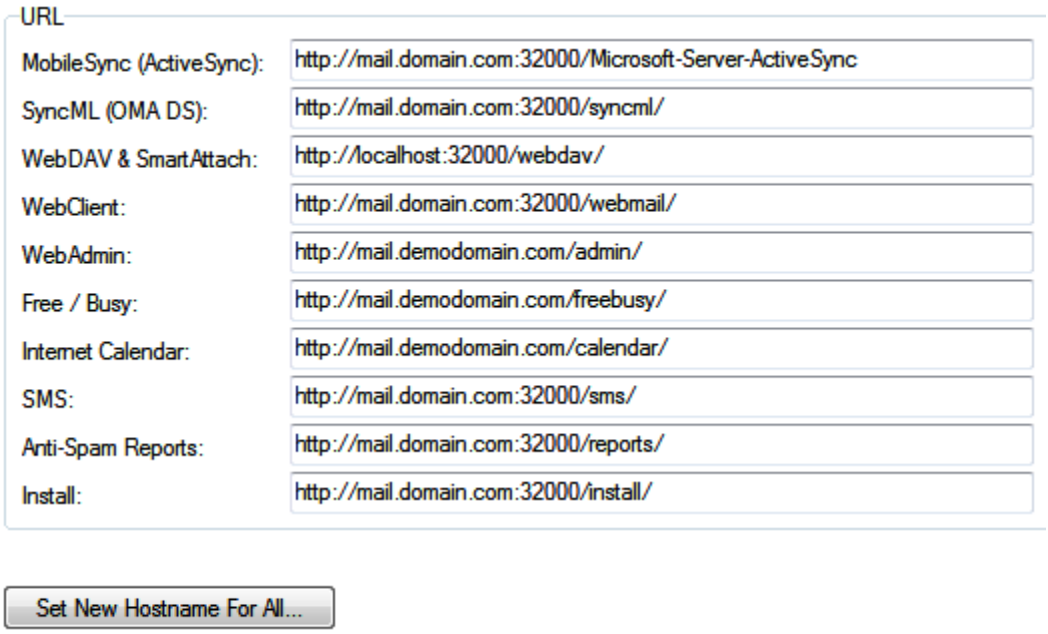
2. A non-expired, CA-issued SSL certificate needs to be installed on the server for AutoDiscover to work with iPhone. Windows Mobile requires a non-expired, either self-signed or CA-issued SSL certificate public key to be installed on the device, corresponding to the certificate installed on the server. Otherwise the AutoDiscover will fail due to untrusted connection with the server (and therefore untrusted authentication).

On-server Setup



Field	Description
Public Hostname	Hostname or alias of the server where IceWarp Server runs. This field must not be left blank as it is used when IceWarp Server authenticates or introduces itself to another mail server. This should be the hostname of your IceWarp Server which is registered on DNS. You may also want to ensure your IceWarp Server's IP address has a PTR record registered as this is a spam-fighting requirement that some receiving mail servers require. *NOTE: This value is the same as in the **Mail – General – Delivery – Public Hostname** field. When changed in one field, it is changed within the second one accordingly.*
SMTP	Hostname or alias of the server where the SMTP service runs.
POP3	Hostname or alias of the server where the POP3 service runs.
IMAP	Hostname or alias of the server where the IMAP service runs.
XMPP	Hostname or alias of the server where the XMPP service runs.
SIP	Hostname or alias of the server where the SIP service runs.
Standard / TLS/SSL `for all services`	Select from the list what type of connection a device will use for SmartDiscover (standard v. secured one).

*NOTE: Ports for these services are defined under the **System – Services – General** tab.*



Field	Description
MobileSync (ActiveSync) SyncML (OMA DS) WebDAV & SmartAttach WebClient WebAdmin Free/Busy Internet Calendar SMS Anti-Spam Reports Install	URLs of the services running under the HTTP (Control) service. These URLs consist of: ▪ Name or alias of the server where the HTTP service runs. These names (aliases) can differ but all have to be aliases of the same server. E.g.: It is possible to use alias ***webdav.domain.com*** for the WebDAV service provided that it is valid alias for ***mail.domain.com***. ▪ Port number. Number of the port defined for the HTTP service (32000 here); it is possible to use HTTPS (usually with the port number of 32001). ▪ Name of the service folder. *NOTE: For ActiveSync it is not possible to change this name.*
Set New Hostname For All ...	Click the button to open the **Server/Hostname** dialog where you can set a new hostname for all above fields. Within the URL section fields, only the relevant address parts are changed, other parts are kept.

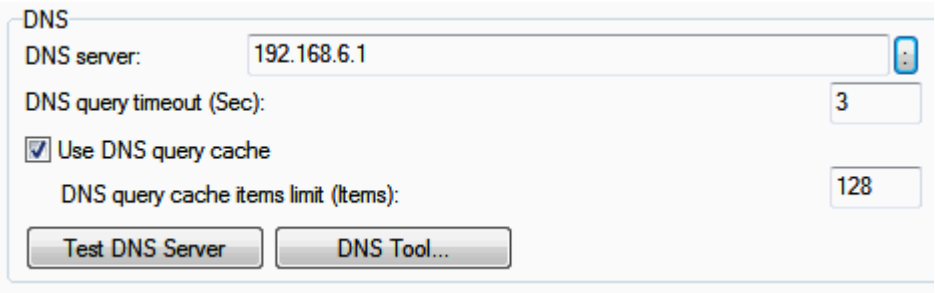
*NOTE: Some of the defined **URLs** are also **used internally** by IceWarp Server mechanisms – such as WebClient's "forgot password" feature (if enabled by an administrator in WebClient). Make sure all paths are correctly specified, so that internal mechanisms work as expected.*

DNS SRV Records Configuration

For information about **DNS Records Configuration,** refer to the chapter of the same name in **IceWarp Server GUI Reference** or follow the link.

Connection

General

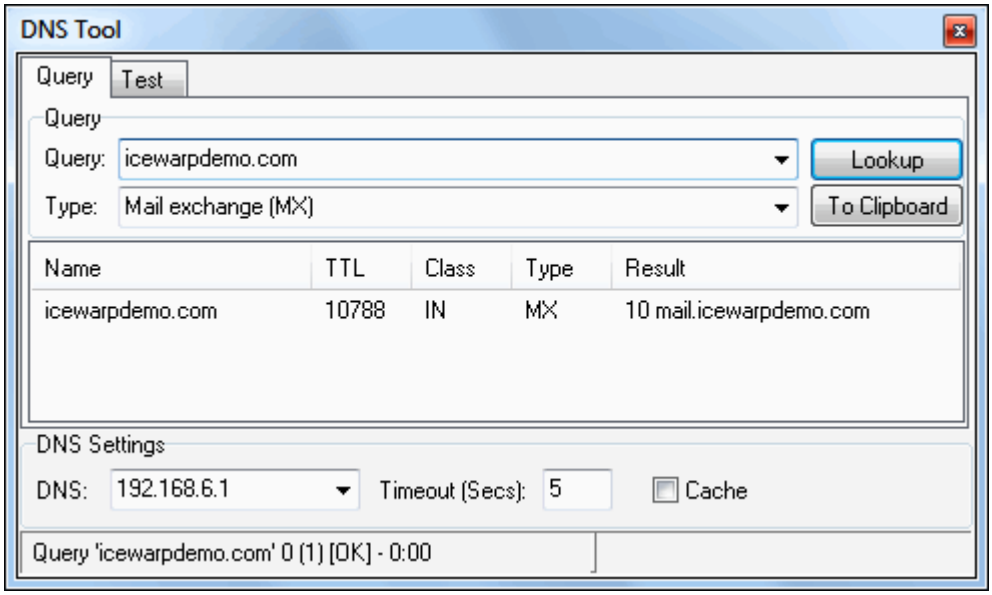


Field	Description
DNS Server	Specify IP addresses for your DNS servers here. Separate multiple entries by semicolons. You should specify two or three DNS servers so if one is unavailable, then the second one can be accessed and so on. Examples of public DNS servers: OpenDNS (208.67.220.220), Google (8.8.8.8), level3 (4.2.2.1). *NOTE: IceWarp Server will attempt to locate your DNS servers automatically on the initial installation. (Or click on the ":" button to fetch the DNS servers specified in your server's NIC automatically. If connection is not available, the server tries also system DNS (Windows configured).)*
DNS query timeout	The amount of time (in seconds) to wait for a DNS server response before considering this a timeout and trying the next DNS server in your list. This timeout is used for each defined DNS server (if accessed). In performance logs, the total timeout is logged.
Use DNS query cache	Allows IceWarp Server to cache the results of DNS queries, which can greatly enhance server performance on high load servers.
DNS query cache items limit	Specify the number of DNS queries to be cached. The higher the number, the greater the performance improvement can be, but we recommend not specifying a value greater than 2000 as the cache will use up some of your server's memory.
Test DNS Server	Use this button to test the functionality of the servers you specified. You should always perform this test when you add or change DNS servers. Just connection to the specified DNS server(s) is tested.
DNS Tool	Click the button to open the **DNS Tool** dialog. See the **DNS Tool** chapter.

DNS Tool

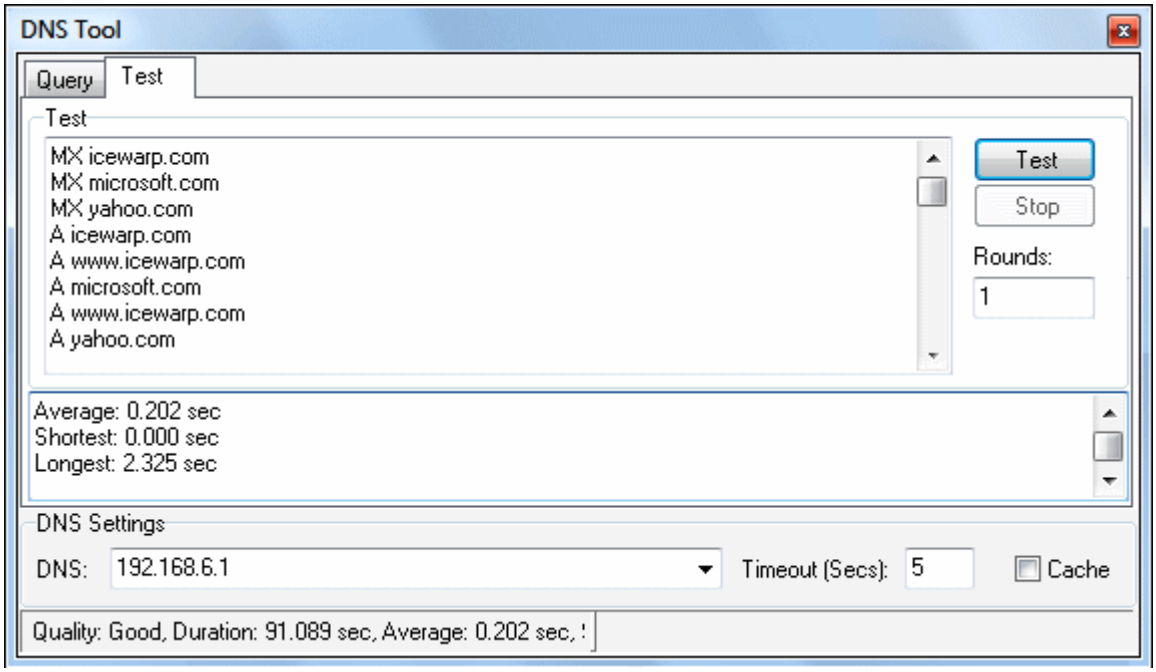
This tool is designed to ease DNS queries.

Query Tab



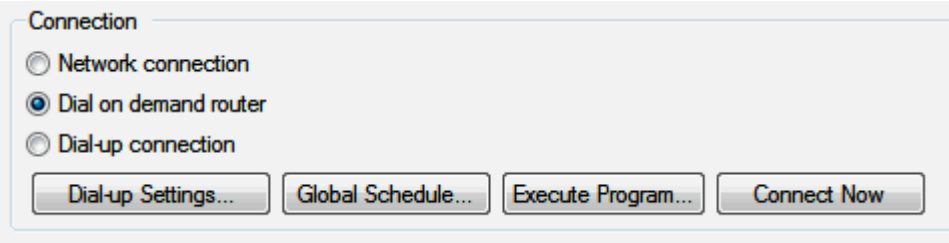
Field	Description
Query	Fill in a domain you want to check.
Type	Select a type of DNS record you want to check a domain for.
Lookup	Click the button to perform a query.
To Clipboard	Click the button to copy query results to a clipboard.
Name, TTL (time to live), Class, Type, Result	Query results.
DNS	Fill in the IP address of the DNS server you want to perform query against. By default, the IP address obtained by Windows from your local network is used.
Timeout (Secs)	Fill in a maximum time your query should last.
Cache	Tick the box if you want to have query results cached. If the same query is launched, it is not really performed – results are loaded from a cache.
Status bar	Result summary is shown here.

Test Tab

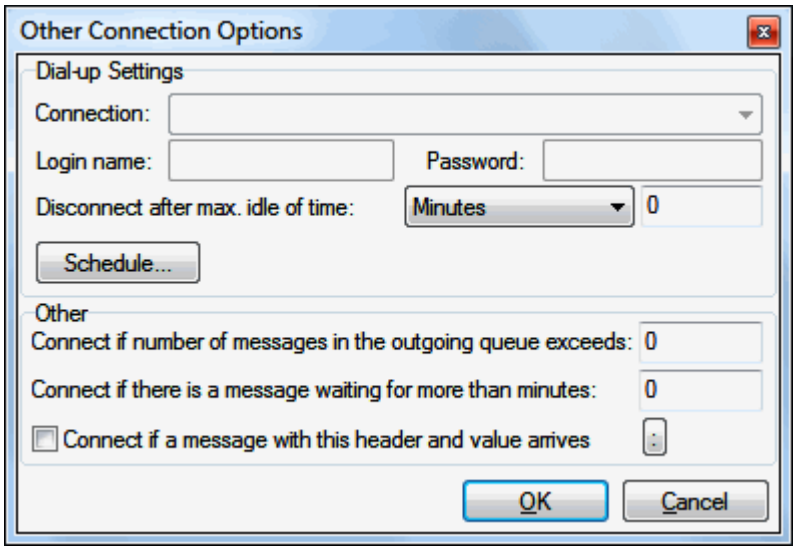


Field	**Description**
Test	Click the button to perform connection test against the list of global DNS servers defined in the left-hand frame.
Stop	Click the button to stop an ongoing test.
Rounds	Fill in a number of test rounds to be performed.
Middle frame	This frame includes test results.
DNS, Timeout, Cache, Status bar	See the **Query** tab description.

Advanced



Field	Description
Network connection	Select this option if you have a ***permanently-on*** connection to the Internet.
Dial on demand router	Select this option if your server is connected to the Internet via a dial-on-demand router. Use the ***Dial-up Settings button*** to specify connection information (see the **Other Connection Options** dialog below). You can also use the ***Execute Program*** button to specify an external application to run prior to connection (for example, a program that starts your router's connection).
Dial-up connection	Check this option if you use a standard dial-up connection.
Dial-up Settings	Use the button to specify connection information (see the **Other Connection Options** dialog below).
Global Schedule	Use this button to specify a schedule for connecting to remote accounts. If no schedule is specified here, all of your remote accounts should have their own schedules specified. If you have a global schedule specified and also a schedule for a remote account then the remote account schedule will override the global schedule. If you do not have any remote accounts, this (global) schedule is not used at all.
Execute Program	If you use a dial-on-demand router, you can specify an application to be run before the connection is established.
Connect Now	Use this button to connect immediately to the Internet. This is useful to test your connection settings and also to collect messages manually.



Field	Description

Connection	The drop-down box will list all connections defined on your computer. Select the one you wish IceWarp Server to use.
Login name / Password	The login username and password for the connection chosen.
Disconnect after max idle time:	You can have the connection terminated after a set period of inactivity. Useful for dial-up connections where you incur connection charges.
Schedule	Use this button to specify a schedule for connections to be established.
Connect if number of messages in the outgoing queue exceeds	Specify a number of outgoing messages – when this number is reached, IceWarp Server will establish a connection. A value of 0 disables this option.
Connect if there is a message waiting for more than minutes	Specify an the maximum amount of time a message should be in the outgoing queue before a connection is made. A value of 0 disables this option.
Connect if a message with this header and value arrives	Check this option to have IceWarp Server check outgoing message headers and establish a connection if certain criteria are met. Use the '***:***' button to specify the criteria in a simple file. Examples are given.

Logging

The **Logging** node allows you set the activity log options for all services.

Each service can create ***Summary, Debug*** (detailed) and ***Extended*** activity logs which can help greatly when trying to solve any problems within IceWarp Server.

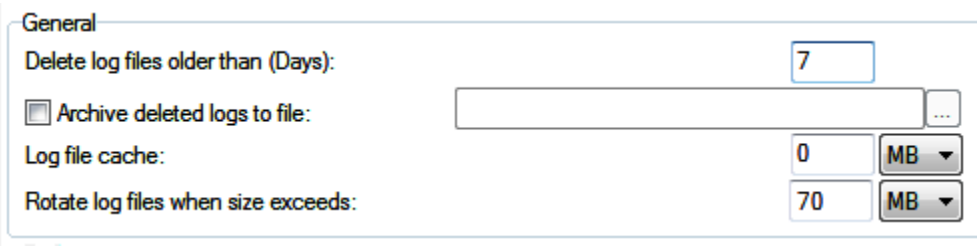
Logs can be written to simple files.

Log files can be rotated based on size and/or deleted after a number of days.

Log entries can be written to the standard system *syslog* (or sent to a remote syslog server).

General

In the **General** tab you decide how log entries will be saved.



Field	Description
Delete logs older than (Days)	By default, a new log file is created on a daily basis. This option allows you to delete old log files by specifying a threshold in days. In the screen shot above logs older than 7 days are deleted automatically. A value of zero here means the logs should never be deleted.
Archive deleted logs to file	Check this option and specify a fully qualified path to a file (ZIP or, older versions, MCB) where deleted logs will be archived. *NOTE: Specifying just a folder name here could cause deletion of all other files in this folder.*
Log file cache	Here, you can specify an amount of memory to be used as a cache for logs. Log entries are written to the cache until the cache is full, at which point the cache is written and consequently it is cleared. A value of 0 specifies that no cache is used.
Rotate log files when size exceeds	On a very busy server with a high level of logging, the daily log files could become too large to be readable. If you specify a number here then the logs will be rotated when the file reaches that size. In the above screen shot files will be rotated when they reach 70 MB in size.

Log files are saved into the **<install_dir>/logs** directory (if not changed within the **System – Storage – Directories** tab) or a subdirectory thereof:

Saved in **<install_dir>/logs** directory with a file name of ***<axyyyymmdd-nn.log>***, where:

Field	Description
x	server ID defined within the load balancing setting
a	type of logs – logs for: ***c*** – Web/Control Service ***e*** – general errors (including DB errors) ***f*** – FTP Service ***g*** – GroupWare Service ***i*** – Instant Messaging ***m*** – IMAP Service ***p*** – POP3 Service ***s*** – SMTP Service
yyyy	year
mm	month (2 digits)

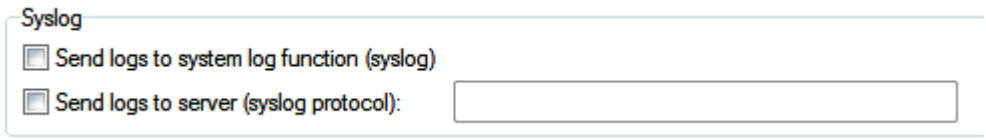
dd	day (2 digits)
nn	two digit incremental value, starting at 00, used if the log rotates within a one day period

So, ***m20060913-01.log*** is the first server second IMAP log for 13th September 2006.

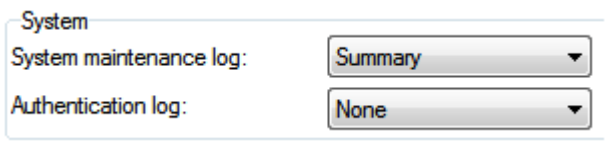
Subdirectories are named according to the logging data contained therein, they are:

- activesync
- antispam
- antivirus
- ldap
- loganalyzer
- maintenance (settings changes – eg.: 'System' updated '123@icewarpdemo.com')
- purple
- reports (for spam/quarantine reports)
- setup (installer logs)
- sip
- syncml
- syncpush
- voip
- webdav
- webmail

*NOTE: There is the **setup.log** file within the **<install_dir>/logs/setup** folder. This file is valid only for Windows installations. For information on Linux setup, refer to the **Installation and Control in Linux.pdf** guide.*



Field	Description
Send logs to system log function (syslog)	You can check this option to have all logged events sent to the system log. Events are written using the ***C_System_Logging_General_SystemLogFunction*** Windows API function.
Send logs to server (syslog protocol)	Check this option to have the syslog sender send its data to an external (remote) syslog server. This is usually used in large multi-server installations where there is a centralized syslog repository. Information packets are sent over UDP using the system log call function.



Field	Description
System maintenance	Select the logging level you want to use: • **None** – no logs at all.

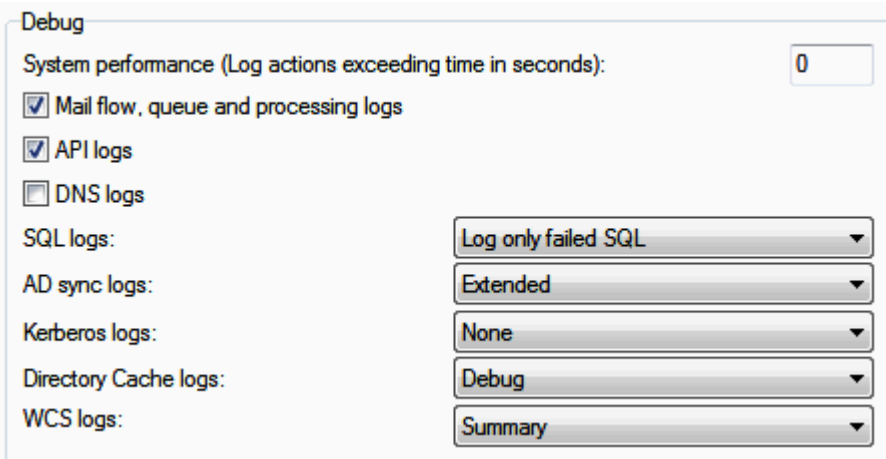
	• **Summary** – system/config updates (creations) are logged. • **Debug** – access denied errors are logged. • **Extended** – summary + debug logs.
Authentication log	Here, you can set authentication attempts logging. Also, login policy logs can be found here. Select the logging level you want to use: • **None** – no logs at all. • **Summary** – only the login policy logs and unsuccessful attempts are logged. • **Debug** and **Extended** – login policy logs and all login attempts are logged. Examples: *194.188.6.143 [21E4] 17:31:40:920 Login policy [IMAP] - increased failed login count to 1, user=b@t.com* *194.188.6.143 [1D14] 17:34:43:897 Login policy [IMAP] - cleared failed login count, user=b@t.com* *194.188.6.143 [1D14] 17:39:16:874 Authentication [IMAP] - Result=0, User=b, Method=0* *194.188.6.143 [1D14] 17:39:16:874 Authentication [IMAP] - Result=1, User=b@t.com, Method=0* Possible *Methods*: ***0=gmPASS*** ***1= gmMD5*** ***2= gmCRAMMD5*** ***3= gmNTLM*** ***4= gmDIGESTMD5*** ***5= gmSHA1*** ***6= gmOTP*** ***7= gmSYNCMLMD5*** User with full email address is logged only when authentication is successful. Otherwise, only the user name provided by the user is logged. This user name may not exist at all in the system. Authentication made through IceWarp Server's API is reported with the common service name of **Control**.

Field	**Description**
Logs	Click this button to access the **Status – Logs** node of IceWarp Server immediately.

Debug

This tab allows you to manage debug settings.

WARNING! Use very carefully! Turning these options on can produce (and probably will!) huge amount of logs.



Field	Description
System performance (Log actions exceeding time in seconds)	Insert time in seconds, if you want to have logged system actions lasting longer than the value specified here.
Mail flow, queue and processing logs	Tick the box, if you want to have logged most actions performed with email messages (antispam, antivirus, etc.) This feature logs actions taken after an email is received via SMTP and can indicate bottle necks, such as heavy content filters (that scan body of messages without a message size limitation). For very experienced administrators. *NOTE: The kind of logs where content filters /rules are menioned differ: When a rule (CF) alters mail delivery, it is written in SMTP logs (e.g.: rejection) . When it alters spam/nospam behavior, it is in AntiSpam logs (e.g.: rejection, change spam score, etc.). For other cases, you would need to enable mail flow logs to know whether a content filter /rule had a hit.* *SMTP log example: 127.0.0.1 [1A40] 14:16:04 Message for <mike@icewarp.com> not delivered. Reasons:[ContentFilter=Viagra,Bypass=Q], Action:REJECT*
API logs	Tick the box, if you want to have logged every API use. This includes not only any server setting change, but also for example any setting changes performed by users in their WebClients etc.
DNS logs	Tick the box, if you want to have logged DNS service and communication with your DNS server.
SQL logs	Select how you want to have logged database actions: ▪ ***None*** – none of database actions are logged. ▪ ***Log all SQL*** – really all is logged! Even showing folders in a WebClient. ▪ ***Log only failed SQL*** – only failed database enquiries are logged. ▪ ***Log connection maintenance*** – provides internal information about working with a

	database such as connecting/disconnecting, parameter binding, results fetching etc. This level includes ALL SQL queries logging.
AD sync logs	Select how you want to have logged Active Directory synchronization: ▪ ***None*** – no logs at all. ▪ ***Summary*** – after each domain synchronization, only one log row is written. E. g. ***[1E84] 13:56:01 Synchronizing domain tests.icewarp.com finished, Users(0 created,20 updated,0 deleted, 7 skipped, 27 listed), Groups(0 created,1 updated,0 deleted, 40 skipped, 41 listed)*** ▪ ***Debug*** – all important operations + failed user synchronizations are logged. Example of a failed synchronization log: *SYSTEM [1DB8] 13:51:47 Skipping item 1, because of missing email* ▪ ***Extended*** – all data obtained from a remote AD server are logged. Logs are really vast – use advisedly. (The AD output can be truncated. Maximum size of one log record is limited by the ***c_system_log_maxlogsize*** API variable. AD result is logged as one record.) These logs are available for GroupWare, SMTP and IMAP.
Kerberos logs	Select how you want to have logged Kerberos authentication. Only the ***Debug*** and ***Extended*** levels produce outputs. For more details, refer to the **Domains and Accounts – Domain – Directory Service chapter – Kerberos/GSSAPI/SSO** section.
Directory Cache logs	Select how you want to have logged directory cache: ▪ ***None*** – no logs at all. ▪ ***Summary*** – start and stop of wave mode is logged. ▪ ***Debug*** – the summary level plus reading from memory, disk, database, getting information about a directory and SQL errors are logged. ▪ ***Extended*** – all previous plus SQL queries and internal parts locking are logged. For more details on directory cache, refer to the **System – Advanced – Directory Cache** chapter.
WCS logs	Select how you want to have logged WCS (Web Coverage Service): ▪ ***None*** and ***Summary*** – no logs at all. ▪ ***Debug*** and ***Extended*** – any WCS communication is logged.

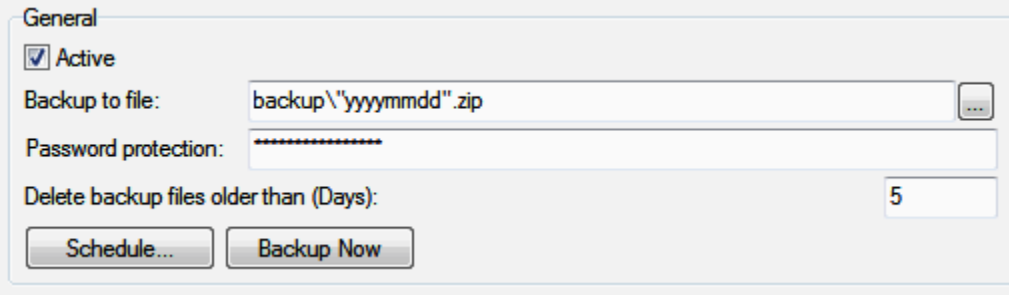
Tools

This chapter discusses various tools that are built in to IceWarp Server to help automate tasks and monitor systems.

System Backup

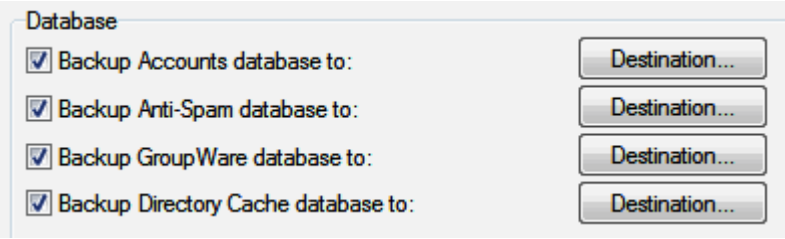
The **System Backup** tool allows you to schedule regular backups of your server.

You can also run a manual backup or restore using the **File – Backup Settings** and **File – Restore Settings** menu items.

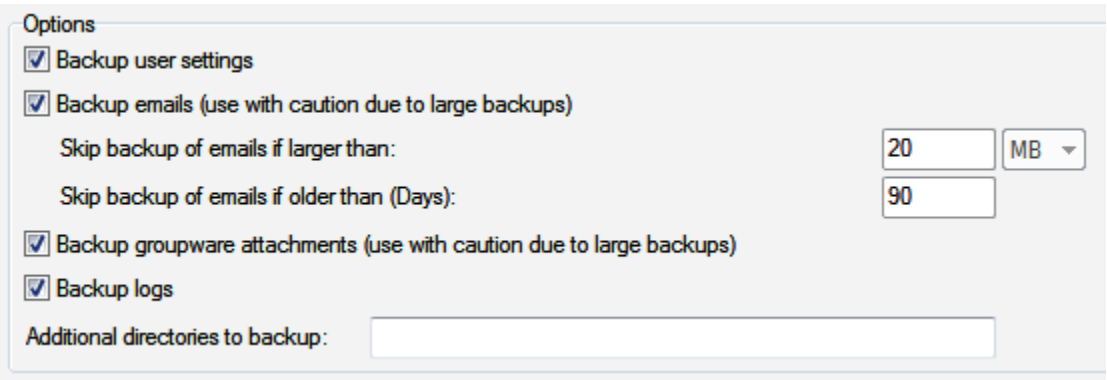


Field	Description
Active	Check this option to enable scheduled backup.
Backup to file	Enter the name of the backup file that the backup will be written to. Use the "..." button to browse to a directory or type directly to the text area. If you specify a folder that does not exist, it will be created when a backup is run the first time. By default, the path is **<install_dir>/backup**. You can use various variables within the file name, see the table below for more details. BE AWARE: Do not try to backup to the directories included into the backup itself – i.e. **config**, **spam (/rules**, **/reports)**, **logs**, **calendar (/attachments)**, **mail**. The backup would not work! *NOTE: Use these variables if you want to keep more (day) backup files – else these backups are overwritten.* *NOTE: In case the directory is on network share, the backup directory path must be specified in UNC format. Do not use drive mapping letters.* *If you want to set this path to another server, then IceWarp Control service has to run under an admin account which exists in both places (server and destination storage/server) and has appropriate NTFS permissions.* *If a backup is called with an empty string as a file name, the default name is used – yyyy-mm-dd-HHnn.*
Password protection	Fill in a password if you want to restrict access to ***.zip*** backup files.
Delete backup files older than (days)	If you use variables to create dated/timed files, you should use this feature to delete files older than a set number of days. Specify any non-zero amount to have files deleted. In the screenshot above, any ***.zip*** files over 5 days old will be automatically deleted.
Schedule	Use this button to set a schedule for regular automatic backups of your IceWarp Server configuration. BE AWARE: In the case you have set a backup schedule but backup files are missing, check the *Backup to file* field – see the warning within this field description (above). *NOTE: Setting a backup schedule is HIGHLY recommended.*
Backup Now	Click this button to backup your system immediately.

Variable	Description
YYYY	Current Year
MM	Current Month (01 – 12)
DD	Current Day (01 – 31)
HH	Current Hour (01 – 24)
NN	Current Minutes (00 – 59)
SS	Current Second of the actual time (00 – 59)



Field	Description
Backup Account database to	Tick the box if you want to backup your account database to another database server. Click the button to define this server.
Backup Anti-Spam database to	Tick the box if you want to backup your anti-spam database to another server. Click the button to define this server.
Backup GroupWare database to	Tick the box if you want to backup your groupware database to another server. Click the button to define this server.
Backup Directory Cache database to	Tick the box if you want to backup your directory cache database to another server. Click the button to define this server.
Destination	Click the button to define a backup destination. The **Database** dialog appears. For more details refer to the **IceWarp Server GUI Reference –Database Settings** section. *NOTE: The dialog described there has also the **Backup Connection** section, which is not present here. Also some buttons are not present here.*

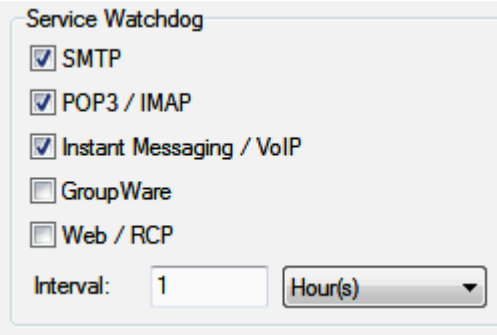


Field	Description
Backup user settings	Check this option to include all user data contained in the **mail/** directory (**autorespond.dat, imapindex.dat, flags.dat**, etc.). Use this option with care if you have a large number of users as the backup could take a long time. If you backup the entire **mail/** folder outside the IceWarp Server, it is not necessary to

	use this option .
Backup emails (use with caution due to large backups)	Check this option to include all mail messages into the backup. *NOTE: Use this option with care. A large production server could contain millions of emails and including them in your backup could cause major degradation in your server's performance.*
Skip backup of emails if larger than	If you choose to include mail messages in your backup you could cut down the size and duration of the backup process by excluding larger messages. Specify a non-zero value to exclude messages greater in size than that value. In the above screenshot messages larger than 20MB will be excluded from the backup.
Skip backup of emails if older than (Days)	When including mail messages in your backup you can also help performance by skipping messages older than the specified number of days. A value of 0 means do not skip any messages. In the above example, messages over 90 days old will be excluded.
Backup groupware attachments	Check this option if you want to have attachments of all groupware items backed up.
Backup logs	Check this option to include a copy of any log files that exist into the backup.
Additional directories to backup	You can add other directories to your backup by specifying them here. Multiple entries should be separated by semicolons. *NOTE: Use relative paths otherwise restore will not work. You can still use an absolute path but you will need to restore directories manually, as backups are zipped and zip does not support absolute paths. When restored, these files are unpacked to different folders and have to be copied to the appropriate locations manually.* *./ or .\ is not supported.* *E. g. to backup WebClient images directory:* ***html/webmail/client/skins/default/images*** *To backup the same directory with manual restore:* ***C:\Program Files\IceWarp\html\webmail\client\skins\default\images*** *ALSO: When restoring a backup file (.ZIP), if it refers to paths witch do not exist in the server where restore is being done, be them paths defined here or paths to centralized configuration/emails (**paths.dat** in the case of load balancing), the restore may fail. One workaround in the case of servers that have centralized configurations whose paths do not exist in the server where backup is being restored, is to manually extract **paths.dat** from the backup file.*

BE AWARE: The **php.ini** file is not backed up. If you perform any changes here, you will have to redo it. The **php.user.ini** file, used to copy customized **php.ini** file parameters, IS backed up.

Service Watchdog



IceWarp Server provides a basic service watchdog feature that monitors the specified services and if any of them is stopped, or uncontactable, it will automatically try to restart it.

Check the box next to each service you wish to monitor.

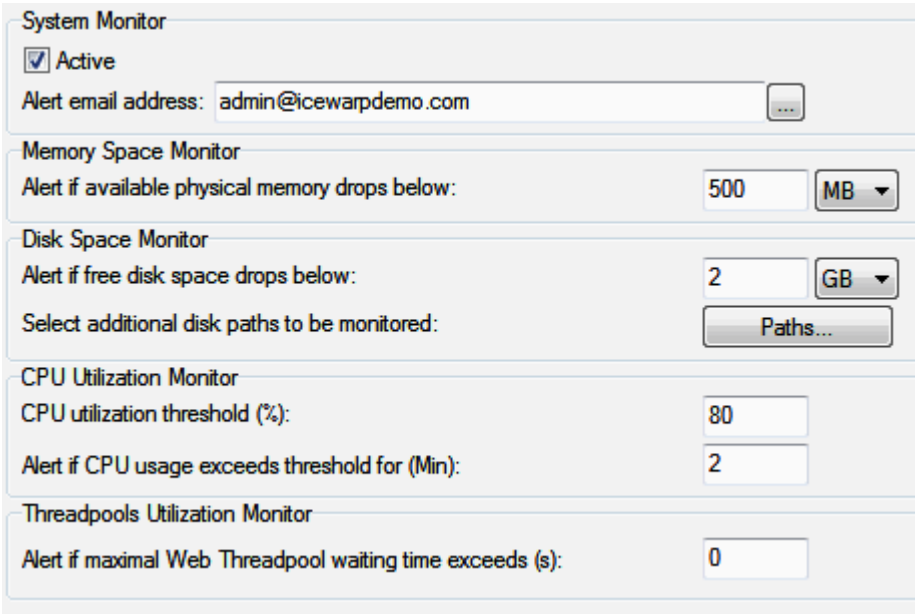
Specify in the ***Interval*** field text area and drop-down how often the watchdog should check the services (every 1 hour in the above screenshot). When ***0*** is set, the watchdog operates every minute.

NOTE: Service Watchdog is working correctly only if the SMTP service or Control one (or both of them) is running.

System Monitor

System Monitor monitors various aspects of your server.

You can have alerts sent to a user if thresholds you define are broken. We recommend that this user is an administrator so he/she can access the system and fix, or suggest a fix for the problem.

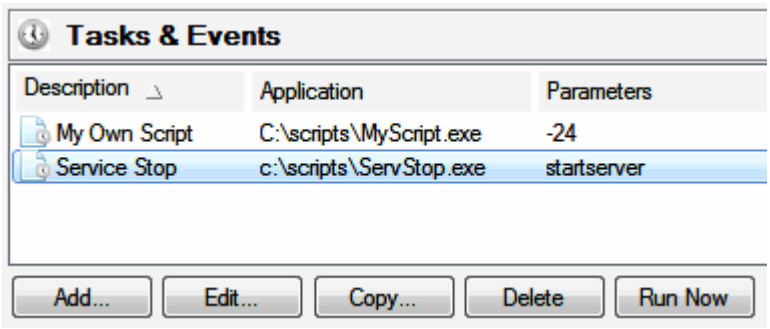


Field	Description
Active	Check this box to activate System Monitor.
Alert email address	Alerts will be sent to the address(es) specified here Multiple addresses can be entered, separated by semicolons.
Alert if available physical memory drops below	Enter a non-zero value here to have an alert sent based on available memory. In the screen shot above, an alert will be sent if the available memory falls below 128 kB.
Alert if free disk space drops below	Enter minimum free disk space – figure which will be used as a threshold. When available space on the IceWarp Server installation directory disk falls below this figure, an alert will be sent to the alert email address. If the value is zero, no disk space monitor is applied.
Select additional disk paths to be monitored	The ***Paths*** button opens the **diskspace.dat** file where different values can be entered for different disk drives. Examples are included in the editor. *NOTE: An alert is sent if any of paths has insufficient space even if the **Alert if free disk space drops below** value is set to 0.*
CPU utilization threshold	Enter a non-zero value to indicate a CPU utilization threshold for alerts. If CPU usage is higher than this threshold for the length of time specified in the next text box, an alert will be sent. This applies also for multi-CPU/multi-core servers in the case only one os CPUs/cores is high.
Alert if CPU usage exceeds threshold for (Min)	The length of time the CPU utilization must break the threshold before an alert is sent. In the above screen shot, a CPU alert will be sent if the utilization exceeds 80% for more than 2 minutes.

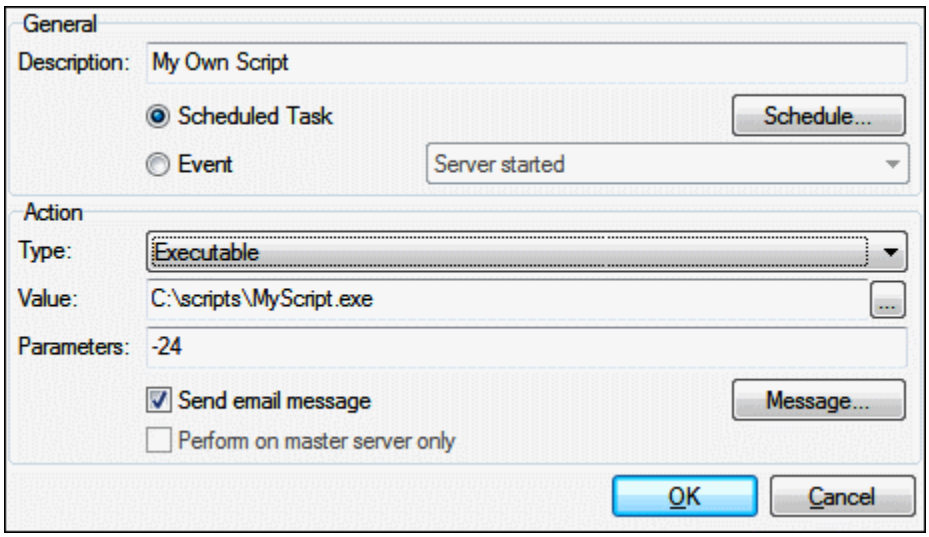
Alert if maximal Web Threadpool waiting time exceeds (s):	Enter a waiting time after which an alert is sent. Web service has set some thread pooling (use the **webserver.dat** file). When this number of threads is met, other requests have to wait. Thread pool indicates how many **php.exe** processes can be used at the same time by WebClient. The default is 15. This option can tell you for how many seconds you are out of threads. For details check Web/Control logs in debug mode.

Tasks & Events

Tasks & Events is a feature that lets you execute any application or process at a given time using the schedule settings.



Button	Description
Add	Click the button to add a new task/event. The **Task/Event** dialog opens.
Edit	Select a task (event respectively) and click the button to edit this task. The **Task/Event** dialog opens. See lower.
Copy	Select a task (event respectively) and click the button to copy this task. The **Task/Event** dialog opens. See lower. Useful if you want to create a similar task/event.
Delete	Select a task (event respectively) and click the button to remove this task.
Run Now	Select a task (event respectively) and click the button to run this task immediately.



Field	Description
Description	Simple description of the task or event item which is then shown in the **Tasks & Event**s list.
Scheduled Task	Choose this option to make this item a scheduled task. Use the ***Schedule*** button to define a schedule for this item.
Schedule	Pressing this button allows you define a schedule for this item. (Use the ***Add*** button + **Schedule Task** dialog.)

Event	Choose this option to run this item when the selected trigger event happens. There are three trigger events you can chose from: **Server started** Run this item when the ***Control service*** starts. **Server stopped** Run this item when the ***Control service*** stops. **Settings changed** Run this item when settings are changed.
Type	Specify the interface to be used to run this item: **Executable** is used for a DOS executable. **StdCall** and **Cdecl** are library interface specifications when you are calling a DLL file. In the case one of these types is specified, the *MerakFilterProc2* (*MerakFilterProc* respectively) procedure is called with empty parameters. **URL** should be specified for a remote executable script.
Value	Specify the full path or URL to the executable.
Parameters	Specify any parameters that should be passed to the executable.
Send email message	Check this option to send an email when this item is triggered. Use the ***Message*** button to specify the email details.
Perform on master server only	If load balancing is set (**System – Storage – Load Balancing**), tick this box, if you want to have the task/event executed only on the master server.
Message	Click this button to open the **Message** dialog which allows you to configure the details of the email to be sent.

*TIP: It can be advantageous to call **php.exe** (executable) to run scheduled tasks that execute **html/php** files instead of using the **URL** function.*

*The benefits of using **php.exe** instead of **URL**: When you run script via URL it will occupy a PHP slot and moreover there is a time limit for maximal script execution duration. Running it using **php.exe**, you can specify another timeout, memory limits, etc.*

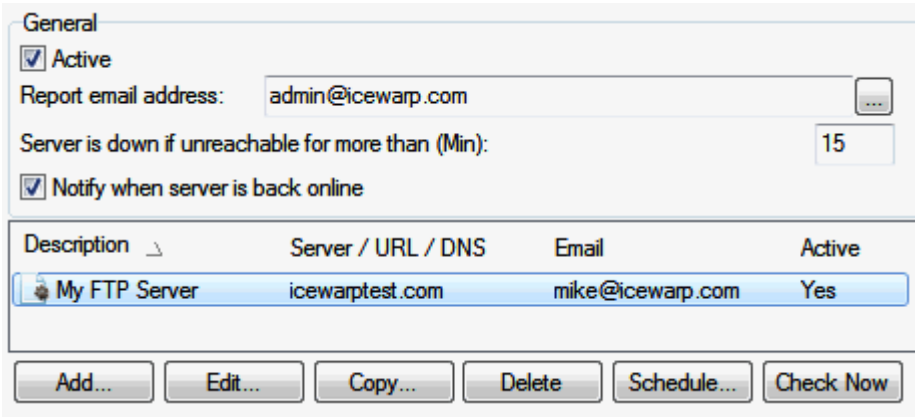
Remote Watchdog

Remote Watchdog allows IceWarp Server to check remote servers automatically and raise an alert if the server cannot be contacted for a specified length of time.

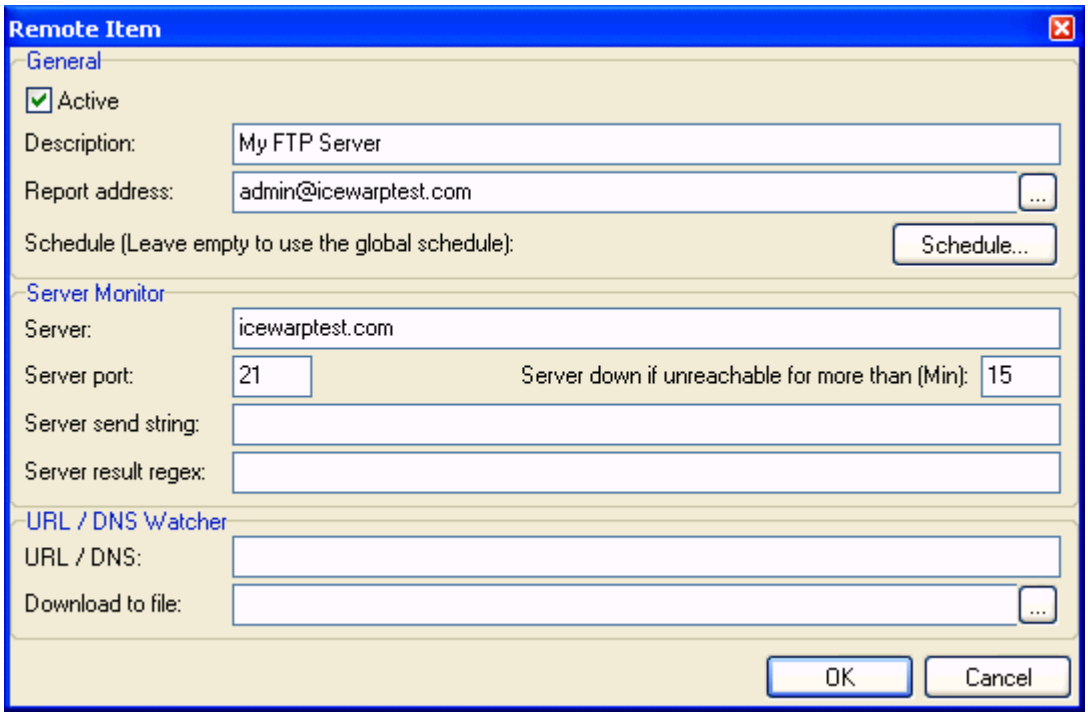
You can also monitor a URL and its content. In addition, you can automatically download the content of the URL if it has changed.

The **General** section defines default options – if you leave any of these options empty in an item definition, these default settings are used.

A list view of monitored servers is available.



Field	Description
Active	Enables the Remote Watchdog.
Report email address	The default email address for reports. Use the "..." button to open the **Select Accounts** dialog.
Server is down when unreachable for more than (Min):	Enter a non-zero value here to effectively allow a monitored server to be down for this length of time. In the above screen shot, a server will not be considered down until it cannot be contacted for more than 15 minutes.
Notify when server is back online	Check this option IceWarp Server to send a report when an unreachable Server becomes reachable again.
Add	Click the button to add an item. The **Remote Item** dialog opens. See lower.
Edit	Select an item and click the button to edit this item. The **Remote Item** dialog opens.
Copy	Select an item and click the button to copy this item. The **Remote Item** dialog opens. Useful when crating a similar item.
Delete	Select an item and click the button to remove this item.
Schedule	Click the button to open a simple schedule dialog where you can specify how often the servers should be checked. (The **Schedule** dialog – ***Add*** button – **Schedule Task** dialog.)
Check Now	Click the button to check all (defined) servers immediately.



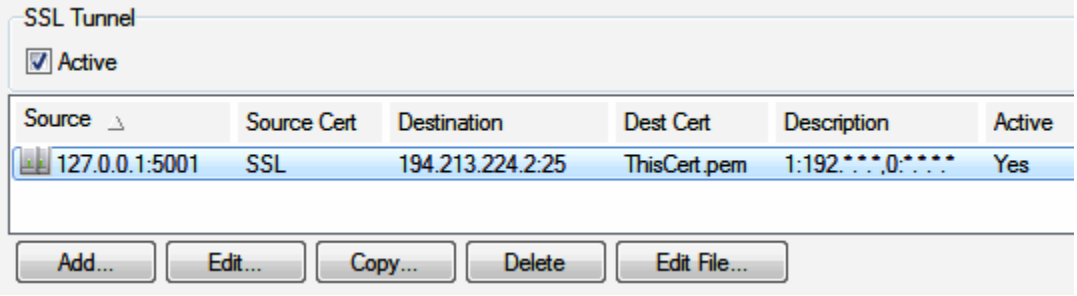
Field	Description
Active	Check this box to activate Remote Watchdog. This allows you to define watchdogs for different servers and only activate them when you need to.
Description	A short description of the item that is shown in the list.
Report address	Specify the email address for reports on this item to be sent to. Use the "..." button to open the **Select Item** dialog. This overrides the address specified in the **General** area.
Schedule	Use this button to set a schedule for checking this server. This overrides the schedule set in the **General** area.
Server	Specify the server hostname or URL to be checked.
Server port	Specify the port to contact the server.
Server down if unreachable for more than (Min)	Set to a non-zero value IceWarp Server not to consider the server unreachable until it is unreachable for this length of time.
Server send string	String that will be sent to the server on defined port after the connection is established. Example: 'GET /download/icewarp.zip HTTP/1.1'#13#10'Host: www.icewarpdemo.com'#13#10#13#10 Each line should be separated in the simple quotes and the decimal values of the CRLF should be specified using the format #13#10. If you leave this field blank, no string will be sent to the server.
Server result regex	Regular expression that describes the required remote server response. If the server responds differently, it will be considered as being down. If you leave this field blank, no returned-string checking is performed.
URL/DNS	If URL is specified, IceWarp Server will monitor the URL. IceWarp Server will record the last date, time, and size of the content. If anything has changed, it will send a notification and optionally download the content (if enabled). This feature supports the ***"datetime"*** and ***%%filename%%*** variables. If HTTP redirect is

	applied, you can find out the final file name using ***%%filename%%*** variable in the ***Download File*** variable. The ***"datetime"*** format is ***"yyyymmddhhnnss"***. E.g.: You may want to download the ***../download/icewarp-beta.html*** file when redirect script is used. The ***%%filename%%*** variable will contain the real name of the downloaded file. It is also possible to use **DNS Watcher**: Use the ***URL*** feature with the following syntax: ***dns://<server>:<type>*** E.g.: ***dns://yahoo.com:a*** or ***dns://yahoo:mx*** Supported query types are: ***a, aaaa, mx, txt, ptr, cname, srv, naptr*** E.g.: For ***dns://ebay.com:mx*** this server is checked for a change of the ***DNS MX record***; in the case of any change, the email address filled in to the ***Report address*** field is notified by an email message.
Download to file	If checking a URL, you have the option to automatically download the content of a local file if the contents change. Specify a full file name (path) that you wish the content to be saved to. In this path, you can also use: ▪ Time formatting – e. g. ***C:\Temp\"yyyymmdd"\x.zip*** ▪ The ***%%filename%%*** variable – ***C:\Temp\%%filename%%*** In this case, a final downloaded file name is used. E. g.: ***http://www.icewarp.com/download/beta/icewarp-latest.html?type=nb*** is downloaded. When ***C:\Temp\%%filename%%*** is filled in***,*** the appropriate nightly build version file name is used. Leave the field blank and no download will be performed. *NOTE: Do not delete **downloaded** file otherwise no further download will be performed. Also, do not delete the **\config_remotewatchdog** folder, otherwise you delete the cache.*

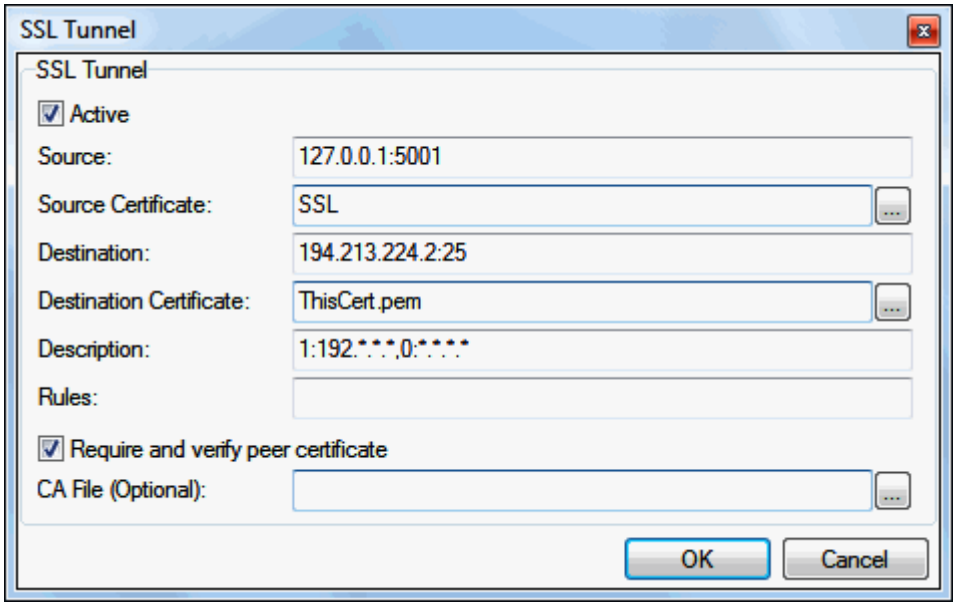
SSL Tunnel

An TCP/IP tunnel is a gateway listening on a specific port that forwards all communications to a specific destination.

IceWarp Server allows you to create multiple TCP/IP tunnels on your system, which can optionally be SSL encrypted.



Field	Description
Active	Tick the box to activate the service.
Source	Shows the listening IP address and port.
Source Cert	Shows whether the connection to the tunnel should be SSL encrypted and whether a certificate should be used.
Destination	Shows the destination of the tunnel.
Dest Cert	Shows whether the connection to the destination should be SSL encrypted and whether a certificate should be used.
Description	A free-form field where you can describe this tunnel.
Active	Shows whether this tunnel is currently usable.
Add	Click the button to define a new tunnel. The **SSL Tunnel** dialog opens.
Edit	Select a tunnel and click the button to edit this tunnel. The **SSL Tunnel** dialog opens.
Copy	Select a tunnel and click the button to copy this tunnel. The **SSL Tunnel** dialog opens. Useful when creating a similar tunnel.
Delete	Select a tunnel and click the button to remove this tunnel.
Edit File	Opens a plain text editor showing the tunnel definitions file content. Syntax and examples are given in the file.



Field	Description
Active	Tick the box to have this tunnel active.
Source	Where IceWarp Server will listen. Syntax: [IP]:port **IP** – optional, the listening IP address **:port** – mandatory, the listening port Examples: :5001;SSL Listens on all interfaces on port 5001 as an SSL server 127.0.0.1:5001 Listens on IP 127.0.0.1 port 5001
Source Certificate	Use this field to specify whether the connection to the tunnel should be SSL encrypted and whether a certificate should be used. ▪ **Leave Blank** to define this connection as an un-encrypted TCP/IP tunnel. ▪ Enter **SSL** to have this connection encrypted without checking a certificate. ▪ Enter a **path to a certificate** to have this connection encrypted and the specified certificate used for verification. A full path or relative to the certificate file can be used and you can use IceWarp Server's main certificate file by typing "cert.pem".
Destination	Where IceWarp Server will send received data. Syntax: [IP]:port **IP** – optional, the IP address **:port** – mandatory, the port Examples: gate.icewarpdemo.com:80 Sends data to gate.icewarpdemo.com port 80

	194.213.224.2:25 sends data to 194.213.224.2 port 25
Destination Certificate	Use this field to specify whether the connection to the tunnel destination should be SSL encrypted and whether a certificate should be used. ▪ **Leave Blank** to define this connection as an un-encrypted TCP/IP tunnel. ▪ Enter **SSL** to have this connection encrypted without checking a certificate. ▪ Enter a **path to a certificate** to have this connection encrypted and the specified certificate used for verification. A full path or relative one to the certificate file can be used and you can use IceWarp Server's main certificate file by typing "cert.pem".
Description	Enter a free-form text description so you can easily identify this tunnel.
Rules	Here you can specify rules as to which IP addresses are allowed to establish incoming connections. Syntax: [**Rights**]:[**IP Range**];[**Rights**]:[**IP Range**] **Rights** – 1 to allow, 0 to deny **IP Range** – IP address or mask Examples: 1:192.*.*.*;0:*.*.*.* Allows connections only from 192.*.*.* 0:192.068.6.* Deny connections from 192.068.6.* *NOTE: Using of these rules is not recommended. We recommend to use certificates to control access.*
Require and verify Peer Certificate	Check this box to force all connections for this tunnel to have a peer certificate. Any connection that does not supply a certificate will be dropped. Any connection that connects with SSL but has no certificate will be dropped. If a certificate is supplied, it will be checked against the CA file specified in the next field. If no CA file is specified, the file defined in **Certificates – CA** will be used for verification.
CA file (optional)	You can enter a path to a specific certificate file here if you need to. This can be useful if you want to use a highly secure certificate for certain protocols or tunnels.

Server Migration

The biggest challenge for today's system administrators when moving to a new email server is working out a painless way to move all the users and data from the old server to the new one.

The classical approach to this problem is to utilize a custom program to extract the data directly from the old server's database and then import it into the new server's database. The problem here is finding a safe, reliable program designed to work with both the server technologies.

Not with the IceWarp Server Integrated Migration Tool included in IceWarp Server administration console.

The IceWarp Server Migration Tool uses a smart proxy approach by sitting between the users of the old server and your new IceWarp Server installation. When the users login to IceWarp Server for the first time, via POP3 or IMAP, IceWarp Server will use the user/password combination given to access the old server and retrieve the user's email messages.

Email accounts are migrated automatically, so you even do not need to know who your users are.

Before actually going through the migration process, you must first prepare the system for the migration:

- Lets say your old mail server handles mail for a domain called "navi.com".
- Users access the mail server via a host name called "mail.navi.com".
- They use that address in their POP3/IMAP and SMTP settings of their mail client.
- Now, you modify your DNS records so that the migrator machine becomes the new "mail.navi.com" and create a new A DNS record called "oldmail.navi.com" that points at the original mail server (POP3/IMAP).
- You have to make sure that MX records for domain "navi.com" point at host name "mail.navi.com".
- You can use the DNS Query tool to check DNS records are setup correctly.

Migration Message

When the migration is in progress, migrated users cannot access their accounts. For users using email clients (e.g. MS Outlook, IceWarp Desktop Client, etc.), you can use the *Migration account* feature (**Server Migration – General**). (Refer there for details.) It is the only possibility, because these clients are not able to show IceWarp Server messages.

However for WebClient, the situation is different. When a user is trying to login, the following message is shown:

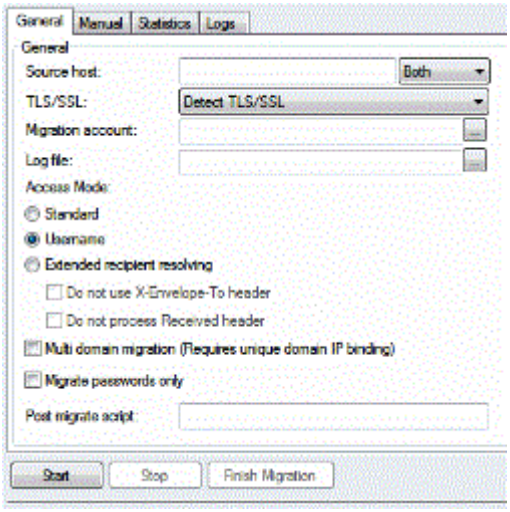
Migration in progress, try it again later.

It is possible to customize the message:

Edit the **data.xml** file (**<install_dir>\html\webmail\client\languages\<language_code>**, where the language code is e. g. ***pt***, ***en***, ***cs***, etc.) – *<migration_in_progress>* tag.

For example, you may want to inform users that they can send/receive emails using their email clients, even if migration has not finished yet.

General



Field	Description
Source host	Defines the source for migration and the type(s) of account(s). Enter a server domain name or IP address. (Server domain name can be used with a port.) **POP3** – only POP3 **IMAP** – only IMAP **Both** – POP3 & IMAP accounts *NOTE: Options including IMAP are recommended, as it keeps read/unread flags, correct message dates and migrates all folders (if remote system is set to IMAP too).*
TLS/SSL	Select from the following options: **Detect TLS/SSL** First attempt to establish connection is done by usual (non-encrypted) communication. After connection is established, encrypted communication is used. **Direct TLS/SSL** Whole communication is encrypted. **Disable TLS/SSL** Whole communication is non-encrypted.
Migration account	When the migration is in progress, migrated users cannot access their accounts. You may want to create a migration account and insert a notification email into ***Inbox***. Users will be redirected there and notified about temporary inaccessibility of their emails. Specify this migration account here. *NOTE: Only works if you use the proxy mode.*
Log file	Specify a full path and file name where the migration log will be saved. E. g.: ***c:\migration.log*** The "**...**" button can be used to select the file. The **Open** dialog is shown.
Access Mode	Select one of: **Standard** This mode will create one alias per account, based on the ***From:*** header of received messages.

	Username This mode does not parse messages at all and the alias of a new account is the same as the login name. This is the recommended option. **Extended recipient resolving** This mode will parse received messages for all possible aliases for a new account and will create those aliases with the account. This option has two further sub-modes: **Do not use X-Envelope-To header** Check this option if you are sure that all old messages have strictly correct MIME headers. If they do not, this option will cause migration failure. **Do not process Received header** Tick the box if you do not want the server to look for a user's email address within the ***Received*** header.
Multi domain migration (Requires unique domain IP binding)	Use this option with care. It enables the multi domain migration where you can migrate more domains at once. This feature however requires certain rules. Every domain to be migrated requires a virtual IP binding. (See the **Domains and Accounts** guide **– Management – Domains – <domain> – Options** tab **– Options** section.) All domains must have a unique IP set. Now all your email login attempts must come directly to the correct IP. The migration will then exactly know the domain name the new account belongs to and will create it in that particular domain ***Example***: Two domains to be migrated. navi1.com – IP binding – 192.168.0.1 navi2.com – IP binding – 192.168.0.2 The actual ***Backup Domain*** settings can be set to the same mail server. The incoming mail server still has to be the only one. Now for your navi1.com users you give them an incoming mail server host name that points to 192.168.0.1. It can be mail.navi1.com. navi2.com will get also a host name mail.navi2.com that points to 192.168.0.2. By this, you have set all. Now, when somebody connects to server to either of those IPs, IceWarp Server already knows what domain the account belongs to thus it will migrate all users to proper domains. The advantage of this feature is that it does not require previous IP bindings on the old mail server. *NOTE: You can also migrate multiple domains if you use full emails as your login policy on the both – the old server and IceWarp Server (**Domains & Accounts/Policies/Login Policy** tab – **Users login with their email address** option). When full emails are used, this option (**Multi domain migration**) is not necessary, it only is if you want to use unique IP binding for each domain on IceWarp Server. This method is easier.* *If you do not have full email login enabled on your remote server (only on your IceWarp Server) and use username access mode in the migration tool, IceWarp Server will migrate accounts to its primary domain (the first one show in the console). If you need to migrate users from other systems that do not have full email login policy, you can temporarily set a domain as primary one during migration. (Within the Management node, right-click the domain name and select the **Set as primary domain** item.)*
Migrate passwords only	Tick the box if you want to migrate passwords only. Use this feature in the case, you have migrated accounts data manually (passwords are not migrated in such a case). IceWarp Server will not migrate the data again but will just verify passwords against the old server. *Passwords will **NOT** be reset (changed).*

Post migrate script	You can enter a fully qualified path to an executable script that can perform some additional operations with migrated accounts. This script is launched after migration of every single account with an email address and password as parameters. E. g. you can create a script for migration of groupware items, as server migration applies to email items only.
Start	Click the button to start the migration process.
Stop	Click the button to stop the migration process.
Finish Migration	This button instructs IceWarp Server to complete all remaining account migrations. After migration of a single account is done, some email messages can arrive to the old email box. Clicking this button tells the server to look for such items.

Example of a successful migration log:

[0001BA4C] Mon, 22 Apr 2013 18:30:44 -0300 Migrating messages for 'alba@icewarpdemo.com'...

[0001BA4C] Mon, 22 Apr 2013 18:30:44 -0300 Migrating messages for 'marco@icewarpdemo.com'...

[0007032C] Mon, 22 Apr 2013 18:30:45 -0300 Messages for 'alba@icewarpdemo.com' migrated, 2 messages

[000713A4] Mon, 22 Apr 2013 18:31:32 -0300 Messages for 'marco@icewarpdemo.com' migrated, 114 messages

[00070C40] Mon, 22 Apr 2013 18:31:48 -0300 Bulk migration finished

[0001BA4C] Mon, 22 Apr 2013 18:32:49 -0300 Finishing 'alba@icewarpdemo.com' migration...

[0001BA4C] Mon, 22 Apr 2013 18:32:49 -0300 Finishing 'marco@icewarpdemo.com' migration...

[00070D1C] Mon, 22 Apr 2013 18:32:50 -0300 'alba@icewarpdemo.com' migration finished, 0 additional messages

[000710E8] Mon, 22 Apr 2013 18:33:20 -0300 'marco@icewarpdemo.com' migration finished, 1 additional messages

Manual

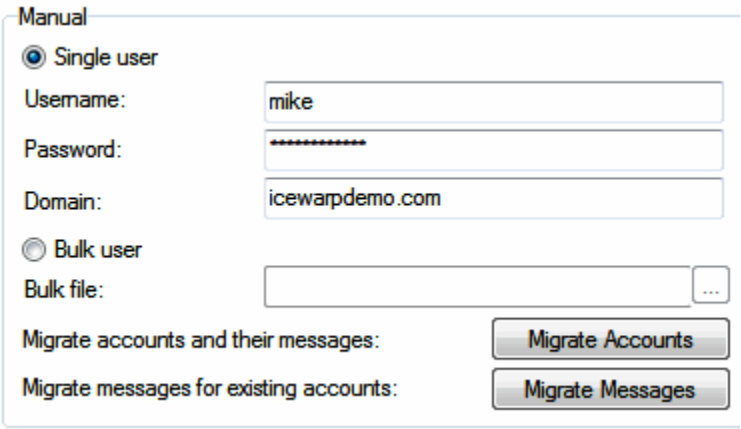
The **Manual** tab allows you to migrate accounts manually. To migrate an account, you must know the account name and password. You can migrate a single account or a batch of accounts (via a text file containing accounts information).

If you do have a list of accounts and passwords available then the ***Bulk user*** method is the recommended way to migrate accounts, as you can control when and what accounts are migrated.

NOTE: To start the manual migration process:

- *Click the **Start** button in the lower part of the tab.*
- *Select the appropriate user type.*
- *Either fill in the user's data or add a bulk file.*
- *Click the **Migrate Accounts** button.*
- *When the migration is finished, click the **Stop** button.*

The domain you want to migrate users to has to exist prior to this migration. You can use the **tool.exe** command: ***tool create domain [domain_name]***.



Field	Description
Single user	Select this option if you wish to migrate a single user manually.
Username	Specify the username of the single account you wish to migrate.
Password	Specify the password for the single account you wish to migrate.
Domain	Name of the domain that the migrated account belongs to.
Bulk user	Select this option to use a file containing a list of users to be migrated. See below.

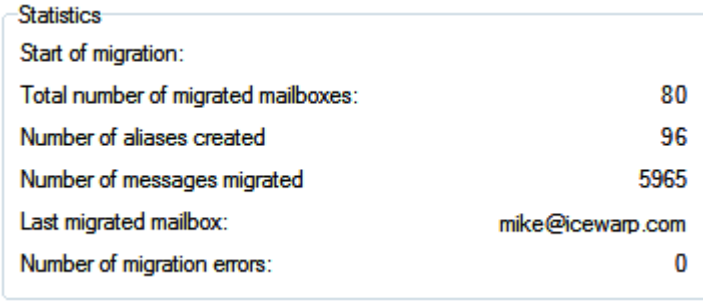
Bulk file	You should create a file listing the accounts you wish to migrate, in the following format:
	`user1:pass1`
	`user2:pass2:alias@domain`
	with one account/password/address per line.
	Use the '...' button to open a standard browser to locate and select your file.
	*NOTE: In the case the **Users login with their email addresses** option (**Login Policy**) is*

	enabled, use whole email addresses for `user1` and `user2`. *BE AWARE: When using a remote console, the bulk file must be on the local computer where this console is running.*
Migrate Accounts and their Messages	Click this button to have IceWarp Server migrate the specified accounts, creating each account during the process. IceWarp Server will log in to the original server using the account(s) specified and retrieve the data.
Migrate messages for existing accounts	Click this button to migrate messages for existing accounts only. You can use this option if you have already created the accounts specified (maybe you need to do a phased migration). *NOTE: If you have a complete list of your accounts, you can use **tool.exe** to create the accounts in a batch mode, ready for message migration.* IceWarp Server will log in and retrieve any messages.

NOTE: If migrating accounts with RSS folders, it is also necessary to copy the **<install_dir>/mail/_rss** folder into the respective directory to keep the RSS settings.

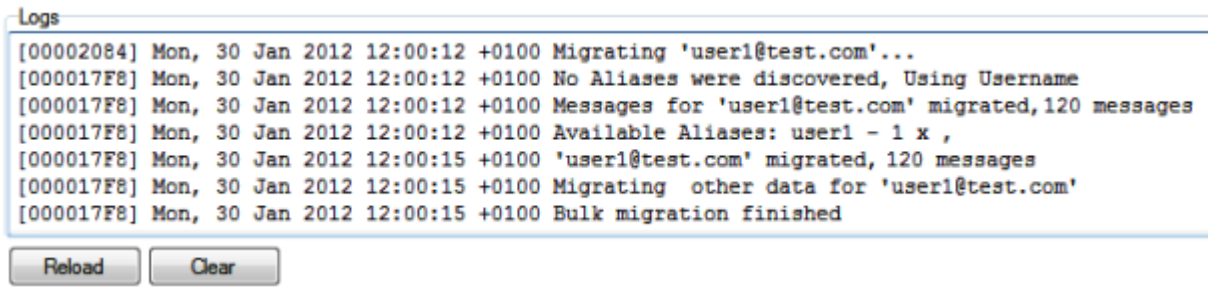
Statistics

The **Statistics** tab shows the progress of the migration process. It is highly recommended to check this tab – in particular the ***Number of migration errors*.**



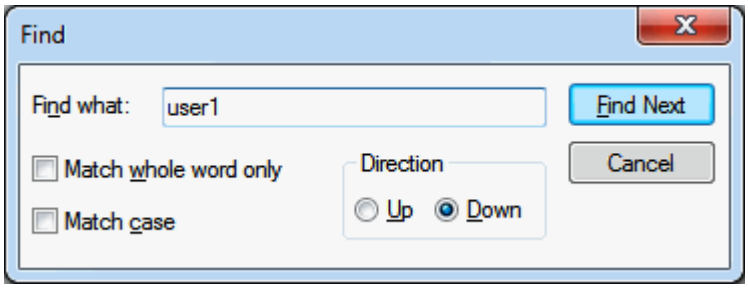
Logs

The **Logs** tab allows you to view log information for the server migration in progress.



Button	Description
Reload	Click the button to reload/refresh logs.
Clear	Click the button to clear the log window.

*TIP: Hit the **CTRL + F** keys to open the Find dilag.*



Contacts Migration Script

When migrating a whole mail server to IceWarp Server, you can use existing migration tools specific to each mail server. There are available tools for migration from Kerio, MDaemon, MS Exchange, Axigen GroupWare 602 and LANSuite.

Where there is not a specific migration tool available, it is possible to use a very handy script for migration of contacts in the *vCard* format.

Example of this script can be found in **<install_dir>/api/php/importcontacts.php**. This script imports contacts for one single user, but it uses all files from a specified folder (so there can be either always one *vCard* in one file, or all *vCard*s in one file, or even a mixture). Feel free to modify the script to your needs.

IceWarp to IceWarp

As this topic is very complex, it is described in an individual document – **IceWarp Migrator Guide.pdf**.

For detailed description of the **Migration Wizard**, follow this link:

http://dl.icewarp.com/documentation/server/tools/IceWarp_Migrator_Guide.pdf#page=10

Database Migration

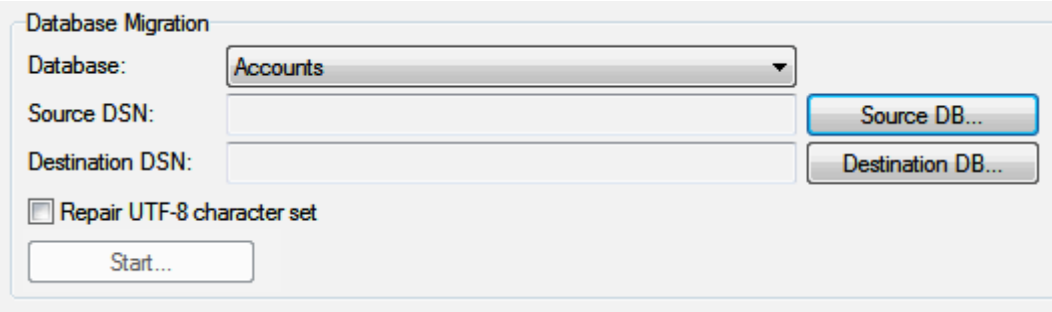
The **Database Migration** node allows you to easily migrate the IceWarp Server's database from one database server to another one.

You may want to do this to change the physical server or to change the database technology in use (for example, upgrading from MS Access to MySQL or MS SQL Server).

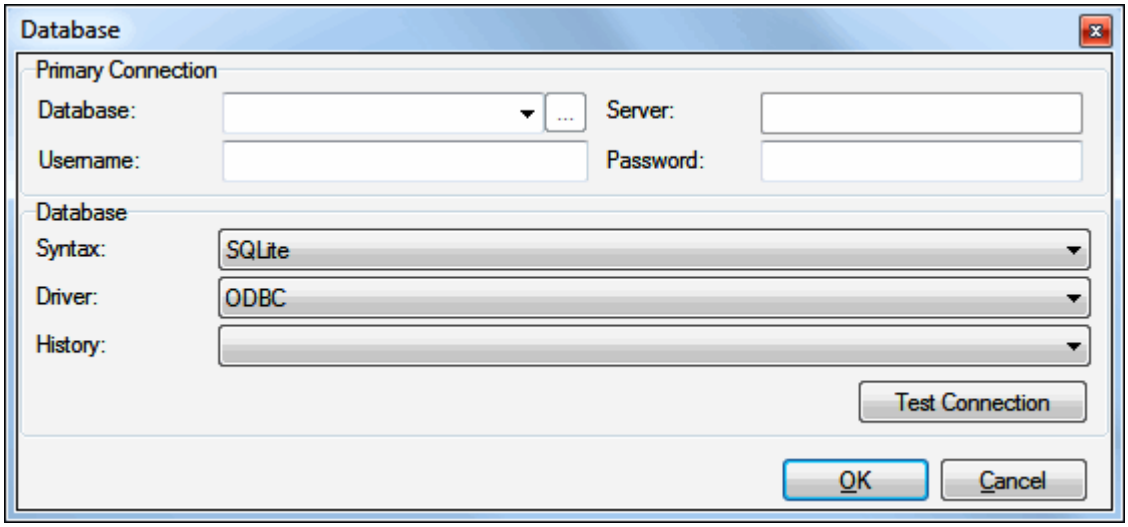
WARNING: In the case you are migrating a WebClient database, it is possible to migrate only from SQLite one to other engine.

Before you switch WebClient to a new database, stop control and delete all php sessions. Otherwise you will loose flags and other email statuses.

The MS SQL engine is not supported for Spam Reports and Active-Sync databases.



Field	Description
Database	Select which IceWarp Server database you want to migrate from the dropdown list. Available databases are: • Accounts • Anti-Spam • GroupWare • Directory Cache • WebClient • ActiveSync • Spam reports
Source DSN	Click the ***Source DB*** button to define the source DSN for migration. The **Database** dialog opens.
Destination DSN	Click the ***Destination DB*** button to define the target DSN for the migration. The **Database** dialog opens.
Repair UTF-8 character set	Tick the box if you want the server to check if the source database character set is valid UTF-8. If the data contains characters that are not valid UTF-8 ones, these characters are removed.
Start	Click the button to start migration process.



Field	Description
Database	Select the DSN of the database.
Server	Enter the hostname of the database server.
Username	Enter a username to access the database.
Password	Enter the password for the user.
Syntax	Select the database technology in use (this is required because of minor differences in SQL syntax).
Driver	Select a driver for the database technology you are using.
History	Select a DB connection string from the list of previously used ones.
Test Connection	Click the button to test whether IceWarp Server can access the database with the details entered.

Spam Reports Database Migration

This migration (for MySQL) uses a migration script that can be executed also via the ***command line***. See the example (default install path, default reports db, migrate to MySQL on localhost/root/root).

"c:\Program Files (x86)\IceWarp\php\php.exe" -c "c:\Program Files (x86)\IceWarp\php\php.ini" "<install_dir>\html\reports\migrate.php

" parameters="srcdbconnection=sqlite:c%3A%5CProgram%20Files%20(x86)%5CIceWarp%5Cspam%5Creports%

5Creports.db&srcdbuser=%s&srcdbpass=%s&srcdbsyntax=%s&destdbconnection=mysql%3Ahost%3Dlocalhost%3Bdbname%

3Dreports&destdbuser=root&destdbpass=root&destdbsyntax=%s"

Database Migration Logs

All database migration logs are saved within the **icewarp\logs\migration** directory.

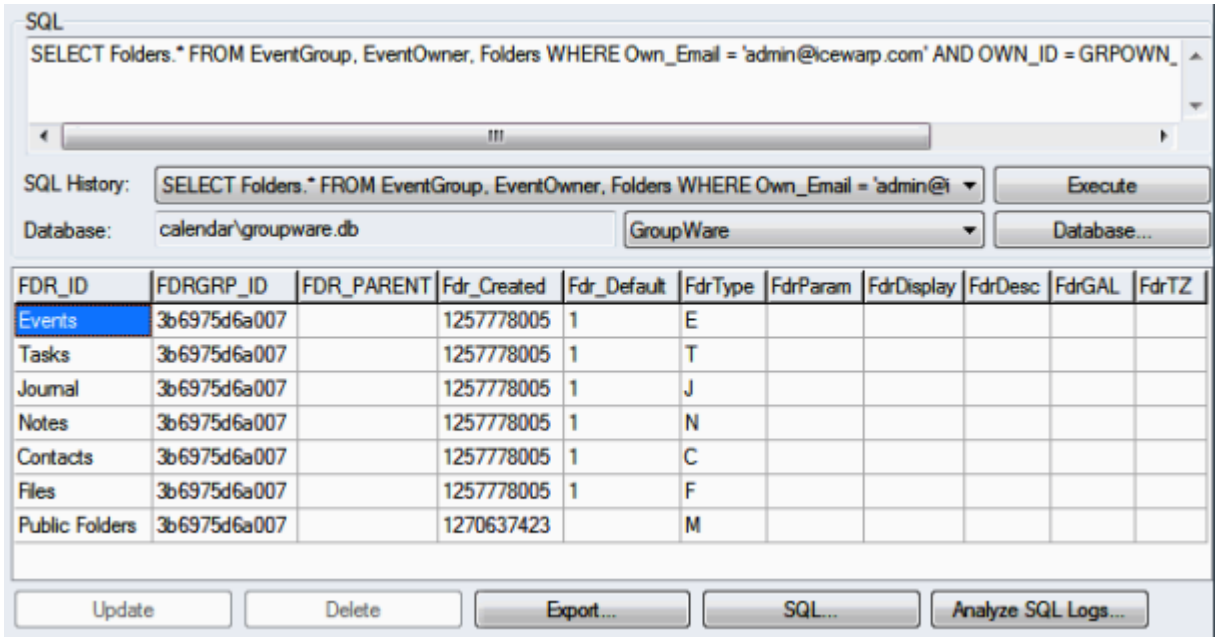
The log filename is *mig_YYYYMMDD_HHNNSS_<database_type>.log*.

<database_type> can be: 'Storage', 'Logs', 'GroupWare', 'ChallengeResponse', 'DirectoryCache', 'Webclient', 'EAS', 'Reports'.

SQL Manager

This tool can ease your work with IceWarp Server databases. It allows you to perform SQL queries and manage databases.

*NOTE: You can use SQL Manager over Remote Connection Protocol (RCP) for remote servers. See the **Remote Server Administration** chapter.*

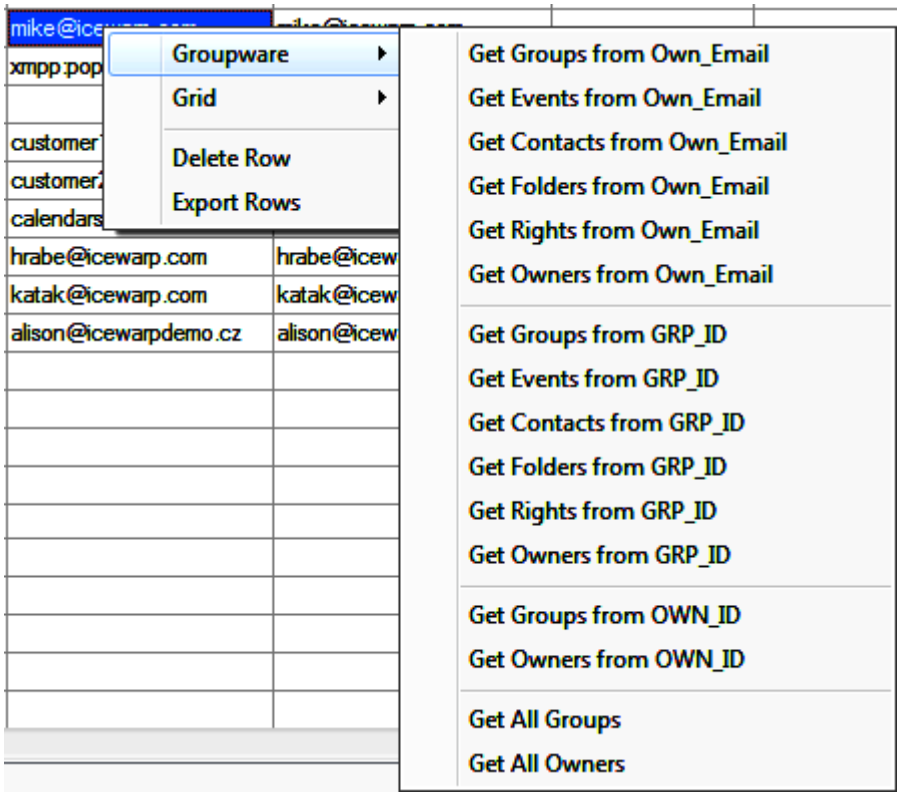


Field	Description
SQL	Write an SQL query here. You can select one of pre-defined ones using the ***SQL*** button.
SQL History	You can select a query from the list of previous queries.
Database (field)	Path and name of the selected database.
Database (list)	Select a database type (GroupWare here).
Database (button)	Click the button to view or edit properties of the selected database. The standard **Database** dialog is shown.
Result table	Results of your query (found records) are shown here.
Update	Perform a change in a result row and click the button to update a database table. *NOTE: This button is enabled only after an SQL query that uses the* ***SELECT ** command and is directed only to one database table.* *E. g.: **SELECT * FROM Event WHERE EVNOWN_ID = '3b6975d6f006'***
Delete	Click the button to delete the current row from a database. *NOTE: This button is enabled only after an SQL query that uses the* ***SELECT ** command and is directed only to one database table.* *E. g.: **SELECT * FROM Event WHERE EVNOWN_ID = '3b6975d6f006'***
Export	Click the button to export query results to a file. The standard **Save As** dialog is shown.

SQL	Click the button to select from the pre-defined SQL queries. Queries are same as in the figure bellow. *NOTE: NOTE: The **Email Address** dialog is shown – enter email address/GRP_ID/OWN_ID.*
Analyse SQL Logs	Click the button to open a log file. Here you can analyze how much time single queries took. Logs are shown according to time in descending order.

Pop-up Menu

Right-click any result row to reveal this menu. It can be used for selection of pre-defined SQL statements. It also allows you to delete a selected row or export it to a ***.csv*** file.



Storage

The **Storage** node allows you to modify where, and in some cases how, various information is stored.

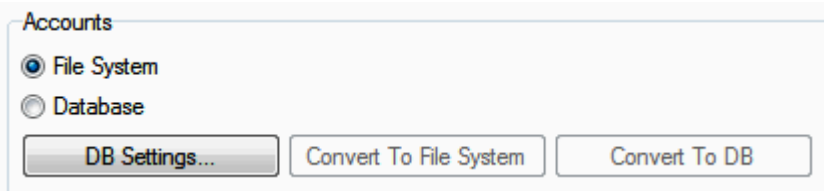
Here you can set how your email accounts will be stored – either in the integrated file system (in this case they are included in a backup ***.zip*** file) or in a database, where all settings (username, pwd, forwarders, etc.) are stored – this is recommended for over 500 accounts.

Settings for load balanced scenario are also managed here.

Accounts

The **Accounts** tab allows you to choose the type of storage system that IceWarp Server will use to store accounts and domains information.

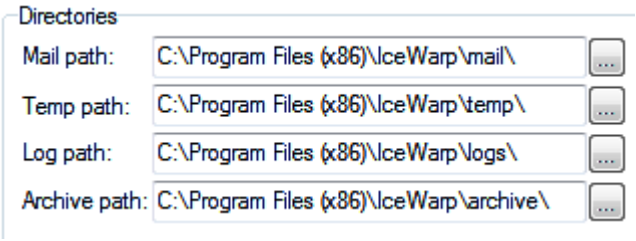
The size of your installation (number of accounts and domains) determines which system you should use.



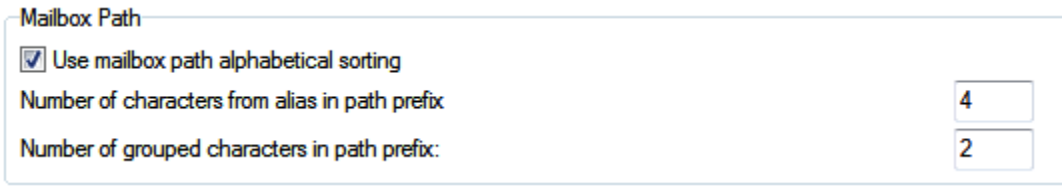
Field	Description
File System	Uses the operating system standard binary files, stored on your hard drive(s). Suitable for installations up to 500 accounts (depending on load).
Database	Uses a database storage system for account and domain information system. As databases use indexing features, this can significantly increase the speed of account and domain information retrieval. Recommended for installations with over 500 accounts (less if load is high). *NOTE: For very large installations we recommend to use a heavy-duty database application rather than something like SQLite, and run the database system on a dedicated server.*
DB Settings	Use this button to open the **Database** dialog where you can specify connection information. See **Database Settings** for more details.
Convert to File System	If you are using an ODBC system and wish to revert to a file system, use this button first to convert the information, then select the file system you wish to use.
Convert to DB	If you are using a file system and are changing to a database system you will need to use this button, after you have set up your **Database Settings**, to migrate your information into the database.

Directories

The **Directories** tab specifies where IceWarp Server stores various files. The directories need not be created in advance, IceWarp Server will create all directories as required.



Field	Description
Mail path	Specify a fully qualified path to the directory where user mailboxes and the outgoing message queue (***subdirectory _outgoing*** inside specified path) should be stored.
Temp path	A fully qualified path where incoming messages are stored before they are processed. The **temp** folder contains subfolders for all services. These subfolders are: ▪ Control ▪ GW ▪ IM ▪ POP3 ▪ SMTP ▪ webmail The services that are not listed above use following subfolders: **Service** / **Uses Subfolder** FTP, (LDAP) — Control SIP — IM IMAP — POP3 The **Other** subfolder is used for storage of items that do not belong to the mentioned services (e.g. **API.dll**). *NOTE: The appropriate subfolder of this directory (**temp**) is automatically emptied when the corresponding service of IceWarp Server starts so you should not store any data here that you wish to keep.* *This does not apply for the **webmail** subfolder.*
Log path	A fully qualified path where all the IceWarp Server log files will be stored.
Archive path	A fully qualified path where all the IceWarp Server archived items will be stored.



Field	Description
Use mailbox path alphabetical sorting	Use this option for larger installation to create additional "alphabetized" subdirectories to the ***Mailbox path***. This is a performance fix for Windows systems where file display can be slow for directories containing many thousands of subdirectories. Specify a number in the ***Number of characters from alias to path prefix*** box. For example, in the above screenshot: User **john** will have messages stored in ***<path>\jo\hn\john*** User **george** will have messages stored in ***<path>\ge\or\george***
Number of characters from alias to path prefix	The number of characters taken from the users alias if you have selected ***Use mailbox path alphabetical sorting***.
Number of grouped characters in path prefix	The number of characters taken to create subdirectories. E. g.: For values from the screenshot above, you will get for **alexander**: ***<path>\al\ex\alexander*** For values of 6 and 3, you will get: ***<path>\ale\xan\alexander*** For values of 6 and 2, you will get for **mike**: ***<path>\mi\ke\mike*** For values of 6 and 2, you will get for **mike1**: ***<path>\mi\ke\1\mike1***

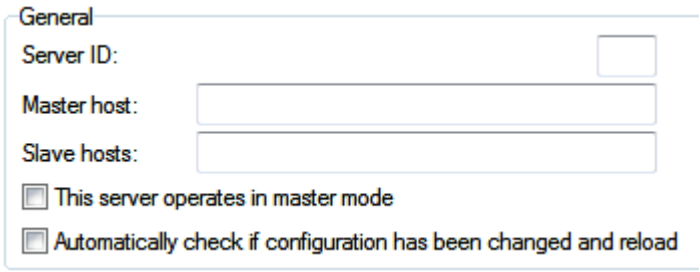
Load Balancing

The **Load Balancing** tab allows you to set up multiple IceWarp Server installations to serve as a load balanced system, with each server taking a share of the processing.

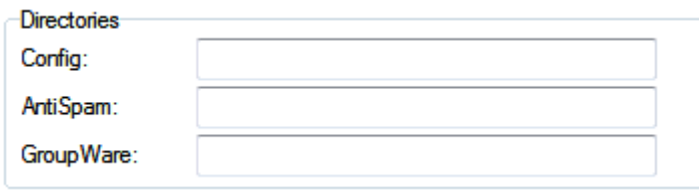
This is achieved by using common folders for Configuration, AntiSpam and GroupWare settings, and for the mail and logs folders. Each instance of IceWarp Server will use these common settings.

For a fully balanced system you should also:

- *Use common folders for mail and logs (**Storage – Directories**).*
- *Make sure that **Automatically check if configuration has changed and reload** is checked (**Storage – Local Settings**).*
- *Do not share the **Temp** folders, these should be separate and local for each IceWarp Server (**Storage – Directories**).*
- *Use different host names and IP addresses for each IceWarp Server (**Storage – Local settings**).*



Field	Description
Server ID	Specifies the prefix for all message files. Maximum two characters. Numbers are recommended.
Master host	Enter a server name or IP address of the server that works in master mode.
Slave host	Enter server names or IP addresses of all servers that work in slave mode. Use semicolon for separation.
This server operates in master mode	If you ***do not*** tick this box, you inform IceWarp Server that this server is a "slave" in a load balanced system. This server will ignore certain features, which will be handled by the master server. These features include Remote Server Watchdog, Backup, AD Sync, AntiSpam Reports, Mail Archive Backups, plus others. Using this option will reduce the workload of your slave servers.
Automatically check if configuration has been changed and reloaded	If enabled, IceWarp Server will automatically check the settings and configuration of Load Balancing and if something has changed IceWarp Server will automatically reload new configuration. In the case two administrators logged to console at once, it will ask administrator what to do regarding the changes other admin made (to accept/reload or not).



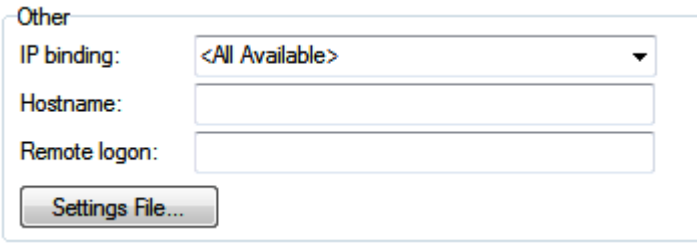
Field	Description

Config	The fully qualified path to the **config** directory ....***\<InstallDirectory>\Config***
AntiSpam	The fully qualified path to the **spam** directory ....***\<InstallDirectory>\Spam***
GroupWare	The fully qualified path to the **calendar** directory ....***\<InstallDirectory>\Calendar***

NOTE: Unless you have direct access to the drive as a letter, these paths are to be UNC pathnames and each IceWarp Server should have full rights to each path.

For example when you use UNC path to access a remote storage, IceWarp services have to run under a user, that has write/read/delete rights to that destination, not under Local System. To check/set it, navigate to the services.msc file – Log On As item and ensure it is set to other user than Local System (IceWarp [service] Properties (Local Computer) dialog – Log On tab).

NOTE: These directories have to be shared between the load balanced servers.



Field	Description
IP binding	The IPs you want the services to listen on. Example: *127.0.0.1;192.168.0.1* NOTE: This setting always overrides settings for individual services within the **<service>** dialog – **Properties** tab – *All Services* field (**System – Services – General**). NOTE: When set, this applies also for single node mode.
Hostname	The hostname you want the server to use in communication with other servers.
Remote logon	You may want to use a shared storage (e. g. for emails) with protected access. Specify the remote path, username and password to logon there with. Example: ***\\server\mail;user;password|\\server\logs;user;password***
Settings File	Click the button to open the **path.cfg** file where all the settings described above are stored. Examples are given in the file.

Load Balancing Setup Considerations

Shared Settings and Data Visualization

- Most of the settings/visualizations are shared, if you centralize the **config** folder in storage. Example – all the settings in the console are shared (with the exception of ***System – Storage – LB*** (**paths.dat**)), but even all the data in the DBs too. E. g. antispam whitelist/blacklist entries, accounts settings (forwarders, limits, etc), volume (Status – Volume), etc.
- Each server does have separate statistics in ***Status – Statistics***, also graphs and sessions, queues, etc. of course.
- Intrusion prevention shows the result of all load balanced servers in each one. So, for example *server A* had 50 items in intrusion, *server B* 40 other records. It shows 90 records on both front end load balanced servers.

NOTE: IM always routes from the master to slave, so master has to be online for IM to work (in the case it is down, you need to make the slave server the new master manually).

Certificates

The **Certificates** node allows you to:

- create your own SSL certificates
- assign any SSL certificate to particular server IP addresses
- secure the connections for any host names and services

Generally, **Server Certificates** are to be used to verify IceWarp Server users within this server. They are used by particular services when running SSL connections (HTTPS etc.). These certificates are not used for example for IceWarp WebClient.

CA (Certificate Authority) certificates verify IceWarp Server (and its users) when contacted from third parties servers. It is necessary the contacting party has this CA installed in Windows. Otherwise, the "Could not verify certificate ..." message is (usually) shown.

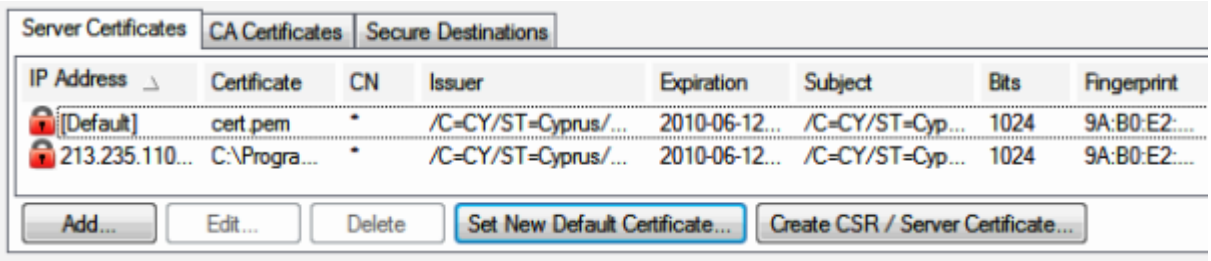
Let´s Encryptservice lets administrators create and maintain server security certificates for free. Certificates are automatically reissued before expiration and need to be reissued manually only if domains are added or removed. Using of this type of certificate need to meet condition that administrator runs the WebService on 80 and 443 ports. IceWarp does not support Wildcard certificates.

Since v11.4.1 the logic process of certificate management in Admin console and WebAdmin has been totally changed. To make certification process easier users can choose certificate from the new wizard. IceWarp joined free certificate initiative and integrated Let´s encrypt service – server security certificates for free.

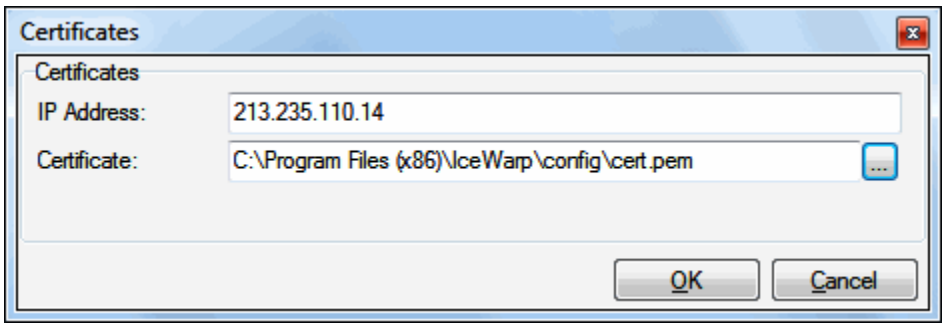
For detailed information about certification process, refer to **IceWarp SSL Certificate Process** – it is available from: ***http://www.icewarp.com/downloads/documentation/server/***.

Server Certificates

The **Server Certificates** tab displays a list of the certificates used within IceWarp Server. The ***[Default]*** certificate, displayed as the first in list, is an integrated SSL certificate that is shipped with IceWarp Server. You cannot delete or edit this default certificate.

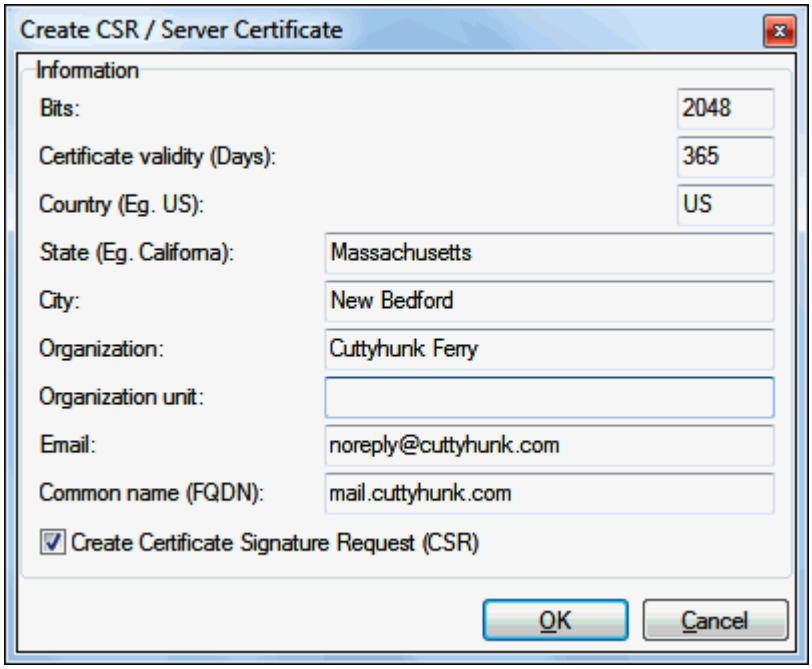


Button	Description
Add	Click the button to assign an SSL certificate to its specific IP address. The **Certificates** dialog opens. *NOTE: Consider obtaining IceWarp certificates. Double click the record in certificates and choose the certificate received form IceWarp, in this case.* *NOTE: For general information, refer to the **Certificates** chapter.*
Edit	Select a certificate and click the button to edit this certificate. The **Certificates** dialog opens.
Delete	Select a certificate and click the button to remove this certificate.
Set New Default Certificate	Click the button to browse for a new server certificate that will be set as the default one.
Create CSR / Server Certificate	Click the button to create an SSL certificate for your server. The certificate **.pem** file will be saved to the IceWarp Server's **config/** directory. The **Create CSR/Server Certificate** dialog opens.



Field	Description
IP Address	Enter the IP address that is associated with your SSL certificate. If this field is empty, IceWarp Server tries to use SNI (Server Name Indication https://en.wikipedia.org/wiki/Server_Name_Indication) to detect which certificate to use for the session. It is based on the common name of the certificate and the information sent by a browser. If more certificates could be used (because of wildcards), then the best matching certificate is used. E.g.

	you have two certificates 1. *common name= *.icewarp.com* 2. *common name= server.icewarp.com* When browser goes to *https://server.icewarp.com*, both certificates could be used, but the second one is more specific and will be used. This SNI functionality is not limited to web browsers only, but other clients (e.g. IMAP/SMTP) usually do not use it (and can not use it). *NOTE: Now, in v11.3, certificates have not to be bind special IP as in previous versions.*
Certificate	Enter the fully qualified path to the **.pem** certificate file or use the '...' button to browse to its location.



The certificate is designed to re-assure anyone connecting to your server that you are who you say you are, so the more accurate and complete the information in the certificate, the more comfortable your users will feel.

Field	**Description**
Bits	Required. Specify the number of bits to be used for the encryption of this certificate.
Certificate validity (Days):	Required. Specify the number of days this certificate is valid for.
Country	Optional. The two letter country code associated with your organization. *EN* – England *US* – USA *CZ* – Czech Republic *CY* – Cyprus etc.
State	Optional. Use this for the country or state associated with your organization.
City	Optional. The city associated with your organization.
Organization	Optional. Your company name.
Organization unit	Optional. Your company's office reference (useful if you have multiple servers).
Email	Optional. The email address associated with your organization.

Common name	Enter the fully qualified domain name here of the domain that you require a certificate for.
Create Certificate Signature Request (CSR)	Check this option to create a file that can be used to request a certificate from an issuing authority.

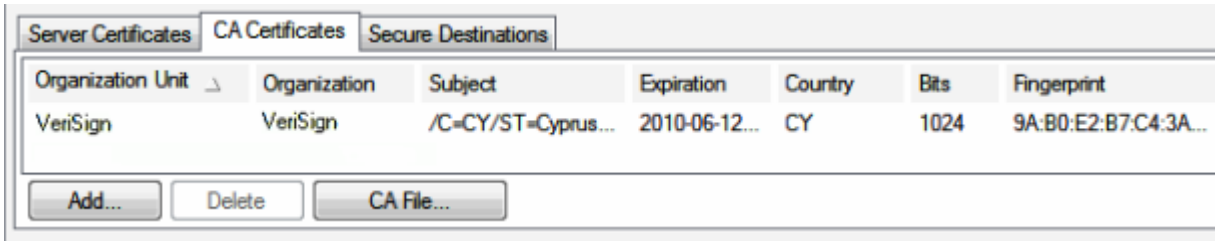
NOTE: If you are using the ***Certificate Signature Request*** option to create a file for an issuing authority, you should ONLY send your public key file to the CA.

Click the ***OK*** button to create the certificate, confirmation is displayed.

NOTE: Server certificates can not have passphrase. Otherwise the certificate will not be used and secured ports will not be open.

CA Certificates

The **CA Certificates** tab allows you to administer certificates provided by a Certificate Authority (CA), such as Thawte or VeriSign.



Field	Description
Add	Click the button to add a certificate. The **Certificates** dialog opens. Fill in a path or click the "..." button to browse for a **.pem** file.
Delete	Select a certificate and click the button to remove this certificate.
CA File	Select a certificate and click the button to open this file.

NOTE: If you have a 3rd party certificate, this process will not work if it requires an intermediate certificate. Then you have to merge the private key with certificate you bought and intermediate certificate of the issuer manually. Refer to support resources of your certificate issuer for details.

*NOTE: For general information, refer to the **Certificates** chapter.*

Secure Destinations

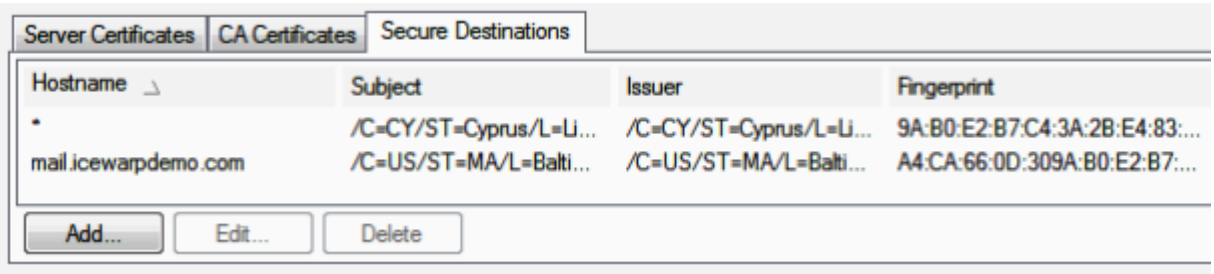
The **Secure Destinations** tab allows you to define your host names which will only accept SSL connections, whether they be POP3, IMAP or SMTP.

This can prevent DNS spoofing.

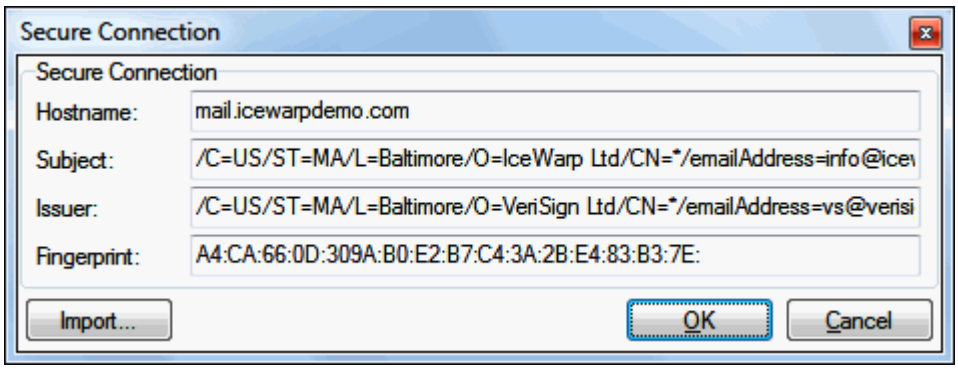
The SSL architecture is very strict:

- If SSL is demanded and the processed message cannot be sent over SSL/TLS (i.e. remote server only offers plain connection), the message is returned..
- If SSL is demanded and the processed message can be sent over SSL/TLS, the certificate of remote server is validated in following way:
  - in case Secure Destination entry for the host does not require Subject / Issuer / Fingerprint, and certificate of remote server is not issued by a trusted CA (defined on System - Certificates - CA Certificates tab), the message is returned.
  - in case Secure Destination entry for the host requires Subject / Issuer / Fingerprint, and they do not match with Subject / Issuer / Fingerprint of remote server certificate, the message is returned.
- Only in case SSL/TLS connection is available and certificate of remote server can be validated (in one of the ways mentioned above), the message is processed.

Host names automatically adapt – if an incoming message is SSL certified, IceWarp Server switches to SSL mode..



Button	Description
Add	Click the button to add a new secure destination. The **Secure Connection** dialog opens.
Edit	Select a secure destination and click the button to edit this destination. The **Secure Connection** dialog opens.
Delete	Select a destination and click the button to remove this destination.



Field	Description
Hostname	Identifies the host that will be secured with certificate.

	You can use patterns here (e. g. *.icewarpdemo.com, or only * will work perfectly).
Subject	The entity that is identified by a certificate.
Issuer	The organization or authority that issued the certificate.
Fingerprint	A unique number (or "fingerprint") associated with a certificate. The fingerprint is not actually part of the certificate itself but is produced by applying a mathematical function to the contents of the certificate. If the contents of the certificate change, even by a single character, the function produces a different number. Certificate fingerprints can therefore be used to verify that certificates have not been altered. *NOTE: If Subject / Issuer / Fingerprint are not specified, remote certificate is considered as valid in case it is issued by a trusted Certificate Authority (defined on **System - Certificates - CA Certificates** tab).*
Import	Click the button to select a **.pem** file to add to the system. The **Open** dialog is shown. Upon selection of the .**pem** file the certificate is read and the fields populated with the correct information.

Getting a Digital Certificate

You can offer your users secure, trusted access to all of IceWarp Server services, and give them confidence that your server is really your server, by getting yourself a digital certificate from one of the big certificate authorities (CA).

The next few sections will guide you through the process of generating and installing your certificate.

We will use the trial certificate offer from VeriSign to show you the process, but you may wish to purchase your certificate from another CA.

For a list of the larger CAs refer to http://www.dmoz.org/Computers/Security/Public_Key_Infrastructure/PKIX/Tools_and_Services/Third_Party_Certificate_Authorities/.

The free Trial SSL Certificate from VeriSign has 14 days validity period. It's enough to test it on IceWarp Server and familiarize yourself with broad issue of SSL certificates.

There are 5 steps required to get your certificate in place:

1. Generating a CSR (Certificate Signing Request) and private key
2. Sending the CSR to a CA and retrieving your signed certificate
3. Merging the signed certificate with your private key
4. Installing the merged certificate into IceWarp Server
5. Installing the trial certificate into browser (not necessary when you buy a full certificate)

Generating the CSR and Private Key

The easiest way to generate your CSR and private key is to use the process built within IceWarp Server, which can be found at **Certificates – Server**. CSR generators can also be found online if you prefer to use them – two of these are located at:

http://www.myssl.cn/english/openssl/createcsr.asp

https://my.webblake.com/CSRGenerator3266.php

If you use IceWarp Server's generator, you should fill in the file names to generate, for example, **private.pem** and **public.pem**.

If you use another method, you will probably have to create these files manually using a plain-text editor of some description.

Whichever method you chose, you should end up with two files, your private key and your public key.

NOTE: Your private key is exactly that – private! You should NEVER pass out this key to anyone you do not explicitly trust.

Here are examples of what your files should look like, just for information:

public.pem

-----BEGIN NEW CERTIFICATE REQUEST-----

MIIDYjCCAssCAQAwgYYxHjAcBgNVBAMTFW5ldC5jaGlja2Vua2lsbGVyLmNvbTEQMA4GA1UECxMHc3VwcG9ydDEbMBkGA1UEChMSY2hpY2tlbmtpbGxlciBMdGQuMQ8wDQYDVQQHEwZQcmFndWUxFzAVBgNVBAgTDkN6ZWNoIFJlcHVibGljMQswCQYDVQQGEwJDWjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuGry41oVXuJRoaoY/bJdapmX2sj0jpD3aJsr9PG9Mlg+msNvNIFIXAB3QPqGSpB45P5fOwj75VzmoMKu1iusxYwQNWl1Jxm0N58Rx0hugJ8ymRTVO44fxMmNyeClPAIiBeLk3aZjwPQ/AbF030PpQnskAWlAPjwqFGeuBom5MKcCAwEAAaCCAZkwGgYKKwYBBAGCNw0CAzEMFgo1LjEuMjYwMC4yMHsGCisGAQQBgjcCAQ4xbTBrMA4GA1UdDwEB/wQEAwIE8DBEBgkqhkiG9w0BCQ8ENzA1MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZIhvcNAwcwEwYDVR0lBAwwCgYIKwYBBQUHAwEwgf0GCisGAQQBgjcNAgIxge4wgesCAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBuAG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBkAGUAcgOBiQCTSR8dKSviOwRXJreaBSjJpgw7jnoQI1mvgJv5aE+B7F+M47mrA4bWgM5NorJyuRzmkb4g8FCer7hyi1PyFYlDClz6oZvzFQROnEKiSGuE3nTv28Ver/l2weSa05PCRKpKfP3Ku5WjFh4NDyMjcobcdODHAW2jyhmeb4T5jiiyFQAAAAAAAAAAMA0GCSqGSIb3DQEBBQUAA4GBAGDp1WEw9q9tyXM0hfVjPEUPjYoC/XYzLzLiQBtiQluPf0fa61n0ZFj69elcAAgp4ZSRf6uMItWdcn2amq1Cv9KzEvSXyi+7ZkfnX4yhj1aHghRL7HS54lwop5IgzrhewKSXrbffq7Lrg8lx2ehQNiXocaewDtNY9929BrfpVyM6

-----END NEW CERTIFICATE REQUEST-----

and private.pem

-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKGgQCtq6Le1Yyk2h1psJ9+zw0vVpRaVoKrZf6sCo8V3dMJkCxrUZebsM5/6Fw64xe1ZX8KNbbO4Khiqzcb6HrJpzeEmrJuf7bWCe1qmutyWkR+JsX+juHGcP2y/r6zyfpZqFaQhozCjgyQdyXIt9g5whq573AizO0Ny5dUlRoDHouTiwIDAQABAoGBAJqWjQONUwPqowPRFCfsZfAdQTCokOfAglDhlTwBmDiK/P8KQcl0OFvimTZRrmjpT4vnBDJiB4DMpuFQrvuQvPj0ym1VYq6+rcUMa5p2z6UrOrloXhmJKpoSCf5OwgYdiQ0KKy6Hot59MzPl6Je6kJCczEUQ7mkHUIW0oVoEN1cBAkEA1qSus+k1IqrJZhUj9nbTpwaEu1WsEMtp6emUO87dV1ubDCpbyLrkM6gqabZRnUpqZdfdtPZ0RHttU+jf3ZZybQJBAM8h9iR7va9ioYNDY3GFXQFdA/5qQGZbaqiLd6Krvr2a3B3gZbSIIc0sPFEYyhQQ/7c/XvHSZVVtA3VCfIqbItcCQFBgGJ98O46Av6v/TJk1Q+pusXNpEGa1lTKnaf+/ZfkZb4Tts7MF8QA6/67YO9WXkSIT5IyoIT+nrHfYY0QZ2z0CQHL/5gsHcJ8JYabhKTsD0klJfUgpcavioWsGU9vLAtF+QyuLRKxg0HN7Vdmoq7lMXs08r9gO+hfduIfH7CGAVG0CQCkVdxpggzSHBecd61bbAfwEi4mbBQq+BrkXWde5+bqLD5LNf3Fy7dO3YOqSF6riFiu2tJioS6njsM5x90FWS0A=

-----END RSA PRIVATE KEY-----

Sending CSR to CA – Certification Authority – VeriSign in this Tutorial

Now, we will use our public key to request a trial certificate from VeriSign.

Note that the trial certificate has a very simple checking procedure and your certificate will be delivered quite quickly. When you come to buy your full certificate the checking procedure is much more rigorous as you have to actually prove that you own the domain, are a member of the company and so on. Full certificates, therefore, take longer to be delivered and you should bear this in mind when you are ready to order it.

Go to the **VeriSign** website (http://www.verisign.com/) and select the ***Trial Certificate*** ordering page.

Follow the ordering wizard, giving all the relevant information as requested.

When you are requested to enter the Certificate Signing Request, cut and paste the entire contents of you **public.pem** file into the field.

We also recommend that when you are asked to give your server platform you select "Server not listed".

At the end of the process an email will be sent to you containing your signed certificate.

Merge Signed Certificate with your Private Key

The email message from VeriSign contains your signed certificate and will look something like this:

```
-----BEGIN CERTIFICATE-----

MIIFZTCCBE2gAwIBAgIQewZpAA6myxiqkXRZ7a0BCzANBgkqhkiG9w0BAQUFADCByzELMAkGA1UEBhMCVVMxFzA
VBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQLEydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdX
JhbmNlcy4xQjBABgNVBAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc
3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IENBMB4XDTA3MDkx
NjAwMDAwMFoXDTA3MDkzMDIzNTk1OVowgbkxCzAJBgNVBAYTAkNaMQ8wDQYDVQQIEwZQcmFndWUxDzANBgNVBAc
UBlByYWd1ZTEaMBgGA1UEChQRY2hpY2tlbmtpbGVyIEx0ZC4xEDAOBgNVBAsUB0lUIERlcHQxOjA4BgNVBAsUMV
Rlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxHjAcBgNVBAMUFW5ldC5ja
Glja2Vua2lsbGVyLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAraui3tWMpNodabCffs8NL1aUWlaC
q2X+rAqPFd3TCZAsa1GXm7DOf+hcOuMXtWV/CjW2zuCoYqs3G+h6yac3hJqybn+21gntaprrclpEfibF/o7hxnD
9sv6+s8n6WahWkIaMwo4MkHclyLfYOcIaue9wIsztDcuXVJUaAx6Lk4sCAwEAAaOCAdcwggHTMAkGA1UdEwQCMA
AwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TVlJTZWN1cmUtY3JsLnZlcmlzaWduLmNvb
S9TVlJUcmlhbDIwMDUuY3JsMEoGA1UdIARDMEEwPwYKYIZIAYb4RQEHFTAxMC8GCCsGAQUFBwIBFiNodHRwczov
L3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0
jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBqMCQGCCsGAQUFBzABhhhodHRwOi8vb2
NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUHMAKGNmh0dHA6Ly9TVlJTZWN1cmUtYWlhLnZlcmlzaWduLmNvbS9TV
lJUcmlhbDIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYwITAfMAcGBSsO
AwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWY
wDQYJKoZIhvcNAQEFBQADggEBAAFhQEGdvMpjodlzve44n+9rgmxEdg3tzr4E08TOTCK1tg40PWPL5fnJ/6NK7A
SXR0PprjF5bMWJh/QjZS7IRuBEL6iq7xxY7cpIEc94lP0GDYNuN0PI0KOoSUqp1RZg+fRB9WUwMCSsiYRaq+R5P
rEyMMVB5Zhkik8W/Tk2OpGhEKSI8cQXO9V19WF+yiTPijrY1bZQzVXV7mVbcgxduF4+SYNtHOFcoL/51ALS1+68
TewvvuYzUNsMXK0g+Y45+OKpYWddEVB47+Di9j7TjlFMPyS98c8tVYnznbSzzrl4UQYc20kAS/G9VlLCpJa4tlM
fv3Lba2LLeknPtnZ1W2s=

-----END CERTIFICATE-----
```

Copy the signed certificate from VeriSign's email message and paste it at the end of your private key file – **private.pem**.

Save it as a new file – for example **MyCert.pem**.

Again – use a plain text editor only! The result should look like this sample:

MyCert.pem sample:

```
-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKBgQCtq6Le1Yyk2h1psJ9+zw0vVpRaVoKrZf6sCo8V3dMJkCxrUZebsM5/6Fw64xe1ZX8KNbbO4Kh
iqzcb6HrJpzeEmrJuf7bWCe1qmutyWkR+JsX+juHGcP2y/r6zyfpZqFaQhozCjgyQdyXIt9g5whq573AizO0Ny5
dUlRoDHouTiwIDAQABAoGBAJqWjQONUwPqowPRFCfsZfAdQTCokOfAglDhlTwBmDiK/P8KQcl0OFvimTZRrmjpT
4vnBDJiB4DMpuFQrvuQvPj0ym1VYq6+rcUMa5p2z6UrOrloXhmJKpoSCf5OwgYdiQ0KKy6Hot59MzPl6Je6kJCc
zEUQ7mkHUIW0oVoEN1cBAkEA1qSus+k1IqrJZhUj9nbTpwaEu1WsEMtp6emUO87dV1ubDCpbyLrkM6gqabZRnUp
qZdfdtPZ0RHttU+jf3ZZybQJBAM8h9iR7va9ioYNDY3GFXQFdA/5qQGZbaqiLd6Krvr2a3B3gZbSIIc0sPFEYyh
QQ/7c/XvHSZVVtA3VCfIqbItcCQFBgGJ98O46Av6v/TJk1Q+pusXNpEGa1lTKnaf+/ZfkZb4Tts7MF8QA6/67YO
9WXkSIT5IyoIT+nrHfYY0QZ2z0CQHL/5gsHcJ8JYabhKTsD0klJfUgpcavioWsGU9vLAtF+QyuLRKxg0HN7Vdmo
q7lMXs08r9gO+hfduIfH7CGAVG0CQCkVdxpggzSHBecd61bbAfwEi4mbBQq+BrkXWde5+bqLD5LNf3Fy7dO3YOq
SF6riFiu2tJioS6njsM5x90FWS0A=

-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
```

MIIFZTCCBE2gAwIBAgIQewZpAA6myxiqkXRZ7a0BCzANBgkqhkiG9w0BAQUFADCByzELMAkGA1UEBhMCVVMxFzA
VBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQLEydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdX
JhbmNlcy4xQjBABgNVBAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc
3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNlcnZlciBUZXN0IENBMB4XDTA3MDkx
NjAwMDAwMFoXDTA3MDkzMDIzNTk1OVowgbkxCzAJBgNVBAYTAkNaMQ8wDQYDVQQIEwZQcmFndWUxDzANBgNVBAc
UBlByYWd1ZTEaMBgGA1UEChQRY2hpY2tlbmtpbGVyIEx0ZC4xEDAOBgNVBAsUB0lUIERlcHQxOjA4BgNVBAsUMV
Rlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUxHjAcBgNVBAMUFW5ldC5ja
Glja2Vua2lsbGVyLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAraui3tWMpNodabCffs8NL1aUWlaC
q2X+rAqPFd3TCZAsa1GXm7DOf+hcOuMXtWV/CjW2zuCoYqs3G+h6yac3hJqybn+21gntaprrclpEfibF/o7hxnD
9sv6+s8n6WahWkIaMwo4MkHclyLfYOcIaue9wIsztDcuXVJUaAx6Lk4sCAwEAAaOCAdcwggHTMAkGA1UdEwQCMA
AwCwYDVR0PBAQDAgWgMEMGA1UdHwQ8MDowOKA2oDSGMmh0dHA6Ly9TVlJTZWN1cmUtY3JsLnZlcmlzaWduLmNvb
S9TVlJUcmlhbDIwMDUuY3JsMEoGA1UdIARDMEEwPwYKYIZIAYb4RQEHFTAxMC8GCCsGAQUFBwIBFiNodHRwczov
L3d3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIwHwYDVR0
jBBgwFoAUZiKOgeAxWd0qf6tGxTYCBnAnh1oweAYIKwYBBQUHAQEEbDBqMCQGCCsGAQUFBzABhhhodHRwOi8vb2
NzcC52ZXJpc2lnbi5jb20wQgYIKwYBBQUHMAKGNmh0dHA6Ly9TVlJTZWN1cmUtYWlhLnZlcmlzaWduLmNvbS9TV
lJUcmlhbDIwMDUtYWlhLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFowWDBWFglpbWFnZS9naWYwITAfMAcGBSsO
AwIaBBRLa7kolgYMu9BSOJsprEsHiyEFGDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWY
wDQYJKoZIhvcNAQEFBQADggEBAAFhQEGdvMpjodlzve44n+9rgmxEdg3tzr4E08TOTCK1tg40PWPL5fnJ/6NK7A
SXR0PprjF5bMWJh/QjZS7IRuBEL6iq7xxY7cpIEc94lP0GDYNuN0PI0KOoSUqp1RZg+fRB9WUwMCSsiYRaq+R5P
rEyMMVB5Zhkik8W/Tk2OpGhEKSI8cQXO9V19WF+yiTPijrY1bZQzVXV7mVbcgxduF4+SYNtHOFcoL/51ALS1+68
TewvvuYzUNsMXK0g+Y45+OKpYWddEVB47+Di9j7TjlFMPyS98c8tVYnznbSzzrl4UQYc20kAS/G9VlLCpJa4tlM
fv3Lba2LLeknPtnZ1W2s=

-----END CERTIFICATE-----

Install Merged Certificate into IceWarp Server

To add your newly signed certificate to IceWarp Server, you need to configure the settings in **Certificates – Server**.

Use the ***Add*** button to add your certificate to the correct IP address.

And you are finished. Now, you have a certificate installed and can use it to secure and verify any of the services running under IceWarp Server.

NOTE: Because you are currently using a trial certificate, clients like IE and Firefox will probably report a problem with the certificate. Be aware that this is purely a function of the trial certificate and once you have bought the full certificate these problems will go away.

For testing purposes you can install VeriSign's Trial Root CA Certificate IE and Firefox (you need to do them separately as they do not share certificate information).

The email from VeriSign which contained your trial certificate contains a link to the Trial Root CA Certificate and the following section explains how to add the certificate to IE.

Installing VeriSign Trial Certificate into Browser

(Not necessary when you buy the "real" certificate.)

Follow the link to VeriSign's Trial Root CA Certificate and save the file to a file with a ***.cer*** extension, for example ***trial.cer***.

Then follow these steps:

1. Open IE.
2. Go to **Tools – Internet Options**.
3. Select the **Content** tab.
4. Click ***Certificates***.
5. Click ***Import***.
6. Follow the wizard and guide it to the ***.cer*** file you saved from VeriSign.
7. Select ***Automatically select the certificate store based on the type of the certificate*** when you get there.
8. Finish the wizard.

The Trial Root CA Certificate is now installed and you should no longer get any warnings about the validity of your certificate.

NOTE: You will need to install the Trial Root CA Certificate into every instance of IE that you, or your customers, want to use – if you want to avoid the warnings.

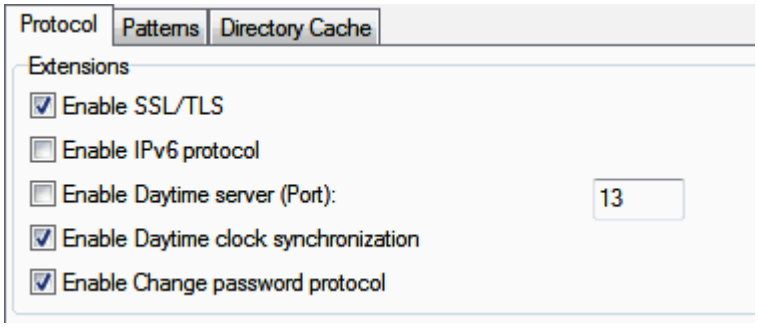
Advanced

The **Advanced** node allows you to enable and manage certain protocol related settings.

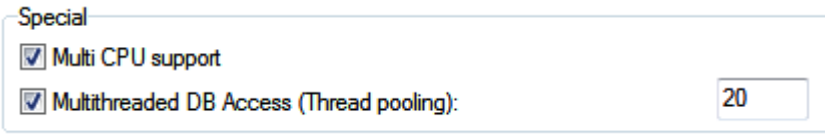
The **Patterns** sub-node is also present – here you can define named sets of items for use in various places within IceWarp Server.

The **Directory Cache** node allows you to define settings for your mail database.

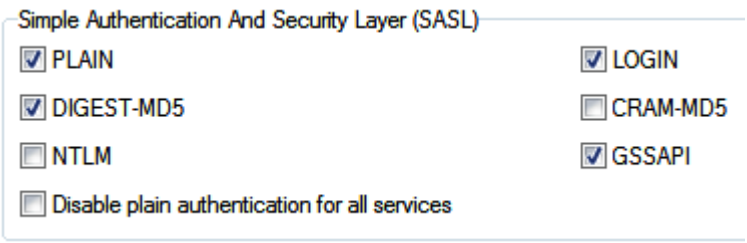
Protocol



Field	Description
Enable SSL/TLS	This option lets you enable or disable the SSL/TLS engine. It is enabled by default. It is used by all protocols SMTP, POP3, etc. depending on client and port defined there.
Enable IPv6 Protocol	This option enables IPv6 protocol support. IceWarp Server supports the IPv6 protocol completely, including AAAA DNS records and IPv6 service binding.
Enable Daytime server (Port)	IceWarp Server can act as a time server for your whole network, allowing you to keep the time synchronized on all your network servers and PCs. Specify which port IceWarp Server will listen on (the default port is 13). Mind the Firewall.
Enable Daytime clock synchronization	When checked, IceWarp Server will synchronize itself with an Internet-based atomic clock on a regular basis.
Enable Change password protocol	This option allows a user to change his/her password via the POP3 protocol. The user's mail client must support this feature. You will also need to manually bind POP3/IMAP to port 106 to use this feature. Mind the Firewall.

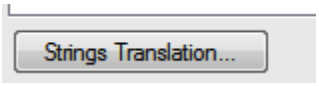


Field	Description
Multi CPU support	If your server is multi CPU, this option allows IceWarp Server to utilize these capabilities. This can significantly improve IceWarp Server's performance on medium to high load servers. In the case of multi-core processors, each core is considered as one processor.
Multithreaded ODBC (Thread pooling)	Check the box to use multiple threads for database activity, and enter the number of threads to use (for all services together).



This section lists all SASL mechanisms (including GSSAPI – SSO/Kerberos authentication). With these settings, you can control the published mechanisms for SMTP, POP3, IMAP, IM, ... protocols. Mail clients detect these mechanisms and automatically choose the best security for authentication.

Field	Description
PLAIN	Tick the box to enable plain text authentication (not encrypted).
LOGIN	Tick the box if you want to enable the Login authentication (base-64 encryption).
DIGEST-MD5	Tick the box if you want to enable the Digest-MD5 authentication. (For more information, refer to RFC 2831.)
CRAM-MD5	Tick the box if you want to enable the CRAM-MD5 authentication. (For more information, refer to RFC 2195.)
NTLM	Tick the box to enable NT LAN Manager (Microsoft Windows) authentication.
GSSAPI	Tick the box to enable Single Sign-On authentication.
Disable plain authentication for all services	Tick the box to prohibit plain authentication for all services. *NOTE: This check box overrides both PLAIN and LOGIN check boxes.* *NOTE: When ticked, WebClient cannot log into the SMTP service. As a work-around, check whether your localhost is in trusted **IP Addresses** (**Mail – Security – General**) – if not, add it – and untick the **Use SMTP authentication** box (**GroupWare – WebClient – General** – see info about user limits counting).*



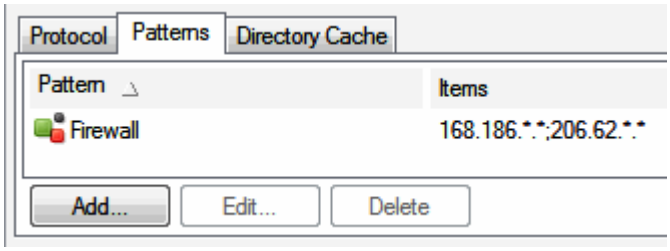
Field	Description
Strings Translation	Use the button to open a simple editor to modify the **<install_dir>\config\strings.dat** file. Here, you can translate/modify internal messages – e. g. "Unknown user." etc. *NOTE: If translating to a language with diacritical marks, save the file as UTF8 – non bom.* *NOTE: Restart the SMTP service after performing changes.*

Patterns

The **Patterns** node allows you to specify groups of items as a single name for use in many places within IceWarp Server. Patterns can help you to overcome string length limitations for particular places in IceWarp Server configuration (patterns can be used on those places). If you need to save longer string(s) than IceWarp Server is able to, use pattern(s).

Patterns can be used within:

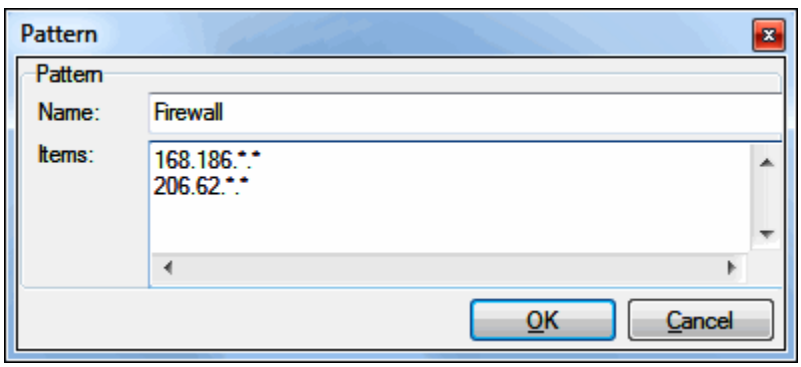
- Account aliases
- Access
- Black & White filters
- Trusted IPs
- Rules (+ Content Filters)
- Bypass dialogs
- Service IP binding
- Firewalls
- <user> – Mail – Forward to
- <user> – Mail – Copy incoming mail
- <user> – Mail – Copy outgoing mail



Button	Description
Add	Click the button to add a new pattern. The **Pattern** dialog opens.
Edit	Select a pattern and click the button to edit this pattern. The **Pattern** dialog opens.
Delete	Select a pattern and click the button to remove this pattern.

The above example shows an item called **Firewall** containing two IP address items – 192.168.*.* and 206.62.*.*

In places where patterns are allowed you can specify **[Firewall]** (note the square brackets) instead of the two items, so, for example, you could use this pattern in a service access definition.



Field	Description
Name	Specify a unique name for the pattern.
Items	Specify a list of items, one per line. You can include: ▪ IP addresses with masks ▪ emails and domains with masks ▪ account names with masks ▪ other patterns

Patterns Examples

For emails *a1@domain.com*, *a2@domain.com*, *a3@domain.com* is possible to use pattern value of ***a*** or ***@domain.com***.

For emails *b@domain.com*, *b@another_domain.com* is possible to use ***b@*** or just ***b***.

You can figure out many other possibilities.

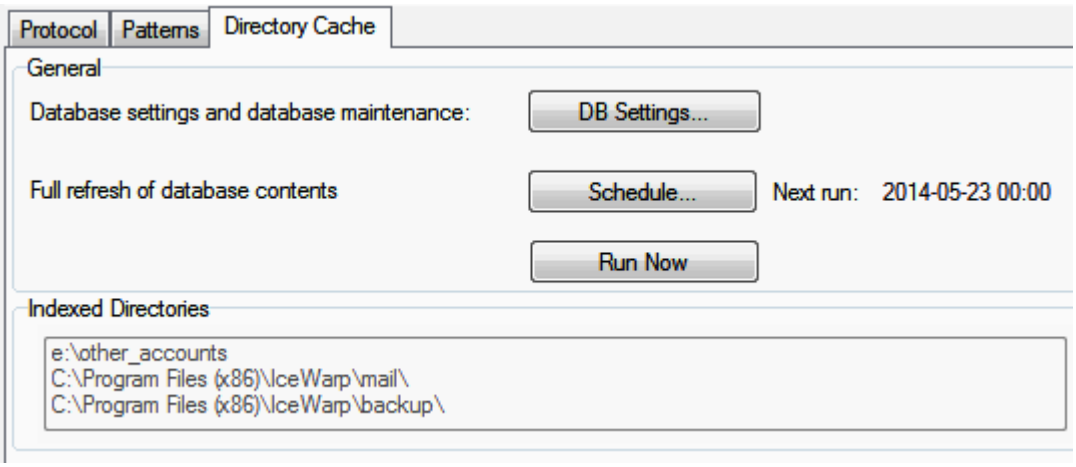
Directory Cache

About

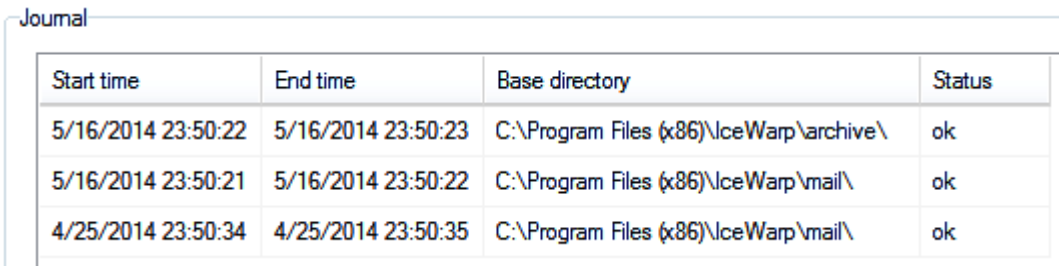
This tab allows you to define settings for your mail database. This database is used to keep information about email boxes – their sizes, numbers of messages, etc. Data are recounted after each change (except for e. g. copying emails manually within a file manager – in this case you can use the ***Run Now*** button).

As access to a drive where the database is kept can take some time, it is convenient to have this database in memory – cache.

To reveal separate logs for directory cache, proceed to **Status – Logs** and select the ***Directory Cache*** item from the ***Log*** list.



Field	Description
DB Settings	Click the button to open the standard **Database** dialog where you can define and maintain the database settings. For more information, refer to the **IceWarp Server GUI Reference – Database Settings** chapter.
Schedule	Click the button to define how often the database content is to be refreshed. The standard **Schedule** dialog opens. For more information, refer to the **IceWarp Server GUI Reference – Schedule** chapter. ***Next run*** – this label informs you when the next database contents refresh will be performed. If a schedule is not set, the label reads "unscheduled".
Run Now	You may want to recalculate database data immediately (e. g. after copying some messages manually using a file manager). Click the button.
Indexed Directories	Indexed directories are shown here. These are mail and archive directories (default or as set on the appropriate places – **System – Storage – Directories**, **Mail – Archive**). Not editable here. *NOTE: The **externaldirs.dat** file has to be used to list non-standard mailbox paths. (For more information, refer to the **Domains and Accounts – Management – Domains – Options** chapter – **Folder** section.) All mailbox paths included in this file are also automatically listed in this field.*



The ***Journal*** field contains the last 10 rows from the directory cache database.

Each row contains these values:

- Start time of DC update run
- End time of DC update run (empty if update is running)
- Running time – how long the update proceeded
- Base directory – DC update base directory
- Status – ***OK***" or ***Fail***.

The field can be refreshed by pressing F5.

Directory Cache Moved to Database

Disk based directory cache (**subdirs.dat**, **size.dat** in user's mailboxes) has been removed in 10.4. When using file system account storage, after upgrade an SQLite database is created to which the directory indices and sizes will be written. When using database account storage, the same database engine will be used to create the directory cache. While the DB is empty, the directories are indexed on demand, whenever requested by server (e.g. IMAP folder list).

Cache is updated continuously as new items are added or changed (***Live Update***). Additionally, each Friday before midnight (but this can be scheduled to custom time), the **/mail** and **/archive** folders are traversed and directory indices and sizes are updated (***Wave Mode***) on the background.

Note that files/folders copied into mailboxes will not appear to users unless the directory cache is updated. An update should then be forced per user (**Management – Options – Refresh Directory Cache**) rather than globally via the **System – Advanced – Directory Cache – Run Now** button. If the files are copied using the built-in File Manager, the cache index is rebuilt automatically (and also **imapindex.dat** files are updated for any files copied).

*NOTE: In the case you need to know when directory cache refresh started and ended, go to the directory cache log (**Status – Logs**). You will see something similar to this:*

control.exe [1118] 10:48:45 Directory cache - Start count=1 sleep=5 c:\IceWarp\mail\testes.icewarp.com.br\flavio

control.exe [1118] 10:48:52 Directory cache - End

The default directory cache database should be changed to MySQL for large installations, and the full index built after upgrade using the ***Run Now*** button. This can take many hours since the indexing runs with a very low priority but will not affect server operation beside some slowdowns when the directory information is requested for the first time.

Directory Cache Wave Mode, Direct Mode Removed

The former modes for directory cache indexing (***Wave Mode*** where cache was built on background and the ***Direct Mode*** which did not employ the cache) were removed and now directory cache is always in database, always updated on the fly (***Live Update***) and additionally indexed on the background (***Wave Mode***) without possibility to change it.

You may want to stop directory cache wave processing – e.g. because it is not set properly. Set the ***c_accounts_global_accounts_directorycache_wavestopped*** API variable to **1** (one). (Server console – *File – API console* – search for the variable.)