iTools 9 User Manual

Tenon Intersystems
232 Anacapa Street
Santa Barbara, CA 93101
805 - 963 - 6983
info@tenon.com

February 19, 2009

Contents

1 Introduction to iTools

1.1 Serious Tools For The Internet

Tenon's iTools is a family of professional quality, high-performance configuration and management tools that makes managing internet services under Mac OS X and Mac OS X Server easy and secure.

Apple's Mac OS X operating system, combined with the strength and ease of iTools, makes the Macintosh a world-class platform for web content delivery. On Mac OS X client, iTools turns the desktop Mac or Mac mini into a powerful, yet inexpensive, webserver. With Mac OS X Server on an Xserve box, iTools gives administrators the freedom of anywhere, anytime Apache management and lets their clients securely administer their own virtual hosts.

iTools extends the internet software that ships with Mac OS X and Mac OS X Server and enhances open source packages by augmenting key internet services with a point to click interface to make configuration and maintenance easy and error-proof. Tenon's iTools GUI and built-in functionality has made the transition to Mac OS X an easy step for Macintosh web masters. At the same time, Tenon's iTools performance, combined with Apple's Intel processing power, is attracting UNIX and NT web masters to Apple's Mac OS X platform.

Tenon's iTools includes an Apache 2.2 Web server, domain name server (DNS) and multi-homing secure file transfer server (FTP). Because we know that creating a world-class web server involves more than simply being able to deliver content quickly and reliably, we've bundled iTools with a variety of open source web development tools (ht://Dig, Tomcat, with SOAP support, PHP, MySQL). These tools are delivered in ready-to-use, separately installable packages. They extend iTools with a search engine, Java servlet support and Java Server Pages, dynamic web page creation tools and SQL databases. eCommerce on Mac OS X is supported by iTools SSL 3.0.(a PCI-compliant Secure Socket Layer) to support the secure exchange of data between iTools and any SSL-enabled browser.

Tenon's iTools 9.0 is a full featured, high performance, easy-to-use Apache web and caching proxy server. Apache, the most popular web server on the internet, is being used today to server over ninety million web sites. Tenon's iTools is the easiest-to-use Apache in the world, on a platform known for its elegant user interface and of late for its power and strength.

Welcome to a new era in Macintosh web service. Tenon's iTools: fast, reliable, secure. Serious tools for the Intenet.

2 Installing Tenon's iTools

2.1 System Requirements

iTools will run on any Mac OS X or Mac OS X Server capable computer. iTools requires:

Mac OS X 10.4 or above.

at least 256MB RAM.

at least 200MB of available disk space.

2.2 Pre-configuration

iTools family of Mac OS X networking applications requires a properly set up network configuration. Each Mac OS X system must be pre-configured, using the Network preference panel from System Preferences. Having a valid hostname (eg. host.domain.com) and IP address is a good beginning for iTools, because the iTools configuration will automatically pickup this information. If you are unfamiliar with these terms, please contact your system administrator.

2.3 Network Control Panel

Application -> System Preferences -> Network -> TCP/IP tab

In most cases, the correct settings in the Network Preferences will be: Location: Automatic: Show: Built-in Ethernet. And in the TCP/IP panel: Configure: Manually.

2.4 Installing iTools

2.4.1 New Installation

After completing the system and network requirements as outlined above, proceed with the install. Chapter 3 is a Quick Start Guide.

2.4.2 Upgrades or transition installs from earlier versions

If you are doing an upgrade or transition, it is a good policy to backup your exiting server. iTools 9 will install gracefully over an iTools 8.2 installation. For other transitions, check the Tenon web site "Support" pages for white papers and hints.

2.5 Installing From A Download

Tenon's iTools can be found at:

http://www.tenon.com/products/itools-osx/

Check Tenon's web site regularly for updates, or subscribe to Tenon's iTools mailing list for automatic notification about updates and technical discussions about the software.

Double-click the package installer. You will need to authenticate yourself as an Admin user. Proceed through the installation process, step-by-step. The last step of the install process, Optimizing System Performance, takes a few minutes, so be patient. Quit the installer when it has completed the process. At this point it will ask you to reboot your computer, then you will have full access to iTools.

Other packages, e.g., PHP, MySQL, etc. are separate downloads and are installed in a similar manner. Always install PHP before installing MySQL.

2.6 What Gets Installed

/Library/Receipts/iTools9.pkg
/Library/Tenon -> assorted files, including a modified httpd.conf.
The original "httpd.conf" is backed up during the install process. Your web site's content will reside in folders and sub-folders within the folder:

/Library/Tenon/WebServer/WebSites/

2.7 Connecting to the Administration Server

When you start up your Mac, the servers (set to be on by default) are automatically launched and run as invisible background applications.
On the iTools machine, you can use your web browser to connect to the iTools Admin server, using "localhost" or 127.0.0.1. From other locations, use the machines fully qualified host name or IP address.:

For example:
https://127.0.0.1:85/ for SSL enabled Admin server

or

http://127.0.0.1:84/ for non-SSL Admin server.

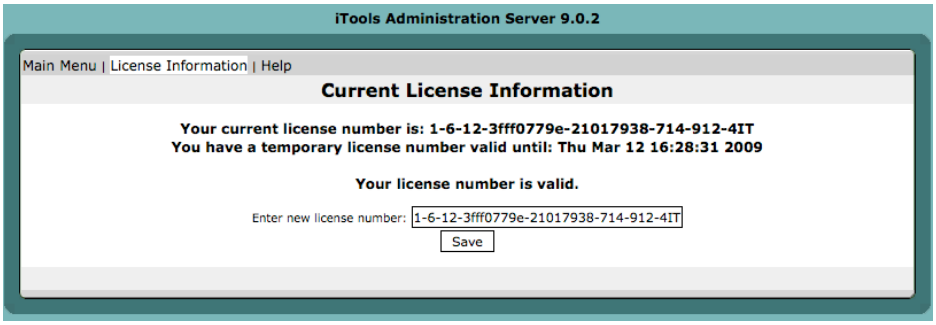
The secure admin server runs on port 85, and the non-secure admin server on port 84; the URL will reflect that. If you have a firewall, and will be connecting from outside locations, you will need to open those ports to have access to iTools administration functions.

The secure administration uses a self-signed certificate. Naturally for uses other than iTools administration, you will want to purchase an official certificate from a valid certification authority.

For new installations, the default login and password is "admin". To change the password go to the Users Settings page, select the admin user and enter a new password for the admin user. You may also add additional users to the iTools admin group. Users in the iTools Admin group are used only by Tenon's iTools. The admin password need not exist in the system password database nor does Tenon's iTools enter it into the system password database.

Creating other users and additional groups will be covered in a subsequent section. Note "admin" is a very special user and has certain privileges that other users will not have.

Tenon's iTools license can be entered or changed in the License Information section (the Red Seal). To enter or change the license, login as the iTools Administrator (admin), enter your license in the text field, being careful to observe case sensitivity and click Save. The license program will return information about the validity of the license you have entered and for what time frame it remains valid.



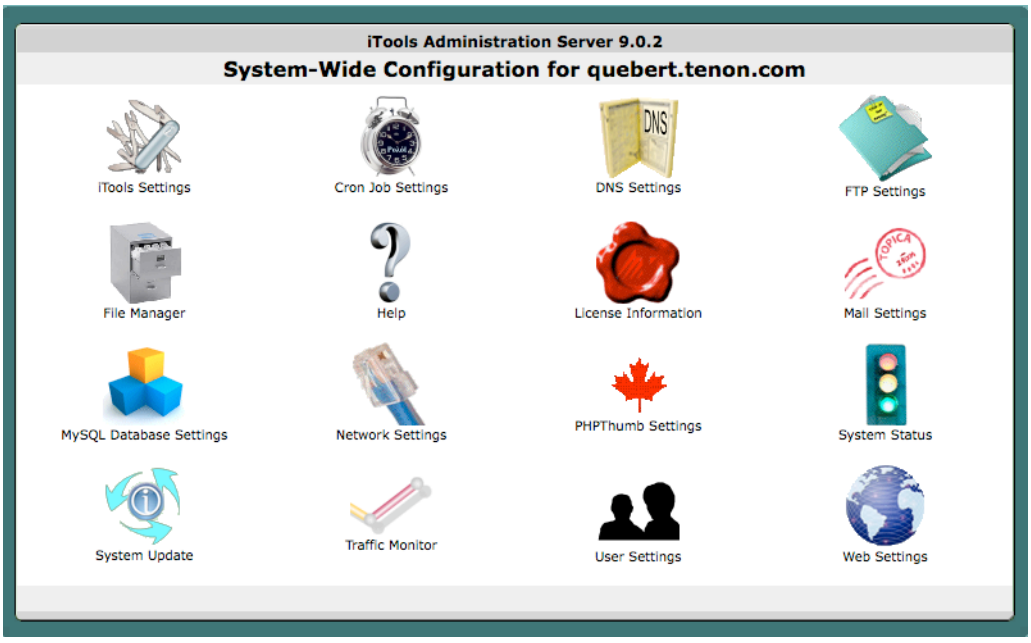
The next chapter is a Quick Start Guide to help you to set up your web server. Later chapters contain detailed information about all aspects of the server and administration.

3 iTools Quick Start

Once iTools is installed on a properly networked machine, you can start setting up your web server by connecting to the iTools Administration Server. Configuration and management can be done from any platform by using the traditional browser-based administration tools. This chapter will show you how to use the iTools Administration Server to set up a virtual host.

Go to https://ip-address-of-yourserver:85/

You will be presented with a login screen. The default login is admin, with password admin. (Change the admin password using User Settings.)



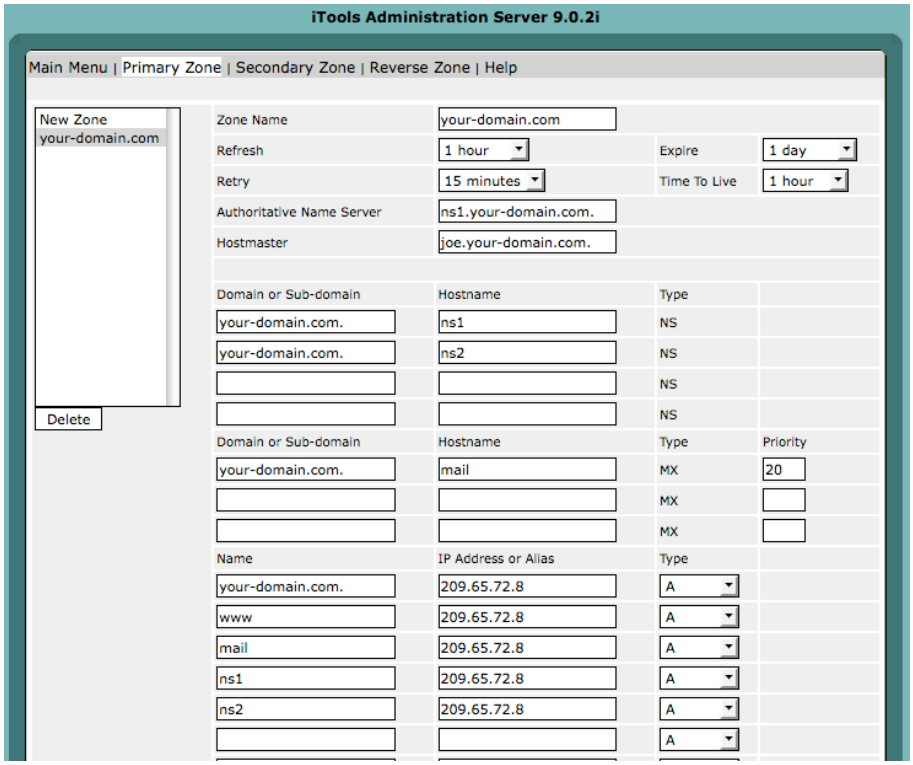
This is the main menu of iTools Administration Server. Each icon takes you to other pages with configuration options. To set up virtual hosts, you need to have valid DNS entries and valid IP address on the server.

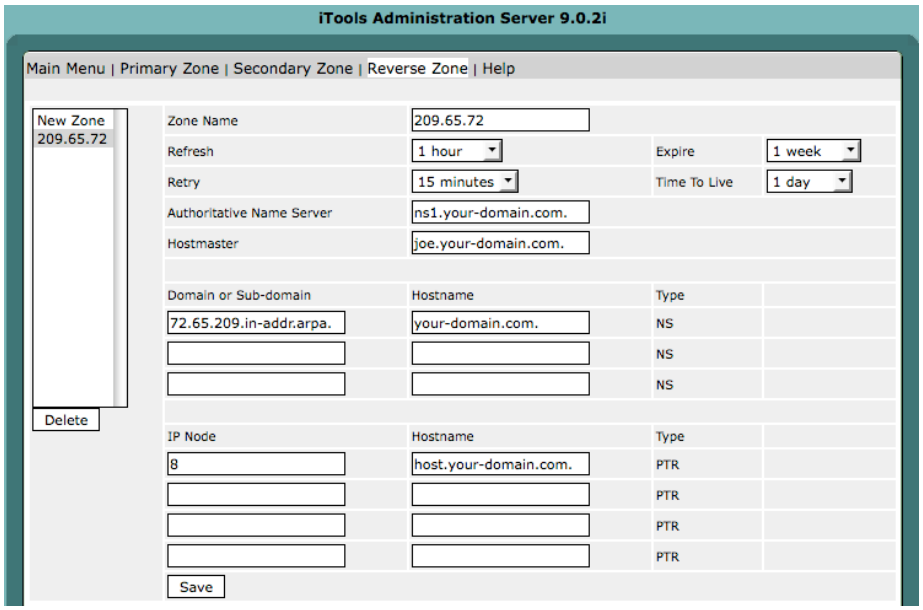
3.1 DNS

You may already have your DNS served by your ISP or some other provider, however, if you will be using iTools DNS services and you are familiar with setting up a DNS server, read this section before proceeding. If you are new to running a DNS server, or feel uncertain about the DNS portion of iTools, please read the full chapter about DNS before proceeding.

Click on the DNS button on the Admin home page. The figure below shows the DNS zone list after adding an example primary zone.

To set up a new primary zone in iTools, choose “New Zone” from the zone selection list. The figure below shows appropriate entries for the new primary zone “your-domain.com” using an arbitrary IP address and for a PTR record.





IMPORTANT: This form displays a few text fields where you configure the Start-of-Authority record (SOA). The Start of Authority record stipulates time intervals for your DNS refresh, retry, expire and time to live (TTL) parameters. iTools will automatically try to fill in the information for you, if fields are left empty (Refresh, Retry, Expire, Time To Live). It is very important to enter correct information in this section.

Enter the authoritative name server for this zone; in most cases that will be the primary DNS server for the domain. Enter the email address for the contact person for the DNS records or websites. Note: The "@" sign in the email address should be replaced by a ".", and the domain name followed by a ".". The default value for Refresh, Retry, Expire and Time-to-live should be fine in most cases.

In this example, the values entered are:

Domain Name = your-domain.com

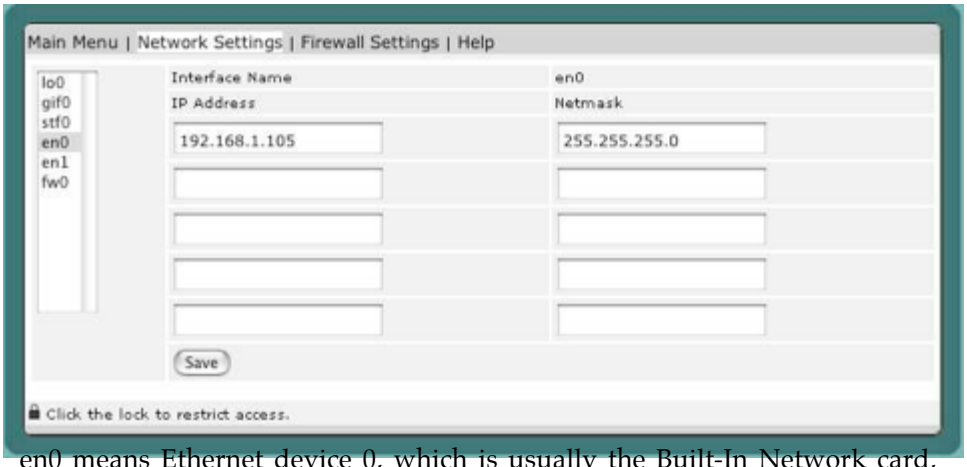
Authoritative Name Server = ns1.your-domain.com.

Hostmaster = dnsmaster.your-domain.com.

Click "Save" to save the zone.

3.2 IP Address

Once DNS is configured, it's time to setup IP address for your hosts. If you have only one IP address, or have already added all of your addresses in Apple's Network preferences you can skip this section. Click on the Network Settings icon, and a screen will be displayed similar to this:

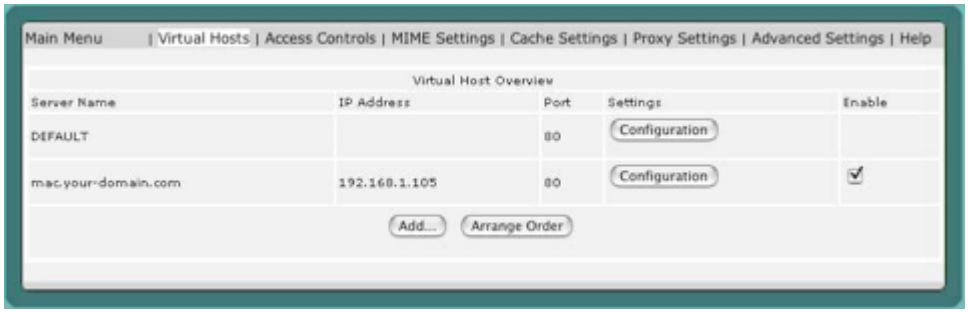


en0 means Ethernet device 0, which is usually the Built-In Network card, simply add the IP addresses that you wish to host on the appropriate interface. If you are unsure about this section, please contact your system administrator. Click "Apply" to save the settings.

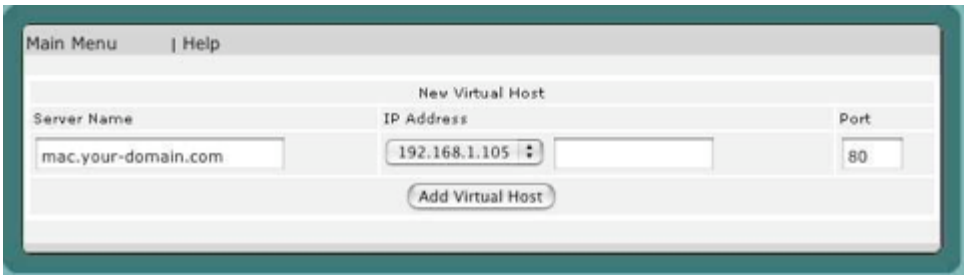
3.3 Virtual Hosts

The virtual host concept is a way to host more than one website on a particular machine. Each website has its own hostname (e.g. www.whatever.com), without requiring the user to know any other pathname, and is referred in Apache terminology as a virtual host (VH).

Once DNS and IP address are correctly set up, it's a simple matter to add virtual hosts.

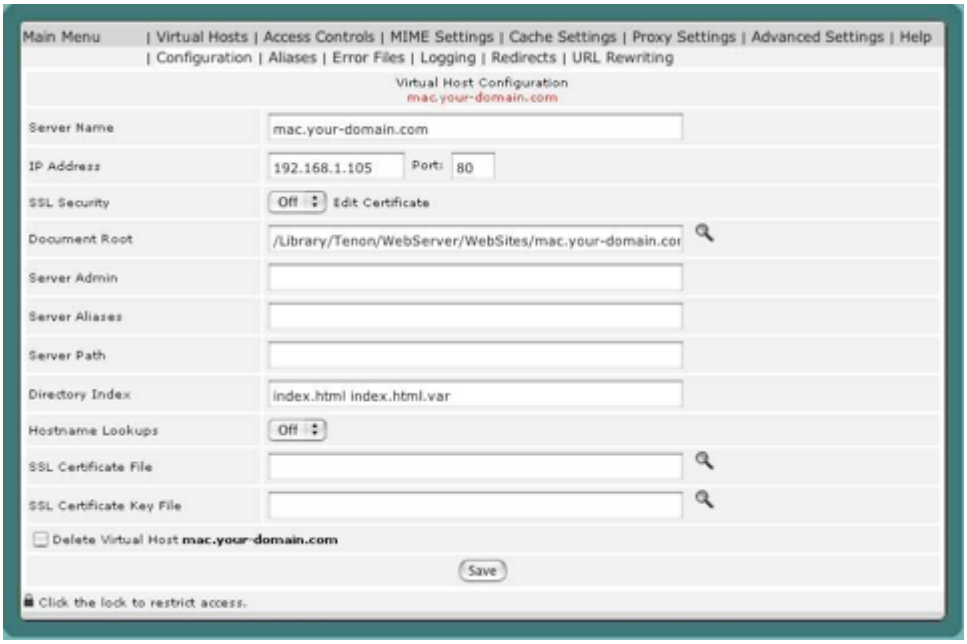


Click on the Web Settings icon, and click on "Add. . . ". Virtual hosts can be added by entering a hostname, IP address and port number.



Click "Add Virtual Host" to confirm the addition of the new virtual host.

For now the important thing is to make sure that the Directory Index field contains the name of the index file for your web site. Also, if your site is to be accessible from multiple URLs such as www.your-domain.com and your-domain.com, make sure that the other ones are listed (separated by spaces) in the Server Aliases section.



If you make changes to the virtual host configuration, click “Save" to save the Virtual Host configuration. The web pages go into the folder (which is automatically created):

/Library/Tenon/WebServer/WebSites/www.your-domain.com

For now, you’re all set!
Your first host is up and running and can be accessed with a browser.

4 iTools Administration Server

Using iTools Administration Server, iTools services (Apache, DNS, FTP, SSL, etc.) can be configured using a web browser. The browser may be running directly on an iTools system, or on a remote host connected via a network to the iTools system. The web browser interface includes easy-to-use tables and forms that eliminate dealing with cryptic Apache directives. Built-in error checking identifies redundant or incomplete entries. Updates are immediately available to the network. And, of course, all documentation is available on-line via the web.

iTools Administration Server is a stand-alone, special purpose web server that runs within iTools. This server uses different port numbers than the Apache web server (the defaults are port 84 and 85).

4.1 Connecting to the Administration Server

Tenon's iTools Administration Server is automatically started when your server boots up. You can connect to the Administration Server remotely using any web browser. For example, if your Tenon's iTools system is named "www.your-domain.com" the URL to connect to the Administration Server would be:

https://www.your-domain.com:85/

or

http://www.your-domain.com:84/

4.2 Administration Server Access

Access to the iTools Administration Server is restricted to users in the iToolsAdmin group. At installation, a default iTools administration

user is created with a user name of “admin" and password “admin." For security, it is strongly advised that you change this immediately after installation. To change the admin password, go to the Users Settings page and enter a new password for the admin user. You may also add new users to the iTools admin group, but you need to keep “admin” as the primary user because “admin” has special privileges.

Additional users may be added to the iToolsAdmin group by using Users and Groups tables accessible from within the iTools Administration Server -> User Settings page (see Chapter 16, “Users & Groups").

4.3 Navigating the Administration Pages

The iTools administration pages use HTML forms and Perl scripting to present the web server’s configuration information in tables that are easy to read and easy to modify. How the information is displayed depends on the type of permissible entries. Related entries are grouped together. Lists are sorted alphabetically. Default or system-wide entries are displayed in the lower portions of the tables, while user-defined changes are displayed in the top portions of the tables. Buttons are provided to save or reset any changes made to these forms, to return to the main iTools Administration Server page, or to move on to other tables related to the current table. Each page has a menu item labeled “help" for quick access to a specific section in the documentation. The following sections explain the conventions used for navigating the configuration settings and making changes to those settings.

4.3.1 Types of Information Fields

Information in the tables may be displayed in the following ways:

- Text edit fields
- Radio buttons
- Check boxes
- Pop-up lists

4.3.2 Making Changes

To make changes to an item; either re-type its text, change the radio button or check box settings, or select a different item from a pop-up list. Then click the Save button. If an entry in a table is not presented in a text edit field, or as a radio button, check box, or pop-up list, that entry may not be changed. Multiple changes per save are permitted. In most cases, once changes are saved, the table is re-displayed with the corresponding changes in place. In some cases, you are returned to a previous window. Changed items may move to a different row in a table if the rows are sorted and the key used in the sort was one of the changed items.

4.3.3 Adding Entries

New items are usually entered in the last row of a table, which has been left blank by design. When new entries are saved, the table is re-displayed and the new entries appear in their proper place in the table. The last row of the table reverts to blank, awaiting input of another new entry.

4.3.4 Removing Entries

Removing an item from a table can be accomplished by one of the following:

- Deleting any entry which is displayed in a text edit field (which should leave that field blank)
- Unchecking all of the possibilities for a check box
- Selecting None from a pop-up list or radio button selection

The Save button can then be clicked to remove the item. The key field to be deleted is in the first column of the listed item.

4.4 Inheritance

If certain settings for a particular item are not explicitly set, they are inherited from the global settings (if the corresponding settings exist) or the “DEFAULT" virtual host. In addition to pre-set defaults, webmasters can also customize a default virtual host." See section 17.1.2 for this option.

Subsequent chapters will include details about each configuration option.

4.5 System-Wide Configuration at a Glance

4.5.1 System-Wide Configuration

The System-Wide Configuration panel is the starting point for administering iTools; it may also be called the Admin Home Page. It contains icons for each of the major areas of iTools administration. Clicking on a button will present a table with forms for that specific area and links for in-depth information on what the forms do.

4.5.2 iTools Settings

The iTools Settings contains configuration settings that are global to iTools Administration Server. The administrator can choose to restart services manually after all the settings are configured properly in iTools Administration Server. This is handy if you plan to make a lot of changes and only want to restart the server after all changes have been made.

4.5.3 Cron Job Settings

The Cron Job Settings section contains configuration settings for scheduling tasks. Details on Cron Job Settings are provided in Chapter 5, “Cron Job Settings".

4.5.4 DNS Settings

The DNS Settings section contains configuration settings for Tenon’s iTools built-in domain name server. Details on DNS settings are provided in Chapter 6, “DNS".

4.5.5 FTP Settings

The FTP Settings section contains configuration options for Tenon’s iTools file transfer protocol server. Details on the FTP settings can be found in Chapter 7, “FTP".

4.5.6 License Information

The License Information section contains your registered license information for iTools 9. For more information, see Chapter 10, “License Information".

4.5.7 Mail Settings

iTools, itself, does not include a mail server. However, it reflects the status of whatever mail server is running on the system. The Mail Settings section supports very minimal configuration for Apple’s as-delivered mail server (sendmail or Postfix). Alternately, you can install Tenon’s Post.Office. and the Mail Settings icon will take you to the Post.Office web-based administration page. For more information, see Chapter 11, “Mail Settings".

4.5.8 Network Settings

The Network Settings section contains configuration parameters for IP address and Firewall settings. For more information, see Chapter 13, “Network Settings."

4.5.9 System Status

The System Status section provides a quick look at the status of all of the servers included in iTools. These servers can be turned off and on here as well. For details, see Chapter 14, “System Status".

4.5.10 System Update

This section is used to keep Tenon’s iTools up to date with the latest security

4.5.11 Traffic Monitor

The Traffc Monitor section provides the real time server status for Web server, FTP server, and DNS server. Please refer to Chapter 12, “Traffic Monitor" for details.

4.5.12 User Settings

This section is used to set up users for various Tenon’s iTools services including Web, FTP and Mail. Please refer to Chapter 16, “Users and Group" for details.

4.5.13 Web Settings

This section provides configuration options for the Apache Web Server. Please refer to Chapter 17, “Web Settings" for details.

5 Cron Job Settings

The “cron daemon" is an automatic task machine. This is a powerful tool that enables you to perform repetitive tasks at specific intervals on your webserver. For example, you could add a cron job that automatically copies an MySQL database to a separate location on your site as a backup.

5.1 To Add Or Modify A Cron Job

- Click on the Cron Job Settings button on the home page.
- Enter the command that you want to run in the Command-to-run field.
- Click on one option from each of the available lists.
- Enter the times for the cron job in the minute, hour, day, month, or weekday fields. You can use star (*) as wild card to represent every cycle. For example, a star (*) in hour, means every hour. In addition, you could also use numeric expressions, such as 1,2,3 to represent from 1 to 3, for example, to indicate the first three months, first three days, or first three hours. You could also specify*/15 in minutes represent every 15 minutes.
- Enter the cron job script in the Command field.

Click on the Save button. Your cron job has now been added or updated.

5.2 Delete a Cron Job

Remove the command field to remove the specified cron job. Click on the Save button. Your cron job has now been deleted.

6 DNS

6.1 Configuring and Administering DNS

The Domain Name System (DNS) acts very much like a telephone company directory assistance service. It provides mapping between Internet “host" computer names and Internet IP addresses. Given a host name, it will look up and return an IP address. Without DNS entries, your server has the equivalent of an “unlisted telephone number."

The Domain Name System itself is a distributed database of domain names and Internet addresses. DNS translates names (for example, ftp.apple.com) to IP addresses (for example, 17.254.0.26) and vice versa. A client/server scheme, supported by replication and caching, enables these mappings to be available throughout the Internet.

Domain name servers make up the server half of the client/server mechanism. Name servers contain information about some segment of the DNS database and make that information available to clients, called resolvers.

iTools DNS includes a complete implementation of the Berkeley Internet Named Domain (BIND) DNS, version 9. BIND, version 9, is the latest version of what is considered the definitive implementation of the DNS protocol. The software is maintained and continually enhanced by the Internet Software Consortium (http://www.isc.org). This latest version includes significant enhancements, including performance improvements and security-related fixes. BIND under iTools functions independently of Apache, and has been designed to either totally replace or operate in concert with other DNS servers for your domains.

This chapter contains basic DNS information and how-tos for configuring iTools DNS server. The definitive resource, for an in-depth understanding of DNS, is “O’Reilly & Associates, “DNS and BIND"": 400+ pages covering both DNS theory and detailed configuration information for BIND.

It is important to properly configure DNS entries before adding virtual hosts to your server. The DNS server can be your iTools machine, another machine on your network, DNS provided at another location or from your ISP.

In most cases, servers will have static (unchanging) IP numbers. Occasionally, people run servers with dynamic IP allocation. Dynamic IP allocation creates significant complications for configuration and is not recommended.

6.2 Running iTools With DNS Off

If you have disabled DNS (BIND) in iTools you will need to have another DNS server configured with zone data for the hosts/domains you wish to host on your iTools server.

Be sure that your system has a valid entry for the appropriate DNS server.

6.3 Running iTools With DNS On

iTools DNS server can be started and stopped from the System Status page of the iTools Administration Server. For more details see Chapter 14, “System Status".

It is a good idea to have your system pointed directly to your server’s IP address for DNS lookups. Details about setting this can be found in Chapter 2. “Installing iTools." Section 2.2 “Pre-Configuration" on page 9.

6.4 iTools DNS Administration

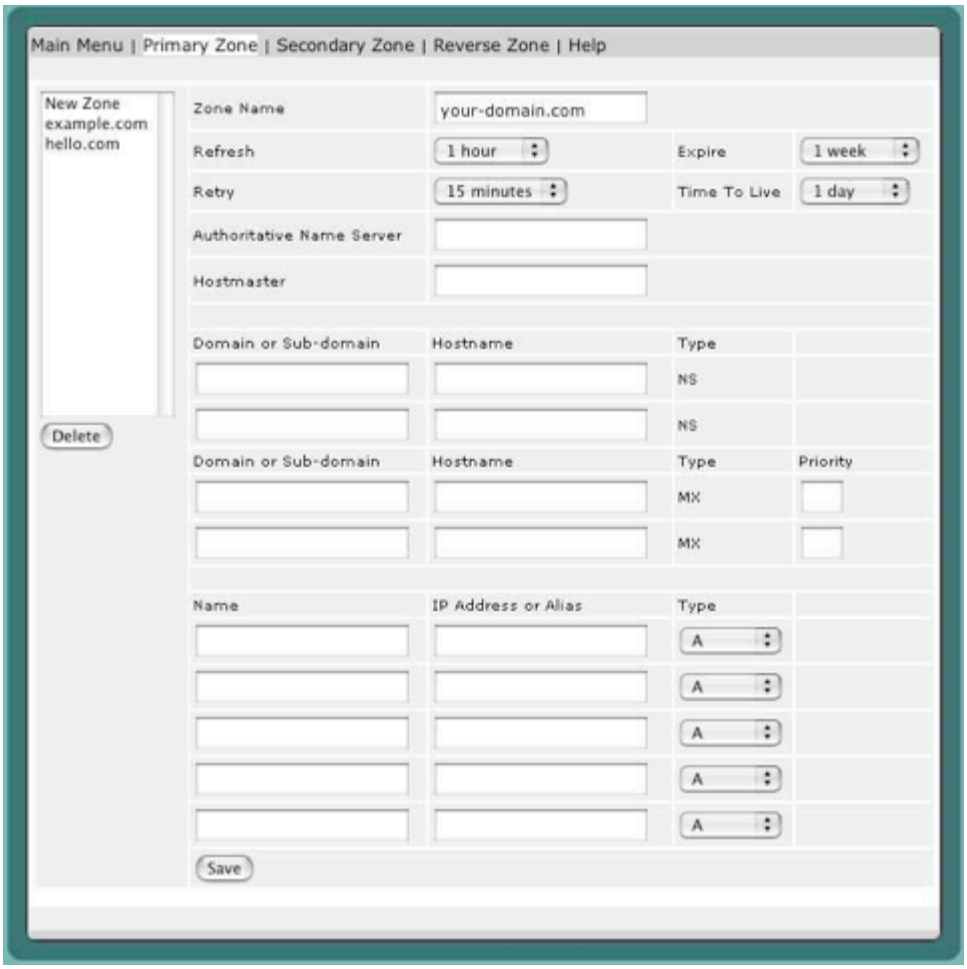
iTools contains an integrated, browser-based interface for configuring your DNS zones. Changes to the DNS databases are automatically merged into the running DNS. If you hand edit DNS config files, you will need to reload the database to update the server; a reload can be performed by restarting the DNS service from the System Status page.

When you select the DNS Settings button from the Administration home page, the web page displays a listing of the Primary Zones currently being managed by this system. The DNS Settings page also presents buttons for creating new Primary Zones, creating new Secondary Zones, and new Reverse Zones. On initial launch, iTools may create a Primary Zone for the domain configured during the install process.

6.5 Primary Zones

6.5.1 New Primary Zone

From the main DNS Settings page, click on the New Zone to add a new primary zone. This page is used to enter the Domain Name of a Primary Zone to be managed by this system. The Domain Name must be unique; no other Primary or Secondary Zone may have the same Domain Name on this system. The name entered here should correspond to a domain name registered at a company such as Register.com or Network Solutions.



6.5.2 Domain Name

Enter the Zone Name of the Primary Zone. For example: new-zone-here.com

6.5.3 Refresh, Retry, Expire, And TTL Values

These Start of Authority values govern how often other Domain Name Servers check with this server to ensure that their information is up to date. The Refresh, Retry, and Expire values are only used by other DNS servers if they are acting as Secondary Servers for this Zone. Choosing the time values is about determining the right balance between how rapidly data is updated versus how much load is placed on the DNS server.

These values can be changed later by modifying the Start Of Authority table. For details on making these changes and for definitions of the Start Of

Authority values, please see section “Start of Authority" on page 33.

6.5.4 Authoritative Name Server and Hostmaster Values

The authoritative Name Server value should contain the name of the server that is the best source for the data contained within the zone. This field usually corresponds to a Name Server host that was registered when you bought your domain. The name should usually be a host name that resolves to the IP address of your iTools server. For this field, be sure to place a trailing dot at the end of the server name if it includes a domain name.

The Hostmaster value is an E-mail address for the person who should be contacted in the event of a problem. Instead of “@" sign used in the normal email address field, the sign should be replaced by a “.".

These values also maybe changed later by modifying the Start of Authority table. For details on making these changes and for definitions of all of the Start of Authority values, please see section 6.5.6 “Start of Authority" on page 33.

Select the Save button to submit the New Primary Zone information. The new Primary Zone name will now be included (in alphabetical order) in the table of Primary Zones in the DNS Settings page.

6.5.5 Configuring Entries for a Zone

The primary DNS Settings page shows currently configured primary this DNS server. To access the Primary Zone page to edit entries for a particular zone, click on the Primary Zone name.

The Primary Zone page displays Host Names and aliases (sorted alphabetically) that are currently in this Zone. Each row of the zone table shows the Host Name, its IP Addresses, Alias, Mail Exchangers, or Name Servers. To change the information about an entry in the table, replace the text field with DNS information specific to each row.

Primary Zones will have DNS records of a number of types:

- Start of Authority (SOA records)
- Name Server (NS records)
- A Host Name to IP Address mapping (A records)
- An Alias of a Host Name record (CNAME records)
- An IP Address to Name mapping (PTR records)
- Mail Exchanger (MX records)
- SPF: Sender Policy Framework (TXT records)

Any host names records entered that do not end in a period “." will have the zone name automatically appended on to them when the record is requested. This is to make the set up of a zone faster, but an administrator must remember

that all fully qualified domain names and any names outside of the zone should have a period added to the end.

6.5.6 Start of Authority

From the Primary Zone page of the zone to be edited, the top section is the Start of Authority where you can alter the values that govern how other Name Servers will communicate with yours to ensure that their data is up to date.

6.5.7 Refresh

The Refresh value indicates the interval for how often Secondary DNS servers for this zone validate and update their data if there have been changes to the records in the primary (Master) DNS server. Most zones do not have rapidly changing data, so a value of 3 hours to 24 hours is reasonable.

6.5.8 Retry

If the primary DNS server failed to respond at the last check, the Secondary DNS servers for this zone will attempt to contact the Primary DNS server for the update/validate process at the interval specified in the retry value. This value should be significantly smaller than the refresh value. A value of 1/3 to 1/5th of the refresh value is appropriate.

6.5.9 Expire

The Expire value indicates how long the secondary servers for this zone should preserve their data if the primary fails to respond to retries. This value should not be too small - if the primary DNS server is not responding for hours or days, there is probably something seriously wrong, and you will want the Secondary DNS servers to preserve the current data they have so that your DNS information will still be available until your Primary DNS server is back online. One to two weeks are common settings for this.

6.5.10 Time-to-Live

The Time-To-Live value is used by any other Domain Name Server that queries any piece of data within this Zone. The Time-To-Live tells the other DNS Servers how long they may cache the data before checking back with this Server to see if the data has changed. Unfortunately, not all DNS servers are well-behaved with regard to honoring TTL values.

It is appropriate to change the default time values when hosts/domains are being transferred to a different server, or when the IP numbers of various hosts are changing for some other reason, such as moving to a different upstream ISP. In this event, you would want to shorten the time values for the Refresh and Time-to-Live fields.

6.5.11 Authoritative Name Server

The Authoritative Name Server value should contain the name of the primary master Name Server for this zone. This server that is the best source for the data contained within the zone. This field usually corresponds to a Name Server host that was registered when you bought your domain. The name should usually be a host name that resolves to the IP address of your iTools server. For this field, be sure to place a trailing dot at the end of the server name if it includes a domain name.

6.5.12 Hostmaster

The Hostmaster value is an E-mail address for the person who should be contacted in the event of a problem with information contained in this zone. The “@" sign is replaced by a “.".

6.5.13 Name Servers

Registrars require that you provide two name servers for each domain being registered. Every primary zone should have also have a minimum of two name servers associated with it; more are allowed.

It is optimal to have a secondary name server that is on a completely different network than your primary name server. If one of the secondary name servers is geographically distant, you are provided with additional redundancy in the even that there are Internet problems affecting a widespread area. Many people trade DNS services with other people to achieve this. Some ISPs provide secondary DNS at a low cost, and many nationwide providers have DNS servers placed in geographically dispersed locations.

6.5.14 Primary VS. Secondary Name Servers

These terms have two different meanings depending on whether you are referring to name servers for this zone, or other name servers that will query them.

The way primary and secondary name servers relate to each other, is that the secondary is a “slave" to the primary, “master", server. Editing of individual DNS records happens on the primary name server; the secondary name server(s) records are updated and validated at the Refresh interval specified in the Refresh for the zone.

To other names servers, the primary and secondary names servers are all considered to have valid information for the zone. Other name servers will check the response time of all name servers listed for the zone and preferentially query the one with the fastest response time. If the first DNS server queried doesn’t respond, the other DNS server might then try one of the others authoritative for this zone.

6.5.15 Adding Name Servers For A Zone

There should be an initial name server added when you add the primary zone which corresponds to the Authoritative NS entry. If any of these entries are not name servers for this zone, delete them.

Be sure that there are a minimum of two valid name servers entered for each zone. You will want to add all name servers for this zone. Click the Save button to get more blank rows to enter additional name servers. Enter a dot, “.", at the end of the Host Name of the DNS server to prevent the zone name from getting appended to it.

Save the Name Server record by clicking the Save button. Repeat the process to add all of the name servers associated with this zone.

6.5.16 Domain Name

This entry should generally be the same as the zone name unless you wish to delegate a sub-domain with in your Primary Zone. Entering

“marketing.company1.com"

here would delegate all requests for any hosts in the “marketing.company1.com" domain to the server listed under Hostname.

6.5.17 Host Name

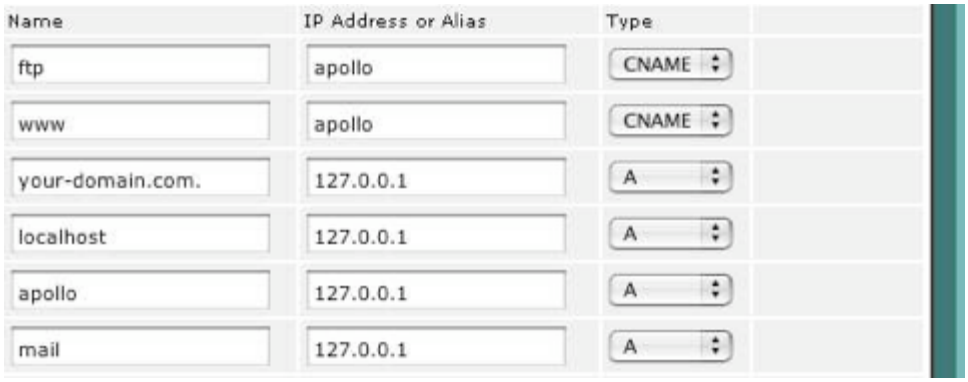
The name entered should correspond to a host name listed on a DNS server somewhere.

6.5.18 Host Name (A) Records

6.5.18.1 Adding a Host

The New Zone page is accessed by selecting the New Zone entry in the Primary Zone page. This page is used to enter the Host Name of a domain to be included in this Zone, its IP Addresses, and the optional Machine Name

and Systems Name information. Host records are called “A" records in BIND terminology.



Each host name, and alias, must be unique within the zone. When adding new hosts, it is not necessary to append the Domain Name at the end of the Host Name, iTools automatically expands them. However, if you do enter the domain name portion, you need to add a trailing period “.".

Host entries expand like this:

www	www.your-domain.com
www.your-domain.com.	www.your-domain.com
www.your-domain.com	www.your-domain.com.your-domain.com

If a trailing dot (“."), is omitted on an entry that contains the full domain name, the host record ends up with an extra copy of the domain name appended - this won’t work correctly.

Enter the new Hostname in the Name field and an IP Address in the Internet dot (“.") notation, for example, “192.83.246.73", for the IP address.

Select the Save button to submit the new Host Name information. The new information will be updated in the Primary Zone’s records and will be presented in the Zone Table for this Zone.

6.5.18.2 Deleting a Host

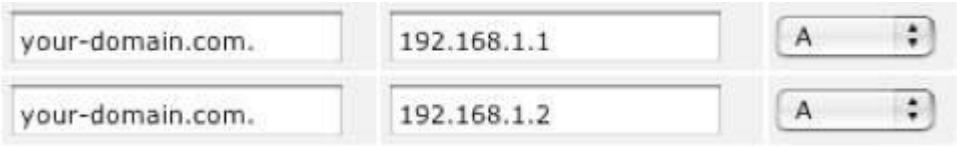
To delete a host, from the DNS Settings page, select the zone containing the host you wish to delete. From the Zone page, empty the Name field for the unwanted host record. Click the Save button to see the changes.

6.5.18.3 Modifying a Host Record

If a host record needs to be changed, click on the Hostname in the Zone page and modify as desired. The page is the same one as is displayed for creating a new Zone. Click Save when you have finished.

6.5.18.4 Adding Load Balancing Hosts

It may useful for busy web servers, to spread the load among two or more machines. This can be done by adding IP Addresses to a Host Name record.



The DNS server will load share resolver requests to this Host equally among the IP Addresses entered. Enter one IP Address per line. The machines do not have to be part of the same network.

6.5.19 Alias Records

Aliases are records that refer to other Host Name records or aliases. You should not enter an IP Address in an alias record. Host Name records should be used if you are pointing a Hostname at an IP address. Alias records are also known as “CNAME" records or Canonical Name records.

6.5.19.1 Adding an Alias

The new Alias is set by selecting the CNAME from the Type pull down menu on the Primary Zone Page, and filling out the name of the configured Host corresponding to the nickname.

Enter the new Alias Name. The new alias name must be unique within this Zone (i.e., it must be different than any other Host Name or alias in this Zone). It is not necessary to append the Domain Name at the end of the alias name, in other words, it is not necessary to enter fully qualified Host Names. If the Domain Name is appended, either with or without a trailing dot “.", the Domain Name will be stripped off and the abbreviated form will be used in the database and in the presented tables.

If the entered Host Name is not in this Zone, it is necessary to enter a fully qualified Host Name including the dots “." and a trailing dot.

Select the Save button to submit the new alias name information. The new information will be updated in the Primary Zone’s records and will be presented in the ZoneTable for this Zone.

6.5.19.2 Deleting an Alias

To delete an alias, from the DNS Settings page, select the zone containing the alias you wish to delete. From the Zone page, empty the Name field for the unwanted host record. Click the Save button to see the changes.

6.5.19.3 Changing An Alias

To change an alias record, click on the name of the alias from the Primary Zone page. The page that displays is the same page as for creating a new alias. Modify the entries as desired, then click Save.

6.5.20 Mail Exchangers

When you first create a Primary Zone, one new Mail Exchanger record is created in the zone with a Hostname of “mail"; you will need to add a new Host Name record with this name and the IP address of your mail server to get the Mail exchanger to work correctly.

To insure proper delivery of mail, it is important to have at least one Mail Exchanger record for each primary zone. Most administrators choose to have several if they have backup mail servers available. The Mail Exchanger is usually added to the Host Name record that matches the Zone name, but any individual hosts within the zone can have different mail servers if desired.

The precedence value in Mail Exchanger records determines which mail server preferentially gets the mail on the first attempt at delivery. In most cases, users will be collecting their mail from the primary mail server. If the first (primary) mail server is unavailable when delivery is attempted, mail will instead be delivered to the second one (in precedence). That mail server will hold the mail until it can be delivered to the first mail server for delivery to end users. If the secondary mail server is down, mail goes to the next server in precedence, and so on if there are additional backup mail servers.

A smaller precedence number means that server is closer to the head of the line for delivery of mail.

0 mail delivered here if the server is up and reachable

10 this server is second in line, and gets the mail if 1st is unavailable

20 third in line (gets mail if both 1st and 2nd are unavailable, and so on)

The absolute values used are arbitrary; what matters is relative value in relation to the other Mail Exchanger records for this zone and host.

This model assures that mail will get delivered to your domain even if an individual mail server is down.

Mail Exchangers are commonly referred to as “MX" records.

To access the Mail Exchanger listings for a host, go to the Primary Zone page and click on the domain for which you want to view Mail Exchange records. Doing so brings up a page listing the information about the currently configured domain.

6.5.20.1 Adding/Changing Mail Exchange Records

To add a mail server for a host, in the Primary Zone page, scroll to the rows that displays Type as “MX" records. Fill out Domain Name, and Hostname.

Enter the host name for the mail server and enter a precedence value for this MX record. The mail exchanger may be another host in this zone, or another zone.

Domain or Sub-domain	Hostname	Type	Priority
your-domain.com.	mail	MX	20
		MX	
		MX	

For a host within the zone, the Hostname is sufficient, you don't need to include the domain name. If the host is outside the current zone, be sure to use a fully qualified Hostname and add the trailing dot ".", to the name.

Select the Save button after configuration. The new mail server record(s) will be displayed for this host when you view the primary zone page, or when you view the mail exchangers page specifically for this host.

Host names that have Mail Exchanger or Name Server records pointed to them must have Host Name records listed in the Primary Zone rather than alias records.

6.5.20.2 Deleting Mail Exchangers

To delete Mail Exchangers for this Host. Empty out the existing Mail Exchange record, and select Save button to save the changes.

6.5.21 Adding an SPF Record

Sender Policy Framework (SPF) is one of the new technologies in the war against SPAM. Soon major carriers, like AOL, will begin to require SPF records. The SPF lookup uses DNS to verify that the sending mail server is valid for the domain of your email address. The SPF record must specify the valid mail servers for your domain. You can use an SPF wizard on the internet to generate the syntax of the SPF record, for example,

http://spf.pobox.com/wizard.html

Each domain can have an SPF record. Enter the domain name in the "SPF Name" field and the text generated by the SPF wizard in the "SPF Text" field.

6.5.22 Reverse DNS Records (PTR Records)

This type of record is also known as a pointer or "in-addr.arpa" record. Selecting the Reverse Zone link from the Primary Zone page displays the Host List sorted numerically by IP address. This is the reverse lookup table, allowing the DNS Server to reference a Host Name when queried with an IP

address. Changes to the Reverse Zone are not automatically updated in the Primary Zone table because a single Reverse Lookup Zone may serve multiple primary zones sharing the same network number.

It is important to realize that reverse records on your server may not be authoritative for your server's IP number.

Here is a simple explanation of why:

- There are a finite number of IP addresses
- Different major ISPs (or organizations) "own" blocks of these IP numbers
- The ISPs are authoritative for the reverse record lookups of those IP numbers because they "own" them
- Customers of ISPs are "renting" one or more IP numbers from the ISP, which may retain reverse authority for those IP numbers

For example, a server with a DSL connection through a local phone company might have a static IP address. Even if it is running a DNS server and that server is configured with PTR records, it won't matter, because the phone company will continue to be responsible and authoritative for the reverse zone.

For example, a reverse lookup of IP 216.102.92.1, returns:

1.92.102.216.in-addr.arpa. 7200 IN PTR adsl-216-102-92-1.dsl.snfc21.pacbell.net.

Indicating that this is an ADSL connection belonging to Pacific Bell. Notice the structure of reverse records - it's the IP address inverted, with ".in-addr.arpa" added on.

If your organization has less than a full class "C" block of IP addresses (256 addresses), you likely do not have reverse authority for your IP numbers. Classless delegation (meaning reverse delegation of less than a full class "C") is possible, but not all ISPs are willing to provide this service.

6.5.22.1 Adding a PTR Record

The New Reverse Zone page is accessed by selecting the Reverse Zone entry from the navigation bar. This page is used to enter the PTR records of a class C IP address.

Each IP Node must be unique within the zone. When adding new hosts, it is not necessary to append the Domain Name at the end of the Host Name, iTools automatically expands them. However, if you do enter the domain name portion, you need to add a trailing period ".".

If a trailing dot ".", is omitted on an entry that contains the full domain name, the host record ends up with an extra copy of the domain name appended - this won't work correctly.

Enter the new Hostname in the Hostname field and an IP Node in the Internet dot "." notation, for example, "1", for the IP Node.

Select the Save button to submit the new Host Name information. The new information will be updated in the Reverse Zone's records and will be presented in the Zone Table for this Zone.

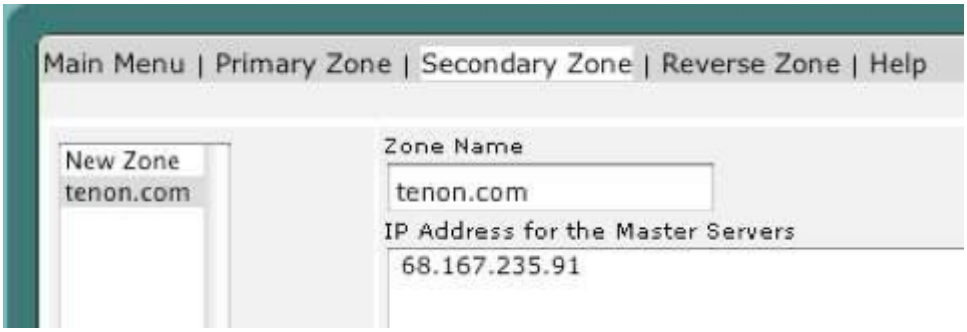
6.5.22.2 Deleting A PTR Record

To delete a PTR record, from the DNS Settings page, select the zone containing the PTR record you wish to delete. From the Reverse Zone page, empty the IP Node field for the unwanted PTR record. Click the Save button to see the changes.

6.5.22.3 Modifying a PTR Record

If a host record needs to be changed, click on the zone name in the Zone page and modify as desired. The page is the same one as is displayed for creating a new Zone. Click Save when you have finished.

6.6 Secondary Zones



A Secondary Zone is a Zone that a Domain Name Server loads from another Domain Name Server, called a Master Server. Secondary Zones are always redundant copies of existing Zones on other systems.

6.6.1 New Secondary Zone

The New Secondary Zone Page is accessed by selecting the New Zone entry from the Secondary Zone Settings page. This page is used to enter the Domain Name of a new Secondary Zone to be managed by this system. Enter the Domain Name for the Secondary Zone. The Domain Name must match the Domain Name for an existing Zone on another DNS server. Enter one or more IP Addresses (in the Internet dot "." notation, for example "205.1.2.66") for the Master Servers (Primary DNS Servers) of the Zone.

The list may include a single IP Address or multiple IP Addresses (up to ten). Multiple IP Addresses can increase the availability of a Zone's database. In cases where a Master Server has several IP addresses by which it may be contacted, or when multiple Master Servers exist for a given Zone, multiple IP Addresses should be used. The order in which the IP Addresses are entered is the order this Domain Name Server will use when attempting connections to

the master server(s) to verify and update its records for this secondary zone. The Domain Name Server will cycle through the list until it successfully contacts a Master Server.

In the case where a Secondary Zone is being created simply to move a Zone from an existing Server, a single IP Address is sufficient. Enter the IP Address of the Master Server for the existing Domain.

Select the Save button to submit the New Secondary Zone information. The new Secondary Zone name will now be included, in alphabetical order, in the table of Zones on the DNS Home Page.

6.6.2 Modifying Secondary Zone Information

The Secondary Zone Page is accessed by clicking Secondary Zone link from the navigation bar. This Secondary Zone page presents a list of the IP Addresses of the Master Servers for this Secondary Zone.

To change any of the information for the Master Servers for this Secondary Zone, modify any of the IP Addresses in the list.

Select the Save button to submit the Secondary Zone information. The new information will be updated in the Secondary Zone's records and will be presented in the Secondary Zone Page the next time it is accessed.

6.6.3 Deleting a Secondary Zone

Secondary Zones are listed along with Secondary Zone table. Select the zone you wish to delete, and click Delete button to save your changes.

6.6.4 Converting a Secondary Zone To a Primary Zone

If you wish your server to become a primary server for a secondary zone you can click the "Convert to Primary" button to make that zone a primary zone. You must wait until bind has downloaded the zone information from the master server and a db s.your domain.com file has been generated for the domain before attempting to convert to primary. This is useful when transitioning from a different DNS server to BIND with iTools.

6.7 DNS Database Files

The /Library/Tenon/DNSServer/Configuration directory holds the database files for BIND DNS under iTools. The database can be viewed using any text editor.

Primary Zones on this DNS server each have a "db" file. For example, the domain "company1.com", has database file in the listing called, "db.company1.com".

Secondary Zones each have a "db s" file. In our example we had a secondary domain called "organization2.org", which shows a database file in the

listing named “db s.organization2.org". The secondary zone file data is obtained from a Primary/Master DNS server for the zone and should not be edited.

Reverse Zone Lookup files are designated as “db.xx.xx.xx" where the “xx.xx.xx" represents the IP number. In the above list of files, several represent reverse zone data, one example being “db.192.83.246".

The startup file for BIND is “named.conf". It contains the list of zones, both primary, secondary and reverse, managed by this iTools server, the names of their corresponding database files and any DNS options.

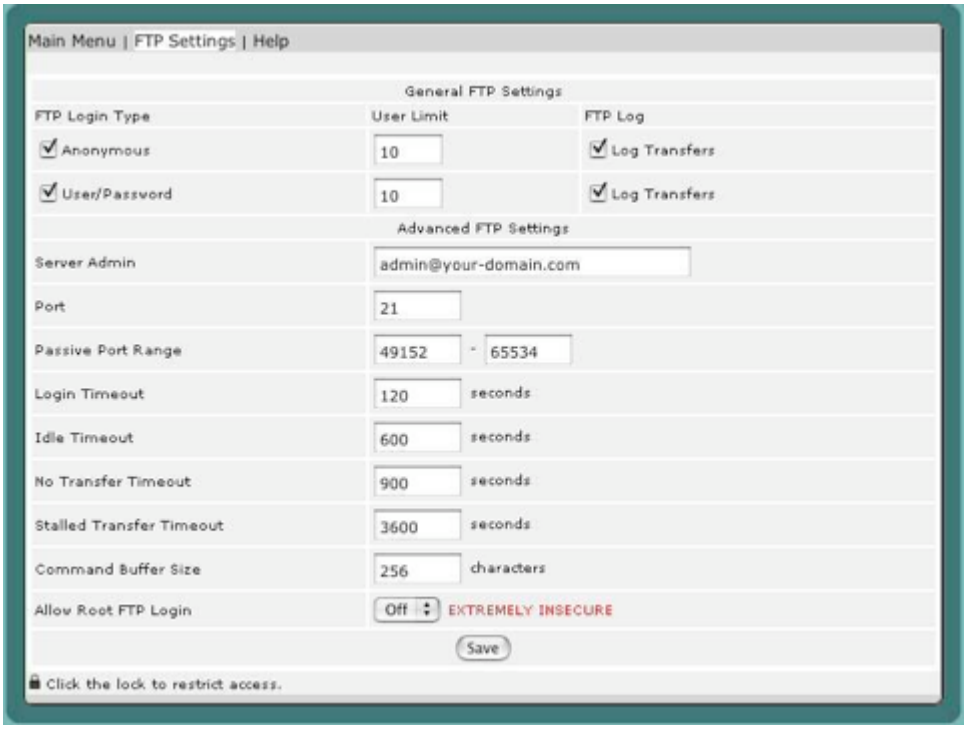
The “name.root" file contains the names of root domain servers used to initialize the iTools DNS cache. Root servers know what DNS server is authoritative for top level domains (such as “com" and “edu").In most cases, root name servers do not themselves provide the final answer to a query for the IP# of a requested Hostname; instead, they refer to a DNS server that may have the answer. They are iterative, rather than recursive in their behavior. This file should generally not be edited.

7 FTP

7.1 The File Transfer Protocol

The File Transfer Protocol (FTP) allows the transfer of files between networked computers. The FTP service provided with iTools is based on the ProFTPD project source and is integrated into the iTools suite of applications. The iTools FTP Server provides advanced features such as anonymous FTP, FTP virtual hosting, and fine-tuned controls on upload and download access to the iTools server. The iTools FTP implementation can also be configured to allow or deny anonymous or iTools user access to the servers file system. Secure data transfers are supported using FTP (TLS/SSL).

7.2 FTP Settings



The FTP server is an integrated component of iTools and is designed to provide separate access points based on virtual hosts for different FTP users. The FTP Settings table contains some options that control the iTools FTP service. The FTP server can also be configured to permit or deny anonymous FTP access (off by default for security!), and FTP transfers can be logged for either anonymous or password-based accesses.

7.2.1 Anonymous

The Anonymous check box enables or disables anonymous FTP access. When a user accesses the iTools system via anonymous FTP, the iTools FTP server automatically places that user in a special FTP user directory (/Users/ftp/).
Anonymous FTP users are thus restricted from accessing any other directories on the system.

The FTP directory generally contain some default sub-directories which provide different kinds of access to the anonymous FTP clients.

The pub directory is the generic placeholder for documents targeted for public consumption. Anonymous FTP users can get files from this directory, but they cannot put files into this directory, or modify any files within this directory. Generally the iTools administrator controls the organization

and contents of this directory. However, password-based FTP users can place files in this directory if their FTP Home directory is either All iTools directories or Anonymous FTP.

The hidden directory provides a level of security by obscurity. Anonymous FTP users cannot list or see any of the files within this directory, but if they know the exact name of the file they are looking for, they can get that file from this directory.

A hidden directory is created by using the command “makedir dirname" to create the specified directory dirname and then the command chmod 511 dirname to set permissions on the directory which will not allow listing of the folder by anyone except the root user.

The incoming directory provides a place for anonymous FTP users to put files on this server. Generally these files are deposited here for consumption by the administrator of the iTools system. Anonymous FTP users cannot list or see the files in the incoming directory, so other anonymous FTP users cannot get a file deposited by a different FTP user unless they know the exact name of that file.

An incoming directory is created by using the command “makedir dirname" to create the specified directory dirname and then the command chmod 733 dirname to set permissions on the directory which will not allow listing of the folder by anyone except the root user, but will allow anyone to upload to it.

7.2.2 User-Pass

The User-Pass checkbox enables or disables password-based FTP access. When a user accesses the iTools system via an FTP user name and password, the iTools server automatically places that user in the directory indicated by the FTP Home setting for that user.

Password-based FTP users can read or write files into the directories to which they have access.

7.2.3 Limit

The Limit setting controls how many simultaneous sessions the iTools FTP server will permit for each class of FTP service. Subsequent attempts to FTP into the server will be denied when this limit is reached. A message is provided to the FTP client that the limit has been reached and that they should try again later.

7.2.4 Logging

The Logging checkbox controls whether or not FTP transfers are logged for each class of FTP service. The iTools FTP server logs FTP transfers in the /Library/Tenon/FTPServer/Logs/ftp.log file. The contents of this file

can be viewed by clicking on the FTP Log button in System Status under sub-menu Log Report.

7.3 Advanced FTP Settings

7.3.1 Server Admin

The Server Admin directive sets the email address of the administrator for the server.

7.3.2 Port

The Port directive configures the TCP port which proftpd will listen on.

7.3.3 Passive Port Range

Passive Ports restricts the range of ports from which the server will select the PASV command from a client. The server will randomly choose a number from within the specified range until an open port is found. Should no open ports be found within the given range, the server will default to a normal kernel-assigned port, and a message logged.

The port range selected must be in the non-privileged range (eg. greater than equal to 1024); it is STRONGLY RECOMMENDED that the chosen range be large enough to handle many simultaneous passive connections (for example, 49152-65534, the IANA-registered ephemeral port range).

7.3.4 Login Timeout

The Login Timeout directive configures the maximum number of seconds a client is allowed to spend authenticating. The login timer is not reset when a client transmits data, and is only removed once a client has transmitted an acceptable USER/PASS command combination.

7.3.5 Idle Timeout

The Idle Timeout directive configures the maximum number of seconds that proftpd will allow clients to stay connected without receiving any data on either the control or data connection. If data is received on either connection, the idle timer is reset. Setting Idle Timeout to 0 disables the idle timer completely (clients can stay connected for ever, without sending data). This is generally a bad idea as a hung TCP connection which is never properly disconnected (the remote network may have become disconnected from the Internet, etc) will cause a child server to never exit (at least not for a considerable period of time) until manually killed.

7.3.6 No Transfer Timeout

The No Transfer Timeout directive configures the maximum number of seconds a client is allowed to spend connected, after authentication, without issuing a command which results in creating an active or passive data connection (i.e. sending/receiving a file, or receiving a directory listing).

7.3.7 Stalled Transfer Timeout

The Stalled Transfer Timeout directive sets the maximum number of seconds a data connection between the proftpd server and an FTP client can exist but have no actual data transferred (i.e. stalled). If the seconds arguments is set to 0, data transfer are allowed to stall indefinitely.

7.3.8 Command Buffer Size

The Command Buffer Size directive controls the maximum command length permitted to be sent to the server. This allows you to effectively control what the longest command the server may accept it, and can help protect the server from various Denial of Service or resource-consumption attacks.

7.3.9 Allow Root FTP Login

Normally, proftpd disallows root logins under any circumstance. If a client attempts to login as root, using the correct password, a special security message is sent to syslog. When the Allow Root FTP Login directive is turned On, the root user may authenticate just as any other user could (assuming no other access control measures deny access); however the root login security messag is still written to the system log. Obviously, extreme care should be taken when using this directive.

7.3.10 Encrypted File Transfers: FTP (TLS/SSL)

The iTools 9 FTP server (proFTPD) utilizes an encryption layer called TLS (Transport Layer Security). TLS is very similar to SSL, only more secure. A toggle switch on the FTP Administration Page invokes the TLS directives in the proftpd.conf file.

7.3.11 "Enable TLS/SSL Operation" OFF

Unless you are absolutely certain that every person who will be using FTP on your server has a TLS-capable client, you should not change this. It is a system-wide switch; FTP (TLS) cannot be invoked on a user-per-user basis. The default ON setting allows unsigned certificates and all proFTPD ciphers. These defaults may be changed directly in the proftpd.conf file.

7.4 Additional FTP Capabilities

…The iTools FTP server (proftpd) has capabilities beyond those that are presented in the user interface provided by the iTools Administration Server. These features are configured by editing FTPs directives in the /Library/Tenon/FTPServer/Configuration/proftpd.conf file. The documentation for the ftpaccess file is available at:

http://www.proftpd.org/

8 File Manager

Using the File Manager, you can upload, create or delete files, organize files in folders, and change file permissions. The File Manager is not intended to replace any content creation tools you may be using, but it offers a simple way to make small changes on your site via the web, without having to use the Terminal application or a third party FTP tool.

Note: All of the other topics in this section assume that you are already in File Manager.

To open and navigate in File Manager:

- Click on the File Manager button on iTools Administration Server.

Navigate by using the following:

- Open a folder by clicking on the folder icon.
- Use the path links at the top of the window to move up and down the path.
- Select a folder or a file, so as to view or modify its properties, by clicking on the name link.

8.1 Creating a new folder

Folders are a very useful way of adding organization and structure to your web site. They make maintenance of the site much easier, as you can easily see what files are in which folder. Most web sites include at least an /image folder to keep all the image files separate from the HTML files.

To create a new folder:

Navigate to the area in which you will create the new folder.

Click on the Create New Folder link.

Enter the name of the new folder in the available text field of the File Manager.

Press Enter and your system will create the specified folder.

8.2 Uploading files in File Manager

Using the File Manager:
Navigate to the folder where you want to upload your files.
Click on the Choose File button.
Search for and double-click on the file to upload.
Click on the Send button to upload the file when you have finished selecting the file. The contents of the folder is displayed in the main area, including your uploaded files.

8.3 Changing file/folder permissions

All files on UNIX (including Linux and other UNIX variants) machines have access permissions. These tell the operating system how to deal with requests to access these files. There are three types of access:

Read - Denoted as r, files with read access can be displayed to the user.

Write - Denoted as w, files with write access can be modified by the user.

Execute - Denoted as x, files with execute access can be executed as programs by the user.

Access types are set for three types of user group:

Owner Flags - The owner of the file.

Group Flags - Other files which are in the same folder or group.

Others Flags - Everyone else.

The web server needs to be able to read your web pages in order to be able to display them in a browser. The following permissions need to be set in order for your web site to function properly.

All HTML files and images need to be readable by others. The setting for this is rw-r-r- (readable by User, Group, and World, and writable by User), and is set automatically when you upload files.

All folders need to be executable by others. The setting for this is rwxr-xr-x (readable by User, Group, and World, writable by User, executable by User, Group, and World), and is set automatically when you create a folder.

All CGI files (all files in the cgi-bin folder) need to be executable by other. The setting for this is rwxr-xr-x (readable by User, Group, and World, writable by User, executable by User, Group, and World), and is not set automatically when you upload files. You need to change file permissions manually.

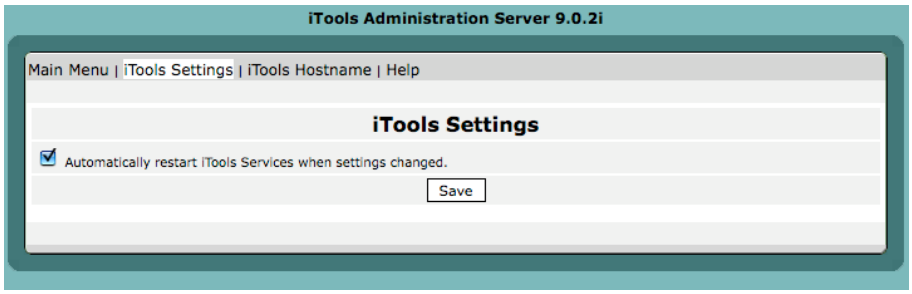
Warning: It is important that none of your files or folders are writable by anyone else. Any file or folder which is writable by others can be erased by them. Generally there is no problem, just be careful how you set your permissions.

To change file or folder permissions:

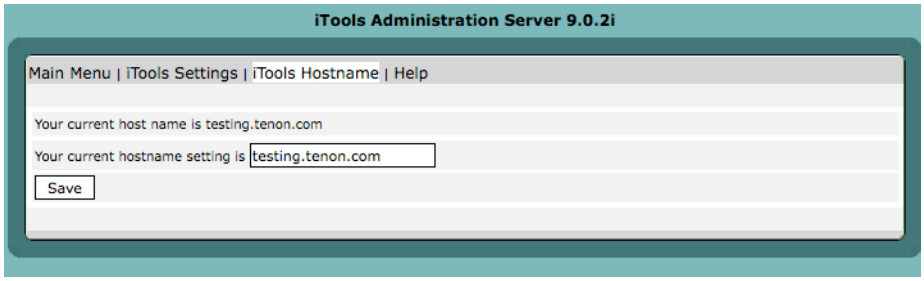
Navigate to the file or folder that you need to change.
Click on the name of the file or folder.
Click on the pull down menus for changing Owner Flags, Group Flags, or Other Flags. The permission will update automatically.

9 iTools Settings

iTools configuration settings are global. When the automatic restart option is checked, a particular service (e.g. Apache) will restart whenever a configuration change mandates a restart. Alternatively, the iTools administrator can choose to restart services manually after all the settings are properly configured.

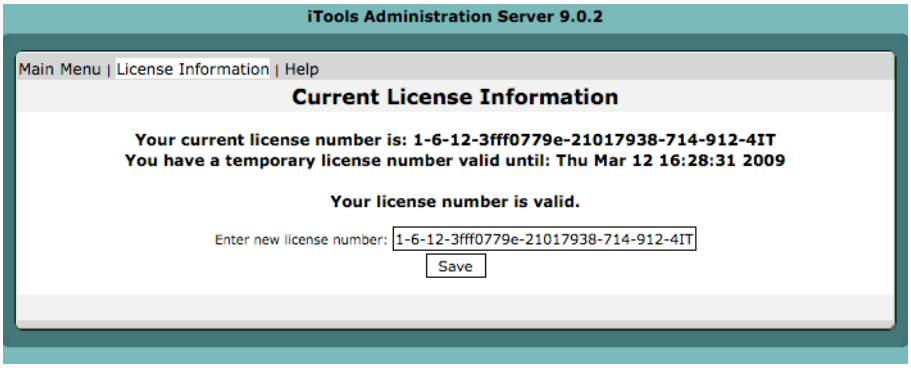


Use the "iTools Hostname" form to set the hostname for your system. This information will be saved in the /etc/hostconfig file.



10 License Information

To change the license, enter your permanent license in the text field, being careful to observe case sensitivity, and click “Save". The license program will return information about the validity of the license you have entered, and for what time period it remains valid.



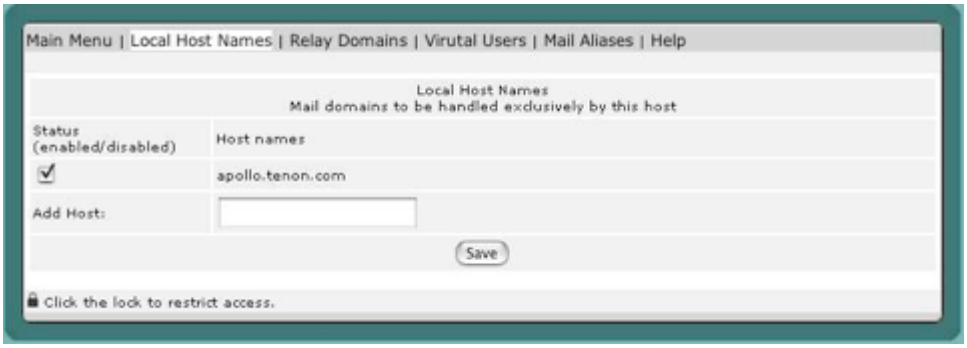
11 Mail Settings

The Mail Settings control the configuration of Apple's in-place sendmail or Postfix mail server or, if Tenon's Post.Office is installed, will take the user to the Post.Office administration screen. Clicking on the Mail Settings button in the Administration Server home page will bring up the Mail Settings screens. Note that a mail server is not part of iTools, but that the Mail Settings screen is just a convenience to allow minimal configuration of the mail server that came with whatever version of Mac OS X you are running.

11.1 Sendmail/Postfix Configuration

11.1.1 Local Host Names

The Local Host Names table should contain an enabled entry for every Host-name that the mail server should accept mail for. These host names correspond to the part after the "@" sign in an email address.



Enabled entries are added automatically for any virtual host added in the Virtual Host Configuration table. iTools will not automatically enable entries for a domain name added as a virtual host in order to avoid conflicting with established mail servers.

To manually add a host name, enter it into the Add Host: field at the bottom of the table. The host name will be enabled by default, but can be disabled

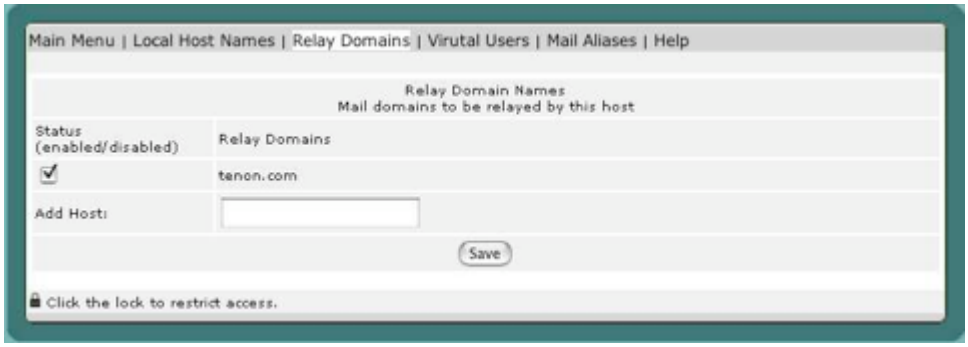
by unchecking the Status check box. Host names should be disabled if other servers are supposed to accept mail for those hosts names.

The iTools server can accept email for any domain name or host as long as the DNS is configured with the appropriate MX record. See section “Changing MX Records" on page 38 for details on MX records.

11.1.2 Relay Domains

The Relay Domain Names table can be configured to include any domain names, host names, or IP addresses for which the mail server should relay mail to those destinations. Any mail that is sent through the SMTP server, which is not to be delivered to a local account is considered to be relayed. Since relaying can be used to hide the identity of senders of unsolicited “SPAM" mail, relaying is disabled in iTools by default.

In general, clients should use their ISP’s SMTP server for relaying mail. If this is not possible, or you are acting as the user’s ISP, the domain name, Hostname, or IP address of the client’s machine may be entered in the Add Host: field of the Relay Domain Names table. Click on the Save button to save the added host.



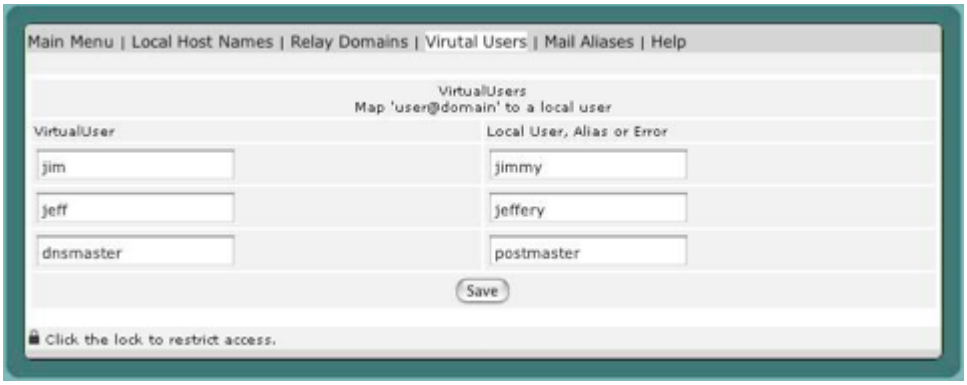
11.1.3 Virtual Users

Virtual users should be configured in situations where fake e-mail addresses are needed to deliver to real accounts. If a mail account were alredy established on the server for the user “support”, they would not need an entry. That user would automatically get mail for the e-mail address support@ all of the enabled Local Host Names.

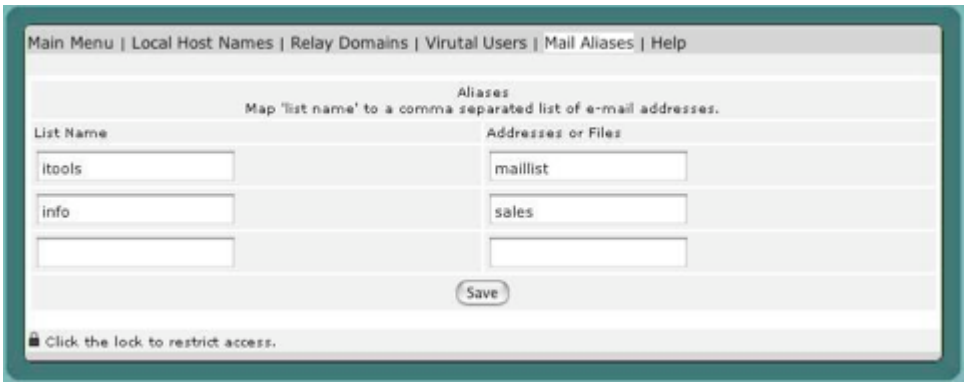
If the user “support" requested that their account also receive all of the mail for “help@localhostname", but there is no “help" account established (or it is in use by another client), help@localhostname should be added in the Virtual User column, and support would be added the Local User column.

The pull down menu is added as a convenience to list the Local Host Names for the server, but does not need to be used to add a virtual user.

In the event that different domains need separate accounts for the same user name, virtual users would be added for both of the domains and would be mapped to accounts with different names as in the example figure below.



A "catch all" account may also be configured for a domain using the Virtual Users table. This account will receive any mail for the specified domain regardless of the address. "@domain.to.catch" would be entered in the Virtual User field, and the account name to receive the mail would be listed in the Local User field.



Virtual users can be used in conjunction with Mail Aliases for a very powerful control of your mail server.

11.1.4 Mail Aliases

Mail Aliases can be used to set up simply mailing lists or for redirecting emails to programs on the server. A list of email addresses can be entered in the Addresses or Files field, or a path to a file containing a list of e-mail addresses can be entered there. The List Name field would receive the

name of the fake user that the mail would be sent to. Again, this user does not need to have a mail account on your server, it just represents what email address the list mail would be sent to.

11.2 Post.Office Configuration

If Post.Office is installed on the same machine as the iTools, then mail administration is forwarded to port 9090 of the same server. Tenon recommends Post.Office for all mail needs. Post.Office is a powerful mail server and list sever for Mac OS X with features not available in either sendmail or Postfix. All configuration and management is done using a browser-based GUI. Even though Post.Office is a proprietary mail server, it seamlessly supports CGIs that rely on “sendmail" and Post.Office is FREE for 5 mail accounts or less, so you can use the FREE Post.Office to support webforms and scripts. Please refer to Post.Office Administration Manual for Post.Office mail administration.

12 Traffic Monitor

Traffic Monitor provides non-stop monitoring of your server and all its key elements. When there is a problem, you will be the first to know, so you can begin trouble shooting before your customers call you. You will be able to evaluate your web site performance from your customer's perspective and optimize it to improve customer satisfaction.

12.1 Web Traffic Monitor

The Web Traffic Monitor will plot the number of http requests in the most recent five minutes. The intervals are sampled every 10 seconds. The Web Traffic monitor will keep up to four different monitor connections alive, therefore you should always subtract four from the number of requests to your website.

12.2 FTP Traffic Monitor

The FTP Traffic Monitor will plot the number of FTP requests in the most recent five minutes. The intervals are sampled every 10 seconds.

12.3 Mail Traffic Monitor

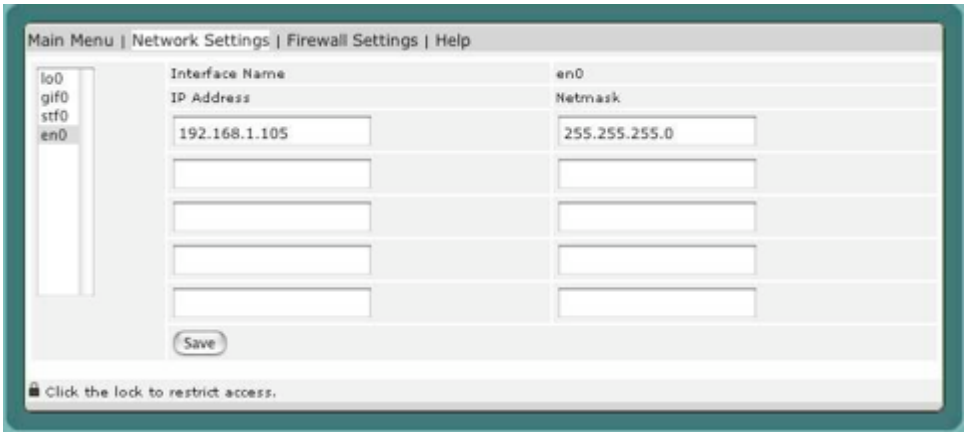
The Mail Traffic Monitor will plot the number of FTP requests in the most recent five minutes. The intervals are sampled every 10 seconds.

13 Network

The Network Settings panel provides network card management and firewall management. Network Settings lets you configure your network cards (for example, your computer's Ethernet card). Firewall Settings lets you set up filters to block unwanted network communication.

13.1 Configure IP Addresses

Clicking on the Network Settings button in the Administration Server home page will bring up the Network Settings Screens. Clicking on Network Settings will let you assign IP addresses to the various machine interfaces. The list of interfaces on the left are the network interfaces currently detected on the system. In general, IP addresses will bind to the Ethernet interface (en0, en1, . . .).



The IP address is the 32-bit Internet host address, de ned by the Internet Protocol in STD 5, RFC 791 and usually represented in dotted decimal notation,

e.g. 128.121.4.5. The address can be split into a network number (or network address) and a host number, unique to each host on the network, and sometimes also a subnet address. The way the address is split depends on its class , A, B or C as determined by the high address bits:

Class A - high bit 0, 7-bit network number, 24-bit host number. n1.a.a.a
0 <= n1 <= 127

Class B - high 2 bits 10, 14-bit network number, 16-bit host number.
n1.n2.a.a 128 <= n1 <= 191

Class C - high 3 bits 110, 21-bit network number, 8-bit host number.
n1.n2.n3.a 192 <= n1 <= 223

The Internet address is usually provided by your network administrator or your Internet Service provider. If you don't have an IP address, you will have to contact them for an IP address available to use on your iTools server.

Netmask is a 32-bit bit mask which shows how an Internet address is to be divided into network, subnet and host parts. The netmask has ones in the bit positions in the 32-bit address which are to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion (as determined by the address's class), and the subnet field should be contiguous with the network portion. Contact your network administrator or Internet Service provider for the correct netmask to use with your IP address.

The stf interface supports "6to4" (IPv6 in IPv4 encapsulation). It can tunnel IPv6 traffic over IPv4, as specified in RFC 3056. IPv6 is a newer IP protocol specification (RFC 2460), a "next generation" IP, with expanded addressing capabilities (128 bits, instead of 32 bits).

The gif interface is a generic tunneling pseudo device for IPv4 and IPv6. It can tunnel IPv[46] traffic over IPv[46]. Therefore, there can be four possible configurations. The behavior of gif is mainly based on RFC2893 IPv6-over-IPv4 configured tunnel.

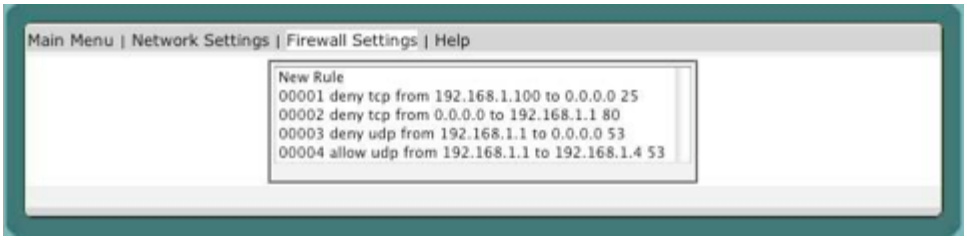
Both stf (six-to-four tunnel interface) and gif (generic tunnel interface) network settings today will be rarely used.

13.2 Configure Firewall Filters

A firewall implements a strict set of rules to allow or deny certain connections to or from your computer. Without a firewall, any connection to your computer is allowed. The firewall software is part of the Mac OS X operating system, and by default lets everything through (which means it is as if you had no firewall).

Configuring your firewall means adding rules to permit only certain connections. The approach taken here is to explicitly allow only certain connections to and from your computer, while blocking everything else. This is by far the most secure configuration.

iTools Firewall interface allows you to filter on protocols, ports, or IP address. It gives you control via any browser over elements that would otherwise require UNIX command line access.



In the list of Firewall rules, the left most column is the firewall rule number, followed by policy of the rule, protocol, and source and destination of the rule. Selecting any rule will bring up the details about that particular firewall rule.

The firewall rule number is the look up order of the rules. The smallest number means the rule is the first one to filter; a network packet is passed through the list of rules before the firewall decides to deny or accept the network packet.

13.2.1 Policy

Allow	Allow packets that match rule. The search terminates.
Deny	Discard packets that match this rule. The search terminates.

13.2.2 Protocols

TCP or UDP protocol to filter

13.2.3 Ports

With the TCP and UDP protocols, optional ports may be specified as:

Port	A single port, for example: 80 is the HTTP port.
Port-Port	A range of ports, for example: 250-260

13.2.4 Source & Destination

Specifying “any" makes the rule match any IP number.

ipno:	An IP number of the form 1.2.3.4. Only this exact IP number will match the rule.
ipno/bits	An IP number with a mask width of the form 1.2.3.4/24. In this case all IP numbers from 1.2.3.0 to 1.2.3.255 will match.
ipno:mask	An IP number with a mask of the form 1.2.3.4:255.255.240.0. In this case all IP numbers from 1.2.0.0 to 1.2.15.255 will match.

13.3 Checklist

Here are some important points to consider when designing your rules:

• Remember that you filter both packets going in and out. Most connections need packets going in both directions.

• Remember to test very carefully. It is a good idea to be near the console when doing this. If you cannot be near the console, use “sudo ipfw flush" to flush the firewall via SSH access.

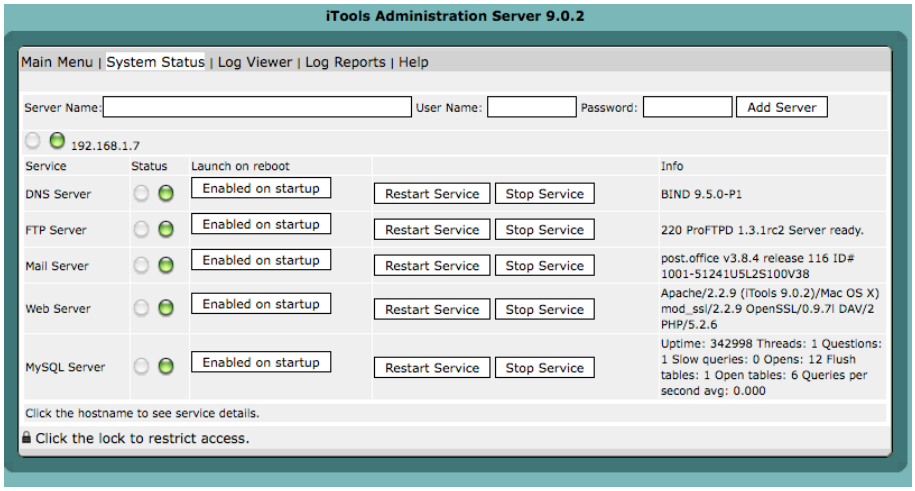
• Don’t forget the loopback interface.

14 System Status

14.1 Monitoring Server Status

The System Status provides some useful information about the current state and version numbers of the various iTools services. The buttons on the System Status page provide a means for the iTools administrator to examine and control certain aspects of the server.

The System Status page first checks on the current state of the various services. If a particular service is active, the status column shows green light and its version number is displayed in the rightmost column of the table; otherwise a red light appears in the status column and unavailable appears in the Info column.



14.1.1 Launch on Reboot

The Enable On Startup button can toggle the service to launch when the computer is rebooted.

14.1.2 Restart Service

Clicking on this button will cause the service to completely restart its operation. If the service is currently running, this button will shut down the service, and restart it again. If changes are made directly to the services configuration files, it is necessary to restart the services in order for these changes to take effect.

14.1.3 Stop Service

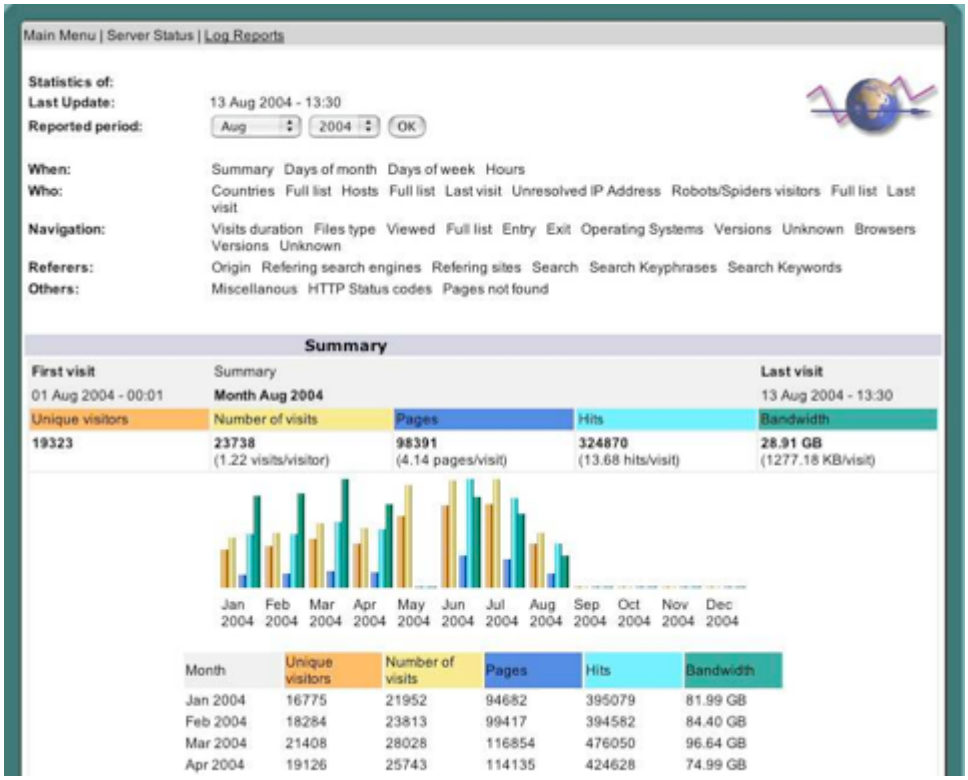
If the service is active, clicking on this button will stop the service.

14.2 Log Reports

The Log report screen creates summary reports of Web and FTP traffic logs statistics. This allows an administrator to keep an eye on the server, even from a remote location.

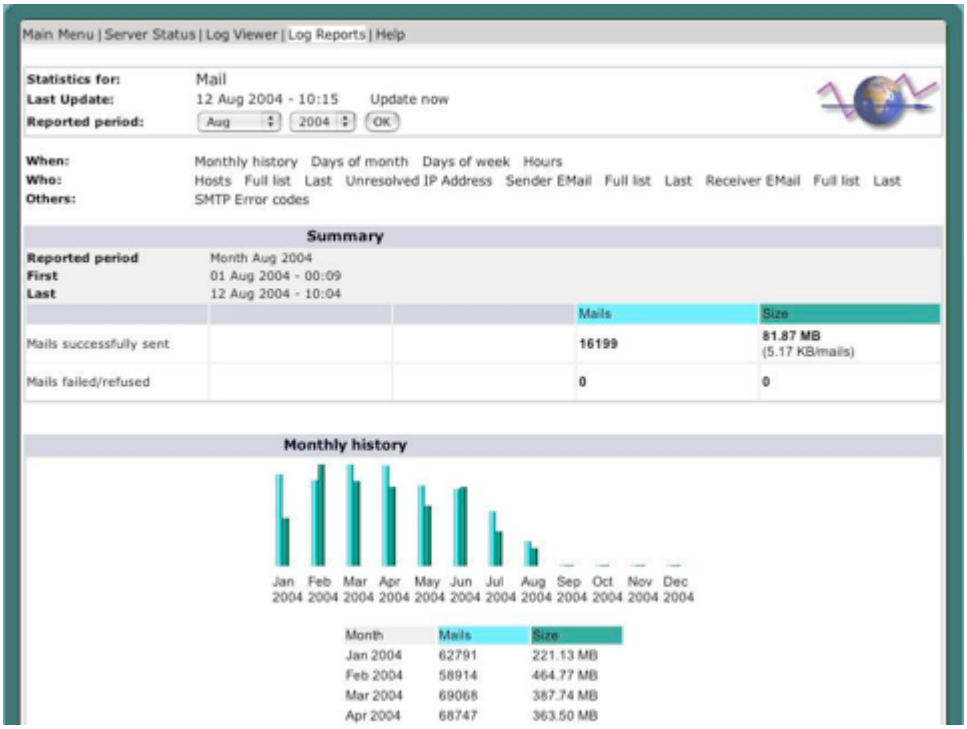
14.2.1 Web Log Report

When a virtual host is created, the virtual host will display in the pull down menu for the Web Log Report. Select the virtual host to see its statistics report.



14.2.2 Mail Log Report

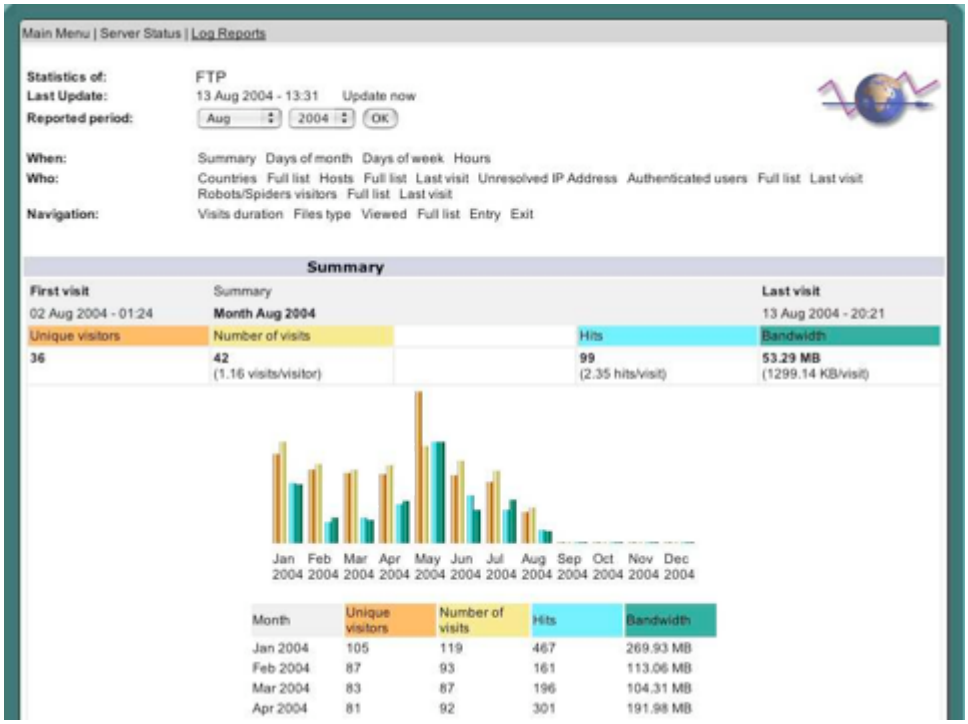
Mail Log Report reports the summary of all the Mail SMTP activities on the server.



Mail Log report works with log files from sendmail, Postfix, and Post.Office.

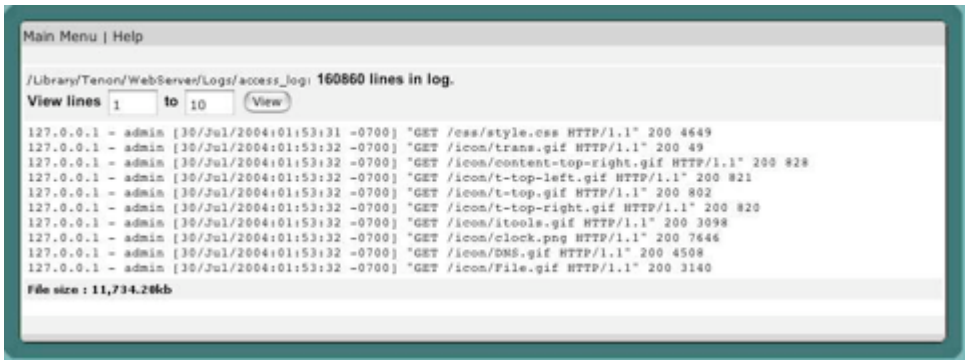
14.2.3 FTP Log Report

FTP Log Report reports the summary of all the FTP transfer activities on the server.



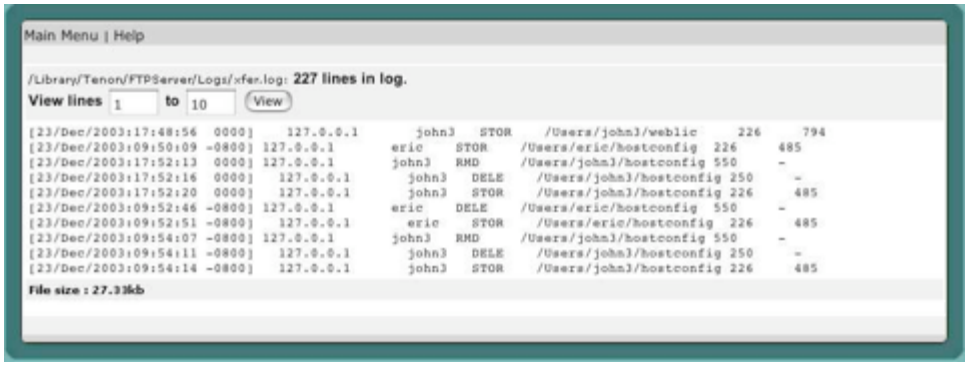
14.2.4 Raw Web Logs

The Raw Web Logs pull down menu contains a list of the web log file from /Library/Tenon/WebServer/Logs. This function will display the entire log file, therefore, you need to be careful about using this feature with large log files.



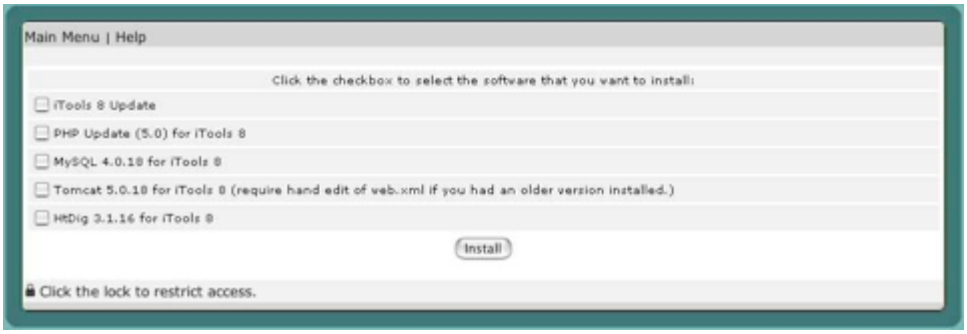
14.2.5 Raw FTP Logs

The Raw FTP Log pull down menu contains a list of the default FTP log Files from /Library/Tenon/FTPServer/Logs. This function will display the entire log file, therefore, you need to be careful about using this feature with large log files.



15 System Update

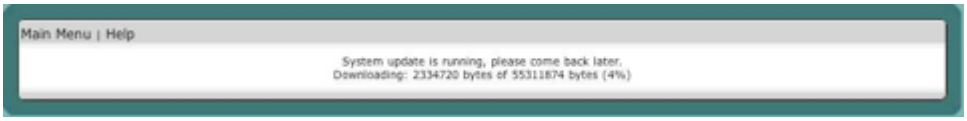
Periodically,Tenon releases updates to iTools. Using the System Update feature, you will be able to get iTools updates immediately.



If you don't see an update, this means your system is up-to-date with the most recent iTools packages.

If your computer is on a network and System Update is reporting: Not Found, the network may not be able to access the Internet or your computer may not be allowed to access Internet locations. You can still download the latest iTools update packages explicitly from Tenon's web site.

When you select the package to update, the system will push the system update to a background job. You may want to check back later to make sure that the update has been completed.



After the update is completed, it is highly recommended that you reboot the server to ensure that all the latest modules are initialized.

16 Users & Groups

16.1 iTools Users vs. System Users

Users on your server can be empowered with different kinds of privileges, which may include:

- Administration of the Mac OS X System settings.
- Access to the server with desktop and other displays for that specific user.
- Logging on over the network via telnet or ssh.
- FTP access to exchange files with the server.
- Access to electronic mail via the E-mail server.
- Access to browse, upload or publish web pages.
- Ability to administer a sub-domain on your web server.

While a System user that has been added via the System Preferences may have all of these abilities, iTools users are designed to be restricted to certain types of access, thus reducing a server's exposure to a potentially dangerous user. There are several classes of iTools users that offer subsets of the above capabilities.

iTools users are created in the Administration Server while System users are created in the system user database. While certain iTools users will show up in the system user database, they will be marked as iTools users and should not be edited there. The names of System users may be added into the Administration Server to give them access to realms, but some settings, including their home directory, may not be edited in the Administration Server.

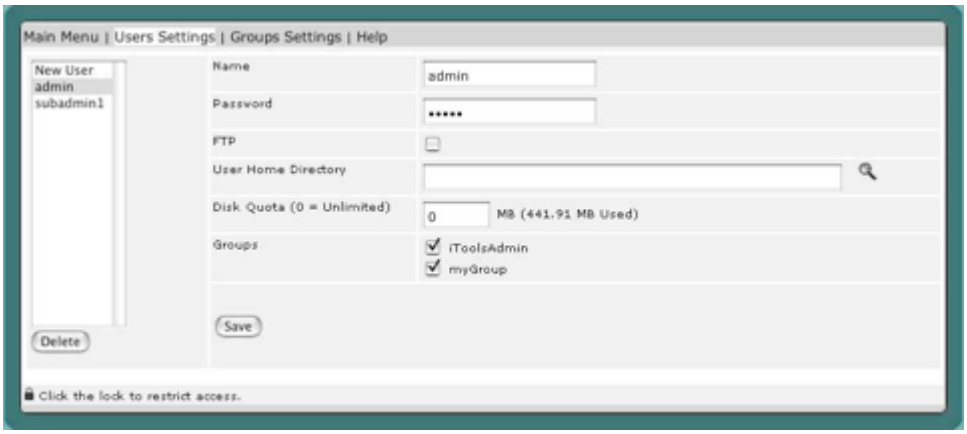
Tenon's iTools provides a set of realm-based access controls that can restrict access to a particular file or directory based on user names and passwords (see section "Realm Based Restriction" on page 111 for details on realms). Tenon's iTools also provides FTP service based on user names and passwords. User

names and passwords for both realm-based access controls and FTP service are entered in the Users table.

iTools User Types	Description
Normal	If a user is not FTP capable, he or she has no Mac OS X privileges. These users can be configured to administer the Tenon's iTools Administration Server (see section "The iTools Admin Group" on page 83), or simply be allowed to log into realm protected directories via a web browser (see section "Realm Based Restrictions" on page 111).
FTP	If an iTools Admin user is listed as an FTP user, enough of a user environment is created to provide for the transmission and receipt of file data, but with significant limitations. An FTP user is not allowed normal 'timesharing' login. While the username and password may be recognized as a successful login, the user's session is immediately terminated, as if the user logged in and immediately logged out. In addition, when a user is designated as an FTP user, login to the Mac OS X Server's FTP server causes the user's home directory to be set to the directory specified when the user was created in the Administration Server. This means that the user's ability to move around a file system is strictly limited to the directory that he or she is logged into and the directories below. If IMAP-iPOP3 Module is installed, iTools users with FTP access will also be granted access to send and receive mail using POP and IMAP servers.
System User Types	**Description**
Admin N.B. The user "admin" has special capabilities. Do not delete this user (but do change the password) and do not give this user FTP privileges. This user is the supreme administrator of the iTools system and will have privileges that other users in the iTools Admin group do not have.	User has all the login capabilities (including email and FTP if those services are enabled) and can administer system settings on the server. Admin users are members of the iTools Admin group.
Normal	User has all the login capabilities (including email and FTP if those services are enabled) but cannot administer system settings on the server.

16.2 Users

The Users table contains all of the data for adding and configuring iTools users. It is accessible by clicking the User Settings from the iTools Admin Server home page.



16.2.1 Adding Users

To enter a new user name and password, type the user name into the empty text field in the first row of the table in the Name row. Type a corresponding password into the second text edit field. The password will not be displayed as it is typed. Instead, bullet characters will be displayed (so type carefully). Click the Save button to submit the new user name and password. You will have to save after adding each new user, before moving on to the next one you wish to add.

For each user, check the boxes for FTP if you wish to enable FTP. A user without FTP checked would have web page access only.

Click on the FTP checkbox to enable FTP access for this user. If FTP access is enabled, select an FTP Home for this user. The FTP Home is the directory that this user will be given access to when they FTP into iTools.

When logging in via FTP, users will be placed directly into their de ned root directory (folder). They will have access to that folder and all sub-folders within it. They will not be able to move to a higher (parent) directory above their root directory.

Using the pop-up menu FTP user's root folder can be set to:

- Restricted to access only a particular virtual hosts root folder

(/var/www/)

- The anonymous FTP hierarchy (/home/ftp)
- Access to all of the virtual hosts root folders
- All of the iTools directories, including the anonymous FTP hierarchy

Using the text edit field, a path to any valid directory can be entered for this user's FTP root directory. If no FTP root directory is set for an individual user, the FTP access is disabled.

Adding a user with FTP enabled, creates a FTP only user in the Mac OS X

databases are not changed to FTP only. However, the system user password and home directory will be synchronized to be the same as defined in the iTools user database; be careful when adding FTP users with the same name as a system user.

Once a user name and password have been entered, the new entry will show up in the table in alphabetical order. FTP user root directories are shown as paths.

16.2.2 Changing a User

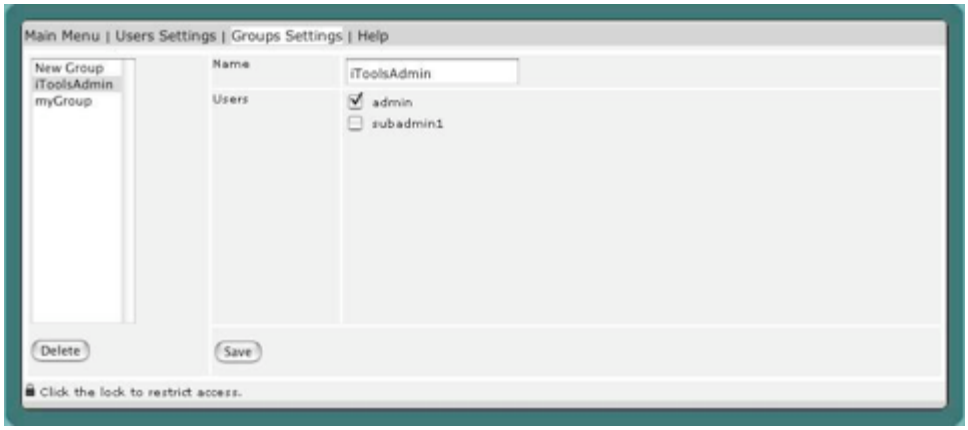
To change an existing user name, modify the password, type of access or FTP Home text field, edit the relevant entries and click Save to submit the changes.

16.2.3 Deleting a User

Select the user you wish to delete, and click Delete button to submit the changes. Under the system user database, the username listed for each iTools user is not very informative; therefore it is best to add, modify and delete iTools users from the iTools Admin Server.

16.3 Groups

iTools provides a set of realm-based access controls that can restrict access to a particular iTools service, file or directory based on groups of users (each user with their own password).



16.3.1 Creating a Group

To enter a new group, from the Admin Home Page, click the Group Settings button to move to the Group page. Type the group name into the empty

text edit field in the first row of the table. Click the Save button to submit the new group. Once a group has been entered, the new entry will show up in alphabetical order in the Groups table.

16.3.2 Users in Group

To select which users are to be members of a group, click on any group in the Group List column. The Users in the group will be selected from the Users table.

To select users for inclusion in a group, click on each username within the scrollable list of all users. To select multiple users, hold the <shift> key and click to select a series of users, or hold the <Apple> key (<control> key on non-Macs) to individually select any combination of users. When a user is selected for inclusion in the group, the user's name will be highlighted. Click on Apply to submit the selected users.

16.3.3 Modifying a Group Name

To change an existing group name, modify the text of the Name field and click Save to submit the change.

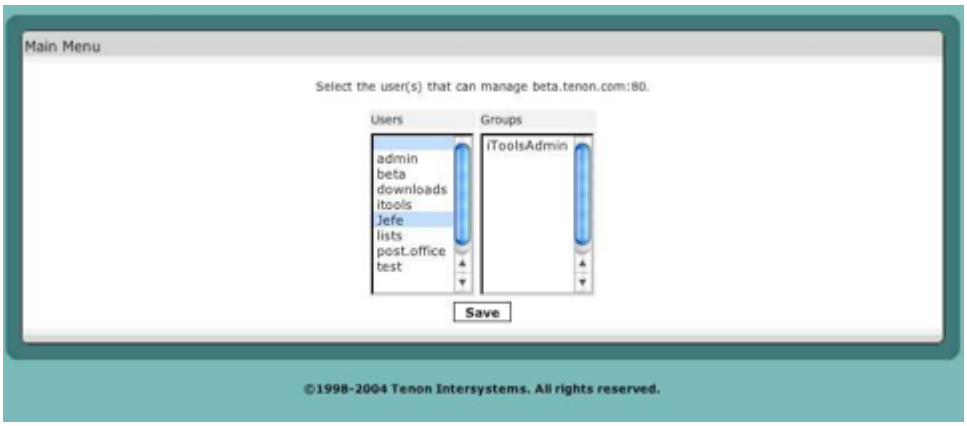
16.3.4 The iTools Admin Group

The iTools Administration Server uses a special group named iToolsAdmin. Members of this group are permitted access to all the iTools administration pages, and may make changes to the iTools configuration, including adding and deleting users and groups. If the iToolsAdmin group is deleted, or if this group is empty, access to the iTools Administration Server is completely cut off . In this case, use the Admin menu item in the iTools application and follow the instructions to add an initial user to this special iToolsAdmin group.

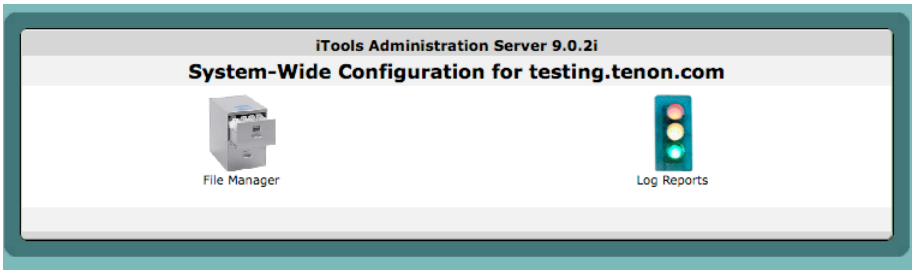
16.4 iTools Sub-Administration

To take advantage of the sub administrator features of iTools 8 you simply need to create a user (or group) in iTools and grant them access to certain parts of iTools. Once the user has been created in iTools you can go to the page that you want that user to have access to and click on the little lock icon for restricting access to that page:

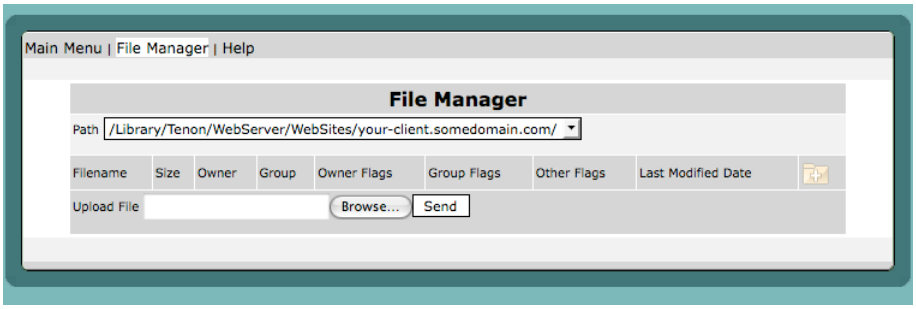
This will bring up a screen where you can select which users have access to that page:



After granting access to the portions of iTools allowed for that particular user, close your browser and head back to your iTools Admin. This time, instead of logging in as "admin", login as the user you created above. Now, instead of seeing all of the icons that you would normally see, you will only see the subset that this user has access to.



This user was given access to his own Log Reports. Clicking on the Log Reports icon will only display the Logs from his virtual host. As a default, the user is also given access to File Manager which will allow upload access only to his virtual host.



If access to a virtual host was granted to the user, then they will only see the virtual hosts that they have access to edit when they click on web settings.

If the user tries to access something that they do not have permission to access, such as network settings for a network interface that they were not assigned access to, then they will be shown an error informing them that they do not have enough privileges.

NOTE: Only the user named “admin” has the ability to create sub-administrators.

17 Web Settings

17.1 Virtual Host

Apache provides the capability to support multiple servers on a single machine. Each server is differentiated by a unique host name. This feature is called virtual hosting. For example, it is often desirable for companies sharing a web server to have their own domains, with web servers accessible as http://www.company1.com and http://www.company2.com, without requiring the user to know any extra path information.

Virtual hosts can have unique IP numbers called IP-based virtual hosts, or they can share an IP number and use host name information that is included in the header sent from browser to server in each request. You can combine these styles of virtual hosting as well.

Early browser versions didn't support inclusion of host header information (meaning that header-based virtual hosting didn't work with those browsers), but very few browsers in use today have this limitation. iTools has a setting in the virtual host configuration to insure proper redirection for browsers lacking host header support.

17.1.1 Virtual Host Table

From the browser Administration home page, click Virtual Hosts to access the Virtual Hosts Table. This table lists, alphabetically, the virtual hosts configured on this server.

Initially, this table will include a single virtual host, which is the DEFAULT host, and it is the global settings for virtual hosts.

17.1.2 Default Virtual Host

The DEFAULT virtual host settings apply to incoming requests for any virtual host if the corresponding setting is not explicitly set with alternative information in the Virtual Host Configuration table for that host.

To set up a template for your new virtual hosts to inherit from you can go to Configuration for the DEFAULT Virtual Host and select "Virtual Host Defaults" from the menu. Any settings that you set in this form will be applied to all new virtual hosts.

17.1.3 Adding Virtual Hosts

Click the "Add. . . " button to enter additional virtual host names. Simply type the new virtual host name into the empty text edit field below Server Name. Select an IP Address or specify one in the text field. Click on the "Add Virtual Host" button to submit your new virtual host entry.
The new Hostname must be properly configured with your Domain Name Server (DNS) and IP address from Network Settings before the virtual host becomes active. Each virtual host has a "Virtual Host Configuration" section. These sections are accessible via the Configuration button.

17.1.4 Arrange Virtual Host Priority Order

When a client is contacting the web server using an IP address instead of the virtual host name, the web server has to determine which virtual host to serve to the web browser. When multiple virtual hosts are using the same IP address, the server will choose the virtual host that has the highest priority to serve. The virtual host at the top of the list has the highest priority. Select "Arrange Order" to change the Virtual Host priority. Clicking Up and Down changes the serving order of the virtual host.

17.1.5 Virtual Host Configuration

When a virtual host is added to the iTools configuration, the iTools Administration Server sets up an initial Virtual Host Configuration for the new virtual host. Initially, some of these settings are inherited from the DEFAULT virtual host.

Each virtual host is assigned a root directory (folder), which will contain the web pages for that host. Browser requests with a URL containing the virtual host name are mapped to the corresponding directory, and the index file in the root directory for the host will be served.

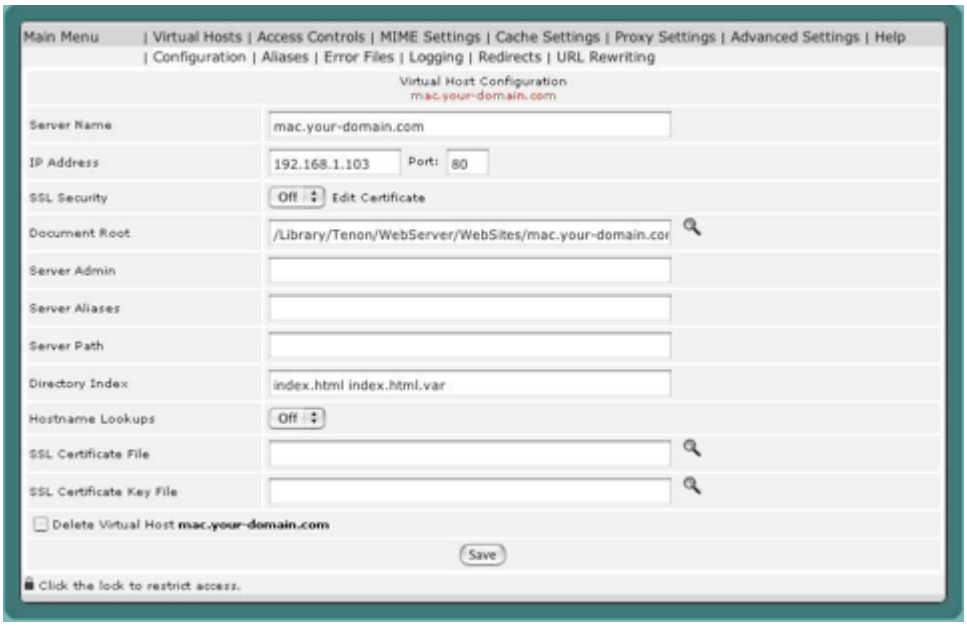
By default, iTools automatically creates a new, empty, directory for each new virtual host created. The name of the directory will match the name of the host that has been created. This directory is called the "document root" and is the repository for that virtual host's content.

The root folder does not need to have the same name as the fully qualified hostname for the virtual host; you can call it whatever you like, but be sure to enter the correct folder name in the DocumentRoot field.

The server settings ensure that browser requests for a particular virtual host are directed to the correct root folder for that host and that pages for other hosts won't unintentionally be accessed.

To access the Virtual Host Configuration table, click the Configuration button beside the name of the virtual host you wish to configure.

To change the virtual host settings, modify an existing setting or group of settings and click on the Save button.



17.1.6 Server Name

The Server Name entry displays the name of the virtual host to which the following settings apply. It is the same name that was entered in the new Virtual Hosts Table. It also includes the IP address and TCP port for this host.

The Server Name setting corresponds to the host name of this server. It is only used in redirection URLs. Internal redirects can happen if a URL request representing a directory lacks the trailing "/". Redirects may also occur after CGI processing.

If the Server Name setting is not set for a virtual host, a reverse DNS lookup of the server's IP address is used. This reverse DNS lookup may not return the desired host name.

17.1.7 SSL Security

An SSL security package is installed with the core iTools package. SSL is disabled for each virtual host by default. Once a Server Certificate has been generated, SSL may be enabled by setting SSL Security to On.

17.1.8 Document Root

Document Root controls which directory will be used as the root directory (folder), for this virtual host's content. When a new virtual host is added, a directory with the same name as the virtual host is automatically created within the WebSites directory. The Document Root entry is set to the name of this directory.

Place the content files to be published for this virtual host in this directory. If Document Root is not set, the default Document Root setting from the DEFAULT virtual host will be used.

If you have three virtual hosts configured, www.some-domain.com, www.your-domain.com and your-domain.net, the following directories (folders) will be created:

/Library/Tenon/WebServer/WebSites/www.some-domain.com

/Library/Tenon/WebServer/WebSites/www.your-domain.com

/Library/Tenon/WebServer/WebSites/your-domain.net

If you change the name of the virtual host's directory or decide to use some other directory, make the corresponding change to the Document Root setting for this virtual host. In the above example, www.your-domain.com and your-domain.net might actually be the same web site, in that case, you would place all content in a single folder, and would need to make sure the Document Root for each host pointed to the correct directory containing that site's content.

17.1.9 Server Admin

The Server Admin setting is an email address. This address is included in messages sent to a browser whenever a web server error occurs. Users are encouraged to, and typically do, use this address to notify Web masters of any problems they are experiencing with a web server. The email address should be an existing account on some email server.

In the case of a virtual host, the Server Admin setting is inherited from the DEFAULT virtual host by default. Many Web sites follow the convention of using an email address “webmaster@virtualhost". It’s generally a good idea for this address to be to a person who can x problems that arise with that host’s web site or the server itself. Be sure this field contains a valid email address.

17.1.10 Server Alias

The Server Alias denotes which alternate host names should also apply to this virtual host. It is used with host header-based virtual hosts. The DEFAULT Virtual Host does not include a setting for Server Alias, so if the Server Alias is not set, no alternate host names will apply to this virtual host. Note that you can change the DEFAULT Virtual Hosts entries and the new settings will be inherited by all Virtual Hosts on that server.

Adding the IP number for this host to the Server Alias field will ensure that requests made to the IP address will go to this host; this defines a “primary" or “default" host for the server for this IP address.

Generally, if users added the virtual host in question as “your-domain.com", they will list “www.your-domain.com" in the Server Alias to ensure that users accessing either Hostname in their web browser will get the same content. If the virtual host was added as “www.your-domain.com", “your-domain.com" would be added here instead.

17.1.11 Server Path

In some cases, a web site previously accessed via a non-virtual host URL on this server, such as

http://www.your-domain.com/some-small-business/

wishes to convert to a real virtual host. Once the proper DNS entries and domain registration occur, the virtual host some-small-business.com can be created.

But what happens to requests for the old, legacy URL? The Server Path field can direct the request to the correct place. This field is also used when the Web server receives a request from a browser incapable of supporting host header-based virtual hosts.

If this virtual host’s home page was previously accessible via a non-virtual host URL, like the example above, the old, or legacy file path portion of the URL, is entered here. Otherwise, this path should be blank.

The Server Path is set initially to a path beginning with a slash (“/") followed by the virtual host name (e.g., /your-domain.com).

17.1.12 Directory Index

The Directory Index setting controls which file is returned when serving a request for a URL that points to a directory, rather than a request for a

specific page. This may be what you want, for example, for a directory of downloadable files. This includes a request for the main page of a website, or those URLs ending with a trailing “/".

Examples:

http://your-domain.com

http://your-domain.com/support/

Requests not ending in a “/", for example, http://your-domain/support result in the server attempting to locate a file by the name “support" (in this example). When the server fails to find a file by that name, it does an internal redirect, changing the URL to add the trailing slash, and attempts to locate a directory (folder) by that name instead.

When such a request is made, the Directory Index filename is added to the end of the URL, pointing the client request to a default file or CGI for that directory. In iTools, the default index filenames are “index.html" and “default.html". Additional index filenames can be added to the list, with a space entered between each. This list is searched in order from left to right for a file with the corresponding name in the directory. Other Macintosh servers use “default.html", while the typical Apache setting is “index.html". The iTools default is chosen to accommodate the Mac OS X web master in transition to Mac OS X.

If the Directory Index field is left empty, the contents of the directory will be listed on the returned page.

17.1.13 Hostname Lookups

The Hostname Lookups setting controls whether reverse DNS lookups are performed for each incoming request using the originator’s IP address. Enabling Hostname Lookups will generally increase the time necessary to satisfy each request, and thus increase the load on your server. However, without Hostname Lookups, Access Controls can be based only on IP addresses, not on host names or domain names. If Hostname Lookups is disabled, IP addresses will be used in the Apache access logs, but these addresses can subsequently be resolved into host names by your log analysis software.

17.1.14 SSL Certificate File

The SSL Certificate File is the name of the SSL server certificate for an IP-based virtual server. Individual SSL certificates require unique IP numbers, but host header-based virtual hosts can share the same server certificate. Multiple IP based hosts may also share a single “wildcard" certificate. This setting allows certificate “wildcarding" among several IP hosts. See Section 17.2, “SSL," for more information.

17.1.15 SSL Certificate Key File

The SSL Certificate Key file is the private key associated with the server certificate.

Keys generated by iTools during certificate signing request generation are normally stored in a secure area of the iTools internal file system; however, this field may be used for private keys of “wildcard" certificates or when a certificate and key are imported from another system.

Server certificates are stored in the directory:

/Library/Tenon/WebServer/Configuration/ssl.crt

17.1.16 Deleting Virtual Hosts

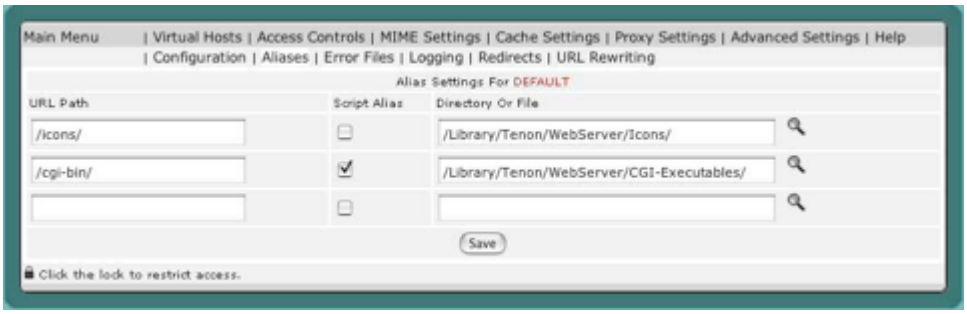
To delete virtual hosts from the Virtual Hosts Table, click on the Con guration button beside the virtual host you wish to delete. Select the Delete Virtual Host check box at the bottom of the Virtual Host Configuration table.

Click on the Save button to submit the changes.

The browser will return to the iTools Administration Server home page and the Virtual Hosts Table should no longer contain the deleted host name.

The DEFAULT virtual host (the one with the same virtual host name as the fully qualified domain name of the machine running the web server) does not have the Delete Virtual Host check box because it cannot be deleted.

17.1.17 Aliases



There is a link at the top of each of the Virtual Host Configuration tables that allows you to access the Aliases for the corresponding virtual host or the default aliases for all virtual hosts.

Aliases specify components of URLs that are “aliased" or mapped to different directories. When a request is received with a URL that contains one of the aliases, the data returned to the client comes from the specified directory or file.

Aliases may also specify a target directory that contains CGIs (or scripts) rather than normal data. In this case, the alias is referred to as a ScriptAlias and is represented in the Alias Settings table using a checkbox.

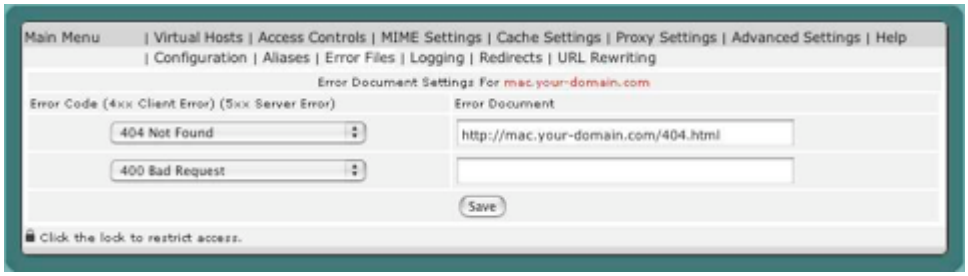
Tenon's iTools's initial DEFAULT virtual host settings contain several Aliases used by the iTools Administration Server, the iTools documentation, and in the examples. The default cgi-bin ScriptAlias is also specified in this table.

To create a new alias, enter the component of the URL to be aliased into the URL Path field of the Alias Settings table and enter the path to the directory or file containing the aliased data in the Directory or File eld. If the URL Path or the target represents a directory, it should begin and end with a "/". If it represents a file, it should not end with a "/". If the aliased directory contains CGI scripts, check the ScriptAlias checkbox. Click Save to save these settings.

The specified target may reside anywhere within the server's directory hierarchy; it does not necessarily have to reside in the DocumentRoot directory for the virtual host servicing the request. In fact, by using an alias, files in any directory may be accessed by a web browser without the client knowing where the files really reside.

17.1.18 Error Files

There is a link at the top of each page containing the Virtual Host Configuration table that allows you access the Error Files settings. These settings specify the file to be returned to the client when a Web server error occurs. When such an error occurs, the originally requested page is not returned to the client; instead, the corresponding error file is returned.



To associate an error file to a specific error, select the error code from the pop-up list and type the path to the error file into the text field. Then click the Save button.

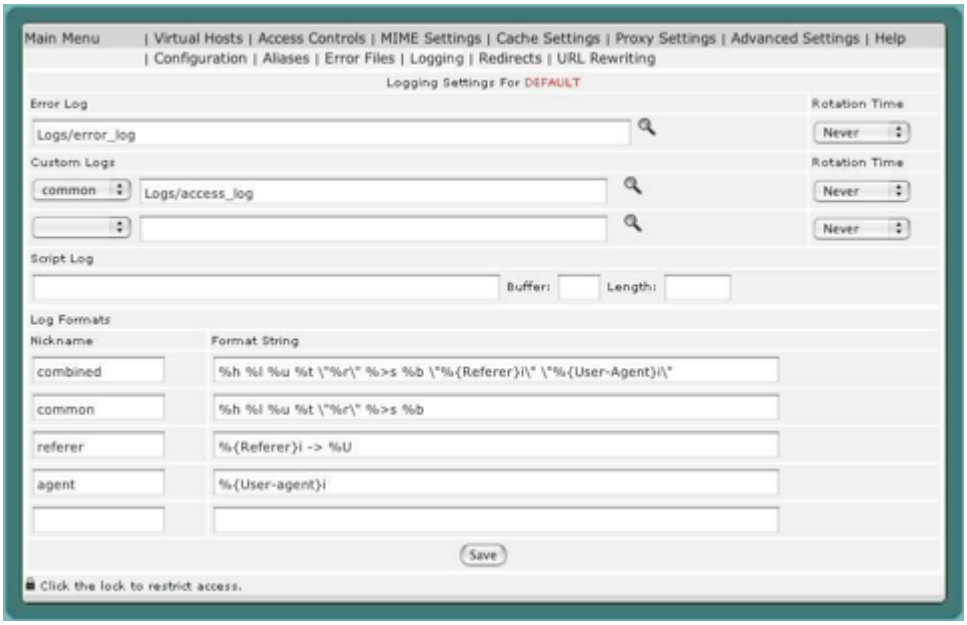
Remember that the path is a full path from the root of your server.

To change an error code for an existing error file or to change the name of an error file, change the selection in the pop-up list or modify the error file name in an existing text edit field. Then click Save to submit the change.

The two most common errors: "403: Access to the requested page is denied." and "404: The requested page does not exist." are usually mapped to files with simple messages explaining those errors. However, any of the error cases, from the most common to the most obscure, can be mapped to any URL (including a CGI) for advanced error logging and reporting.

17.1.19 Logging

The Logging link in the Virtual Host Configuration will display the logging location settings for your virtual host.



NOTE: if you change the location of your log file make sure that the directory exists and is writable by the user www, otherwise your webserver may fail to start.

17.1.19.1 Error Log

The Error Log entry in both the DEFAULT virtual host table and the Virtual Host Configuration table is the name of the file iTools uses to log information about Web server errors. If an Error Log file is not specifically set for a virtual host, the Error Log file setting in the DEFAULT virtual host table will be used.

Errors included in this log include “File Not Found" errors and errors found when trying to execute CGIs or start the server. It is the first place to look when a problem occurs with starting the server or with the operation of the server, since it will often contain details of what went wrong and how to fix it.

17.1.19.2 RotationTime

iTools automatically allows users to create rotated logs without restarting of the web server. Specify the period of rotation, and the log files will be created with the given file name and appended with the Epoch date. The log file can be viewed in System Status. See Chapter 14 for details.

17.1.19.3 Custom Log

By default, Apache will generate three activity logs: access (access from paticular IPs to specific URLs), agent (browsers being used to view your sites, and referrer (referring URLs that direct users to your site).

The “combined" log format combines all three of these logs into one log file. This allows logging analysis software to deal with one file per domain.

The Custom Log entry specifies a log format (as defined by the “Log Format" section on page 96) and a log path.

17.1.19.4 Script Log

The Script Log setting is the name of the file used to log information about errors in CGI scripts. This feature will only be displayed in the DEFAULT virtual host. This feature is meant to be used as an aid in debugging CGI scripts, and should not be used continuously on an active server. It is therefore not entered by default, but can be activated by specifying a file in the given form field.

17.1.19.5 LogFormat

The Log Format setting is a string that controls the format of the log file. The log file can include literal characters copied from the log format setting and detailed information specific to the actual request that is being logged. Details are encoded using a percent sign (“%") followed by a letter.

Each “%" followed by a letter is a directive to the Web server for a specific piece of information about the request being logged. For example, “%h" logs the name of the remote host placing the request, if hostname lookup is turned on.

These log formats can be given nicknames that can be used to format customized logs specified by the Custom Log directive.

The log file is a text file containing space-delimited entries for every request to the server, with data in the order the tokens are set in the log format. If the information is not available for a particular log token, the log will include “-" in the place of the missing information.

If the Custom Log is not customized for a particular virtual host, the Log Format setting will be inherited from the DEFAULT virtual host. This results in the default access log itself being inherited and utilizing the DEFAULT virtual host’ LogFormat.

The characteristics of the request itself are logged by placing % directives in the format string, which are replaced in the log file by the values as follows:

Format String	Description
%%	The percent sign
%…a	Remote IP-address
%…A	Local IP-address
%…B	Bytes sent, excluding HTTP headers
%…b	Bytes sent, excluding HTTP headers. In CLF format, i.e.,a ‘-’ rather than a 0 when no bytes are sent.
%…{Foobar}C	The contents of cookie Foobar in the request sent to the server.
%…f	Filename
%…h	Remote Host

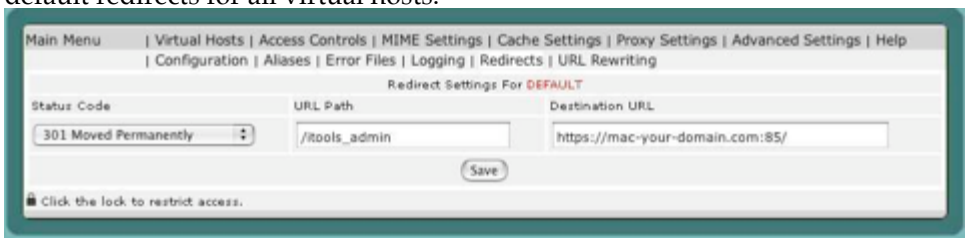
%…l	Remote logname (from identd, if supplied).
%…m	The request method
&…{Foobar}n	The contents of note Foobar from another module.
%…{Foobar}o	The contents of Foobar: header line(s) in the reply.
%…p	The canonical port of the server serving the request.
%…P	The process ID fo the child that serviced the request.
%…q	The query string (prepended with a ? if a query string exists, otherwise an empty string.
%…r	First line of request
%…s	Status. For requests that got internally redirected, this is the status of the original request (%…>s for the last).
%…t	Time, in common log format time format (standard English format).
%…{format}t	The time, in the form given by format, which should be in strftime (3) format; (potentially localized).
%…T	The time taken to serve te request, in seconds
%…u	Remote user (from auth; may be bogus if return status (%s) is 401)
%…U	The URL path requested, not including any query string
%…v	The canonical ServerName of the server serving the request
%…V	The server name according to the UseCanonicalName setting
%…X	Connection status when response is completed. X = connection aborted before response is completed. + = connection may be kept alive after the response is sent. - = connection will be closed after the response is sent.
%…I	Bytes received, including request and headers, cannot be zero. You need to enable mod_logio to use this.
%…O	Bytes sent, including headers, cannot be zero. You need to enable mod_logio to use this.

The "..." can be nothing at all (e.g., %h %u %r %s %b), or it can indicate conditions for inclusion of the item (which will cause it to be replaced with "–"if the condition is not met).

Each Log Format is assigned to a unique nickname, and Custom Log will use the nickname to refer to the Log Format.

17.1.20 Redirects

There is a link at the top of each of the Virtual Host Configuration panel that allows you to access the Redirects for the corresponding virtual host or the default redirects for all virtual hosts.



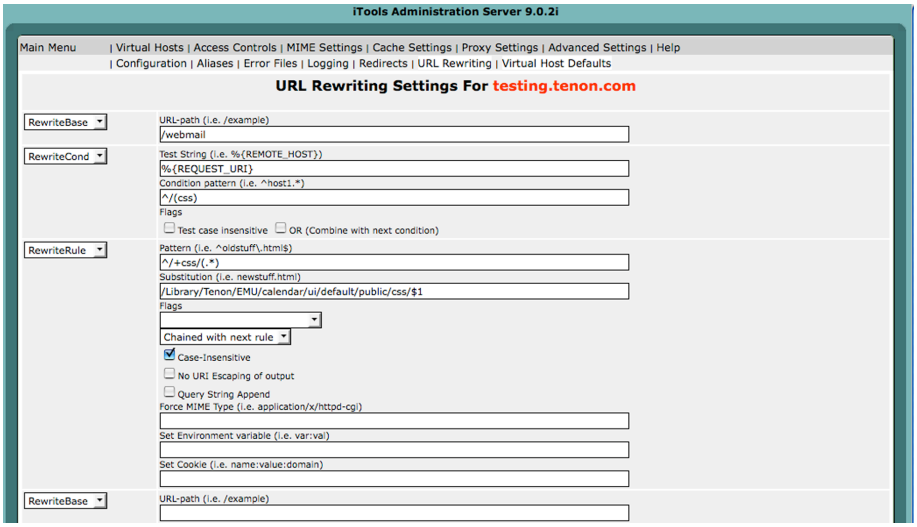
Redirect settings specify URLs that are “redirected" or mapped to different servers. When a request is received with a URL that contains one of the redirected entries, the client is instructed (via a return code) to access the data from a different server using the provided URL.

Redirect responses contain a reply code and may contain a URL. The reply code can be chosen from a pop-up list.

To create a redirect entry, select the redirect reply code from the pop-up list and enter the URL to be redirected into the URL Path field of the Redirect Settings table. If necessary, enter the new URL in the Destination URL field. Click Save to save these settings.

Some reply codes require a destination URL and some do not. If you select a reply code that requires a destination URL and do not provide one, an error will be reported. If you select a reply code that does not require a destination URL and one is provided, the destination URL will be discarded when the settings are saved.

17.1.21 URL Rewriting



Rewriting URLs is very important, especially on dynamic web sites where scripts can generate, sometimes unwieldy, query strings. For example, using URL rewriting, you can change

http://www.company.com/downloads?category=897634598

into

http://www.company.com/downloads/itools

Apache mod rewrite gives you the ability to manipulate URLs as a function of various conditions. It caches URLs that meet specific conditions and then rewrites them according to special instructions. The mod rewrite module is extremely powerful and very complex. For details about mod rewrite, we refer you directly to the Apache online documentation.

http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html
http://httpd.apache.org/docs/2.2/rewrite/rewrite_guide.html

The URL Rewriting Settings in iTools lets you set various mod rewrite directives: RewiteBase, RewriteCond, RewriteLock, RewriteMap and RewriteRule. When you make entries in URL Rewriting, the RewriteEngine directive is automatically enabled.

Note: These rewriting rules can be applied at a global site level, using the DEFAULT host, or they can be designed for specific virtual hosts on your site.

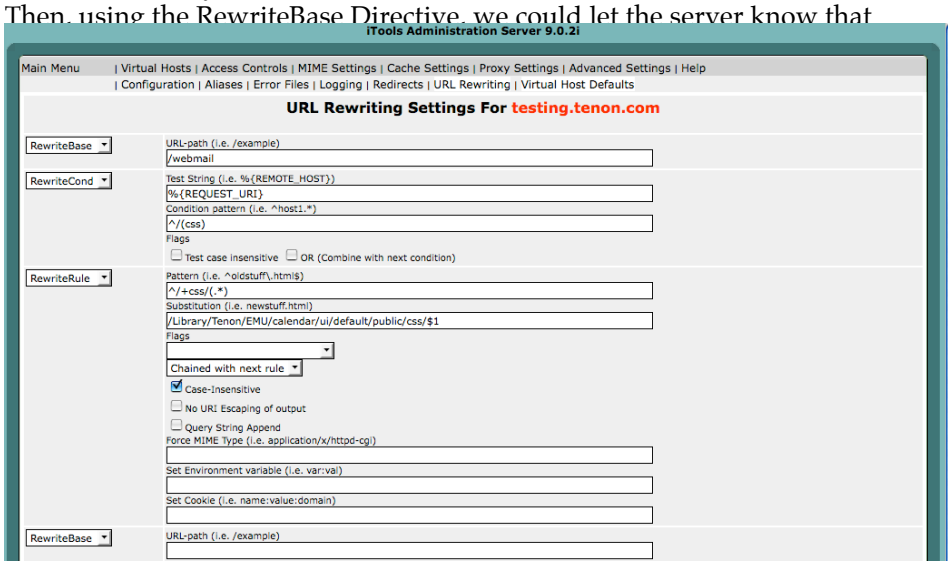
The URL rewriting module uses a rule-based rewriting engine (based on a regular-expression parser) to rewrite requested URLs on the y. It supports an unlimited number of rules and an unlimited number of attached rule conditions for each rule to provide a really flexible and powerful URL manipulation mechanism. The URL manipulations can depend on various tests, for instance server variables, environment variables, HTTP headers, time stamps, and even external database lookups in various formats can be used to achieve a really granular URL matching.

17.1.21.1 RewriteBase Directive

The RewriteBase directive explicitly sets the base URL for per-directory rewrites. In other words, if /abc/def is the physical path of /xyz, i.e. , the server has an Alias directive:

Alias /xyz /abc/def

Then, using the RewriteBase Directive, we could let the server know that



path (not on a NFS-mounted device) when you want to use a rewriting map-program. It is not required for other types of rewriting maps.

17.1.21.4 RewriteMap Directive

The RewriteMap directive defines a Rewriting Map which can be used inside rule substitution strings by the mapping-functions to insert/substitute fields through a key lookup. The source of this lookup can be of various types.

17.1.21.5 RewriteRule Directive

The RewriteRule directive is the real rewriting. The directive can occur more than once. Each directive then defines one single rewriting rule. The definition order of these rules is important, because this order is used when applying the rules at run-time.

RewriteRule ^oldstuff.html$ newstu .html

Thus a request to /xyz/oldstuff.html gets correctly rewritten to the physical file /abc/def/newstuff.html

17.2 SSL

17.2.1 Secure Socket Layer

iTools supports version 3.0 of the Secure Socket Layer (SSL) protocol to encrypt web server transmissions. The secure socket layer intercepts network calls from the server to encrypt the data before forwarding it to the network layer for transmission to the browser.

The web server and the browser negotiate an encryption algorithm, or cipher, to be used for the session. A session “key" is securely communicated to the browser using public key cryptography. The session key is then used symmetrically, i.e., to both encode and decode the actual session data.

The first step in setting up SSL is generating a Certificate Signing Request or CSR. From the CSR, a certificate can be produced by a Certificate Authority or CA.

17.2.2 Server Certificate

The server certificate validates the identity of the server. Server certificates may be signed by a trusted higher authority (the Certificate Authority, or “CA"), who assures the identity of the server.

In a typical commercial virtual host setup, each IP based virtual host will have a unique server certificate.

Name based virtual hosts (hosts that share an IP address) must share the certificate of the common IP host. By default, iTools associates a certificate issued to an IP based virtual host with all configured name based virtual hosts that share that IP address.

17.2.3 Obtaining A Server Certificate

In order to obtain a server certificate, a Certificate Signing Request (CSR) must be sent to the Certificate Authority, along with other proof of identity documents.

Click on the Certificate button in the appropriate virtual host and fill out the SSL Settings form within the iTools Administration Server.

Submit the completed CSR to the Certificate Authority. There are many Certificate Authorities worldwide. Copy and paste the CSR that is generated into the CSR online submission form.

Some browsers do a poor job of copying the CSR from the SSL CSR File form. To test this, copy the CSR and paste it into any empty text document of a text editor (such as BBEdit). If each line of the text is not left justified at the beginning of the line, use the text editor to cut any white space at the beginning of each line. Then copy this properly justified CSR and paste it into the CSR submission form.

Other documents validating the identity of the server must be mailed to the CA, along with a service fee. These documents include:

- Proof of the right to use the organization name, as in a copy of the company articles of incorporation, “doing business as" registration, etc.
- Proof of domain name registration (except for “.com").
- A letter, printed on organization letterhead and signed by an authorized representative, requesting certification of the domain name.

Your official certificate will be digitally signed and emailed to you by the CA.

Rename the certificate to “xxxxxx.crt" (where <xxxxxx> is the name of the virtual host for which the certificate was generated), and place the official certificate in the folder:

/Library/Tenon/WebServer/Configuration/ssl.crt

The official certificate will replace the temporary self-signed certificate generated by iTools for use prior to receipt of the official certificate.

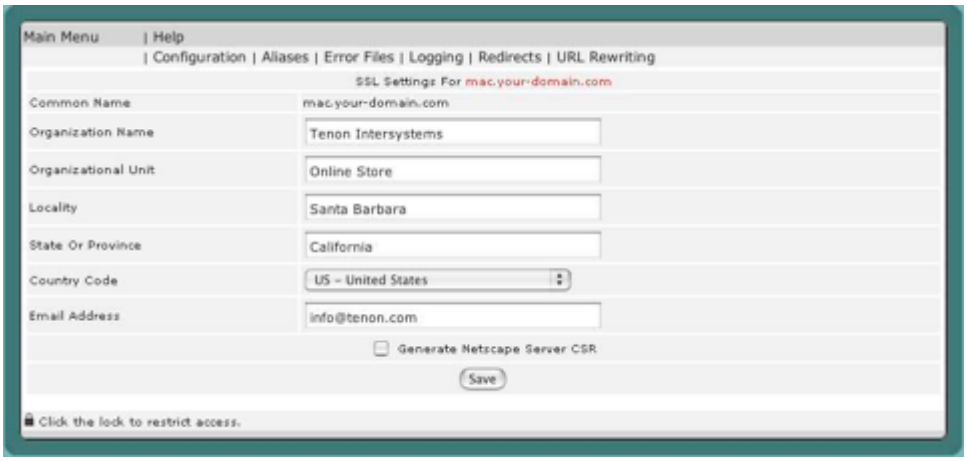
Each SSL Certificate that was produced during the creation of the CSR works in conjunction with the SSL Key file located in:

/Library/Tenon/WebServer/Configuration/ssl.keys

If the SSL Certificate file is lost, you may be able to request it again (at some expense) from the Certificate Authority. If the SSL Key file is lost, the SSL Certificate is useless and a new certificate will need to be issued. See section “Safeguarding SSL Keys And Certs" on page106 , for tips on how to prevent this from occurring.

17.2.4 SSL Settings

To generate an SSL certificate, click on the “Edit Certificate” button beside the SSLSecurity entry in the Virtual Host Configuration table. The SSL Settings page is a form for generating a Certificate Signing Request (CSR).



17.2.4.1 Common Name

The Common Name is the domain name of the web server or of an IP-based virtual host. This must be a fully quali ed domain name, not an IP address or a DNS alias.

17.2.4.2 Organization Name

The Organization Name is the legal organization or business name that will appear in the certificate.

17.2.4.3 Organizational Unit

The Organizational Unit is the department name or the name of a unit within an organization. This field is optional. If this field is omitted, you must put a “." In the field.

17.2.4.4 Locality

The Locality is the name of the city in which the organization resides. This field is optional.

17.2.4.5 State or Province

The State or Province is the name of the state or province in which the organization resides.

17.2.4.6 Country Code

The Country Code is a two-letter code for the country in which the organi zation resides. If anything other than a valid country code is entered, a CSR will not be generated. The correct Country Code for the United States is “US".

17.2.4.7 Email Address

The Email Address is the email address of a contact or representative within this organization.

17.2.4.8 Generating a CSR

To generate a Certificate Signing Request (CSR), save the SSL Settings via the Save CSR button. This action has several effects.

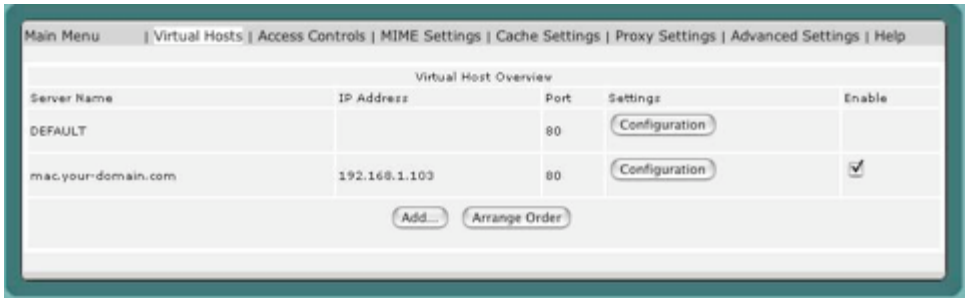
If a private key for this virtual host does not exist, such a key is created and saved in a secure area in iTools’s directory structure:

/Library/Tenon/WebServer/Configuration/ssl.keys

This SSL Key le is important and should be saved once a CSR is produced. See section “Safeguarding SSL Keys And Certs" on page106.

The actual Certificate Signing Request information is displayed in the iTools Administration Server. This CSR is a PEM-encoded document which may be e-mailed to the CA, or it can be copied and pasted into an on-line certificate request form. This CSR is also saved in a file called virtualhost.csr in the folder:

/Library/Tenon/WebServer/Configuration/ssl.crt



A temporary, self-signed certificate (for use while your CSR is being processed by the certificate authority) is created and saved in the

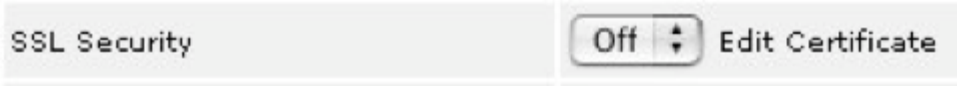
/Library/Tenon/WebServer/Configuration/ssl.crt

folder in a file named <virtualhost>.crt . This file should be replaced by the real certificate when one is returned from the Certificate Authority.
The self-signed certificate will allow your virtual server to perform secure transactions while your offcial certificate is being processed.
Browsers will question the validity of any server certificate signed by an authority of which they have no knowledge. The temporary, self-signed certificates should in no way be construed as proof of the virtual host's identity to your browser clients.

In some cases such as in a corporate intranet, a temporary self signed certificate is all that is necessary. See section "Self signed Certificates" on page 106 for more about these.

17.2.5 Enabling SSL

Once you have a certificate (even an iTools-generated temporary one), you will be able to create a secure virtual host by toggling SSL Security "On" in the Virtual Host Configuration table.



17.2.5.1 Secure and Non-secure Virtual Hosts

iTools supports virtual hosts with both secure and normal (not secure) service. This configuration is represented in the Virtual Hosts Table by two entries with the same virtual host name. One entry will have the SSL designation, and one will not.

To create a virtual host with both secure and normal service, first create the virtual host (if it is not already created) and follow the instructions to make this virtual host secure. Next, create a new virtual host using the same name. The second virtual host is created without SSL enabled. Both virtual hosts will initially share the same DocumentRoot. Either virtual host can be moved to a new DocumentRoot if this shared configuration is not desired.

If you desire all traffic to be directed to the secure virtual host, a redirect can be created in the normal virtual host to redirect all traffic to the secure virtual host.

17.2.5.2 Using Multiple Certificates

Every SSL connection requires a unique IP address. Because iTools supports IP-based virtual hosting, you can easily set up multiple secure IP-based virtual hosts. Each secure IP-based virtual host will need its own Certificate.

17.2.5.3 Safeguarding SSL Keys And Certificate

Each SSL Certificate works in conjunction with the SSL Key file that was produced during the creation of the Certificate Signing Request. SSL Certi - cates do not stand alone. They require the SSL Key file to perform encryption. SSL Certificates will only work with the corresponding SSL Key file that was used to produce the actual Certificate Signing Request.

The SSL Key file is your private key that ensures that no one can replicate or assume your site's identity on the Web. If the SSL Key file is compromised, the inherent security of your SSL Certificate is lost. If the SSL Key file is lost, the SSL Certificate is useless and a new certificate will have to be issued.

As you can see, it is important to preserve a copy of your SSL Key file and to protect it against theft. In iTools, the SSL Key file is tightly protected against unauthorized access (for example, CGIs cannot read the SSL Key file). The SSL Key file is generally located in the folder:

/Library/Tenon/WebServer/Configuration/ssl.keys

17.2.5.4 Self-signed Certificates

If iTools is on an intranet and is not visible to the Internet at large, it can take advantage of SSL without having their certificate signed by a CA (Certificate Authority such as Thawte).Create your certificate, as described earlier in this chapter. That will yield a certificate signed by iTools. While this is not a certificate signed by a CA, it will allow SSL encrypted transactions from your iTools server. Some browsers will complain that the certificate is not signed by a valid authority (CA), but certificates for only internal or intranet use do not need to be validated by any CA.

17.2.5.6 Common Problems

17.2.5.6.1 Line Feed Problem

Traditionally, Unix and Windows PC differ in the format in which they store text files. Windows PC places a carriage return character at the end of each line of a text file, but Unix uses a line feed character. Some Unix applications won't recognize the carriage returns added by Windows, and will display a file as a single line, interspersed with Ctrl-m characters. This appears on the screen as ^M. Similarly, some Windows applications need to see carriage return characters at the ends of lines, and may treat Unix-format files as one long line.

Certificates could potentially have ^M characters in them, when certificate is received from Certificate Authority. The easiest way to remove ^M characters from the certificate file is to run "tr" from the Terminal. For example:

tr 'nr' 'nn' < original certificate.crt > clean certificate.crt

Replace your certificate with the new clean certificate file, and your SSL enabled website should work correctly.

17.2.5.6.2 The issuer is Unknown

Some Certificate Authority credentials are not included in the bundled Certificate Authority Credential file. You can obtain the credential from your Certificate Authority, and append the credential to:

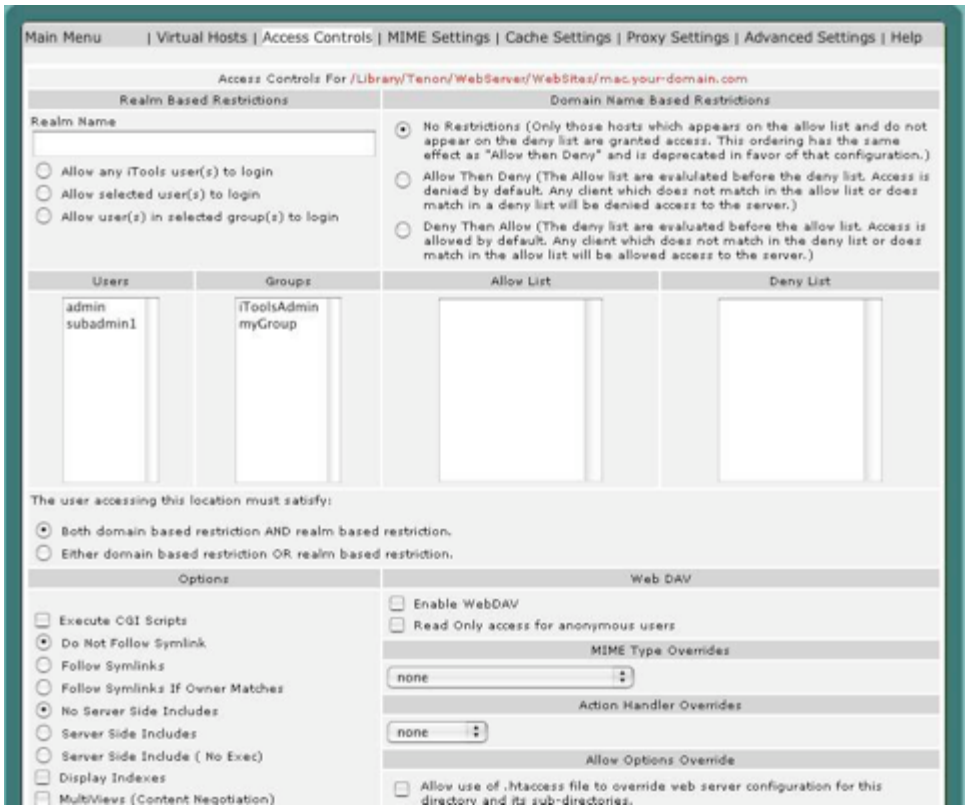
/Library/Tenon/WebServer/Configuration/ssl.crt/ca-bundle.crt

Restart the web server, and the settings will become effective immediately.

17.3 Access Controls

17.3.1 Using Access Controls

The Access Controls settings can be set for the entire virtual host, a particular folder or an individual file. Sub-folders, and files within folders, inherit the access settings of the parent folder unless they have individual settings specifically assigned.

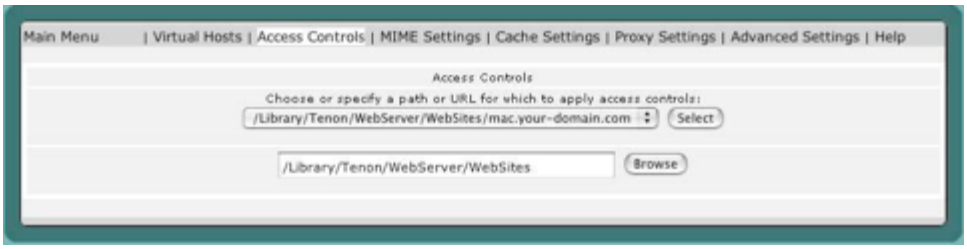


Included in the Access Controls section are settings for “Domain Name Based Restrictions", “MIME Type Overrides", “MIME Type Overrides", “Action Handler Overrides" and “Options". The name of the file or directory to which these settings apply appears at the top of the table. This is a valid URL to this specific file or directory complete with the proper virtual host name.

Clicking on this URL will make a request to the Web server in the exact same manner as any client web browser. Thus, this link provides not only an explicit reference to the file or directory to which the Access Controls apply, but also provides an easy way to test the settings.

17.3.2 Browsing Contents

Each entry in the Virtual Hosts Table has a button for Folder Contents. The Browsing Contents table provides a means for finding any file or sub-directory within a virtual host’s hierarchy.



Clicking this button takes you to the Browsing Contents table which contains an entry for each file and sub-directory contained in the Document Root of the virtual host in question. To display the Browsing Contents table with the contents of a specific sub-directory, simply click on that sub-directory's name in the Browsing Contents table. The Browsing Contents table provides a means for finding any file or sub-directory within a virtual Host's hierarchy. This is useful for setting "Access Controls" on folders or even specific files.

The columns in the Browsing Contents table are described in detail below.

17.3.3 Directories

This column displays an alphabetical list of all sub-directories contained within the specified directory. When the Folder Contents table is displaying the contents of a directory other than the Document Root directory, a "Parent-Directory" link is displayed as the rst entry in the Folders column. Clicking on the "ParentDirectory" link will display the Folder Contents table for the directory in which the current directory resides.

To make any settings specific to a particular sub-directory, click on that directory's name to display a Directory Contents table of that directory, and then click the Access Controls button.

17.3.4 Files

This column displays an alphabetical list of all files obtained within the specified directory. To access any settings specific to a particular file, click on that file's name to display the file's "Access Controls" information.

17.3.5 Access Control Settings

There are two main types of Access Controls for folders and files. "Realm Based Restrictions" are user authentication based. Selected users or groups are given access when the correct username and password have been entered. "Domain Name Based Restrictions" consist of a set of rules that define when to allow access from browsers connecting from some IP addresses or domains, and deny access to browsers from some other IP addresses or domains.

The user accessing this location must satisfy:

- Both domain based restriction AND realm based restriction.
- Either domain based restriction OR realm based restriction.

This option is only useful if access to a particular area is being restricted by both username/password and client host address. In this case the default behavior (AND) is to require that the client passes the address access restriction and enters a valid username and password. With the OR option the client will be granted access if they either pass the host restriction or enter a valid username and password. This can be used to password restrict an area, but to let clients from particular addresses in without prompting for a password.

This page also includes options for "MIME Type Overrides" and "Action Handler Overrides" which affect MIME headers for specific directories and files.

17.3.6 Options

The Options directive controls which server features are available in a particular directory.

Options can be set to None, in which case none of the extra features are enabled, or one or more of the following can be selected:

ExecCGI	Execution of CGI scripts is permitted
Follow SymLinks	The server will follow symbolic links in this directory. Even though the server follows symlinks, it does not change the pathname used to match against <Directory> sections. Note also, this option gets ignored if set inside a <Location> section.
Server Side Includes	Server-side includes are permitted.
Server Side Include (No Exec)	Server-side includes are permitted, but the #exec cmd and #exec cgi are disabled. It is still possible to #include virtual CGI scripts from a Script Alliased directory.
Display Indexes	If a URL that maps to a directory is requested, and there is no Directory Index (e.g., index.html) in that directory, then the server will return a formatted listing of the contents of the director.
MultiViews	Content negotiated "MultiViews" are allowed
Follow SymLinks if Owner Match	The server will only follow symbolic links for which the target file or directory is owned by the same user id as the link. Note: this option gets ignored if set inside a <Location> section.

17.3.7 WebDAV

WebDAV allows users to place and manipulate files in a directory on your web server. This means that you should take particular care in configuring your WebDAV server.

When you enable WebDAV for a directory or location, you should also enable authentication and authorization for that space. If authorization (for authenticated users) is not enabled, then an anonymous user would have full control of the DAV-enabled portion of your web server.

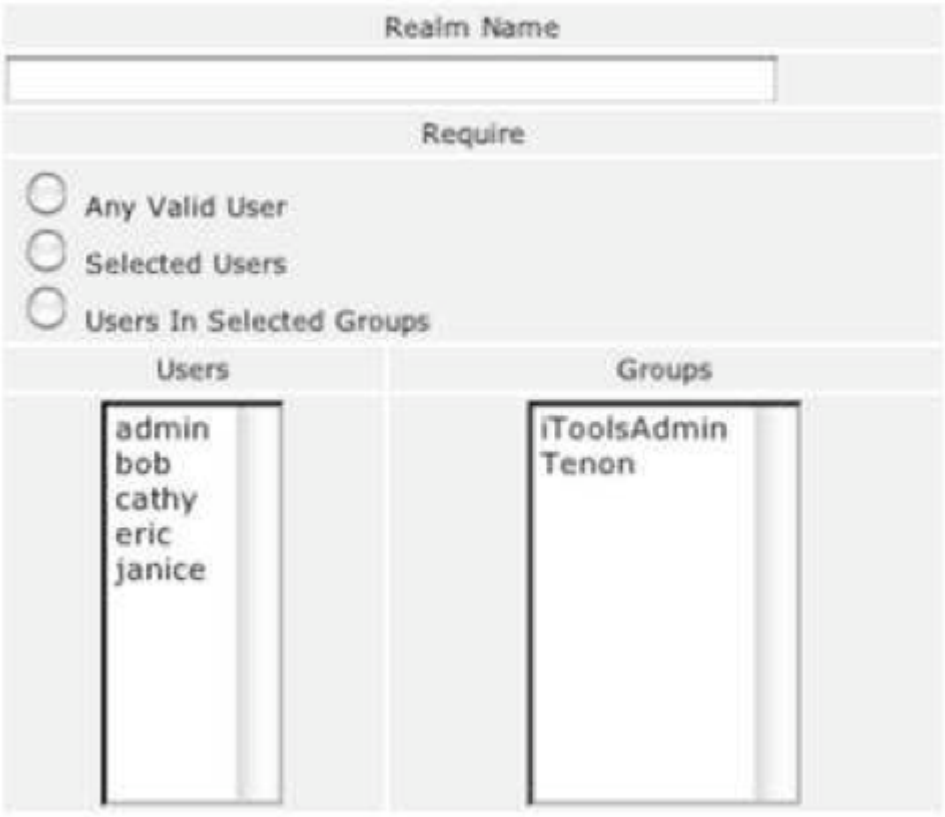
At this time, the files that are managed within the WebDAV directory should be read/write for the web server process. Files and directories that are created by the WebDAV server will have read/write/exec privileges for the user and group (but not the world) of the server process and will be owned by the process' user/group. For example, if you run your web server as www:www , then you will want to create a base directory owned by www:www and give it read/write/exec privileges to the user and group.

17.3.7.1 Read Only Access for Anonymous Users

When this option is enabled, the Realm restriction only applies to publish the web folder with WebDAV. The anonymous users can still read contents of the web folder without login.

17.3.8 Realm Based Restrictions

Realm based restrictions to a specified URL are based on user authentication. If a client fails to provide a correct user name or password, access is denied. before setting up a realm, it is a good idea to have your initial users and groups



To set up a realm, first choose whether the realm will be based on specific users or groups in the Require checkbox. The basis for the realm can be any of the settings defined below:

Setting	Access
Any Valid Users	Any user from the entire list of users is permitted access with the proper password.
Selected Users	Any highlighted user in the Users list is permitted access with the proper password. Details on setting up users can be found in Chapter 13, "Users & Groups"
User in a Group	Any user who is a member of any highlighted group in the Groups list is permitted access with the proper password.

Next, pick a realm name and enter it in the Realm Name field. This is strictly a designation for the collection of users or groups that are allowed access to the folder or file. The name itself isn't significant. The realm name is displayed in the web browser dialog box when user authentication is requested.

Browsers cache the realm name and username/password combination and will send authentication information with the next request to the same realm. This is nice for users since it means they don't have to re-enter the information for every page accessed within a protected section of a website. However, the only way to clear the information is to go to an authenticated page with different username and password, or to quit the browser. This means that a different scheme is needed if sensitive material were being accessed by browsers shared by more than one person (public libraries, schools, etc.).

17.3.9 Domain Name Based Restrictions

Domain name restrictions can use either domain names or IP addresses in the allow and deny fields. If you wish to use domain names, "HostnameLookups" must be enabled either globally in the Default virtual host, or in the "Virtual Host Configuration" for this specific host. Because enabling DNS lookups negatively impacts server performance, this isn't recommended. Using IP numbers is the preferred method.

A range of IP addresses may be specified for a specific subnet by appending a slash ("/") and the number of bits in the subnet mask. For example, specifying 192.30.20.128/25 would mean all IP addresses from 192.30.20.128 to 192.30.20.255, inclusive. Specifying 192.30.20.0/24 would include all addresses in the 192.30.20 class.

Initially, all files and folders are set to No Restrictions. There are two options for the order in which rules are interpreted, and what occurs in the event that rules contradict each other. Examples of their uses include:

(1) Perhaps your web server is for a small company and some documents are for internal use only. You would like to restrict access to these files so that the only browsers that can access them are from the 6 computers on the local network. For this you would choose, Allow then Deny, and in the allow box, you would enter the IP address of each machine on the local network. Browsers attempting to connect from any other IP number would get the "403 - Forbidden" page returned.

(2) A specific client seems to be making a huge number of requests in a very short time, and it's causing problems with excess traffic on your server. You are able to determine the IP address of the machine which is making the requests. You would choose Deny then Allow, and enter the IP address of the o ending client in the deny box. This would block access from that machine, but allow everyone else.

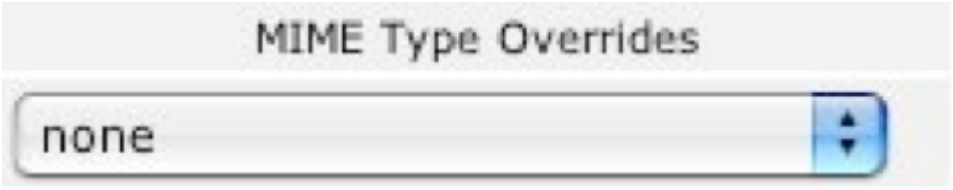
In the case that you experience a distributed DOS attack, you will want to block it further upstream at your router and have your upstream Internet provider block the attack as well.

For more advanced restrictions the general rules are:

Evaluation Selection	Evaluation Order
No Restrictions	All requests are permitted
Allow then Deny	The Allow specifications are evaluated first, followed by the Deny specifications. If any Deny contradicts any Allow, the Deny takes precedence.
Deny then Allow	The Deny specifications are evaluated first, followed by the Allow specifications. If any Allow contradicts any Deny, the Allow takes precedence.

17.3.10 MIME Type Overrides

MIME Type Overrides allow selected files or folder of files to be served with a user defined MIME type, rather than what would be assigned as the MIME type based on the filename extension (suffix).



The server includes the MIME type in the header it sends to the browser for each file. The browser uses that information to determine what type of file it is, and whether the browser itself can parse or display it as is, or if a helper application is required.

The server uses the file suffix, and a table that maps file suffixes (file extensions) to specific MIME types to determine what MIME type to include in the header.

Sometimes users will upload files that have an inappropriate suffix, or you have files that were not created to be served on the web and might lack a suffix altogether. It can be problematic to get these kinds of files correctly displayed; this is where the MIME type Overrides can be helpful. For example, if you have an entire folder of images in GIF format, you can set that folder to assign the MIME type of image/gif to all files served from that folder, regardless of filename or suffix.

Files or folders without explicit MIME type overrides will inherit the settings of their parent folder/directory and the Inherited indicator will be displayed along with the inherited setting. See Section 17.4 for more information about MIMI settings.

17.3.11 Action Handler Overrides

Action Handler Overrides allow a specific file or folder of files, to be passed to a designated action handlers for processing before the file is served. This

overrides the defined action for the files based on suffix (file extension) and the associated MIME types. For example, this would allow you to have a set of files with a filename extension of .html, to have SSI processing without having to rename the files with a ".shtml" suffix.

This also allows virtual hosts to have different server-side processing of files with the same extension; one virtual host could have ".html" files processed by the server while another virtual host could have ".html" files left as-is or have them processed by another script.

Folder or files without an explicit override inherit the settings of their parent folder/directory and the Inherited indicator will be displayed along with the inherited setting.

For more information about action handlers, see Section 17.4, "MIME."

17.3.12 Allow Options Override

When this option is not set, then .htaccess files are completely ignored. In this case, the server will not even attempt to read .htaccess files in the file system.

When this option is set, then any directive which has the .htaccess Context is allowed in .htaccess files.

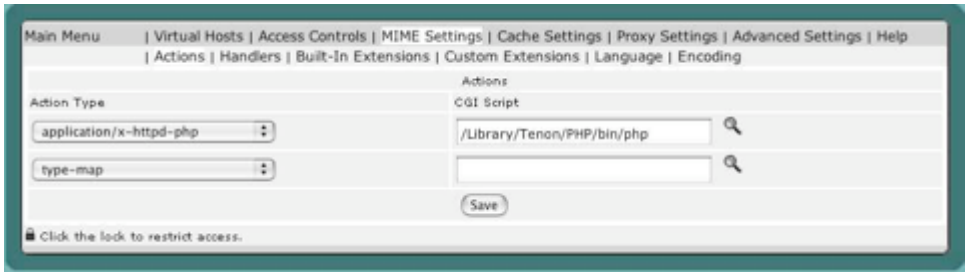
17.4 MIME

17.4.1 Actions

This directive adds an action, which will activate cgi-script when action-type is triggered by the request. The cgi-script is the URL-path to a resource that has been designated as a CGI script using ScriptAlias or AddHandler. The action-type can be either a handler or a MIME content type. It sends the URL and file path of the requested document using the standard CGI PATH INFO and PATH TRANSLATED environment variables.

For example, this will run CGI version of PHP for all PHP scripts.

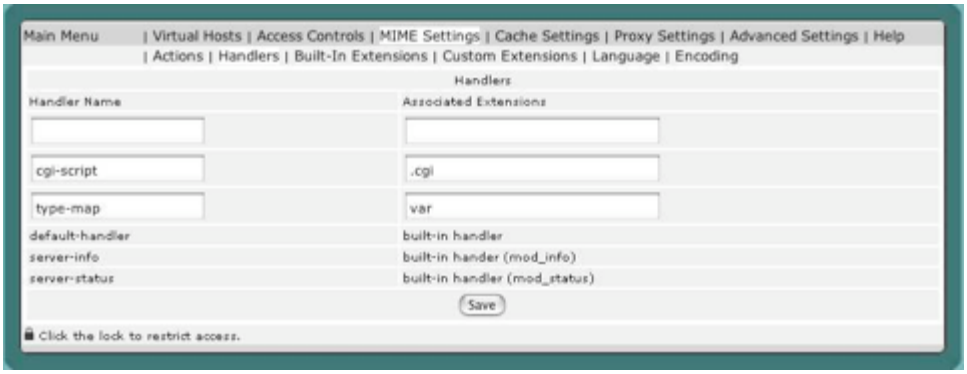
This will run CGI version of PHP for all PHP scripts.



17.4.2 Handlers

Handlers are an entity internal to Apache. Files having the name extension will be served by the specified handler-name. This mapping is added to any already in force, overriding any mappings that already exist for the same extension.

For example, to activate CGI scripts with the file extension .cgi, you might use:



Once that has been put into your configuration, any file containing the .cgi extension will be treated as a CGI program.

The extension argument is case-insensitive, and can be specified with or without a leading dot.

17.4.3 MIME Extensions

There are two MIME Extensions tables: the Custom Extensions table and th Built-In Extensions table. Both MIME Extensions tables map a file name, by its extension, to a MIME type. The extension or MIME type is then mapped to one of the action handlers to control what actions should be taken when any file with this extension is requested. Action handlers can be defined for both MIME types and extensions. If a handler is defined for a specific extension, it overrides any handler specified for that extension's MIME type.

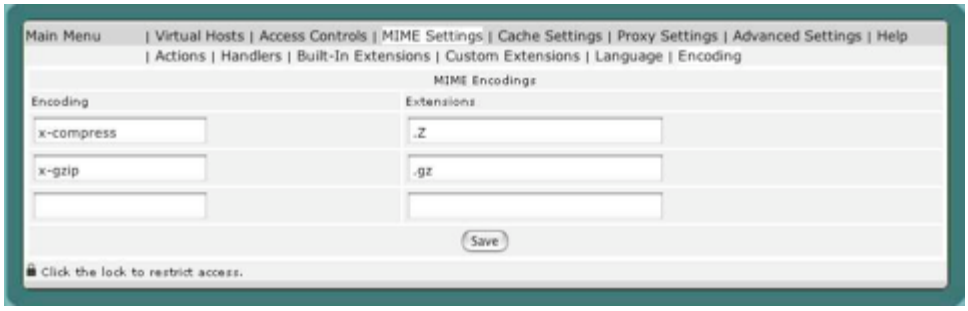
To map a new extension to a MIME type or action handler, enter the new extension into the empty text edit field in the bottom line of the Custom Extensions table. Then enter the corresponding MIME type or select a handler from the pop-up list, or do both. Click Save to submit the changes.

To change an existing extension, its MIME type, modify the extension or MIME type in the text edit eld. Then click on Apply to submit the changes.

iTools includes a long list of well-known extensions and their corresponding MIME types. These extensions are displayed in the Built-In Extensions table, accessible via the Built-In Extensions link, and cannot be explicitly changed. However, these default extensions can be overridden by entering the extension in the empty text edit field in the Custom Extensions table, and assigning it a different MIME type. This extension will then appear in that table, and the default setting will no longer appear in the Built-In Extensions table. If this extension is subsequently removed, the default setting will remain and will reappear in the Built-In Extensions table. Overriding the default extensions in the Built-In Extensions table is not recommended, as this setting a affects all files with this extension on this server.

17.4.4 Mime Languages

The MIME Languages table provides a means for mapping a file name, by its extension, to a language. The web server takes no special action based on the language, but the given language is passed back to the client (in the HTTP header) for any specific interpretation in the browser.



To map a new file name extension to a language, enter the extension in the empty text edit field in the first row of the table, and select a language from the pop-up list. The Priority sets the precedence of language variants for the case where the client does not express a preference, when handling a MultiViews request. Note that this directive only has an e ect if a 'best' language cannot be determined by any other means. Correctly implemented HTTP/1.1 requests will mean this directive has no effect. Then click Save to submit the new setting.

To change an existing setting, either modify the extension in the text edit field or select a new language from the pop-up list, change Language Priority from the pull down list. Then click Save to submit the changes.

17.4.5 Mime Encodings

The MIME Encodings table provides a means for mapping a file name, by its extension, to a MIME encoding. The Web server takes no special action based on the encoding, but the given encoding is passed back to the client (in the HTTP header) for any specific interpretation in the browser.

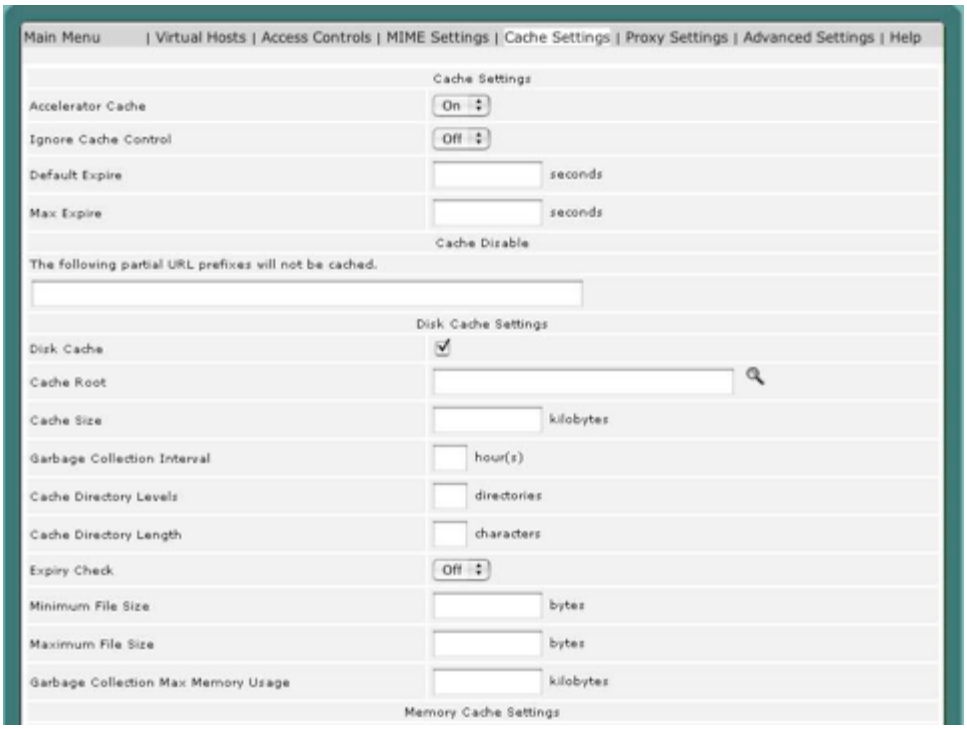
To map a new file name extension to an encoding, enter the extension in the empty Extension text field in the last row of the table, and enter an encoding in the Encoding text field. Then click Save to submit the new setting.

To change an existing setting, modify the extension or the encoding its respective text edit field. Then click Save to submit the changes.

17.5 Cache

17.5.1 Cache Settings

Clicking the Cache Settings link reveals the Cache Settings tables. The Cache Settings tables contains options that control the iTools Accelerator Cache. This cache is object-based and keeps the most recently accessed web pages in memory, making these pages immediately accessible for subsequent requests.



After changing the Cache Settings, click on the Save button to preserve your changes.

17.5.2 Accelerator Cache

The AcceleratorCache setting controls whether the memory cache is “On" or “Off ". The default setting is “On". Turning the cache to “Off " will save some memory, so this setting might be useful for servers that are running low on memory. Turning the cache to “Off " will also affect the performance of the server.

17.5.2.1 Ignore Cache Control

The Ignore Cache Control directive instructs Cache Disable to disable Cache specified URLs.

17.5.2.2 Default Expire

Default Expire is the default time in seconds to cache a document if the page does not have an expiry date in the Expires field.

17.5.2.3 Max Expire

Max Expire is the maximum time in seconds to cache a document. The Max Expire takes precedence over the Expire field from the header.

17.5.2.4 Do Not Cache

The following partial URL prefixes will not be cached
This setting is a list of words or characters. A URL containing any of these values is not cached. The default setting is to not cache URLs containing “cgi-bin" or “?". Other words or virtual host names may be added to this list to force other URLs to never be cached.

17.5.3 Disk Cache

17.5.3.1 Cache Root

The Cache Root directive defines the name of the directory on the disk to contain cache file. If the disk cache module has been enabled, this directive must be defined. Failing to provide a value for Cache Root will result in a configugration file processing error. The Cache Directory Levels and Cache Directory Length directives define the structure of the directories under the specified root directory.

17.5.3.2 Cache Size

The Cache Size directive sets the desired disk space usage of the cache, in KBytes (1024-byte units). This directive does not put a hard limit on the size of the cache. The garbage collector will delete files until the usage is at or below the settings. Please use a value that is lower than the available disk space.

17.5.3.3 Garbage Collection Interval

Garbage Collection Interval is the interval between garbage collections.

17.5.3.4 Cache Directory Levels

The Cache Directory Levels directive set the number of subdirectory levels in the cache. Cache data will be saved this many directory levels below Cache Root.

17.5.3.5 Cache Directory Length

The Cache Directory Length directive sets the number of characters for each subdirectory in the cache.

17.5.3.6 Expiry Check

The Expiry Check directive observes expiration date when seeking files.

17.5.3.7 Minimum File Size

The Minimum File Size directive sets the minimum size in bytes of a file to be cached.

17.5.3.8 Maximum File Size

The Maximum File Size directive sets the maximum size in bytes of a file to be cached.

17.5.3.9 Garbage Collection Max Memory Usage

Maximum kilobytes of memory used for garbage collection.

17.5.4 Memory Cache

17.5.4.1 Cache Size

The Cache Size directive sets the desired space usage of the cache, in KBytes (1024-byte units). If a new entry needs to be inserted in the cache and the size of the entry is greater than the remaining size, older entries will be removed until the new entry can be cached.

17.5.4.2 Maximum Object Count

The Maximum Object Count directive sets the maximum number of objects to be cached. If a new entry needs to be inserted in the cache and the maximum number of objects is reached, an entry will be removed to allow the new entry be cached.

17.5.4.3 Minimum Object Size

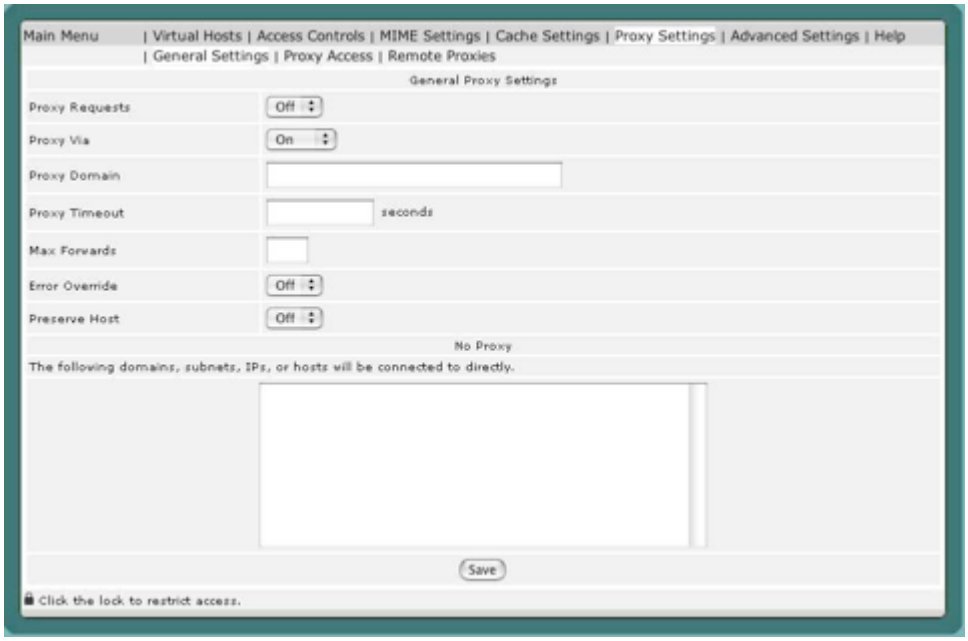
The Minimum Object Size directive sets the minimum size in bytes of an object to be cached.

17.5.4.3 Maximum Object Size

The Maximum Object Size directive sets the maximum size in bytes of an object to be cached.

17.6 Proxy Settings

The Proxy Settings table contains some options that control the proxy capabilities of Apache. For more information on Apache and proxy service, see the on-line Apache documentation



17.6.1 Proxy Requests

The Proxy Requests setting controls whether the proxy service is “On" or “Off ". This setting is “Off " by default.

17.6.2 Proxy Via

The Proxy Via directive controls the use of the Via: HTTP header by the proxy. Its intended use is to control the flow of the proxy requests along a chain of proxy servers.

- If set to off, which is the default, no special processing is performed. If a request or reply contains a Via: header, it is passed through unchanged.
- If set to on, each request and reply will get a Via: header line added for the current host.
- If set to block, every proxy request will have all its Via: header line removed. No new Via: header will be generated.

17.6.3 Proxy Domain

The Proxy Domain directive is only useful for Apache proxy servers within intranets. The Proxy Domain directive specifies the default domain which the Apache proxy server will belong to. If a request to a host without a

domain name is encountered, a redirection response to the same host with the configured domain appended will be generated.

17.6.4 Proxy Timeout

The Proxy Timeout directive allows a user to specify a timeout on proxy requests. This is useful when you have a slow/buggy application server which hangs, and you would rather just return a timeout and fail gracefully instead of waiting however long it takes the server to return.

17.6.5 Max Forwards

The Max Forwards directive specifies the maximum number of proxies through which a request may pass. This is set to prevent in finite proxy loops, or a DoS attack.

17.6.6 Error Override

The Error Override directive is useful for reverse-proxy setups, where you want to have a common look and feel on the error pages seen by the end user. This also allows for included files (via mod_include's SSI) to get the error code and act accordingly (default behavior would display the error page of the proxied server, turning this on shows the SSI error message).

17.6.7 Preserve Host

When enabled, this option will pass the Host: line from the incoming request to the proxied host, instead of the Hostname specified in the proxypass line. This option should normally be turned "off ".

17.6.8 No Proxy

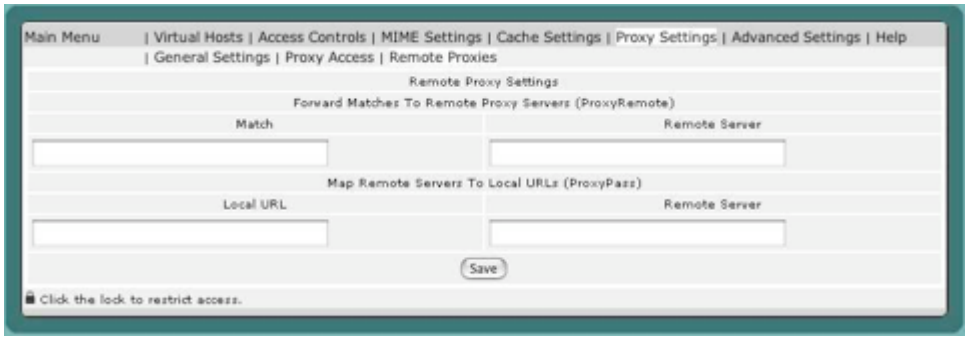
The NoProxy directive specifies a list of words, hosts and/or domains, separated by spaces. HTTP and anonymous FTP documents matching any words, hosts or domains are not cached by the proxy server. During startup, the proxy module will also attempt to determine IP addresses of any list items which may be host names. These IP addresses will also be cached for use in the match list. In the following example:

some host.co.uk widgets.doodads.com

"widgets.doodads.com" would also be matched if referenced by IP address. Note that "doodads" would also be sufficient to match "doodad.com". Note also that "*" disables proxy completely.

17.6.9 Remote Proxies

Remote Proxys are other proxy servers that this proxy server may interact with to satisfy a proxy request.



17.6.10 ProxyRemote

The ProxyRemote setting speci es which remote proxy servers are accessible to this proxy server. Each line in the ProxyRemote text edit field defines a “match" string and a “remote server" to service URLs that match that string. The match string and the remote server are separated by a space.

The “match" string is either the name of a URL scheme that the remote server (“*") to indicate that server should be contacted for all requests.

The “remote server" field is the URL for the remote proxy server. Its syntax is “http://<Hostname>[:port]". Here are some example entries in the Remote Proxies table:

http://goodguys.com/	http://mirrorguys.com:8000
	http://cleversite.com
ftp	http://ftpproxy.mydomain.com:8080

In the last example, the proxy will forward FTP requests, encapsulated as yet another HTTP proxy request, to another proxy which will then handle them as FTP requests.

17.6.11 ProxyPass

The ProxyPass setting allows remote servers to be mapped into the space of the local server. The local server does not act as a proxy in the conventional sense, but appears to be a mirror of the remote server.

Each line in the ProxyPass text edit field defines a “local url" and a “remote server". These fields are separated by a space character.

The “local url" is the name of a local virtual path. The “remote server" is the URL for the remote server. Suppose the local server has address “http://wibble.org".

Typing the following:

/mirror/foo http://foo.com

will cause a local request for:

http://wibble.org/mirror/foo/bar

to be internally converted into a proxy request to:

http://foo.com/bar

17.6.12 Proxy Access

The Proxy Access settings control two things. The Domain Name Restrictions control which hosts may use this iTools server as a proxy server. The ProxyBlock acts as a censor list by restricting access to certain URLs, such as pornographic material.

17.6.13 Domain Name-Based Restrictions

The Domain Name Restrictions control which hosts may use this iTools server as a proxy server. These restrictions are applied the same way as iTools domain name restrictions are applied to any file or directory. See section “Domain Name Based Restrictions" on page 84 for more information.

17.6.14 Proxy Block

The Proxy Block directive specifies a list of words, hosts and/or domains, separated by spaces. HTTP, HTTPS and FTP document requests to matched words, hosts or domains are blocked by the proxy server. The proxy module will also attempt to determine IP addresses of list items which may be host names during startup, and cache them for match test as well.

For example, if the ProxyBlock table contained:

nudes
games
some host.com

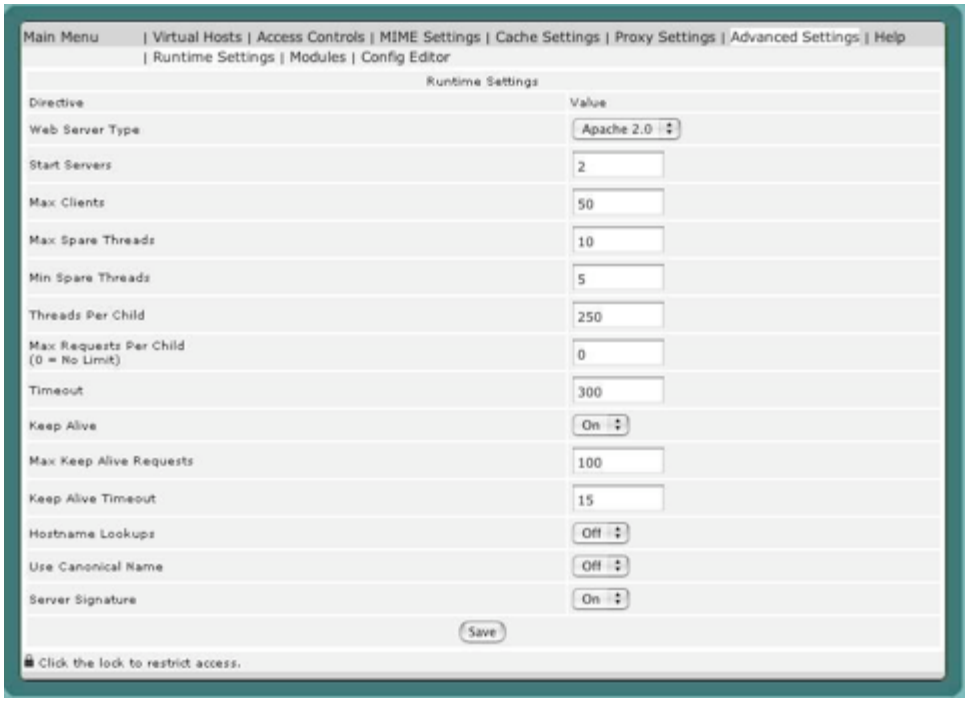
Access to any URL containing the words “nudes" or “games" and to “some host.com"

would be restricted. “some host.com" would also be matched if referenced by IP address. Note that referencing “some host" would also be suficient to match

“some host.com". Note also that the wild card “*" blocks connections to all sites.

17.7 Advanced Settings

The Advanced Settings table contains some options that control the inner workings of the web server. Your choice for these settings may be influenced by certain conditions, such as how much memory the iTools system has, the expected rate of “hits", the size of the average transfer, the number of simultaneous transfers, and the access bandwidth of the web server or the clients.



17.7.1 Web Server Type

The Web Server Type setting controls what version of the Apache Webserver are started on the Mac OS X system.

17.7.2 Start Servers

The Start Servers setting controls how many web server processes are created when the server is initially started. The number of web server processes may be dynamically changed (depending on the server’s load), so changing this setting has minimal effect once the server is up and has serviced its first few requests.

17.7.3 Max Clients

The Max Clients setting controls the number of requests that can be processed simultaneously. If the Max Clients are concurrently in progress, subsequent requests are not necessarily lost. Instead, they are queued until an existing request has completed.

17.7.4 Max Spare Threads

The Max Spare Threads setting controls the number of idle (i.e., not currently servicing any request) web server processes. If the number of idle processes exceeds this number, the excess processes are terminated.

17.7.5 Min Spare Threads

The Min Spare Threads setting controls the number of idle (i.e., not currently servicing any request) web server processes. If the number of idle processes is smaller than this number, extra web server processes are instantiated at a rate of one per second.

17.7.6 Max Requests Per Child

The Max Requests Per Child setting controls the number of requests each web server process will service. web server processes service one request at a time. However, upon completing one request, they may begin servicing another.

Increasing the number of requests each web server process services reduces the overhead of instantiating and terminating web server processes. Restricting this number reduces the likelihood of accidental loss of system resources, as these resources are recovered when a process exits. Also, the dynamic control over the number of currently running processes responds to a reduction in load by allowing some web server processes to exit without instantiating replacements. Therefore, in this case, a smaller number of Max Requests Per Child leads to a faster reduction in web server processes.

If the Max Requests Per Child is set to zero, a web server process will never expire.

17.7.7 Timeout

The Timeout setting controls the maximum time (in seconds) that the web server will wait for receipt of a complete incoming request once any initial part of an incoming request is received. The Timeout setting also controls the maximum time the web server will wait to completely send a response. If the sizes of the files used in the web transfers are large, and the client's or server's network bandwidth is slow, the Timeout setting must be increased to compensate.

17.7.8 Keep Alive

The Keep Alive setting controls whether or not the web server permits multiple incoming requests (from a single client) in a single connection. Using Keep Alive reduces the overhead of connection establishment and termination for each incoming request.

17.7.9 Max Keep Alive Requests

The Max Keep Alive Requests setting controls the number of incoming requests a client may embed in a single connection. The Max Keep Alive Requests setting is ignored if Keep Alive is Off .

17.7.10 Keep Alive Timeout

The Keep Alive Timeout setting controls the length of time (in seconds) the web server will wait for additional incoming requests in a single connection. If the Keep Alive Timeout expires, a client can still send additional requests; however, a new connection establishment overhead is incurred. The Keep Alive Timeout setting is ignored if KeepAlive is Off .

17.7.11 Hostname Lookup

<TBD>

17.7.12 Canonical Name

<TBD>

17.7.13 Server Signature

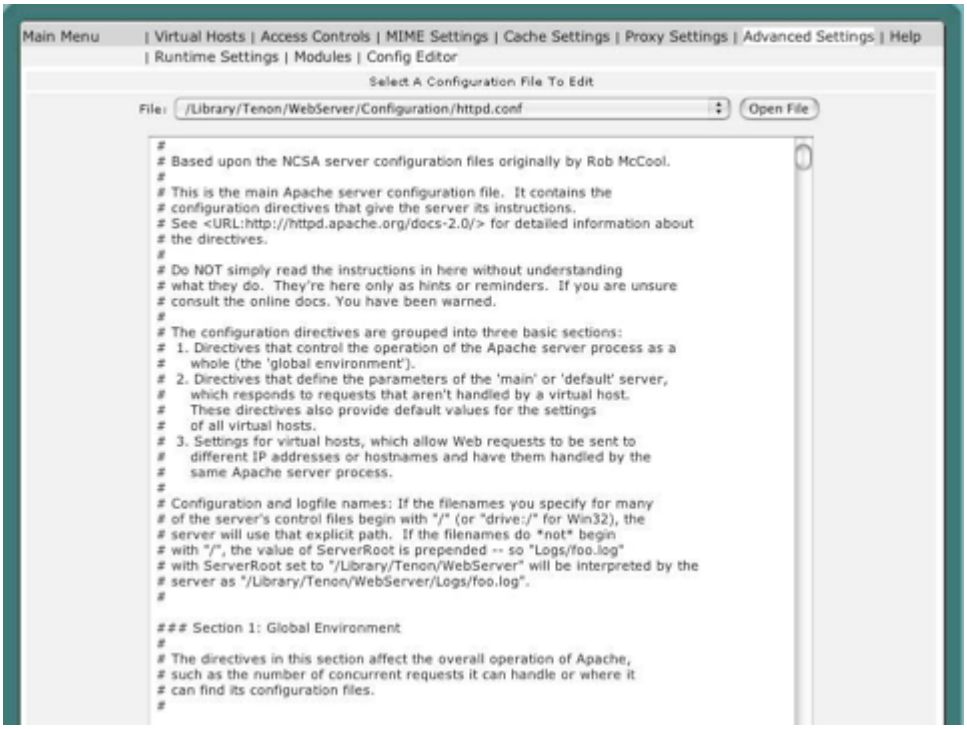
<TBD>

17.8 Apache Module Configuration

The Apache Module Configuration button takes you to a page which displays information about what modules are loaded. The actual window contains many more entries, this is just a small sample. See Appendix A, “Apache Modules," for a complete listing of all Apache modules included with iTools, with a brief description of the module. The Appendix also includes details about using this configuration page.

17.9 Config Editor

There are certain complex directives that can be configured by hand coding in the configuration files. Config Editor provides a list of Apache related configuration files, and power users can add additional directives into the configuration file. Any changes made to the files, the web server will require a restart for those changes to become effective.



Appendix A: Apache

Modules

One of the most powerful features of Apache is its ability to use dynamically loadable modules to increase its functionality and flexibility as the end-user's needs grow. Such add-on modules include SSL, FastCGI, and many others. Though iTools comes with a vast array of Apache modules both from the Apache source itself and modules from third parties, the user may still find the need to expand Apache's capabilities further.

Below is a list of all the modules that come as part of the iTools distribution.

A.1 Environment Creation

Mod_env
: Passing of environments to CGI scripts.

Mod_setenvif
: Set environment variable based on client information.

Mod_unique_id
: Generate unique request identifier for every request.

A.2 Content Type Decisions

Mod_mime
: Determining document types using file extensions.

Mod_mime_magic
: Determining document types using "magic numbers".

Mod_negotiation
: Content negotiation.

A.3 URL Mapping

Mod_alias

Mapping different part of the host file system in the document tree, and URL redirection.

Mod_rewrite
: Powerful URI-to-filename mapping using regular expressions.

Mod_userdir
: User home directories.

Mod_speling
: Automatically correct minor typos in URLs.

Mod_vhost_alias
: Support for dynamically configured mass virtual hosting.

A.4 Directory Handling

Mod_dir
: Basic directory handling.

Mod_autoindex
: Automatic directory listings.

A.5 Access Control

Mod _access
: Access control based on client hostname or IP address.

Mod_auth
: User authentication using text files.

Mod_auth_db
: User authentication using Berkeley DB files.

Mod_auth_anon
: Anonymous user access to authenticated area.

Mod_digest
: MD5 authentication.

A.6 HTTP Response

Mod_headers
: Add arbitrary HTTP headers to resources.

Mod_cern_meta
: Support for HTTP header meta files.

Mod_expires
: Apply Expires: headers to resources.

Mod_asis
: Sending files which contain their own HTTP headers.

A.7 Dynamic Content

Mod_include
: Server-parsed documents.

Mod_cgi
: Invoking CGI scripts.

Mod_actions
: Executing CGI scripts based on media type or request method.

Mod_perl
: Speeds up Perl scripts by keeping them loaded into memory.

A.8 Internal Content Handlers

Mod_status
: Server status display.

Mod_info
: Server configuration information.

A.9 Logging

Mod_log_config
: User-configurable logging replacement for mod_log common.

Mod_usertrack
: User tracking using Cookies (replacement for mod_cookies).

A.10 Miscellaneous

Mod_imap
: The image map file handler.

Mod_proxy
: Caching proxy abilities.

Mod_mmap static
: Experimental file caching, mapping files into memory to improve performance.

Mod_dav
: Provides DAV support.

A.11 Encryption

Mod_ssl
: Secure Socket Layers w/128 bit encryption.