iTools User's Guide

232 Anacapa Street, Suite 2A
Santa Barbara, CA 93101
PH: 805-963-6983•FAX: 805-962-8202
info@tenon.com•www.tenon.com

11/12/03 – iTools 7.1

Introduction to iTools

1

SERIOUS TOOLS FOR THE INTERNET

Apache is the most popular web server on the internet. Today there are more than 30 million Apache web sites; two thirds of the web sites in the world are using Apache. The breadth and extent of Apache is amazing, with hundreds of modules available, each with their own particular set of configuration directives. Tenon's iTools is a suite of web-based Apache configuration and management tools that makes managing Apache easy and safe.

From our decade of experience on the Macintosh platform, we've created a set of professional quality, high-performance tools to make it easy to use Apache, even for the most naïve webmaster. iTools is the most advanced, most mature, and most user-friendly tool suite for managing Apache web sites. iTools extends the internet software that ships with Linux and enhances open source packages by augmenting key internet services with a point and click interface to make configuration and maintenance easy and error-proof. iTools on Linux: the strength of Apache, the simplicity & power of a web-based GUI, the ubiquity of Linux.

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

Installing Tenon's iTools

2

SYSTEM REQUIREMENTS

iTools will run on any x86 Linux capable computer; you can determine whether or not your Linux computer is iTools compatible by visiting Tenon's web site:

http://www.tenon.com/
iTools also requires:

- at least 256MB RAM.
- at least 200MB of available disk space.

PRE-CONFIGURATION

Tenon's iTools family of Linux networking applications requires a properly set-up network configuration. Each Linux system must be pre-configured, using the Setup -> Network Configuration. If you are unfamiliar with these terms, please refer to your Linux documentation.

INSTALLING ITOOLS

New Installation

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

Upgrades or transition installs from other servers

If you are doing an upgrade or transition, it is a good policy to backup your existing server. iTools 7 will install gracefully over the default Apache 2.0.x that comes with Redhat 9 or modern Linux. For other transition, check the Tenon web site "Support" pages for white papers and hints.

INSTALLING FROM A DOWNLOAD

Tenon's iTools can be found at:
http://www.tenon.com/products/itools7-linux/

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.

Use RPM to install/upgrade the package with this command:

rpm -U iTools-7.2-1.i386.rpm

The installer will take a few minutes; so be patient. When the installer is completed, you should restart your computer or run:

sudo /etc/rc.d/init.d/itools start

Then you will have full access to iTools 7.

WHAT GETS INSTALLED

/etc/rc.d/init.d/itools

/usr/local/tenon --> assorted files, including a modified "httpd.conf" file.

For new installations, the default login and password is "admin". To change the default settings, login to Tenon's iTools Admin Server and change the admin user password. This username and password is used only by Tenon's iTools. It need not exist in the system password database nor does Tenon's iTools enter it into the system password database.

License number

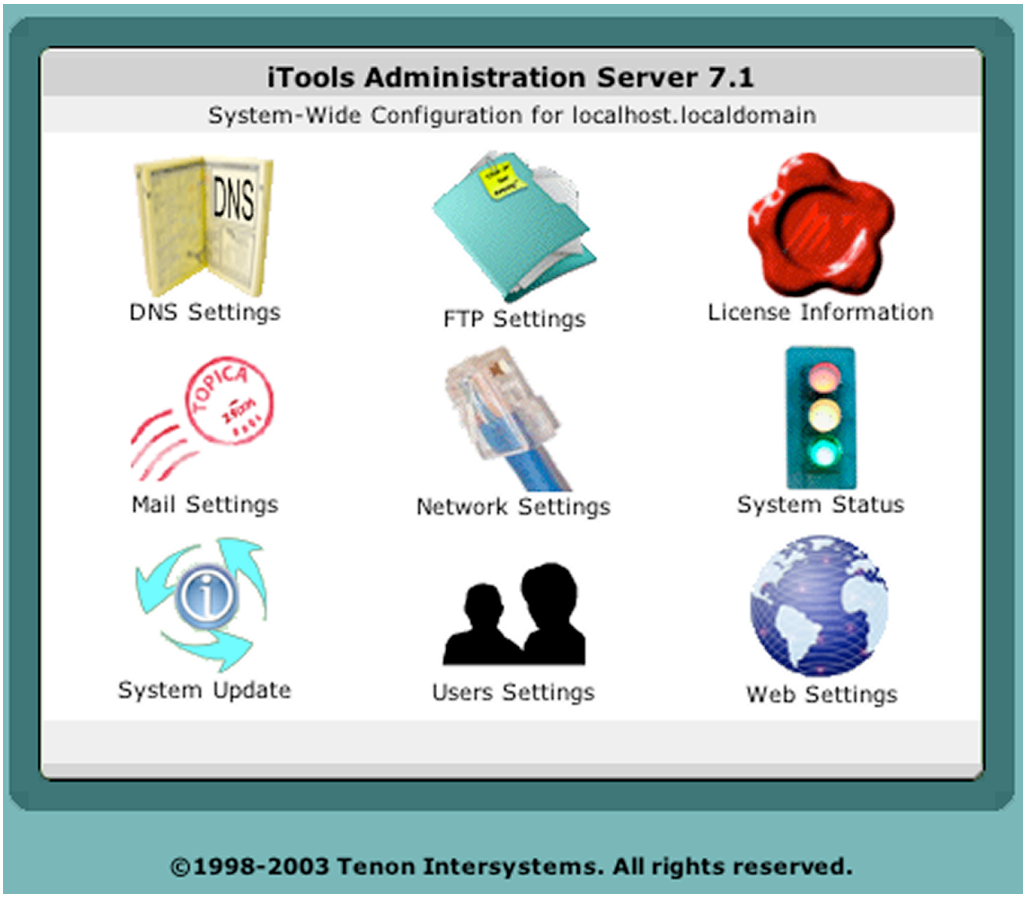
Tenon's iTools license can be entered or changed in the iTools web-based Administration Server. To enter or change the license, and select "License Information" icon. Enter your license in the text field, being careful to observe case sensitivity, and click "Apply". The license program will return information about the validity of the license you have entered, and for what time period it remains valid.

THE BROWSER-BASED ADMIN SERVER

Use your web browser to connect to the Admin server.
Enter:

http://your-hostname.com/itools_admin
or
https://127.0.0.1:85/

You will be prompted to enter your iTools Admin username and password.



The admin server runs on port 85, and the URL will reflect that. If you have a firewall, and will be connecting from outside locations, you will need to open that port to have access to admin functions.

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

iTools Quick Start

3

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 managment can be done by using the iTools Manager on a Mac OS X desktop (From a remote iTools 7 installation) or 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.

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. Our example will be for a server whose primary host is “linux.your-domain.com”.

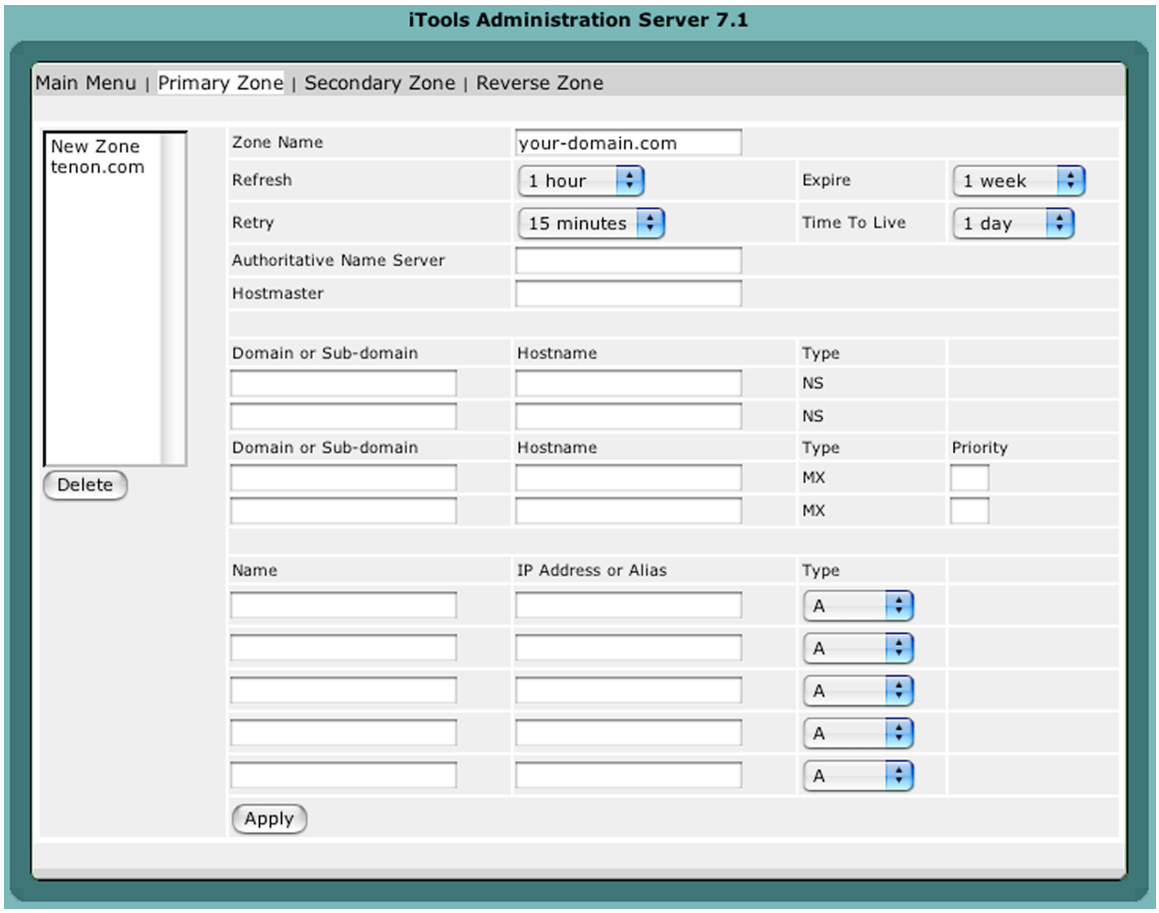
DNS

Using iTools DNS Server

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”.



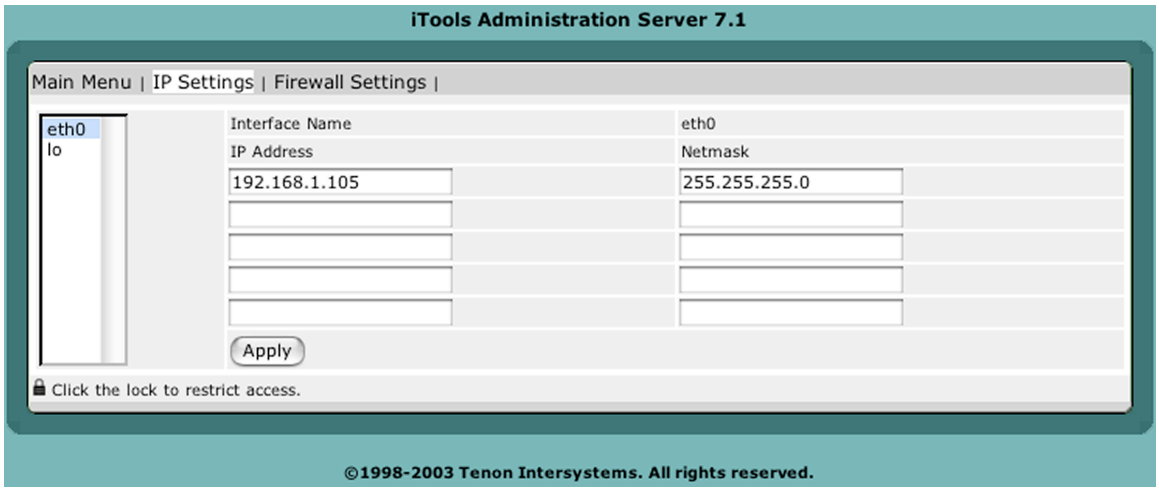
IMPORTANT: This form displays a few text fieldswhere you configure the Start of Authority record. iTools will automatically try to fill in the information for you, if they are left empty. It is very important to enter correct information in this section.

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 is replaced 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 DNS = linux.your-domain.com.
Hostmaster = dnsmaster.your-domain.com.
Click “Apply” to save the zone.

IP ADDRESS

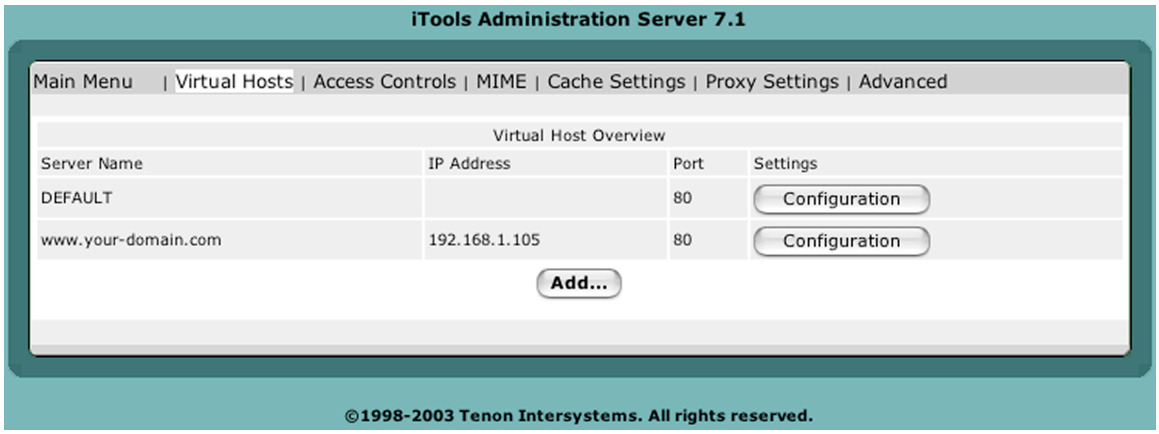
Once DNS is configured, it's time to setup IP address for your hosts. Click on the Network Settings icon, and a screen will be displayed similar to this:



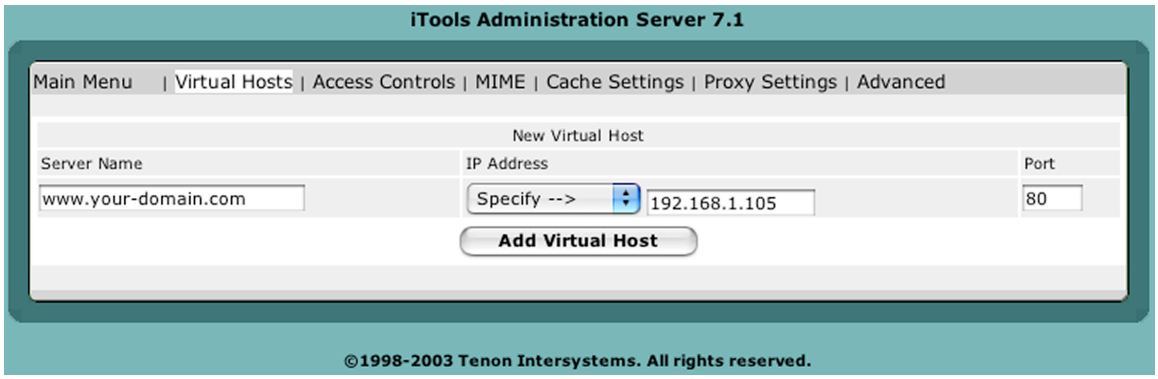
eth0 means ethernet device 0, which is usually the Built-In Network card, simply add the IP addresses that you wish to host on the appropriate interface. If you are unsure about this section, please contact your system administrator. Click "Apply" to save the settings.

VIRTUAL HOSTS

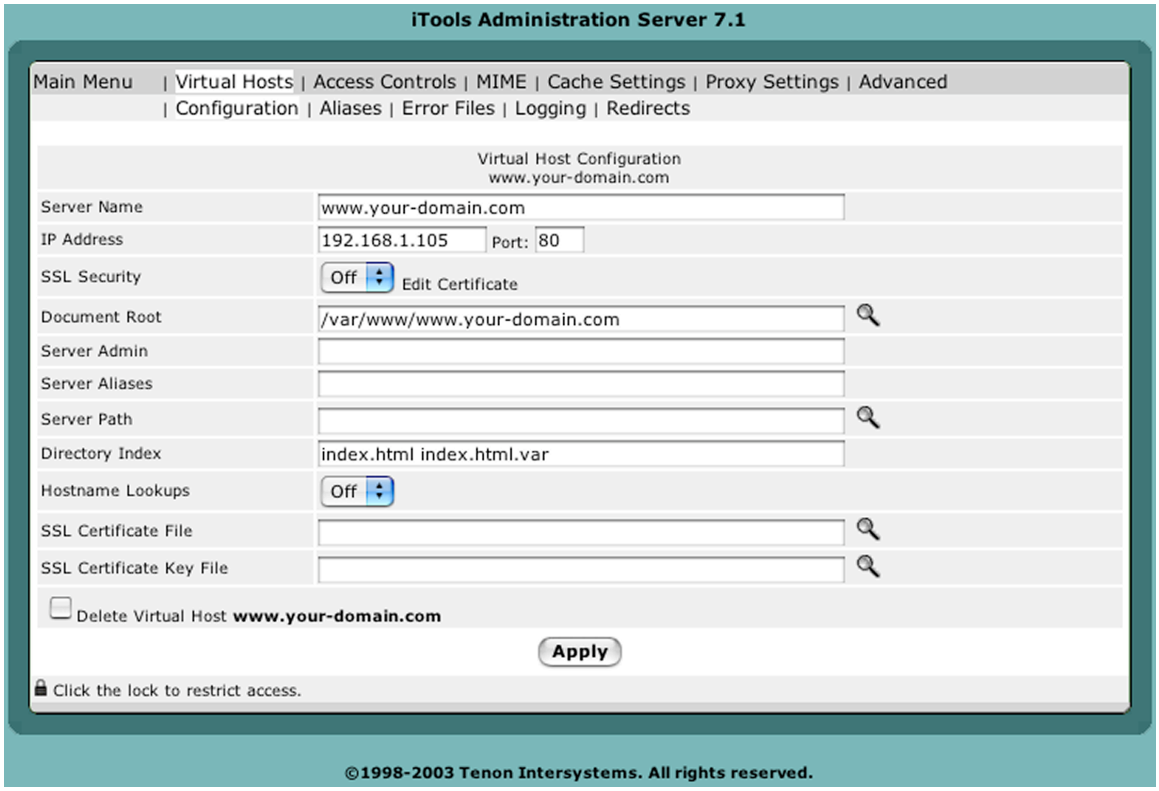
Once DNS and IP address are correctly set up, it's a simple matter to add virtual hosts.



Click on the Web icon, and click on "Add...". Virtual hosts can be added by selecting a virtual 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 “DirectoryIndex” field contains the name of the index file for your web site.

If you make changes to the virtual host configuration, click “Apply” to save virtual host configuration. The web pages go into the folder:

/var/www/www.your-domain.com

For now, you’re all set!

Your first host is up and running and can be accessed with a browser.

iTools Administration Server

4

Using iTools Administration Server, iTools services (Apache, DNS, FTP, SSL, etc.) can be configured using a modern web browsers. The web browser interface includes easy-to-use tables and forms that eliminate dealing with cryptic Apache directives and the nuisance of updating IP address aliases for each virtual server. 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 a different port number than the Apache web server (the default is port 85).

The browser may be running directly on the iTools system, or on a remote host connected via a network to the iTools system. Web browsers equal to or newer than Internet Explorer 5.2 are recommended to be used to connect to the iTools Administration Server.

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

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.

Additional users may be added to the iToolsAdmin group in two ways; they may be added via the menu item, Set Admin Password in the Admin menu of iTools Manager application or by using the Users and Groups tables accessible from within the iTools Administration Server pages (see Chapter 11, "Users & Groups").

In the event that all iToolsAdmin users are accidentally deleted, you will not be able to access the browser admin pages and would need to create an another iToolsAdmin user from the iTools Manager application.

NAVIGATING THE ADMINISTRATION PAGES

The iTools administration pages use many of the features of HTML forms and mod_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. Many items are displayed as under line links 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.

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

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.

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.

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.

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. Subsequent chapters will include details about each configuration option.

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.

System-Wide Configuration at a Glance

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 5, "DNS".

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 6, "FTP".

License Information
The License Information section contains your registered license information for iTools 7.

Mail Settings
The Mail Settings section contains configuration parameters for Tenon's iTools mail server. For more information, see Chapter 15, "Mail Settings".

Network Settings
The Network Settings section contains configuration parameters for IP address and Firewall settings. For more information, see Chapter 8, "Network Settings."

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 9, "System Status".

Users Settings
This section is used to set up users for various Tenon's iTools services including Web, FTP and Mail. Please refer to Chapter 11, "Users and Groups" for details.

System Update
This section is used to keep Tenon's iTools up to date with the latest security fixes and bug fixes from Tenon's Update system. Please refer to Chapater 10, "System Update" for details.

Web Settings
This section provides configuration options for the ApacheWeb Server. Please refer to Chapter 12, "Web Settings" for details.

DNS

5

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-to's 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.

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.

RUNNING ITOOLS WITH DNS ON

iTools DNS server can be started and stopped from the Server Controls page of the iTools Administration Server. For more details see Chapter 9, “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. “Installing iTools.” section “Configuration Before iTools install” on page 7.

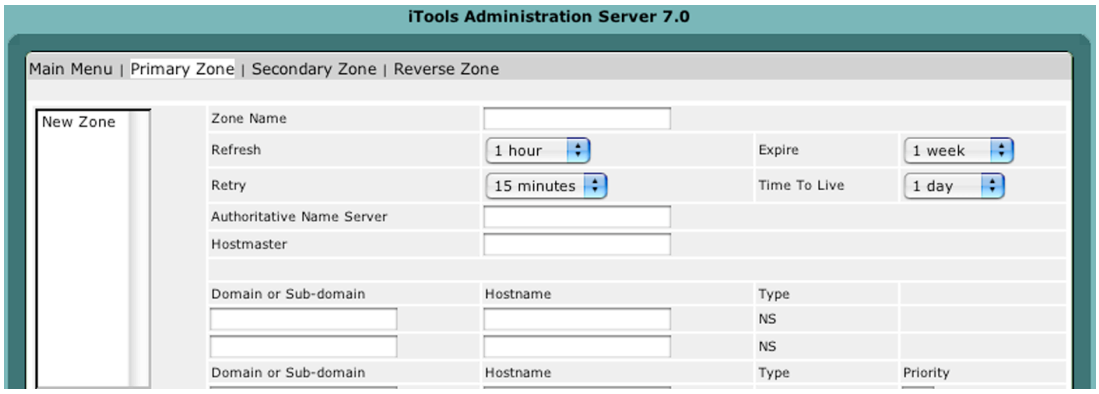
ITOOLS DNS ADMINISTRATION

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 from the System Status page.

When you select the DNS Settings button from the Administration home page, the web page displays a listing of Primary Zone 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.

PRIMARY ZONES

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.



Domain Name
Enter the Zone Name of the Primary Zone. Use the correct spelling For example: new-zone-here.com

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 23.

Authoritative NS and Hostmaster Values
The authoritative NS 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 at Network Solutions or Register.com. 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.

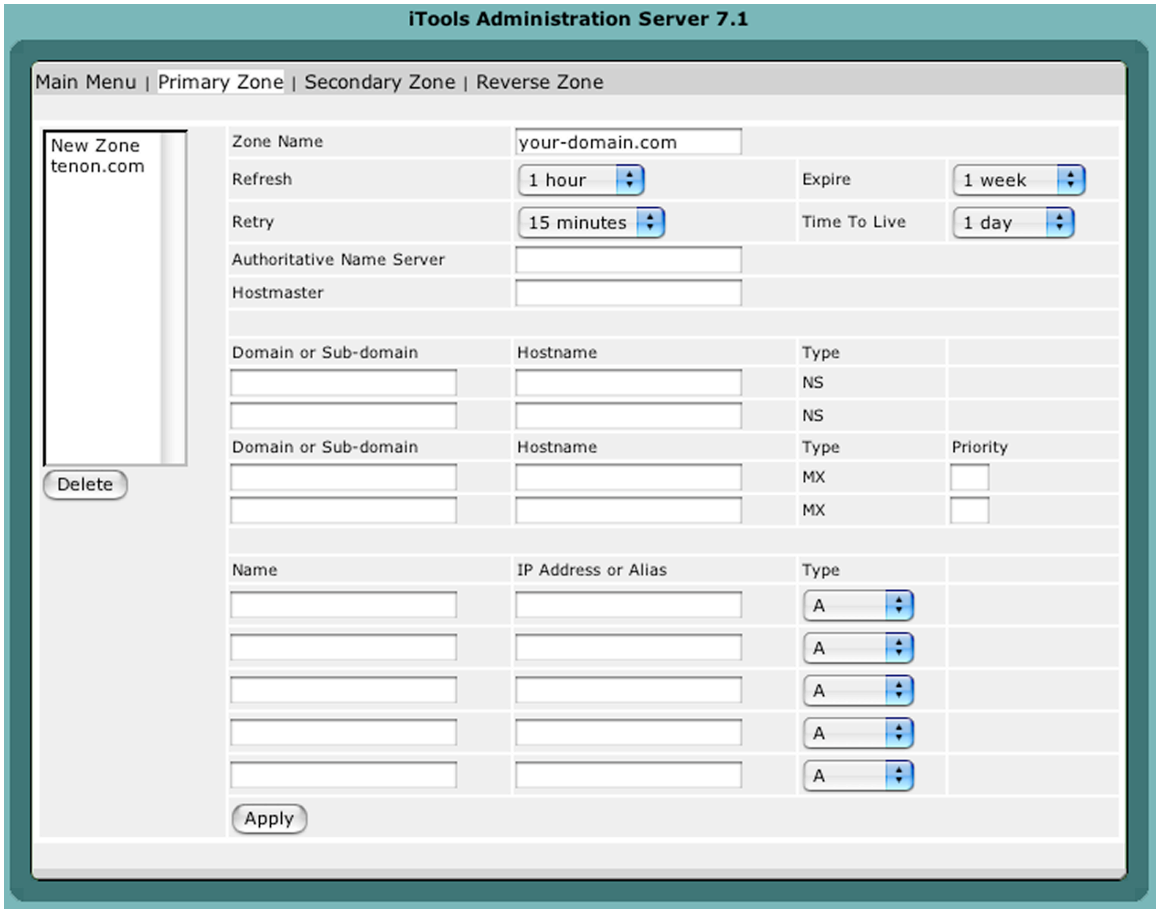
The Hostmaster value is an E-mail address for the person who should be contacted in the event of a problem. Instead of “@” sign used in the normal email address field, the sigh should be replaced by a “.”.

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 “Start of Authority” on page 23.

Select the Apply 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.

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.



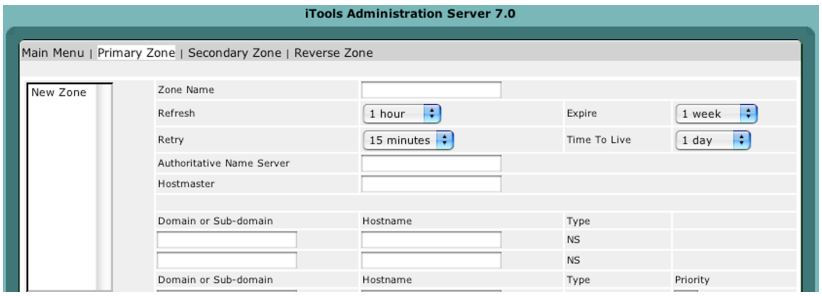
The Primary Zone page displays Host Names and Aliases (sorted alphabetically) that are currently in this Zone. Each row of the zone table shows the Host Name, its IP Addresses, Alias, Mail Exchangers, or Name Servers. To change the information about an entry in the table, replace the textfield with DNS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

There are additional record types which are optional, providing text information for example. And others that are experimental, but that are not currently in widespread use or supported by all DNS servers.

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.

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.

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.

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.

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 serious 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.

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.

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 at Network Solutions or Register.com. 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.

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 ".".

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 event 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.

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 names 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.

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 Apply button to get more blank row to fill out additional name server. Enter a dot, ".", at the end of the Host Name of the DNS server to prevent the zone name from getting appended to it.

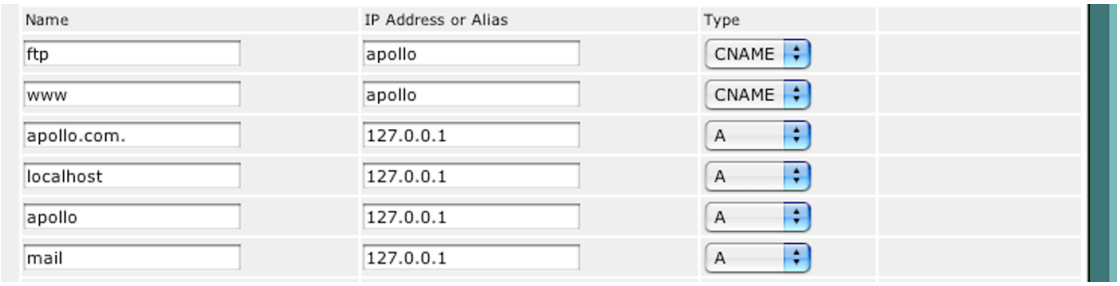
Save the Name Server record by clicking the Apply button. Repeat the process to add all of the name servers associated with this zone.

Domain Name
This entry should generally be listed 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 host name in the "marketing.company1.com"domain to the Host Name listed.

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

Host Name (A) Records

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.

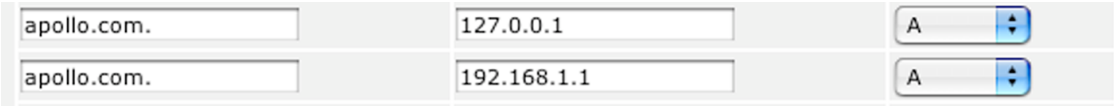
Enter the new hostname in the Name field and an IP Address in the Internet dot (“.”) notation, for example, “192.83.246.73”, for the IP address.

Select the Apply 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.

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 Apply button to see the changes.

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 Apply when you have finished.

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.

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.

Adding An Alias
The New Alias page is set by selecting the CNAME from the Type Pull down in the Primary Zone Page, and fill 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 Apply 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.

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 Apply button to see the changes.

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 Apply.

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.

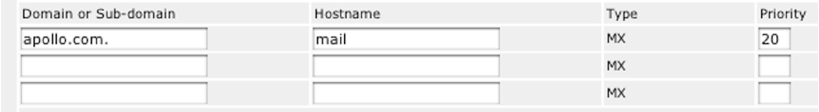
- 0 mail delivered here if the server is up and reachable
- 10 this server is second in line, and gets the mail if 1st is unavailable
- 20 third in line (gets mail if both 1st and 2nd are unavailable, and so on)

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.

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.



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 Apply 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.

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

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 simplistic 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.

Reverse DNS (PTR) Records

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 C class IP address, its IP Addresses.

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 Apply 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.

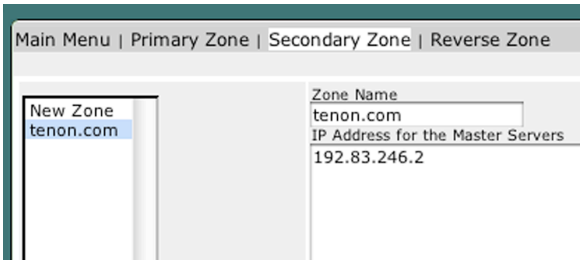
Deleting A PTR Record
To delete a PTR record, from the DNS Settings page, select the zone containing the PTR record you wish to delete. From the Reverse Zone page, empty the IP Node field for the unwanted PTR record. Click the Apply button to see the changes.

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 Apply when you have finished.

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.

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 Apply 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.

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 Apply 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.

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.

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 “x’s” represent 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.

FTP

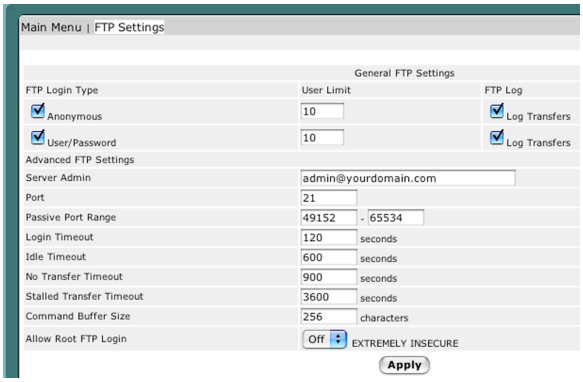
6

THE FILE TRANSFER PROTOCOL

The File Transfer Protocol (FTP) allows the transfer of files between networked computers. The FTP service provided with iTools is integrated into the iTools suite of applications and 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 server's filesystem.

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, and FTP transfers can be logged for either anonymous or password-based accesses.



Anonymous
The Anonymous checkbox 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 their FTP home directory. 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 fictitious “dirname” 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 fictitious “dirname” which will not allow listing of the folder by anyone except the root user, but will allow anyone to upload to it.

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.

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.

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.

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

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

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 hadle many simultaneous passive connections (for example, 49152-65534, the IANA-registered ephemeral port range).

Login Timeout
The Login Tmeout 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.

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.

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).

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.

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.

Allow Root FTP Login
Normally, proftpd disallow root logins under any circumstance. If a client attempts to login as root, using the correct password, a special ssecurity 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 message is still sysloged. Obviously, extreme care should be taken when using this directive.

ADDITIONAL FTP CAPABILITIES

The iTools FTP server (wu-ftp) has capabilities beyond those that are presented in the user interface provided by the iTools Administration Server. These features are configured by editing FTP’s directives in the .ftpaccess file. The documentation for the ftpaccess file is available at http://www.wu-ftpd.org/.

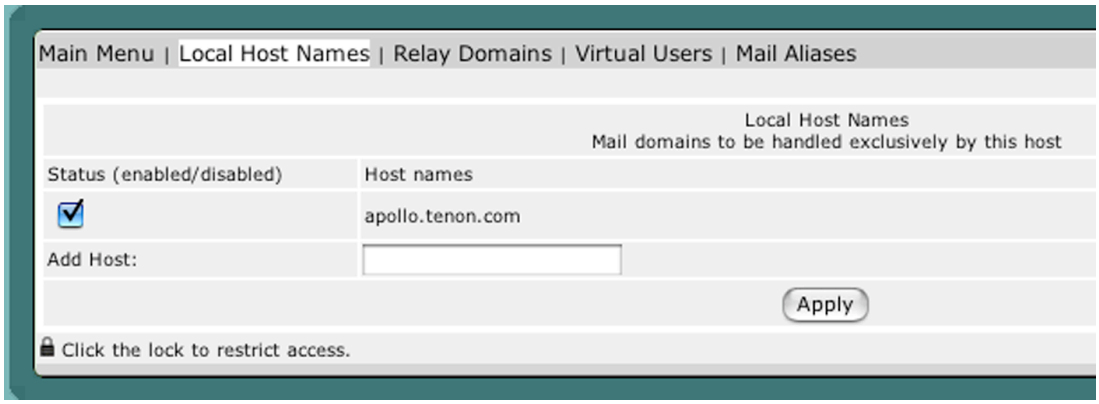
7

Mail Settings

The Mail Settings control the configuration of the sendmail mail server or, if 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.

SENDMAIL CONFIGURATION

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



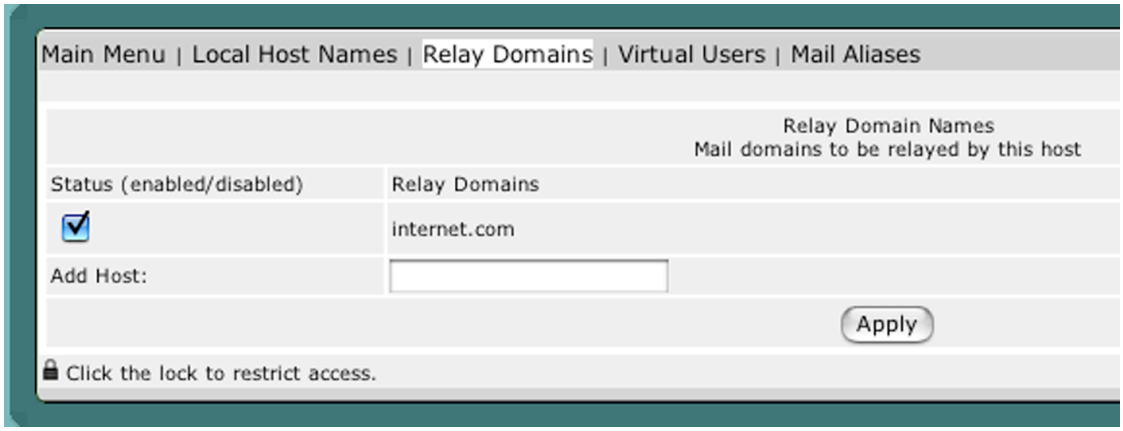
Enabled entries are added automatically for any virtual host added in the Virtual Host Configuration table. iTools will not automatically enable entries for a domain name added as a virtual host to avoid conflicting with established mail servers.

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.

iTools 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 100 for details on MX records.

Relay Domains
The Relay Domain Names table can be configured to include any domain names, host names, or IP address for which the iTools sendmail server should relay mail. Any mail that is sent through the sendmail 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.

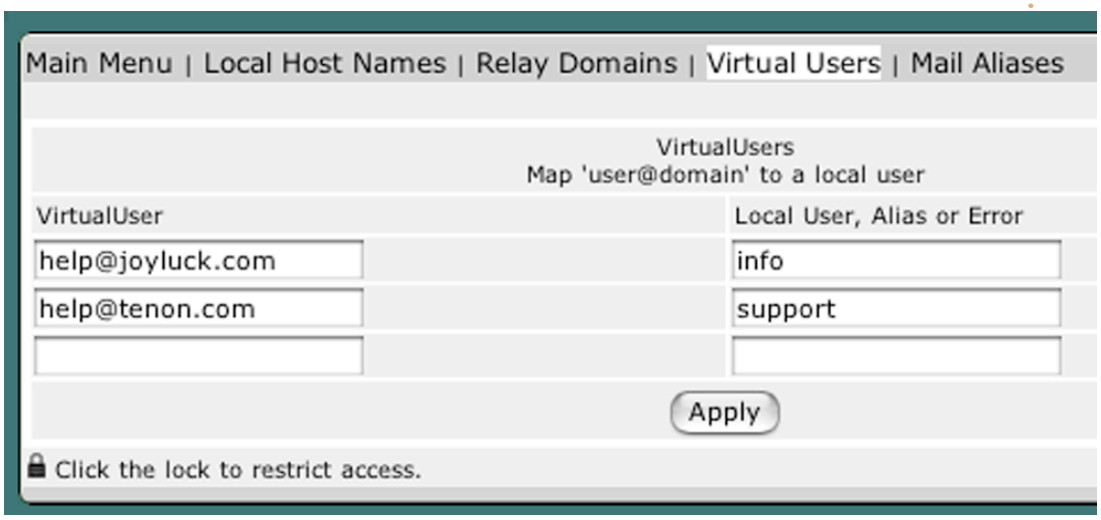
In general, clients should use their ISP's SMTP server for relaying mail. If this is not possible, or you are acting as the user's ISP, the domain name, hostname, or IP address of the client's machine may be entered in the Add Host: field of the Relay Domain Names table. Click on the Apply button to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



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 already established on the server for the user "support", they would not need an entry here.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 VirtualUser 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 VirtualUser 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 very powerful control of your mail server.

For more information on configuring real eMail accounts, see section “Adding Users” on page 65.

Mail Aliases
Mail Aliases can be used to set up simple mailing lists or for redirectingeMails to programs on the server. A list of eMail address 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.

POST.OFFICE CONFIGURATION

If Post.Office is installed on the same machine as the iTools 7, then mail administration is forwarded to port 9090 of the same server. Tenon recomends Post.Office for all mail needs. Post.Office is a powerful mail server and list sever for Mac OS X. 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 10 mail accounts or less. Please refer to Post.Office Administration Manual for Post.Office mail administration.

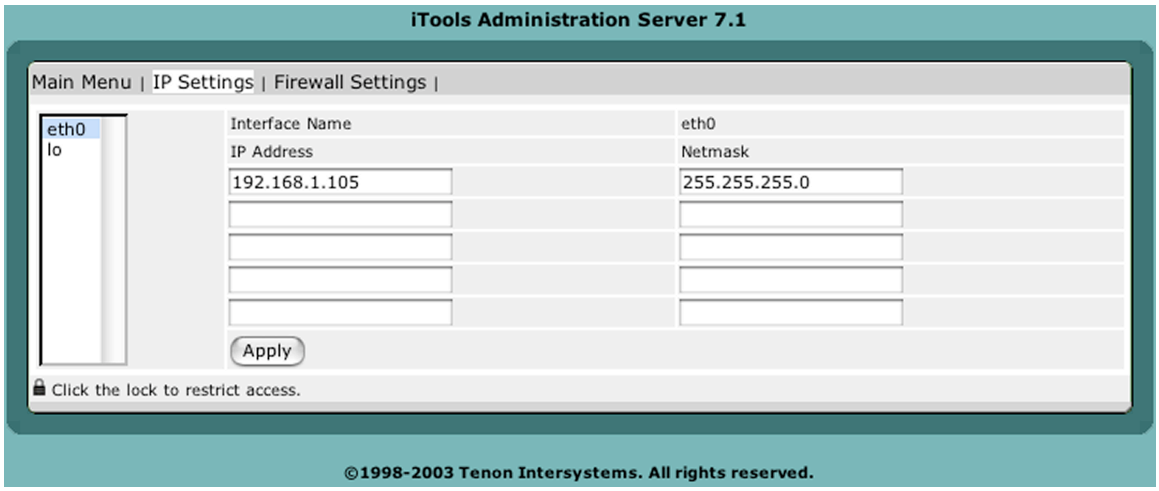
Network Settings

8

The Network Settings panel provides two features new to iTools: network card management and firewall management. IP Settings lets you configure your network cards (for example, your computer's Ethernet card). Firewall filters lets you block unwanted network communication.

CONFIGURE IP SETTINGS

Clicking on the Network Settings button in the Administration Server home page will bring up the IP Settings Screens. 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 en*.



The IP address is the 32-bit Internet host address, defined 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).

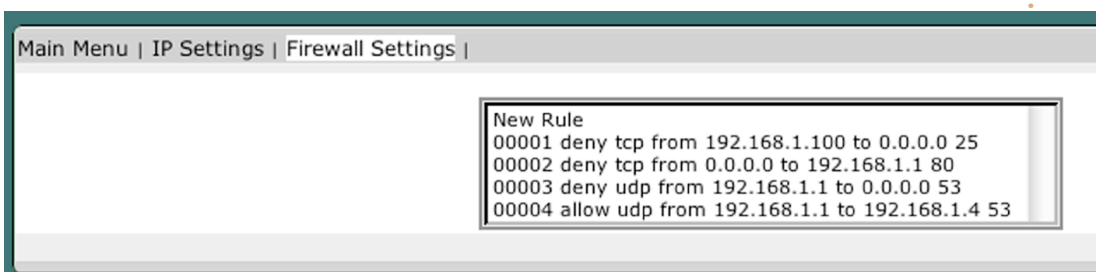
The gif interface is a generic tunnelling pseudo device for IPv4 and IPv6. It can tunnel IPv[46] traffic over IPv[46]. Therefore, there can be four possible configurations. The behavior of gif is mainly based on RFC2893 IPv6-over-IPv4 configured tunnel.

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

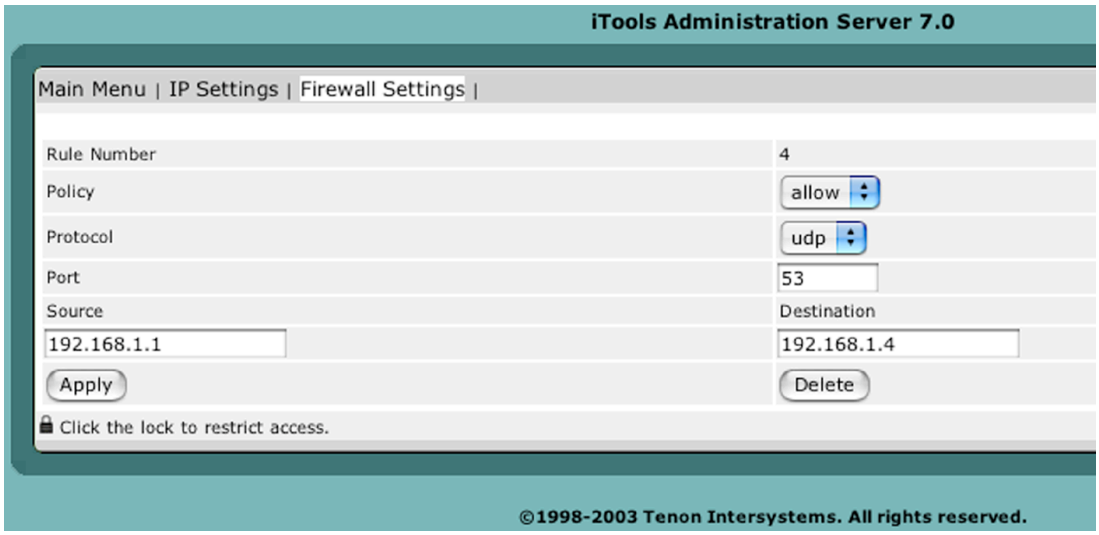
CONFIGURE FIREWALL FILTERS

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 Linux 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 things 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 more controls via the iTools Manager or 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, follow policy of the rules, 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.



Policy

Allow	Allow packets that match rule. The search terminates. Aliases are pass, permit and accept.
Deny	Discard packets that match this rule. The search terminates. drop is an alias for deny.

Protocol

TCP or UDP protocol to filter

Port

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

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.

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 an auto-recovery script such as the one in /usr/share/examples/ipfw/change_rules.sh.
- Don't forget the loopback interface.

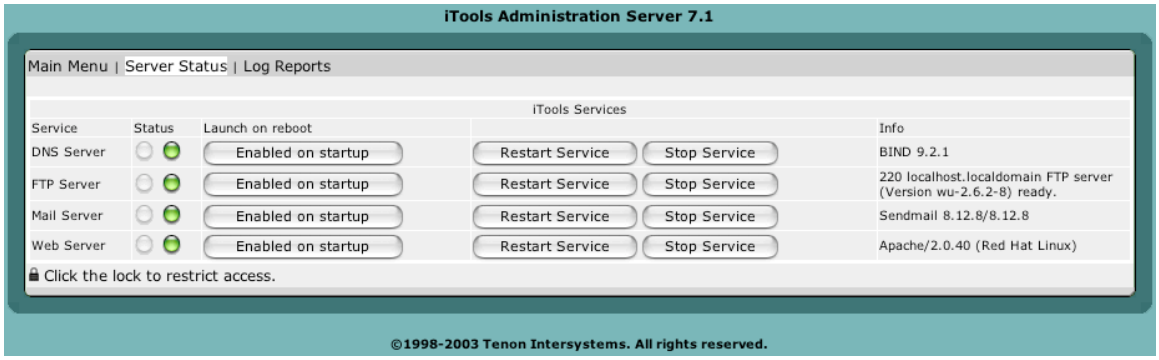
9

System Status

SYSTEM 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 the word Stopped appears in the status column and unavailable appears in the info column.



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

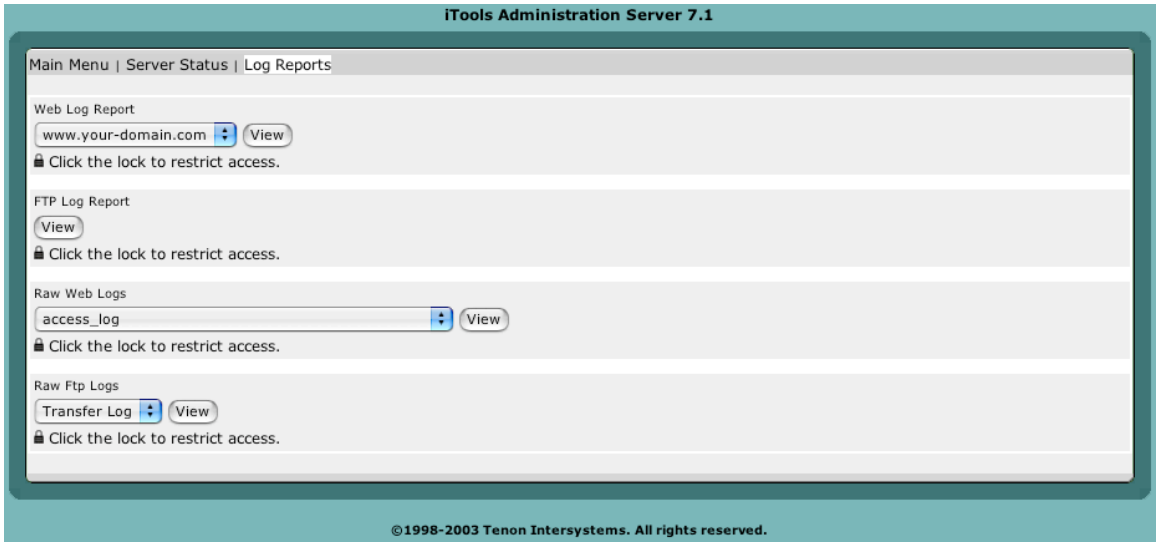
Restart Server
Clicking on this button will cause the web server to completely restart its operation. If the web server is currently running, This button will shut down the web server, and restart the web server again. If changes are made directly to the services configuration files, it is necessary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

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

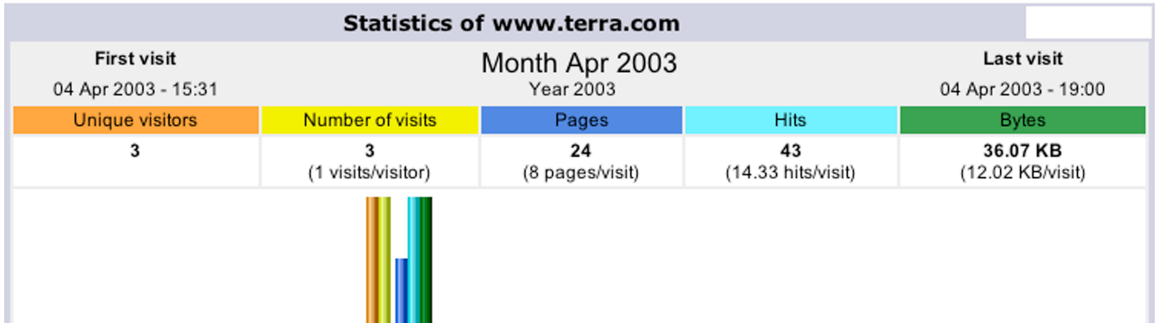
Server Info
The Server Info button provides a connection to service's current configuration information. This information includes details about the version of the software and what its current configuration settings.

LOG REPORTS

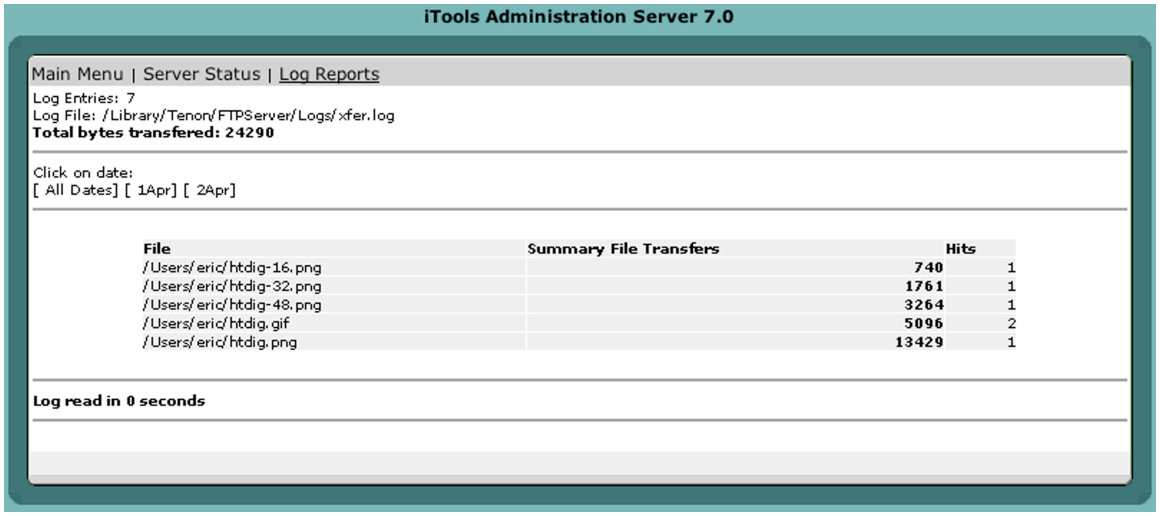
The Log report screen creates summary reports of Web and FTP traffic logs statistics.



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



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



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.

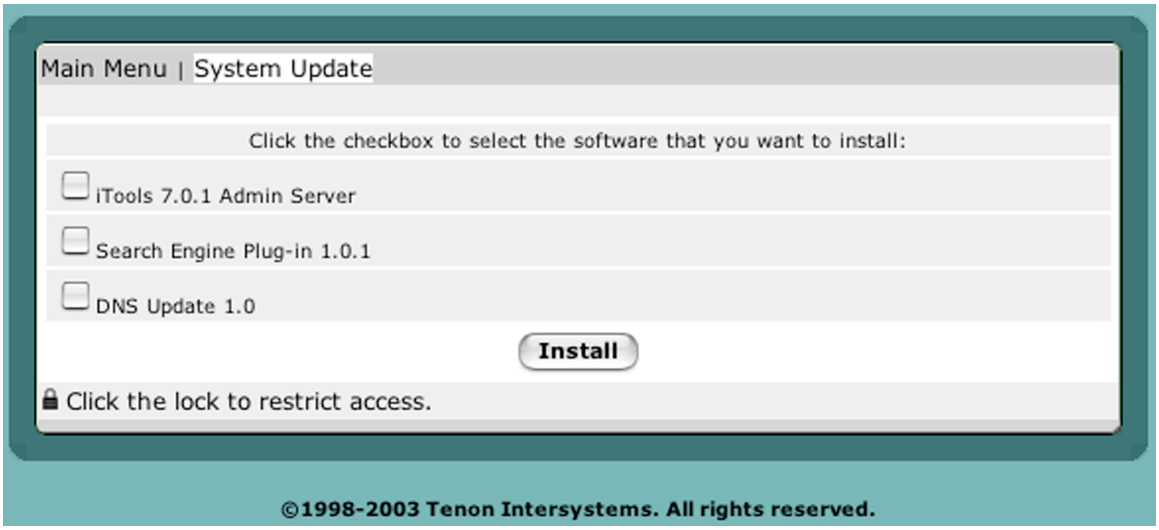
Raw FTP Logs

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.

System Update

10

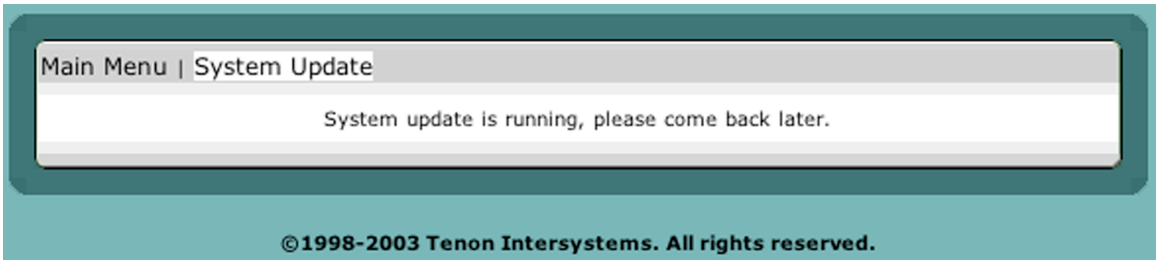
Periodically,Tenon releases updates to iTools. Using the System Update feature, you will be able to get iTools updates immediately.



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.



Users & Groups

11

iTools Users vs. System Users

Users on your server can have a variety of different kinds of access which may include:

- administration of the Linux 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 file with the server
- Access to electronic mail via the E-mail server
- users and groups with different access privileges to web pages.

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.

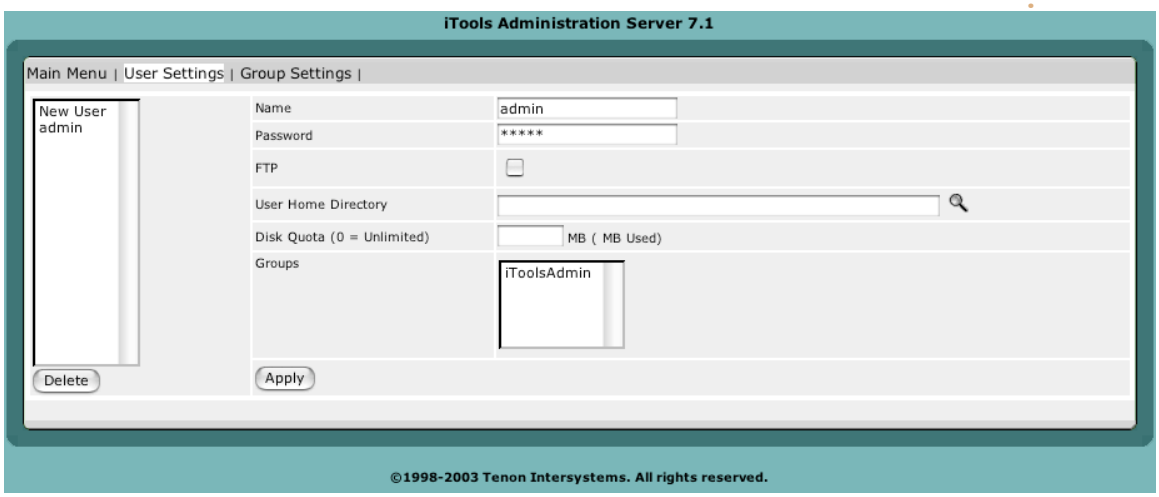
Tenon's iTools provides a set of realm-based access controls that can restrict access to a particular file or directory based on user names and passwords (see section "Realm Based Requirements" on page 41 for details on realms). Tenon's iTools also provides FTP service based on user names and passwords. 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 Linux privileges. These users can be configured to administer the Tenon's iTools Administration Server (see section "The iTools Admin Group" on page 59), or simply be allowed to log into realm protected directories via a web browser (see section "Realm Based Requirements" on page 41).
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 Linux Server's FTP server causes the user's œ 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 grant access to send and receive mail using POP and IMAP servers.

System user types	Description
Admin	User has all login capabilities (including eMail and FTP if those servers are enabled) and can administer system settings on the server.
Normal	User has all login capabilities (including eMail and FTP if those servers are enabled) but cannot administer system settings on the server.

USERS

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



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 Apply 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 defined 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 Linux system user database. Existing Linux users that are added to the iTools user databases are not changed

to FTP only. However, the system user password will be synchronized to be the same as defined in the iTools user database.

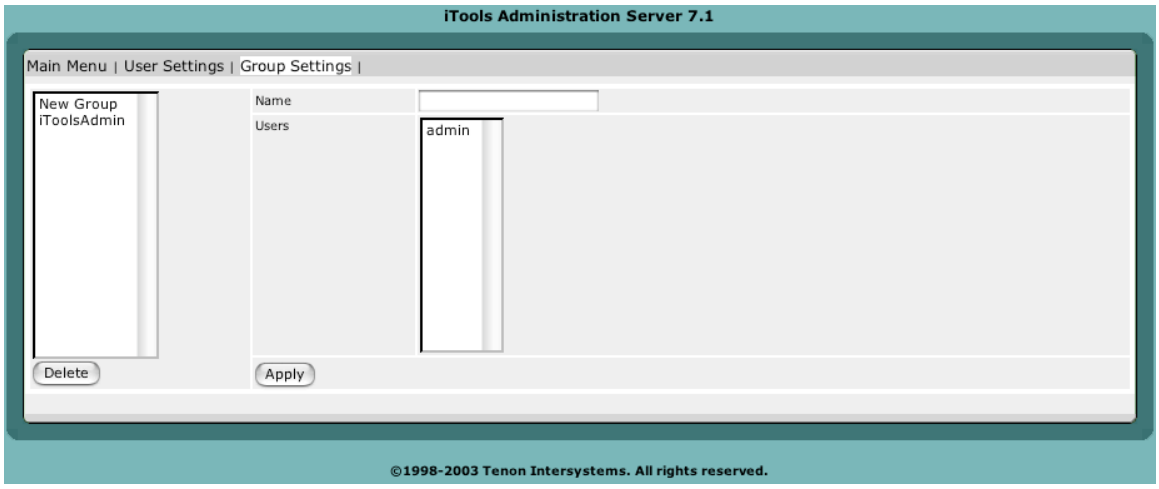
Once a user name and password have been entered, the new entry will show up in the table in alphabetical order. FTP user root directories are shown as paths.

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 Apply to submit the changes.

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.

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).



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 Apply 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.

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.

Modifying a Group Name
To change an existing group name, modify the text of the Name field and click Apply to submit the change.

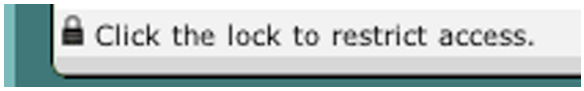
The iTools Admin Group
The iTools Administration Server uses a special group named iToolsAdmin. Members of this group are permitted access to all the iTools administration pages, and may make changes to the iTools configuration, including adding and deleting users and groups. If the iToolsAdmin group 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.

Authorization Service

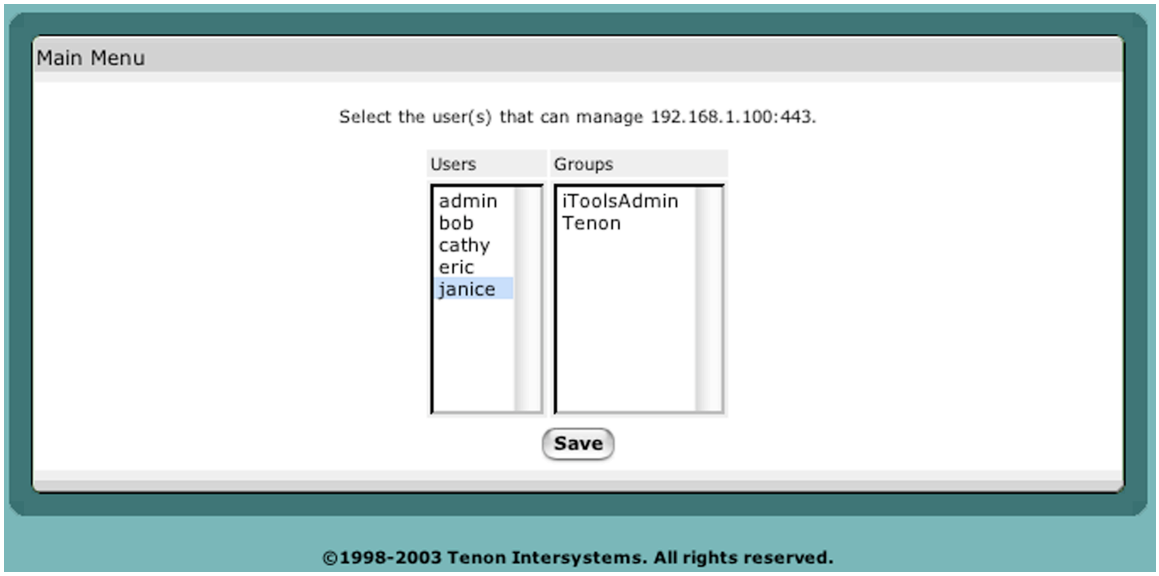
If you're a system or network administrator whose responsibilities include Internet Services administration, this section will help you grant management access to normal iTools users.

For example, Authorization Service let you centralize information about users, and iTools services so that advanced users can customize their own Internet services. And it simplifies the day-to-day management of administrative information by letting you update management access from the network in one central place.

Users can be assigned to manage parts of iTools without giving them full iToolsAdmin Privileges. This is done through clicking the link in parts of the Admin Server like this:



The Authorization service will be displayed a menu similiar to the following:



The authorization service will describe the type of service that can be managed by selected users. Select the users, click Save, and the authorization service will become effective immediately.

12 Virtual Hosts

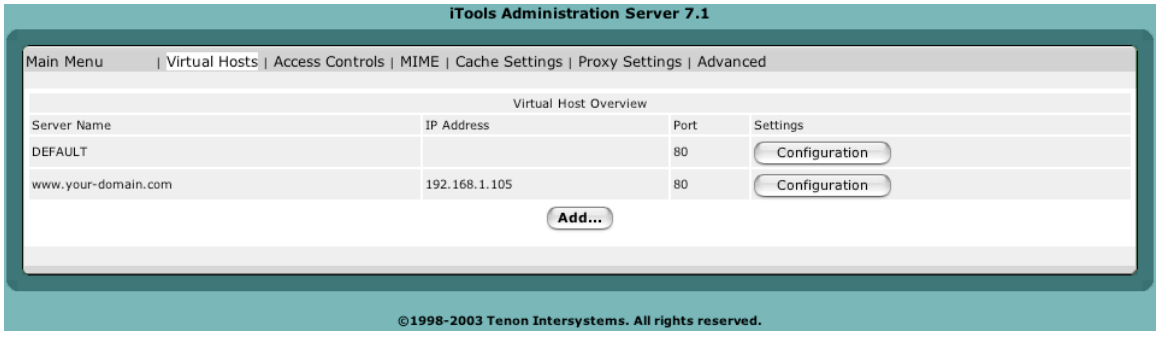
Apache provides the capability to support multiple servers on a single machine. Each server is differentiated by a unique host name. This feature is called virtual hosting. For example, it is often desirable for companies sharing a web server to have their own domains, with web servers accessible as 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.

VIRTUAL HOSTS 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.

Default Virtual Host

There are two key tables in iTools that control important configuration information for both the default Web server and any virtual hosts being served — the DEFAULT. Certain

items in the Virtual Host Configuration table may be inherited from the initial entries in the DEFAULT virtual host table. To view or modify these settings, click on the Configuration button for the DEFAULT virtual host.

The DEFAULT virtual host 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.

Adding Virtual Hosts
Additional virtual host names can be entered by clicking “Add...” button. 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 become active. Each virtual host has its own Virtual Host Configuration. These settings are accessible via the Configuration button.

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.

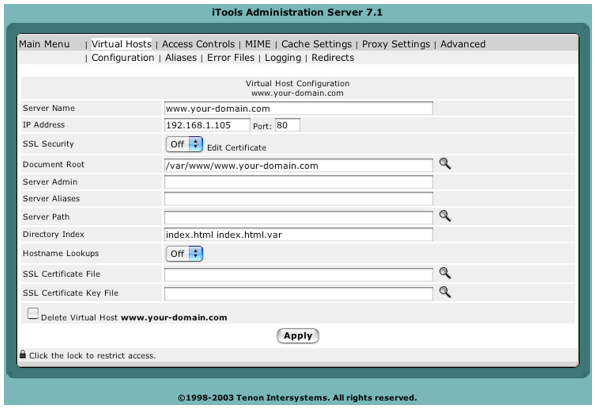
By default, iTools automatically creates a new, empty, directory for each new virtual host created. The name of the directory will match the name of the host that has been created.

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.

From the client point of view, they are unaware whether there are 2 or 200 hosts served by this machine. 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 Apply button.



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.

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.

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:

/var/www/www.some-domain.com
/var/www/www.your-domain.com
/var/www/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.

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 fix problems that arise with that host's web site or the server itself. Be sure this field contains a valid eMail address.

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 Hst do 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.

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.

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).

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 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 Linux web master in transition to Linux.
If the Directory Index field is left empty, the contents of the directory will be listed on the returned page.

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.

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 Chapter , “SSL,” for more information.

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 /etc/httpd/conf/ssl.crt directory.

Deleting Virtual Hosts
To delete virtual hosts from the Virtual Hosts Table, click on the Configuration 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.

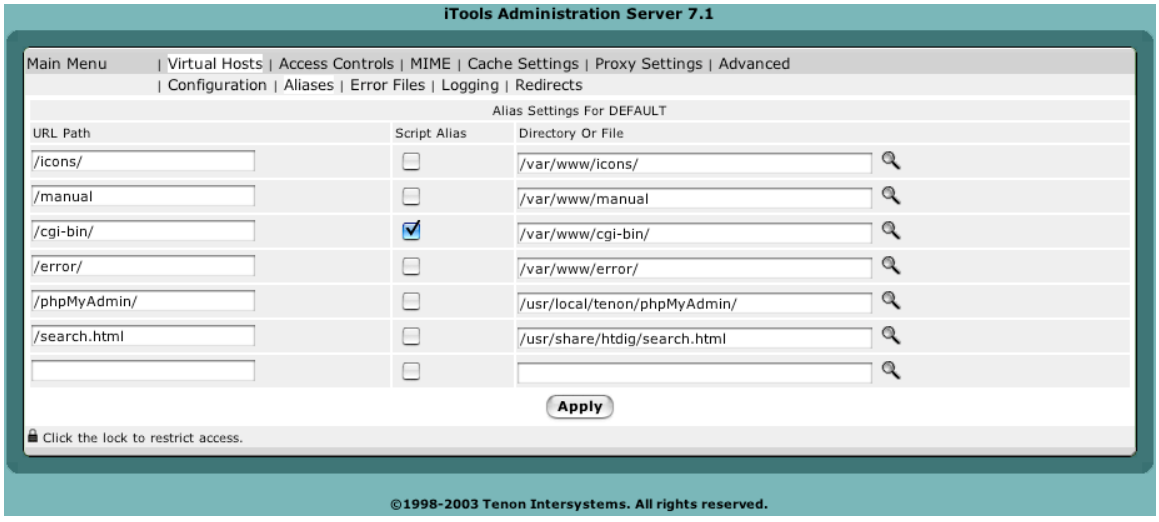
Click on the Apply button to submit the changes.

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.

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.

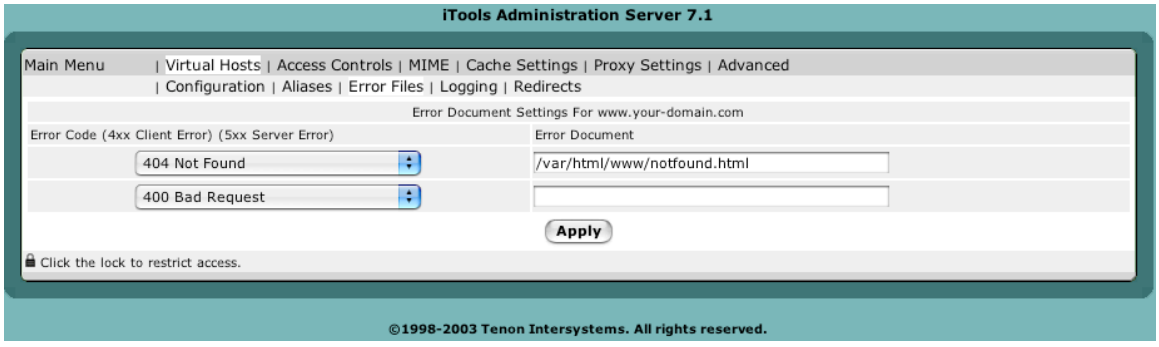
Tenon’s iTools’s initial DEFAULT virtual host settings contain several Aliases used by the iTools Administration Server, the iTools documentation, and in the examples. The default cgi-bin ScriptAlias is also specified in this table.

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 field. 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 Apply 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.

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 Apply button.

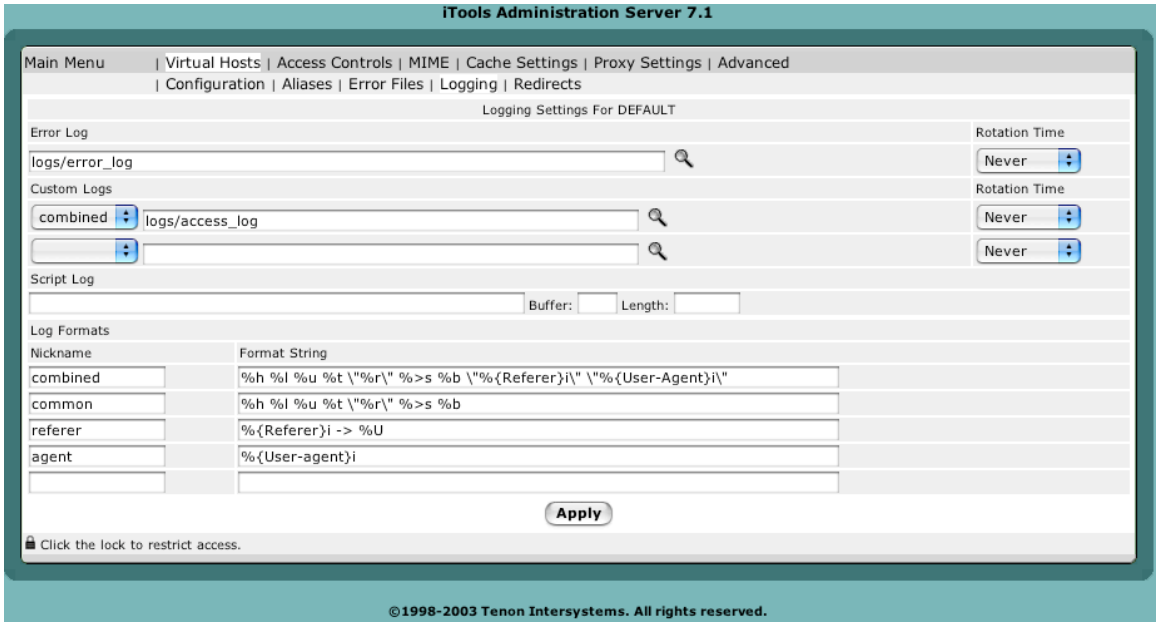
Remember that the path is a full path from the root of your server.

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 Apply 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.

LOGGING

The Logging link in the Virtual Host Configuration will display the logging settings for your server.



Most logging directives that specify a path to a log file will include a button to view the logs. This will allow an administrator to keep an eye on a server even from a remote location.

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.

Rotation Time
iTools automatically allow user to create rotated log without restart of the web server. Specify the period of rotation, and the log files will be created with the given file name and appended with Epoch date. The log file can be viewed in System Status. See Chapter 9, System Status for details.

CustomLog
The Custom Log directive is used to log requests to the server. The CustomLog is used to specify a log path and the log format nickname (as specified by the Log Format directive) to be used to format the log.

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.

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.
%...D	The time taken to serve the request, in microseconds.
%...{FOOBAR}e	The contents of the environment variable FOOBAR
%...f	Filename
%...h	Remote host
%...H	The request protocol
%...{Foobar}i	The contents of Foobar: header line(s) in the request sent to the server.
%...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 of 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)

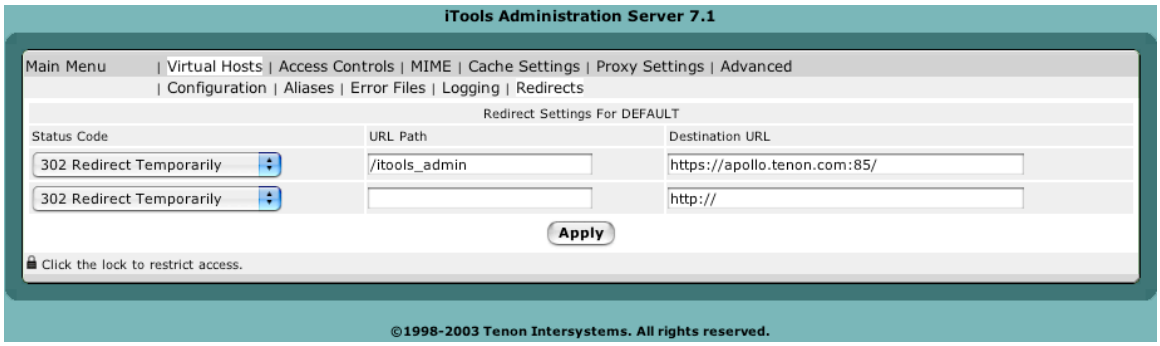
%...T	The time taken to serve the request, in seconds.
%...u	Remote user (from auth; may be bogus if return status (%s) is 401)
%...U	The URL path requested, not including any query string.
%...v	The canonical ServerName of the server serving the request.
%...V	The server name according to the UseCanonicalName setting.
%...X	Connection status when response is completed: X = connection aborted before the response 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.

REDIRECTS

There is a link at the top of each of the Virtual Host Configuration 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 2from 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 Apply 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.

SSL

13

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.

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.

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.

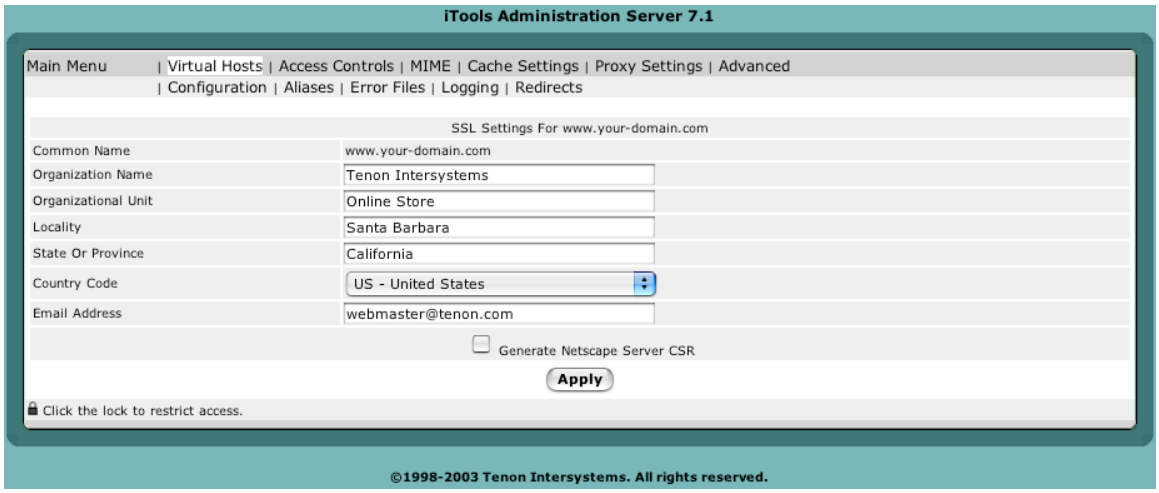
Your official certificate will be digitally signed and emailed to you by the CA.

Rename the certificate to "xx.xx.xx.xx.crt" (where <xx.xx.xx.xx> is the IP address of the virtual host for which the certificate was generated), and place the official certificate in the /etc/httpd/conf/ssl.crt folder. 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 works in conjunction with the SSL Key file located in /etc/ssl/private that was produced during the creation of the CSR. 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 page 80, for tips on how to prevent this form occurring.

SSL SETTINGS

To generate an SSL certificate, click on the 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).



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 qualified domain name, not an IP address or a DNS alias.

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

Organizational Unit
The Organizational Unit is the department name or the name of a unit within an organization. This field is optional.

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

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

Country Code
The Country Code is a two-letter code for the country in which the organization 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”.

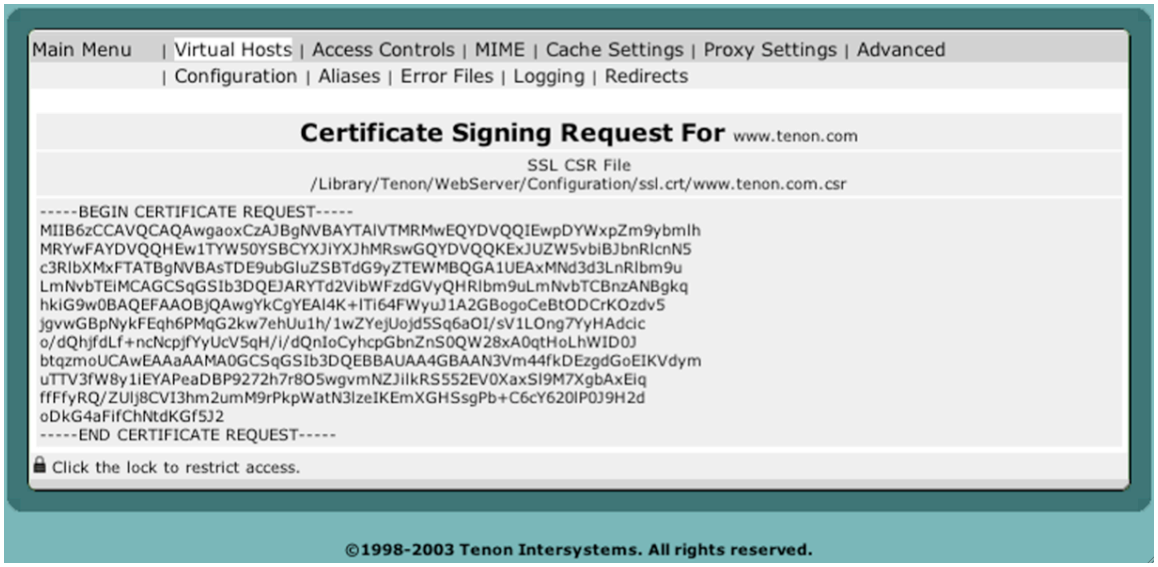
Email Address
The Email Address is the eMail address of a contact or representative within this organization.

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 (/etc/httpd/conf/ssl.key). This SSL Key file is important and should be saved once a CSR is produced. See section "Safeguarding SSL Keys And Certs" on page 80.

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 the /etc/httpd/conf/ssl.crt folder in a file named virtualhost.csr.



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

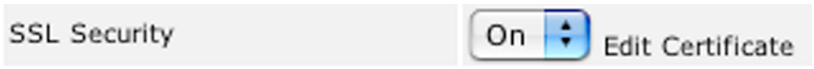
The self-signed certificate will allow your virtual server to perform secure transactions while your official certificate is being processed.

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 80 for more about these.

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.



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.

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.

Virtual Hosts with Both Secure and Un-Secure Service

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. Often, a redirect is created in the normal virtual host to redirect all traffic to the secure virtual host.

SAFEGUARDING SSL KEYS AND CERTS

Each SSL Certificate works in conjunction with the SSL Key file that was produced during the creation of the Certificate Signing Request. SSL Certificates 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 /etc/httpd/conf/ssl.key folder for backup.

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.

COMMON PROBLEMS

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 protentially 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 '\r' '\n' < original_certificate.crt > clean_certificate.crt

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

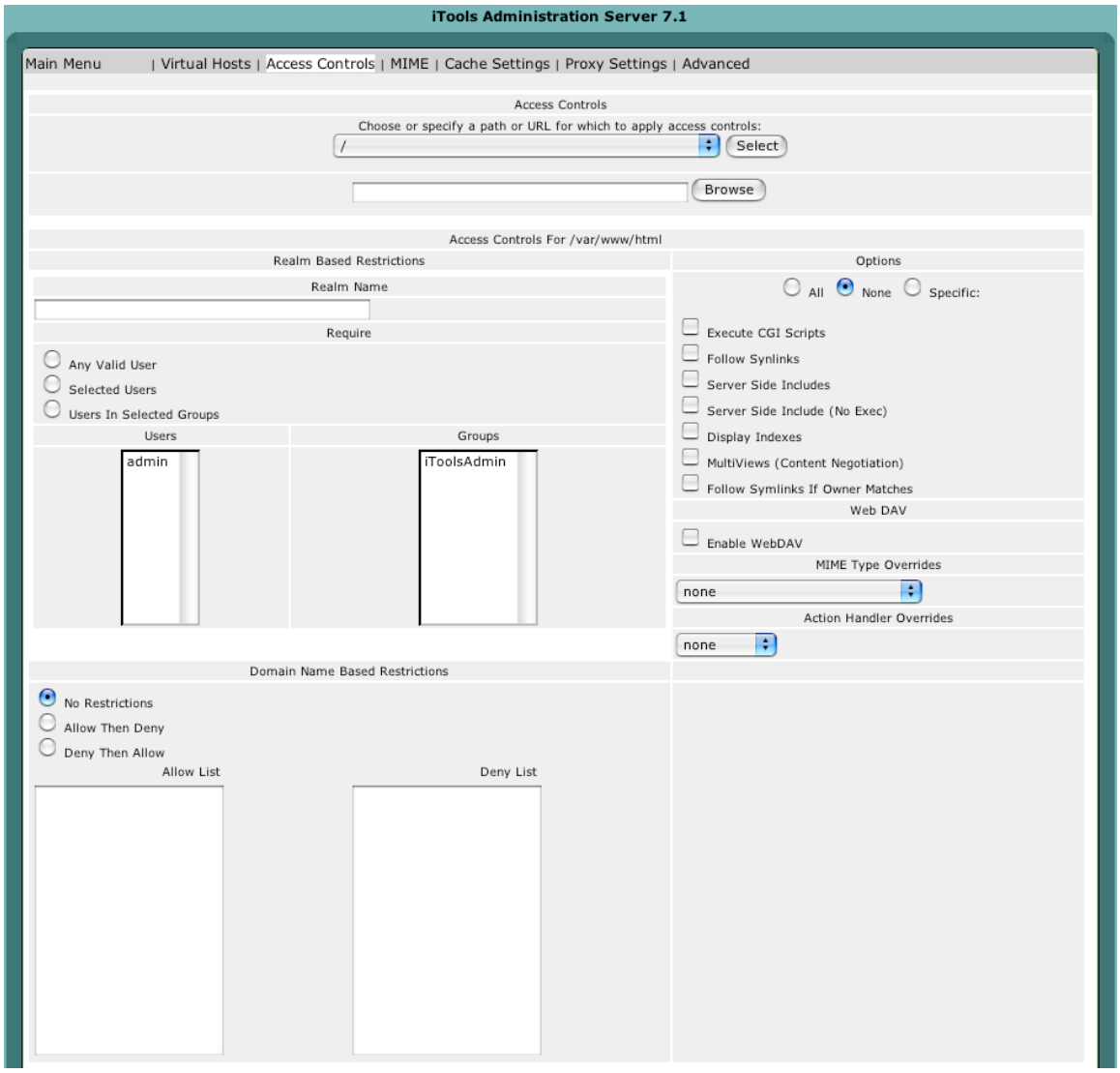
The issuer is Unknown
Some Certificate Authority credentials are not included in the bundled Certificate Authority Credential file. You can obtain the credential from your Certificate Authority, and append the credential to /etc/httpd/conf/ssl.crt/ca-bundle.crt. Restart the web server, and the settings will become effective immediately.

Access Controls

14

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.

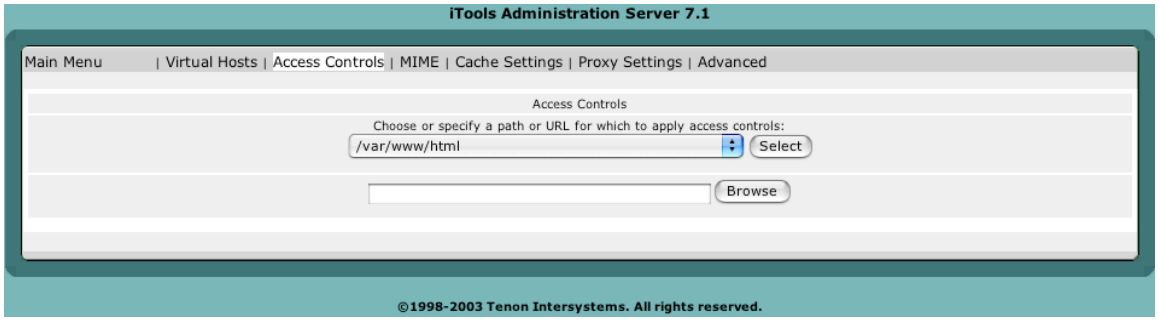


Included in the Access Controls section are settings for “Domain Name Based Restrictions”, “MIME Type Overrides”, “MIME Type Overrides”, “Action Handler

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.

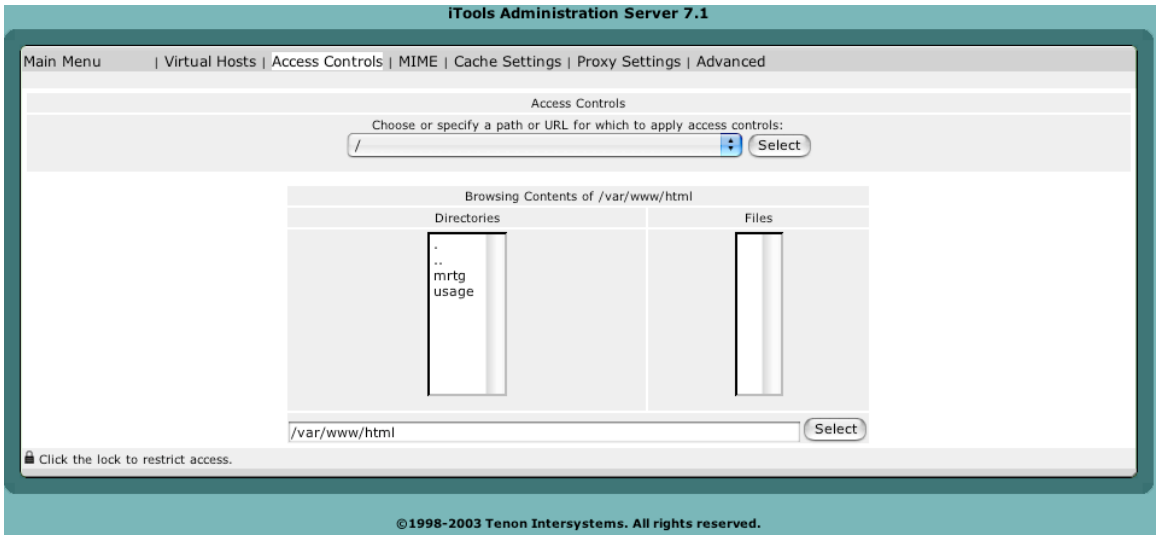
BROWSING CONTENTS

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 hosts'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. If the Browsing Contents table contains no items, it is a good indication that either the Document Root is mis-set or there have simply been no files uploaded for the virtual host.

Thus, the Browsing Contents table provides a means for finding any file or sub-directory within a virtual hosts'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.

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 “ParentDirectory” link is displayed as the first 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.

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.

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

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:

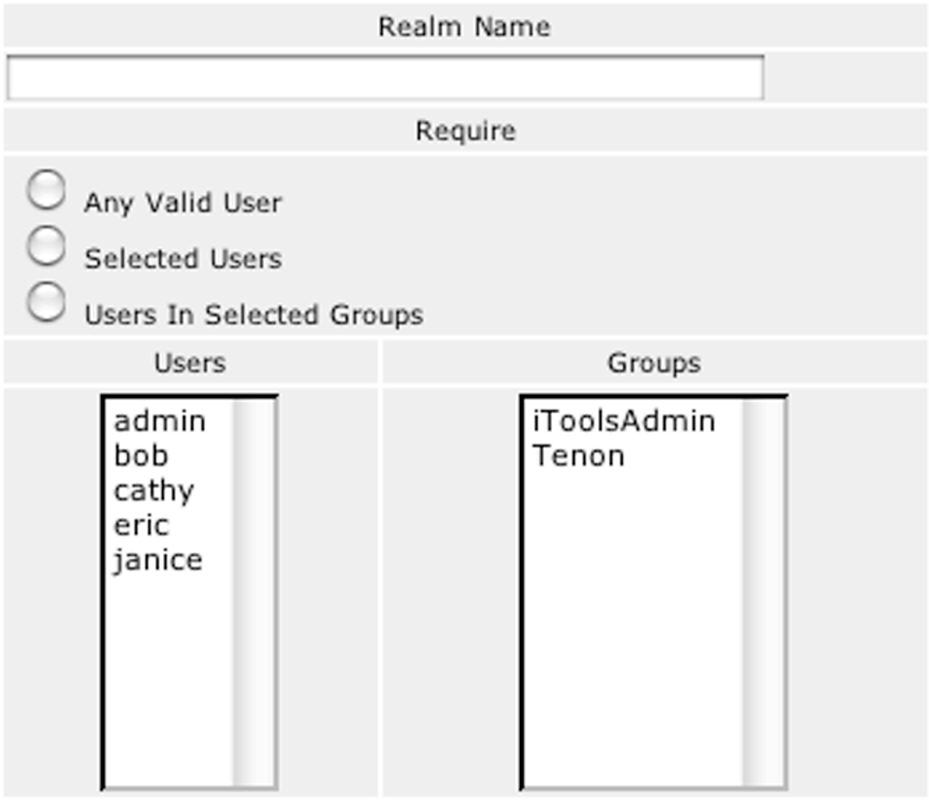
All	All options except for MultiViews. This is the default setting.
ExecCGI	Execution of CGI scripts is permitted.
Follow Synlinks	The server will follow symbolic links in this directory. Even though the server follows the symlink it does not change the pathname used to match against <Directory> sections. Note also, that 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 Script Aliase'd directories.
Display Indexes	If a URL which maps to a directory is requested, and the there is no DirectoryIndex (e.g., index.html) in that directory, then the server will return a formatted listing of the directory.
MultiViews	Content negotiated "MultiViews" are allowed.
Follow SymLinks If OwnerMatch	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.

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 privs to the user and group.

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 already configured. For details on setting up users and groups, see Chapter , “Users & 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 User	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. detail on setting up users can be found in Chapter , “Users & Groups.”
User in 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 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.).

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.

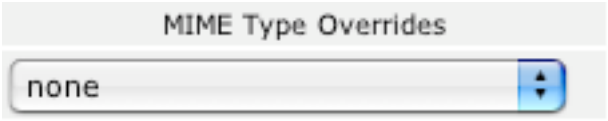
You would choose Deny then Allow, and enter the IP address of the offending client in the deny box. This would block access from that machine, but allow everyone else.

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 should contradict any Allow, the Deny setting takes precedence.
Deny then Allow	The Deny specifications are evaluated first, followed by the Allow specifications. If any Allow should contradict any Deny, the Allow setting takes precedent.

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 Chapter , “MIME,” for more information on MIME settings

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.

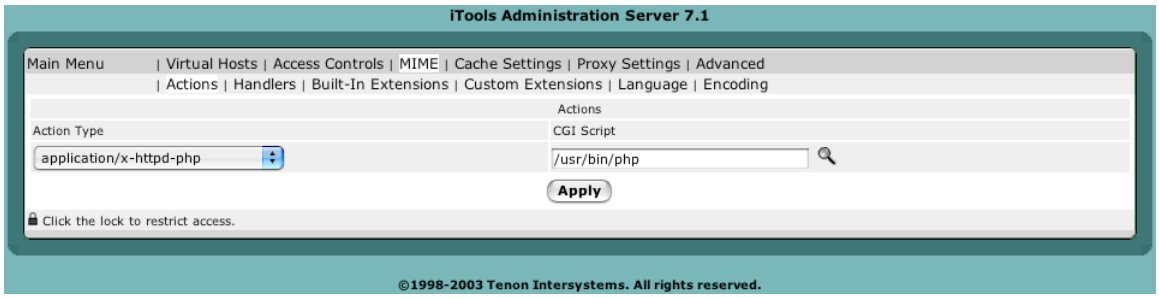
Folder or files without an explicit override inherit the settings of their parent folder/directory and the Inherited indicator will be displayed along with the inherited setting.

For more information about action handlers, see Chapter 15, "MIME."

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:

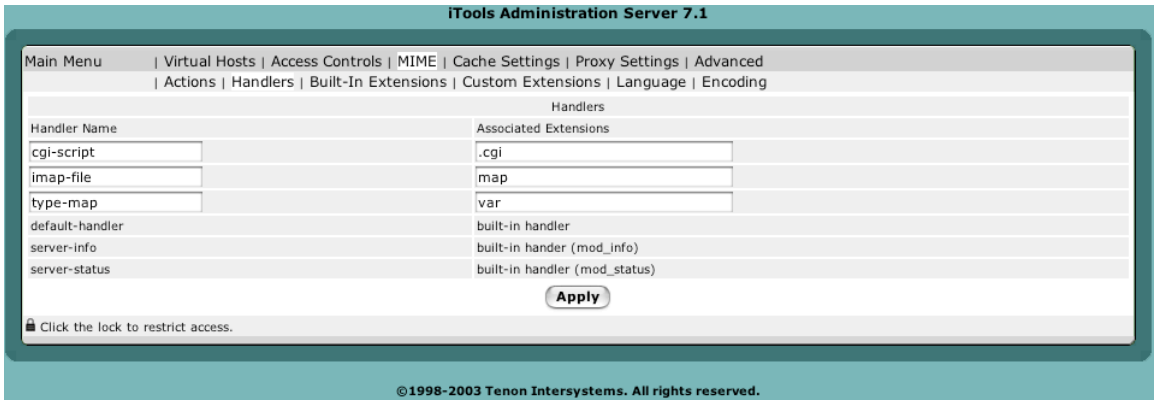


This will run CGI version of PHP for all PHP scripts.

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.

MIME EXTENSIONS

There are two MIME Extensions tables — the Custom Extensions table and the 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 Apply to submit the changes.

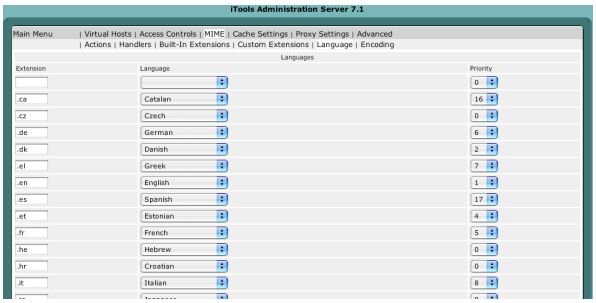
To change an existing extension, its MIME type, modify the extension or MIME type in the text edit field. Then click on Apply to submit the changes.

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 affects all files with this extension on this server.

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.

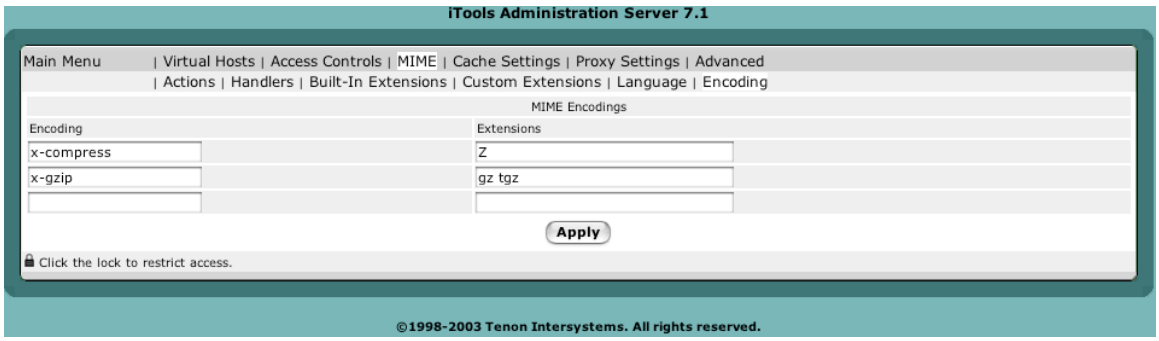


To map a new file name extension to a language, enter the extension in the empty text edit field in the first row of the table, and select a language from the pop-up list. The Priority sets the precedence of language variants for the case where the client does not express a preference, when handling a MultiViews request. Note that this directive only has an effect 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 Apply 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 Apply to submit the changes.

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 Apply to submit the new setting.

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

16 CACHE

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 Apply button to preserve your changes.

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.

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

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.

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.

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.

Disk Cache Settings
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 configuration file processing error. The Cache Directory Levels and Cache Directory Length directives define the structure of the directories under the specified root directory.

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.

Garbage Collection Interval
Garbage Collection Interval is the interval between garbage collections.

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.

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

Expiry Check
The Expiry Check directive observes expiration date when seeking files.

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

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

Garbage Collection Max Memory Usage
Maximum kilobytes of memory used for garbage collection.

Memory Cache Settings
Memory Cache
Enable cache to use system RAM for cache storage manager.

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.

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.

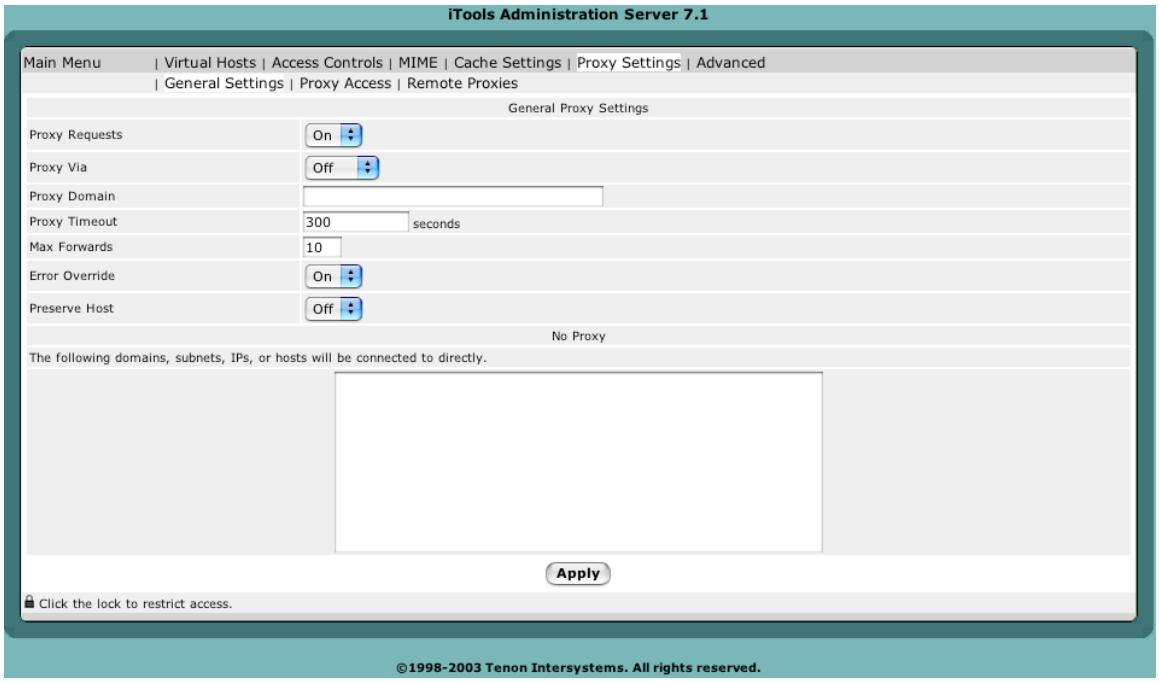
Minimum Object Size
The Minimum Object Size directive sets the minimum size in bytes of an object to be cached.

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

Proxy Settings

17

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.



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

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 lines removed. No new Via: header will be generated.

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.

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 appserver which hangs, and you would rather just return a timeout and fail gracefully instead of waiting however long it takes the server to return.

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

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).

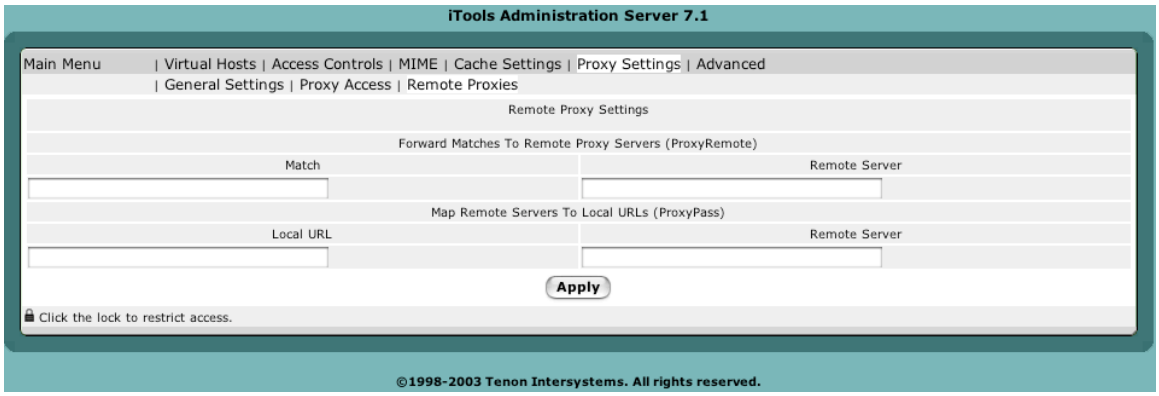
Preserve Host
When enabled, this option will pass the Host: line from the incoming request to the proxied host, instead of the hostname specified in the proxypass line. This option should normally be turned "off".

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.

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



ProxyRemote
The ProxyRemote setting specifies 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.

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

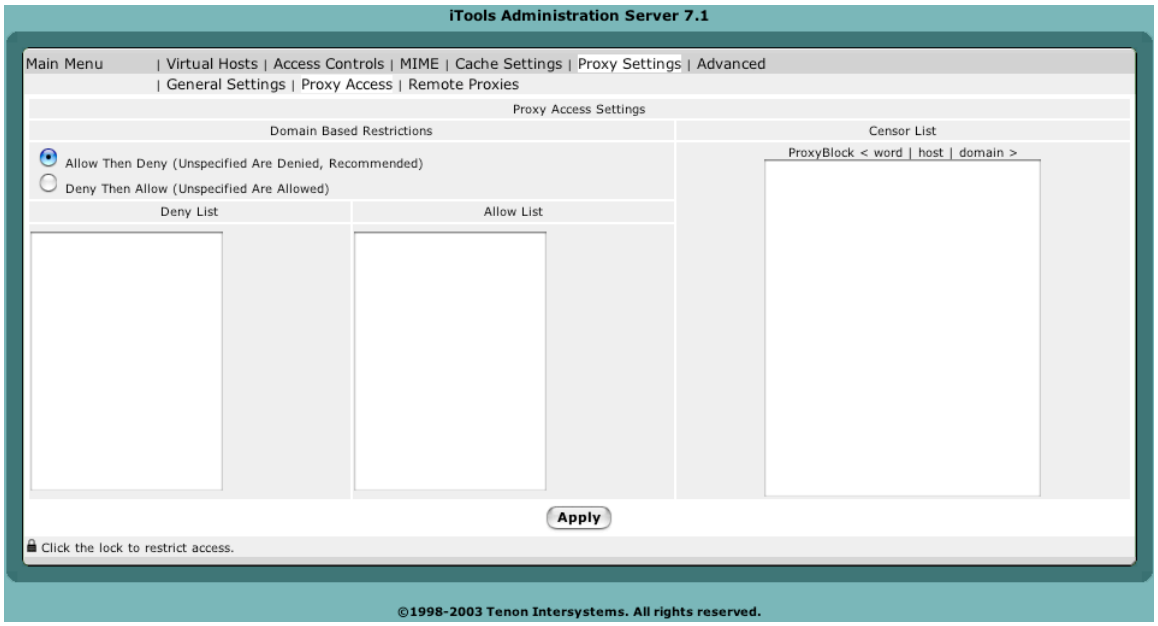
will cause a local request for:

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

to be internally converted into a proxy request to:

http://foo.com/bar

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.



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 40 for more information.

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.

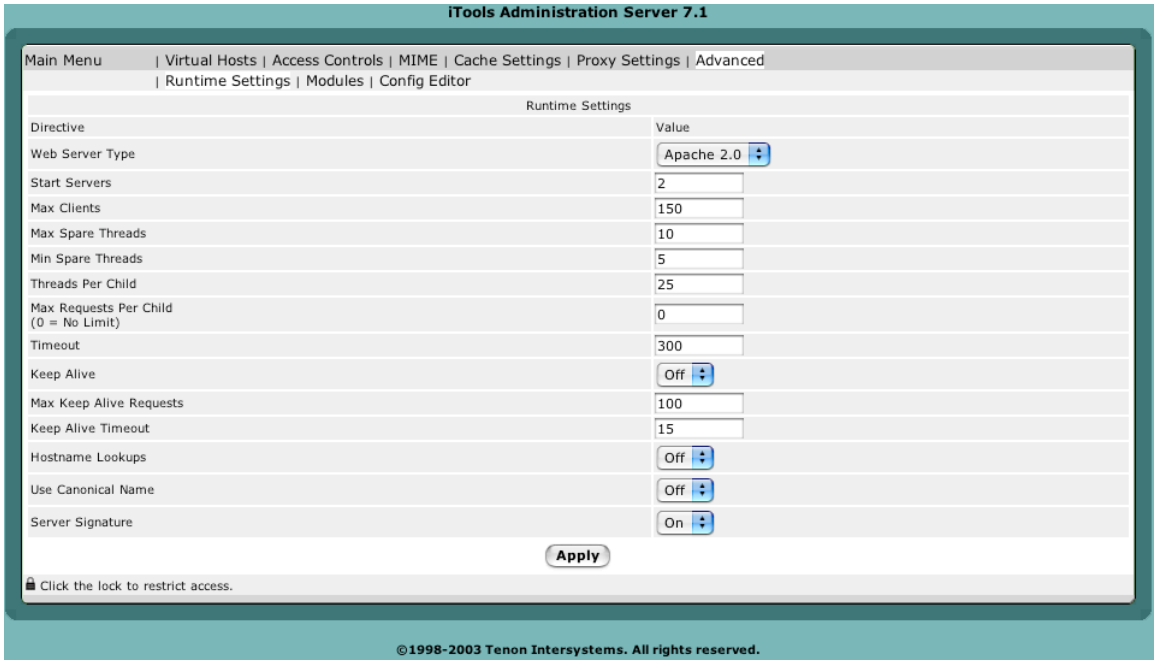
For example, if the ProxyBlock table contained:
nudes
games
some_host.com

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 sufficient to match “some_host.com”. Note also that the wild card “*” blocks connections to all sites.

Advanced Settings

18

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.



Web Server Type

The Web Server Type setting controls what version of the Apache Webserver are started on the Linux system. Apahce 2.0 is currently the only supported Webserver for Redhat 9.

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.

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.

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.

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.

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.

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.

Persistent Connections
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.

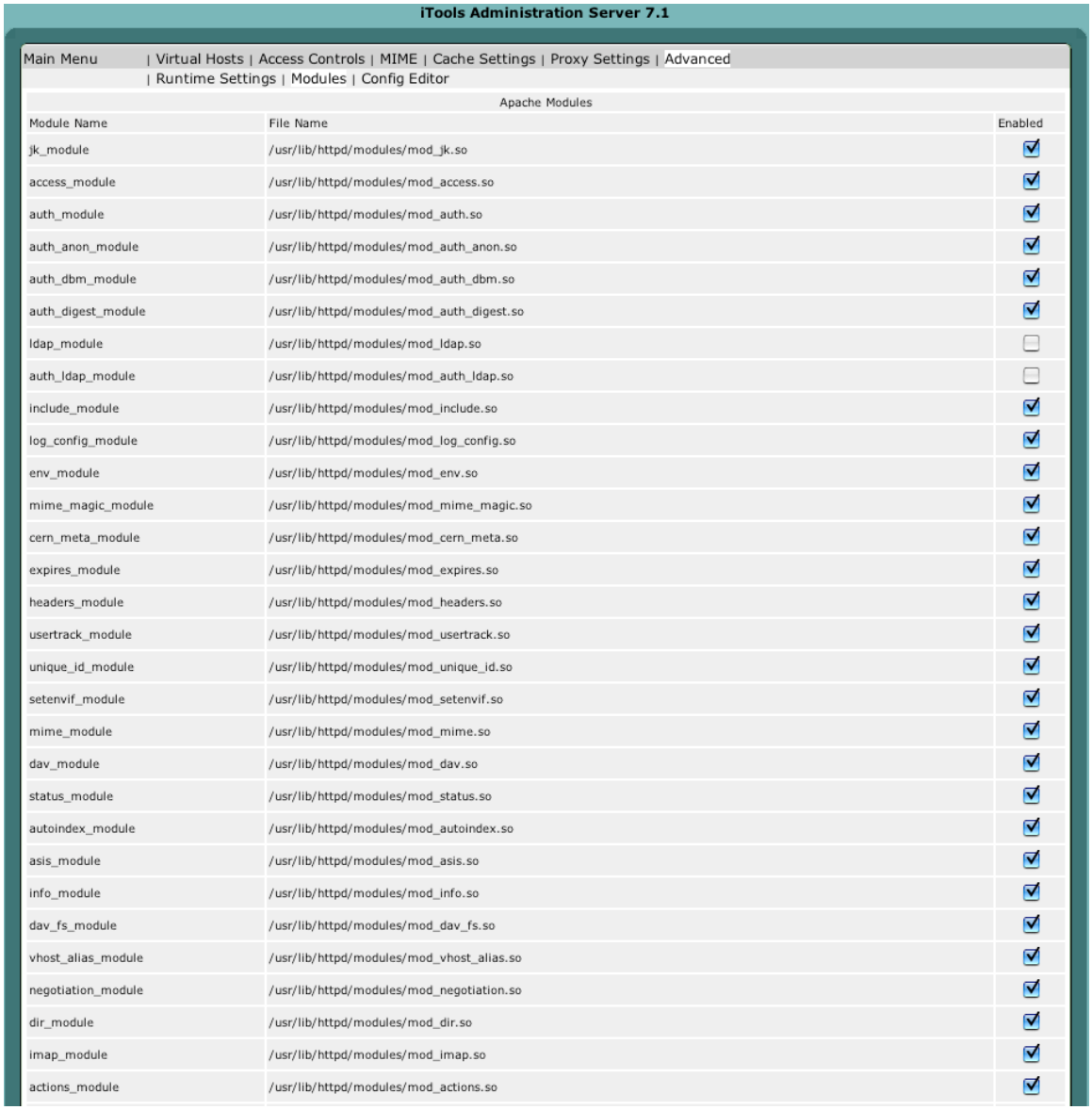
Max Keep Alive Requests
The Max Keep Alive Requests setting controls the number of incoming requests a client may embed in a single connection. The Max Keep Alive Requests setting is ignored if Keep Alive is Off.

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.

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 , “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.



iTools Administration Server 7.1

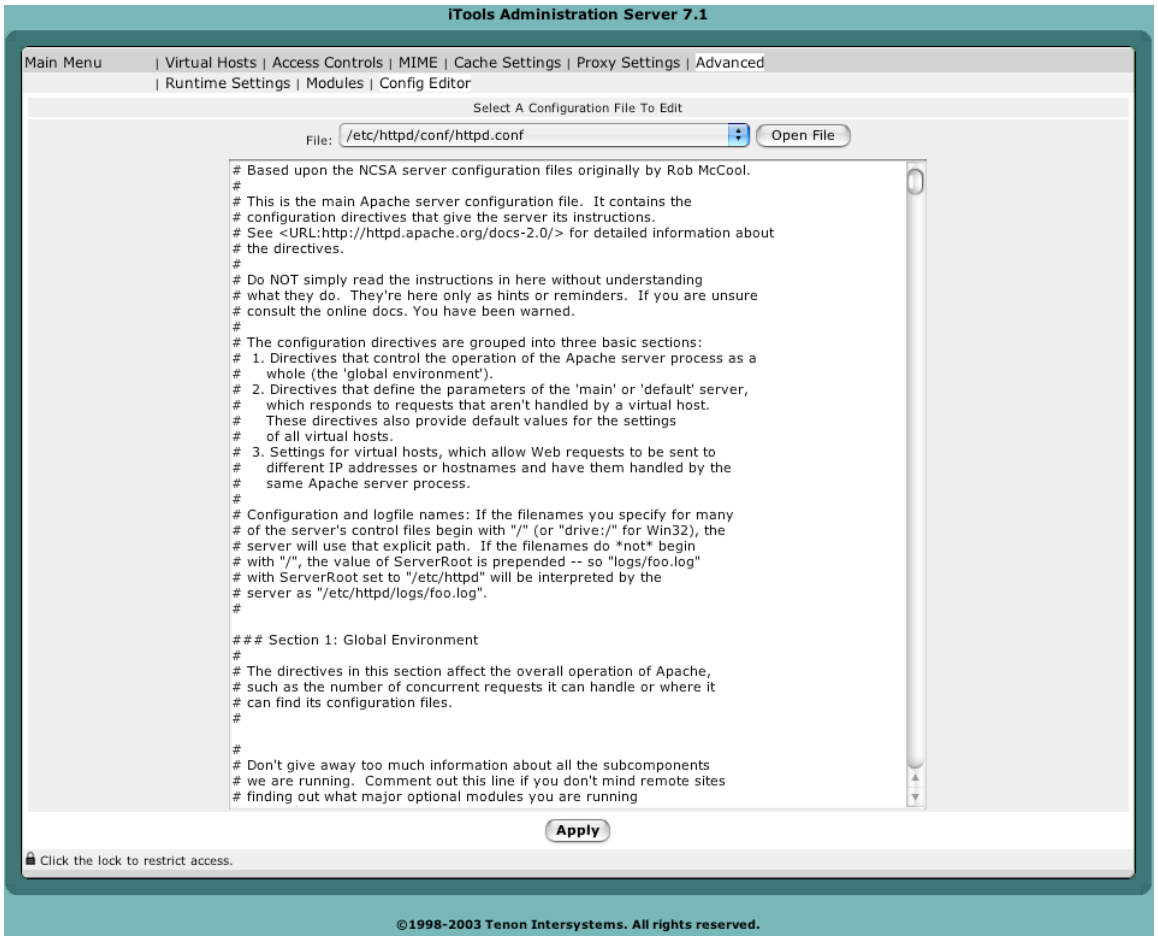
Main Menu | Virtual Hosts | Access Controls | MIME | Cache Settings | Proxy Settings | Advanced
| Runtime Settings | Modules | Config Editor

Apache Modules

Module Name	File Name	Enabled
jk_module	/usr/lib/httpd/modules/mod_jk.so	☑
access_module	/usr/lib/httpd/modules/mod_access.so	☑
auth_module	/usr/lib/httpd/modules/mod_auth.so	☑
auth_anon_module	/usr/lib/httpd/modules/mod_auth_anon.so	☑
auth_dbm_module	/usr/lib/httpd/modules/mod_auth_dbm.so	☑
auth_digest_module	/usr/lib/httpd/modules/mod_auth_digest.so	☑
ldap_module	/usr/lib/httpd/modules/mod_ldap.so	☐
auth_ldap_module	/usr/lib/httpd/modules/mod_auth_ldap.so	☐
include_module	/usr/lib/httpd/modules/mod_include.so	☑
log_config_module	/usr/lib/httpd/modules/mod_log_config.so	☑
env_module	/usr/lib/httpd/modules/mod_env.so	☑
mime_magic_module	/usr/lib/httpd/modules/mod_mime_magic.so	☑
cern_meta_module	/usr/lib/httpd/modules/mod_cern_meta.so	☑
expires_module	/usr/lib/httpd/modules/mod_expires.so	☑
headers_module	/usr/lib/httpd/modules/mod_headers.so	☑
usertrack_module	/usr/lib/httpd/modules/mod_usertrack.so	☑
unique_id_module	/usr/lib/httpd/modules/mod_unique_id.so	☑
setenvif_module	/usr/lib/httpd/modules/mod_setenvif.so	☑
mime_module	/usr/lib/httpd/modules/mod_mime.so	☑
dav_module	/usr/lib/httpd/modules/mod_dav.so	☑
status_module	/usr/lib/httpd/modules/mod_status.so	☑
autoindex_module	/usr/lib/httpd/modules/mod_autoindex.so	☑
asis_module	/usr/lib/httpd/modules/mod_asis.so	☑
info_module	/usr/lib/httpd/modules/mod_info.so	☑
dav_fs_module	/usr/lib/httpd/modules/mod_dav_fs.so	☑
vhost_alias_module	/usr/lib/httpd/modules/mod_vhost_alias.so	☑
negotiation_module	/usr/lib/httpd/modules/mod_negotiation.so	☑
dir_module	/usr/lib/httpd/modules/mod_dir.so	☑
imap_module	/usr/lib/httpd/modules/mod_imap.so	☑
actions_module	/usr/lib/httpd/modules/mod_actions.so	☑

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 user 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.

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.

Content Type Decisions

Mod_mime
: Determining document types using file extensions.

Mod_mime_magic
: Determining document types using "magic numbers".

Mod_negotiation
: Content negotiation.

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.

Directory Handling
Mod_dir
Basic directory handling.

Mod_autoindex
Automatic directory listings.

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.

Http Response
Mod_headers
Add arbitrary http headers to resources.

Mod_cern_meta
Support for http header metafiles.

Mod_expires
Apply Expires: headers to resources.

Mod_asis
Sending files which contain their own http headers.
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.

Internal Content Handlers

Mod_status
: Server status display.

Mod_info
: Server configuration information.

Logging

Mod_log_config
: User-configurable logging replacement for mod_log_common.

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

Miscellaneous

Mod_imap
: The imagemap 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.

Encryption

Mod_ssl
: Secure Socket Layers w/128 bit encryption.