Xoasis Networks

Turn Key v3.5

Reference Guide & License Agreement

KTX3 Server Appliance
Convergence Platform 2004

Turn Key v3.5 Reference Guide

CONTENTS

Overview

Xoasis Networks thanks you for selecting Turn Key v3.5 as your turnkey solution for hosting.

The Turn Key v3.5 software suite provides instant access to Web, FTP, Mail, SQL, and DNS hosting solutions. All services are configurable through an easy-to-use Web interface that allows you to either manage all account administration yourself or to delegate this task to your users.

The Turn Key solution is perfect for users looking to easily set up a dedicated Internet presence without having to pay high-priced technical consultants or worrying about system failures in proprietary systems. The Turn Key software suite can also be used by ISPs to offer existing customers e-mail and hosting solutions, either as part of a package or at an additional cost.

All of the hosting modules contain widely adopted industry-standard technology including:

- Apache Web Server
  - Currently utilized on 58% of Web servers
- Exim SMTP Server
  - Provides anti-spam RBL and per-user virtual domain hosting
- Qpopper POP3 Services
  - Utilizes POP-b4-SMTP anti-relaying security
- BIND DNS Server
  - Support for all DNS record types as well as dynamic DNS
- MySQL Database Server
- VoiceIP SoftPBX
  - Traditional Voice over IP implementation provided by Xoasis

In addition to utilizing industry standard software, the Turn Key suite contains such advanced features as bandwidth capping and monitoring, load balancing, clustering, anti-virus, user rights management, and much more.

Server Appliance Setup Instructions

When you are ready to set up your Server Appliance, unpack shipping box carefully and check that it contains:
1 power cord
1 Xoasis Networks Server Appliance
1 **System Password Security** card

For the initial setup, you will need:
A monitor
A PS/2 keyboard

1. Place Server Appliance next to a monitor and keyboard for initial network configuration.
2. Plug monitor and a PS/2 keyboard into back of Server Appliance.
3. Plug the power cord into the Server Appliance and a wall-outlet.
4. Press power button on the front face plate of the Server Appliance to power-up the machine.
5. Wait for the Server Appliance to load. You will be prompted to enter a username.
6. You will need to enter the correct username and password.

1) Type in **blackbox** for your **username**
2) Type in the **password** listed on the **System Password Security** card which was supplied in the shipping box

7. You will now be presented with the **System Configuration Shell**
8. Type 7 and hit enter to configure your network settings
9. Enter your new IP Address, Subnet Mask, and Gateway Address.
10. The Server Appliance will restart.
11. Power-off the Server Appliance anytime after it begins to restart and move it to its primary or permanent location.
12. When you power-on the Server Appliance from its primary or permanent location, make sure the network cable is plugged into the network jack marked with an arrow located on the right side of the back of the appliance. Continue Server Appliance configuration from http://the-ip-address-you-entered:9999

Network Settings Configuration Guide

After initially configuring the Server Appliance's IP address and plugging it into its final (permanent or primary) network location you should visit the following URL:

http://the-ip-address-you-entered:9999

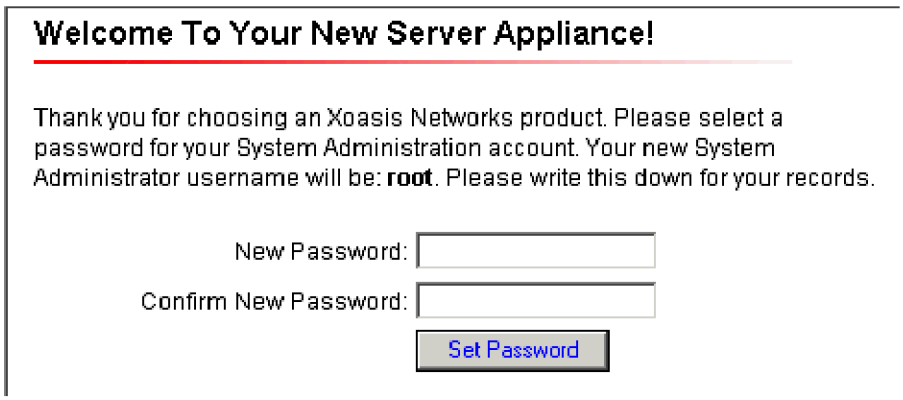
Before you begin final configuration, make sure you have at least one available private or public IP address, gateway address, subnet mask, and DNS server(s) from your network administrator.

The following topics are covered in this section:

- System Administration Password
- Server Configuration
- Server Status

System Administration Password

You will immediately be asked to enter a password for the **root** user account, which will be the default System Administration account for configuring your hosting needs.



After you have set your password, use the username **root** and your new password, log in to your System Administration account.

Server Configuration

The New Server Configuration Wizard will direct you through the setup of your network settings and the services you plan to utilize in the Turn Key v3.5 software suite. Follow each step of the detailed instructions that appear on your screen. You will be able to review the information you provided before saving the changes.

Step 1: Server Name and Domain Name

Pick a server name which contains only letters and numbers and no spaces.
Tip: Pick a name that describes the server's role on your network--for example, web1 to describe a web server.

Enter a registered domain name if you already have one. If you don't and you would like to register one through Xoasis.com, enter the name you would like to register, and follow the registration instructions in ….

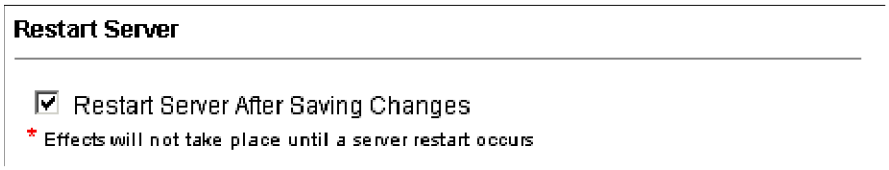
Step 2: Network Configuration
The current network settings for IP address, Gateway address, Subnet Mask, and DNS Servers will appear in the text boxes. If you have questions about any of these settings, please contact your network administrator.

Step 3: Network Services
If you plan on using your Server Appliance as a network router, DHCP Server, or Content filter please select the appropriate option.

Check the services that you would like to configure now. You may configure any of these services at a later date, outside of the wizard.

Step 4: Save System & Network Changes
A confirmation screen will appear that lists all the information that you have just entered. If you would like to make any changes click **Back.**

Before the settings can take effect, you will need to restart the server. On the confirmation screen you will notice a **Restart Server** checkbox at the bottom of the screen. Leave this checked to allow the server to restart after clicking **Save Changes**.



Click **Save Changes** to complete your initial configuration. If you've chosen to restart the server, allow it a minute or two to restart and the Web configuration interface will be available again.

Server Status

After you complete the initial configuration, the Server Status page will appear which will show the current status of all of your server devices. If you wish to stop or start one of these devices, you may chose to do so via the terminal or through an SSH prompt (see SSH Shell Access section).

To begin configuring the individual hosting modules click on the corresponding link in the left menu under Configuration. Easy-to-use configuration wizards will lead you through the setup of each module. These individual hosting modules are covered in detail below:

- Web Server
- Mail Server
- FTP Server
- DNS Server
- System Settings / Tools

Web Server Configuration Guide

The following topics are covered in this section:

Web Server Configuration Wizard

To access the Web server configuration wizard, click the **Web Server Control** link after you configure the network settings.

Step 1: Select Web Server Setup

You have the option to configure the Web server for the performance of one dedicated server or for multiple dedicated servers.

- If you plan on running multiple web servers under several different domain names, click **Next Step**.
- If you're only planning on housing one single dedicated web site, select the Single Dedicated Web Site option and click **Next Step**.

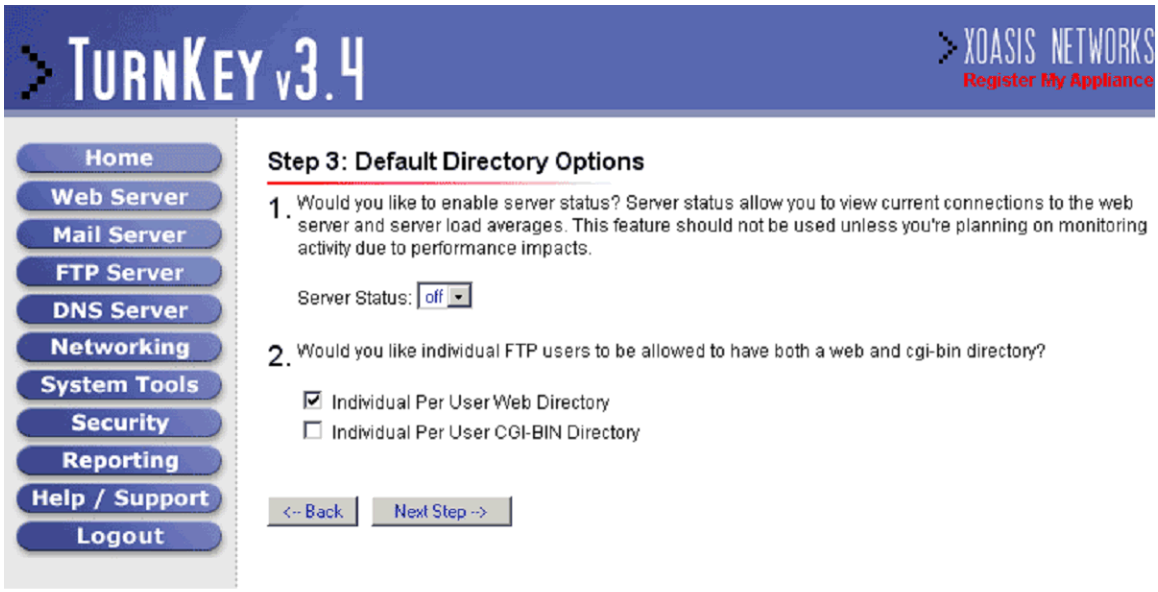
Step 2: Default Server Name and Contact Person

Select a **Server Name** and **Administrative E-mail Address** for logging purposes. The server name and e-mail address will be displayed to users when a file does not exist or an unknown script error occurs. By default, the **Server Name** will be filled in automatically with the server name and domain name you supplied earlier. Fill in the text boxes and click **Next Step**.

Step 3: Default Directory Options

You will be given the option to monitor the server through **Server Status**. If you would like to monitor the files users are accessing as well as the general performance of the server, select **on** in the Server Status dropdown box. You can access your server status report by visiting http://servers-ip-address/server-status/ after the web server configuration is complete. **Note:** The default setting for this option is **off**. This feature should not be used unless you're planning to monitor activity due to performance impacts.

You also have the option to allow FTP users to have their own Web and cgi-bin directories. To choose these options check the boxes under number 2. If you check the boxes, users will be able to access their files from the Web by visiting http://servers-ip-address/~ftp-username/ and http://servers-ip-address/~ftp-username/cgi-bin/ respectively.



Step 4: User Access Account
Select a username and password to be used for uploading files via FTP to the default Web server. You have the option to change the password at a later time if needed.

Save Default Web Server Settings
You may now review the options you've selected and save your changes. With the exception of the server type option, you may change any of these options at a later time under Default Server Settings in the Web Server Control Panel. To save your final settings click the **Save Changes** button. Changes will take effect **without** having to restart the machine.

You may now begin using your web server. To upload files to your web server, FTP to the IP address you supplied earlier and log in with your username and password.

Multiple Server Setup

If you select a **Multiple Server** setup with several different web sites being hosted on your Server Appliance, you will have three additional options within your server configuration:

- Add Virtual Server
- Modify Virtual Server
- Delete Virtual Server

Add Virtual Server
Before configuring a new virtual web server, you should configure the FTP server and create an FTP account for the virtual server. This will allow you to select a root path without having to modify any permissions.

Step 1: Select Virtual Server Type
Your first choice when selecting your virtual server is whether to operate an IP-based virtual server or a name-based virtual server.

- An **IP-based virtual server** is bound to a specific IP and port address of the Server Appliance and no other virtual server may listen on that exact same port and IP address.

- A **name-based virtual server** is bound to one or several DNS resolvable names. For example, a name-based virtual server could be bound to www.demonstration.com and www2.demonstration.com. This type of name-based configuration allows you to operate several different virtual web servers on the same machine without having to acquire a unique IP address for each site.

Step 2: General Server Information
This step requires you to select a server name, administrative e-mail address, and description for the virtual server. One you're entered this information click **Next Step**.

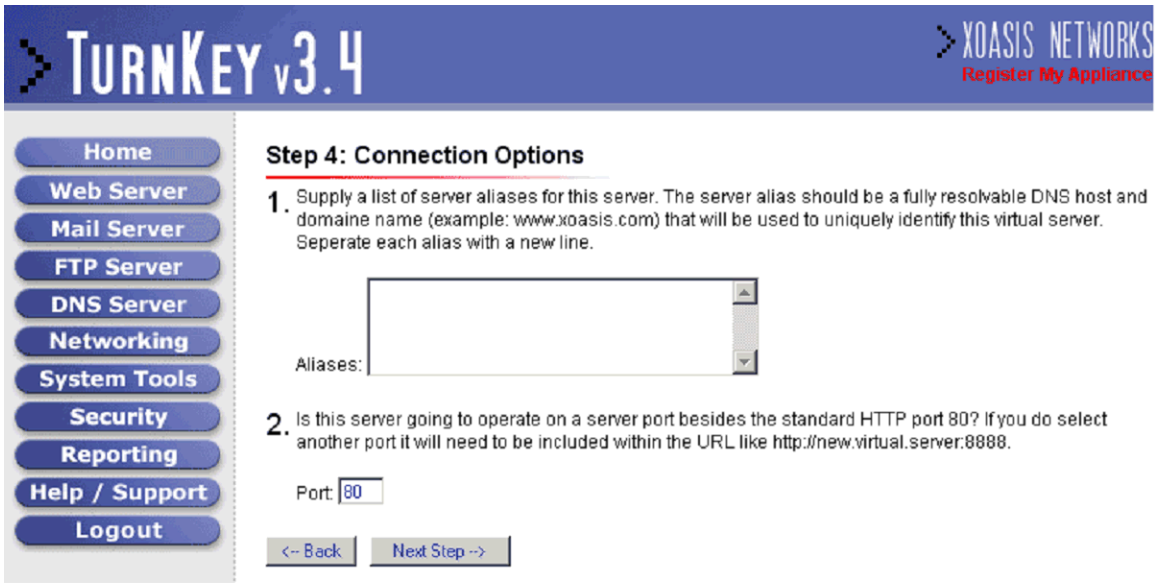
Step 3: Directory and Logging
Select or supply a path for the virtual server. This path is where all of the physical Web pages, server logs, cgi-bin, and other server-related information will be stored. You may either select an FTP username and path from the dropdown box or write in the path to a specific directory on the server in the text box.

You may also select options for the virtual server to maintain its own access and error logs and enable a virtual cgi-bin and FrontPage extensions.

Step 4: Connection Options
The next screen that you will see will depend on whether you've selected a name-based server or an IP-based server.

- **Name-based virtual server**: You will see a text box where you can supply one or multiple, fully resolvable DNS names for the server. You will also see a port box asking you which port the server should listen on. The default web port is 80, if you select a port besides 80 you will be required to access that server from a web browser with the following syntax: http://ip-or-name-of-server:port/

- **IP-based virtual server:** You will see a selection box where you can select which IP address you would like the server to listen on. You will also see a port box asking you which port the server should listen on. The default web port is 80, if you select a port besides 80 you will be required to access that server from a web browser with the following syntax: http://ip-or-name-of-server:port/



Modify Virtual Server
If you need to modify any of the settings of any virtual server, click **Modify Virtual Server** in the Web Server Control Panel and select the name of the virtual server you want to modify. All virtual server settings are configured using the Add Virtual Server wizard. See the above Add Virtual Server section for additional details about each of the settings.

Delete Virtual Server
To free up space or use an IP address for another virtual server on your Server Appliance, you may do so by deleting a virtual server. To delete a virtual server, click **Delete Virtual Server** in the Web Server Control Panel and select the name of the virtual server you want to delete. A confirmation screen will appear that lists the details of the server. To delete, click **Delete Virtual Server**.

Default Web Server Settings

Default Server Settings allows you to configure additional information that will affect the general web server and more specifically the default web server. If you do not have a need to tune the performance of the server or modify anything, we recommend leaving your default entries.

The following topics are covered in this section:

- General Settings
- Connection Settings
- User Support Settings

General Settings
To see the default Web server general settings click **General Settings** under Default Server Settings.

Setting	Description
Server Name	The name displayed for the default server when an error occurs
Server Administrator	The person responsible for maintaining the server

Server Status	An option that will automatically post performance and file access information to the following URL: http://server-ip/server-status/
Error Log	The location of the default server's error log
Access Log	The location of the default server's access log
Default Documents	The files that should be loaded when a file is not specifically accessed in a directory. The files will be looked for in the order listed in the box from first to last.
Directory Options	Specific configuration options for directory control under the Apache Web Server

Connection Settings
To see the default Web server connection settings, click **Connection Settings** under Default Server Settings.

Setting	Description
Request Timeout	The time in seconds that the server waits for a client to respond to a request for a file. Low timeout improves server performance
Web Server Port	The port on which the default server listens
Maximum Users	The maximum number of users who may simultaneously request a file
Unique Servers To Start	The number of servers to start. A server can be thought of as an object waiting to handle requests.
Minimum Spare Servers	The number of servers you would like to have available to listen for new user requests
Maximum Spare Servers	The maximum number of servers you need to have listening for requests. Having too many servers available can impact the performance of the other servers

User Support Settings
To see the default Web server connection settings, click **User Support Settings** under Default Server Settings.

Setting	Description
Enable User Web Directories	Allows users to have a Web site hosted on your default server. For example http://ip-of-server/~username/
Enable User CGI-BIN Directories	Allows users to have a virtual CGI-BIN directory as a sub directory of the default web server
Enable Default CGI-BIN	Maintains a CGI-BIN for the default web server

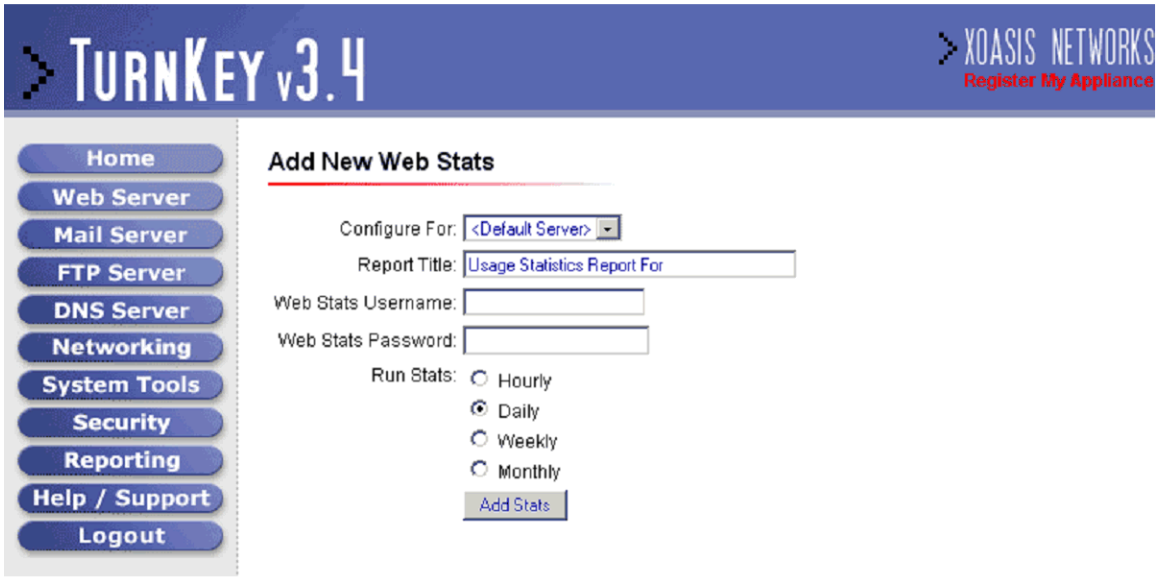
Web Stats Configuration

Users generally like to track the popularity of their Web sites as well as other useful information regarding their site's availability and accessibility. This may be accomplished by providing **Web Stats** to either the default or virtual server.

The following topics are covered in this section:

- Add New Web Stats
- Modify Existing Web Stats
- Delete Existing Web Stats

Add New Web Stats
To add new web stats, simply select **Add New Web Stats** from the Web Server Control Panel. Complete the form and click **Add Stats**.
1. Select the server that you want to configure for Web stats.
2. Choose a title for the report and type it into the **Report Title** text box.
3. Type in a username and password to maintain secure access to the Web server statistics.
4. Choose how frequently you would like the web stats compiled for the given virtual or default server.



Modify Existing Web Stats
You may modify a web stats configuration, reset web stats, or force statistics to be compiled immediately by clicking **Modify Existing Web Stats** and then selecting the virtual or default server you wish to modify.

Delete Existing Web Stats
If web stats for a given server are no longer desired, they may be discontinued by selecting the virtual server after clicking **Delete Existing Web Stats** from the main Web Server Control Panel. A confirmation screen will appear to reaffirm your selection.

SSL Certificates

SSL Certificates allow you to secure your virtual web sites with encryption keys to ensure any sensitive data your clients are passing back between their browser and your web server are secured.

The following topics are covered in this section:

- Add/Create Key for SSL Certificate
- Import Existing SSL Certificate
- Modify SSL Certificate
- Delete SSL Certificate

Add/Create Key for SSL Certificate
In order to enable secure transmissions for your clients web browsers in interaction with your web appliance you will need to create a new SSL certificate or import an old SSL certificate you may have created on another machine.

In order to create a truly valid SSL certificate you'll need to first create a "key" by supplying basic information about your business and the security requirements. You'll then need to submit this key to a 3rd party SSL certificate authority, two of the most common are Verisign (www.verisign.com) and Thawte (www.thawte.com). Once they authenticate the information you'll be asked to provide about your business they'll send you back another key which you'll need to use to sign the original key you created.

If you do not wish to go through the process of creating a key exchange between yourself and a certificate authority you may "Self Sign" a key where you yourself will authenticate the information. Unfortunately, if you select to "Self Sign" your users, when connecting to a secure site via https, will be notified that you have in fact self signed the key and a 3rd party has not verified your information.

The following options are available when creating a new key:

Setting	Description
Name	Simply a descriptive term for the new SSL key, something you can specifically identify the certificate by
Description	Free form text section to place your own comments and where you might be at in the key creation process
Certificate Strength	Before creating a key you'll need to decide what encryption strength you need, most users will want to select 512 as opposed to 1024. Please check with your certificate authority before continueing.
State	The state your company is incorporated in
Country	The country your company is incorporated in
City	The city your corporate address is located in
Business Name	Business name as appears on your organizations articles of incorporation
Business Unit	The group within your company that is creating this request, i.e. Engineering, Sales, etc.
Common Name	The common host and domain name for the site, if I am creating this site for the web page at www.xoasisnetworks.com then I am going to place www.xoasisnetworks.com in the box
Requesters E-Mail Address	The person who will be responsible for providing the information regarding your business
Key/Challenge Password	A password you'll need to remember to import the certificate back into your web server if you choose to move the certificate to another server at some point
Create Key	Simply create a basic key that will need to be signed by a certificate authority
Create Key & Self Sign	Not only create a key but also sign the certificate, users will be notified you "self signed" the certificate

Import Existing SSL Certificate
If you have previously purchased a certificate for another web server, you'll need to export it out of that web server and import it into your Server Appliance in order for it to function on your new appliance.

Once you begin importing the certificate you'll need the following items:

Setting	Description
Name	Free form descriptive term to identify the certificate
Description	Free form descriptive comments regarding your import
Private Key	The original key used to create the certificate when you presented it to the certificate authority
Signed Certificate	The returned key your certificate gave you to sign the certificate once they had validated the private key you had created on the previous web server

Modify SSL Certificate
You may use the modify SSL certificate section for two purposes. The first purpose is to sign certificate key requests you have previously created to have signed by a certificate authority, and the second purpose is to adjust an invalid key request or certificate.

Delete SSL Certificate
If you wish to delete expired or out of date keys you may do so by selecting "Delete SSL Certificate" and then clicking on the appropriate key to delete.

Mail Server Configuration Guide

The following topics are covered in this section:

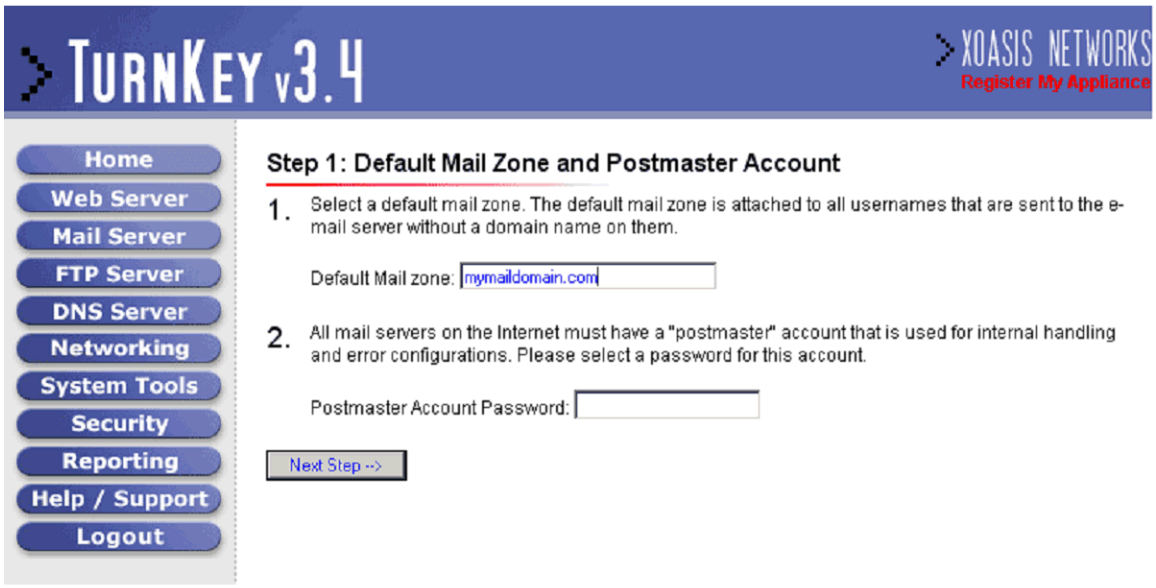
Mail Server Configuration Wizard

To access the Mail Server configuration wizard, click on the **Mail Server Control** link and the wizard will launch automatically.

Step 1: Default Mail Zone and Postmaster Account

The default mail zone is the domain which will be automatically appended to usernames if no domain name is supplied with the username when trying to receive new e-mail. For example, if the user test@demo.com supplies their username as **test** then demo.com will automatically be appended to the username for authentication. If you create e-mail accounts that are not under the default mail zone you will need to supply the full DNS domain name after the username when trying to receive e-mail.

Select an account password for the Postmaster mail account. According to current standards all e-mail servers must have a postmaster account for sending errors and other important information regarding the mail server. Many reporting services will send spam notices and other important information to this account in the event of a misbehaving user.



Step 2: Anti-Spam Support and Message Size
To help limit spam, you can choose to employ the Realtime Blackhole List (RBL) which will automatically deny messages that have come through outbound mail servers that are not properly secured.

If you are concerned about maintaining sufficient bandwidth, you can set the maximum size limit of user's messages. Enter size in kilobytes (1024 kilobytes to 1 megabyte). If you don't need to limit message size, leave the maximum message size at 0.

Step 3: Save Mail Server Settings
Review your settings and click **Save Changes** to complete configuration. Click **ok** in the confirmation dialog box. You can modify server settings at any time by clicking **Modify Server Settings** on the Mail Server Control panel.

Mail Zone Management

A mail zone is a domain name that you wish to use for receiving and sending e-mail. Mail zones are separate from DNS zones because you may not choose to run mail and DNS on the same machine. Whether you plan on running DNS on the same machine or not, you may add mail zones and manage pop3, forwarding, and e-mail lists for that zone.

To add a mail zone click on Mail Zone Management and enter the full DNS domain name that you would like to appear after the @ sign in an e-mail address. For example, if you wish to receive e-mail at test@demo.com enter demo.com in the new mail zone form box. Click "Add Mail Zone" and you will not be able to add mail zones for that account. The domain name will now appear in the drop down box when adding new accounts.

POP3 User Management

A POP3 mail account is considered a **full** mail account that can have mail sent and received through it directly without the benefit of any other account or service. It

utilizes the pop3 protocol, a widely supported format for communication with industry-standard mail clients like Eudora, Outlook, Outlook Express, Netscape Mail, and others. Unlike many mail servers, **the Xoasis Networks Server Appliance requires the user to provide their full e-mail address (username@domain.com) as the username when logging in to the pop3 mail server. This full e-mail address must also be used when configuring mail clients like the ones previously listed.**

The following topics are covered in this section:

Add New POP3 Mail Account

To add a new POP3 e-mail account click **Add User** under the POP3 User Management section in the Mail Server Control panel. You will see a form with several fields:

Setting	Description
Accounts Owners Name	Enter the name of the account owner for your own identification purposes
Username	This unique username will be used with @ and the domain extension (username@domain.com) for sending and receiving mail
Password	A secure password for authorizing access to the given mail account
Web Mail Access	If the box is checked the user will have the ability to check their e-mail throu gh the web based interface provided on the server appliance
Mailbox Size	The maximum amount of space the server will reserve for the user. If the amount is exceeded the mail to that user will not be delivered, a warning message will be sent out to the user when 90% of the space is used.
Spam Assassin Filter	If you wish to have incoming messages checked and marked for spam you may select to enable the Spam Assassin filter marking service. Inbound spam will have the word SPAM in the subject line and can then be processed by your mail client's filter to automatically delete or move the spam message to a specific folder.
Account Notes	Enter any administrative notes you would like to save for this account

Modify POP3 User and Change Passwords

To modify an existing POP3 user account, click **Modify User** under POP3 User Management. Click on the mail account you wish to modify. You will be able to modify the account owner's name, make changes to the password, or edit the account notes.

Delete POP3 User

To delete an existing POP3 user account, click **Delete User** under POP3 User Management. Click on the mail account you wish to delete. A confirmation screen will appear that will allow you to review the account information before deleting it.

Alias Management

A mail alias allows you to forward e-mail from one username to another simultaneously to save having two accounts to check. For example, you could create an e-mail alias john@demo.com that would automatically forward all mail sent to john@demo.com and to steve@demo.com.

The following topics are covered in this section:

- Add New Mail Alias
- Modify Mail Alias
- Delete Mail Alias

Add New Mail Alias

To create a new alias, click **Add Alias** under Alias Management in the Mail Server Control panel. You will see a form with several fields:

Setting	Description
Alias Owners Name	Enter the name of the account owner for your own identification purposes
Alias Username	The username and address (john@demo.com) that will forward all messages to another address (steve@demo.com)
Forward To E-Mail Address	The address that all mail for the alias john@demo.com will be forwarded to (steve@demo.com)
Account Notes	Enter any administrative notes you would like to save for this alias

Modify Mail Alias

To modify an existing mail alias, click **Modify Alias** under Alias Management and then click the mail alias you wish to modify.

Delete Mail Alias

To delete an existing mail alias, click **Delete Alias** under Alias Management and then click the mail alias you wish to delete. A confirmation screen will appear that will allow you to review the alias information before deleting it.

Mailing List Management

A mailing list creates a single point of contact for many mail users. For example you could create a mail list with the alias username **office** that would include all of the users in your office. Any member of the list can send a single e-mail to the entire list using the alias username (office@demo.com). You can create as many lists as you need.

The following topics are covered in this section:

Add New Mail List

To create a new mailing list, click **Add List** under Mailing List Management in the Mail Server Control panel. You will see a form with several fields:

List Name	Enter a description of the mailing list for your own identification purposes
Alias Username	Enter the alias username (for example, office@demo.com) for the mailing list to which all mail for that list will be sent
Forward To	Enter a list of e-mail addresses. **Each address must be**

These Addresses	**entered on a new line.** For example: steve@demo.com sam@demo.com sue@demo.com
Account Notes	Enter any administrative notes you would like to save for this list

Modify Mailing List
To modify an existing mail list, click **Modify List** under Mailing List Management. Click the mail list you wish to modify. You can modify the list name, add or delete e-mail addresses, and edit the account notes.

Delete Mailing List
To delete an existing mail list, click **Delete List** under Mailing List Management. Click the mail list you wish to delete. A confirmation screen will appear that will allow you to review the alias information before deleting it.

Mail Server Configuration Settings

Modify Server Settings
The three server-related options you originally configured in the mail server wizard may be modified by clicking **Modify Server Settings** in the Mail Server Control panel.

The following settings may be changed:

Setting	Description
Default Mail Zone	The mail zone that is automatically appended to a POP3 username when logging in to the mail server
RBL Spam Protection	A service that helps to limit spam by first checking with the Realtime Blackhole List (RBL) spam list service for mail coming through unsecured mail servers. The RBL keeps a global list of unsecured mail servers.
Maximum Message Size	The maximum message size in kilobytes. **If 0 kilobytes is selected the message size will not be restricted**

Web Mail Status
In the event that you need to enable or disable the webmail access for the entire group you may do so by clicking on **Web Mail Status** link in the mail manager window. If you have specified individual users access as granted or denied you will override that settings by making any change in this tool.

FTP Server Configuration Guide

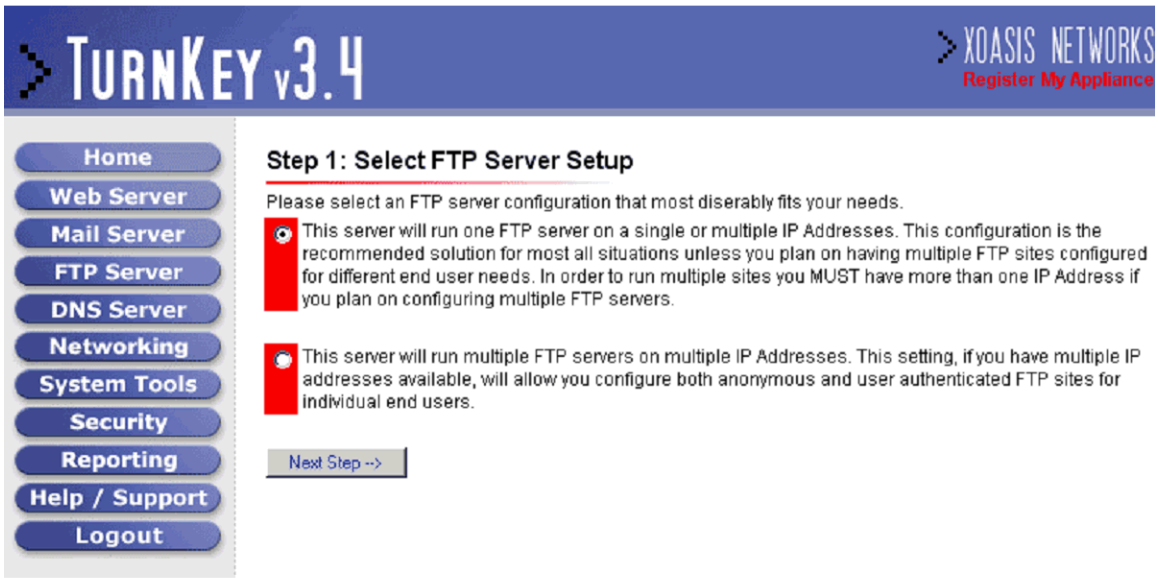
The following topics are covered in this section:

FTP Server Configuration Wizard

The FTP Server configuration wizard allows the server to be configured in two separate ways.

Step 1: Select FTP Server Setup

Select whether you would like to run either a single FTP server or multiple FTP servers on multiple IP addresses. The recommended configuration is to run only a single FTP server on the standard FTP port. However, if you need to provide your users with their own secured FTP server you may do so by selecting **run multiple FTP servers**. Note: To run multiple FTP servers, you must either change the port of a virtual FTP server or have it operate on its own unique IP address. **You may not have two FTP servers listening on the same IP address and port.**



Step 2: Server Name and Description

Enter a server name and description. The server name will appear to users when they're connecting to your default FTP server. An example of a standard FTP server name would be **ftp.yourdomain.com**. The description will help you identify the server if you want to modify its properties at a later time. For example, **Your Company Sales Support FTP Server**.

Step 3: Connection Options
Enter the FTP port, Idle Timeout, and Maximum Connections values:

Setting	Description
FTP Port	The server's port address that the FTP server will listen to for connections. By default, FTP clients will attempt to connect to port 21. Unless you have a specific reason to change it, leave this as the default.
Idle Timeout	Allows you to set the amount of time in seconds a user will be allowed to stay connected to the server without any activity.
Maximum Connections	Allows you to limit the number of simultaneous user connections.

Step 4: Save FTP Server Settings
Review your FTP server settings. Click **Back** to go back and make changes. Click **Save Changes** to complete the FTP server configuration and then click **OK** in the confirmation dialog box.

User Management

In order to allow users secured access to the FTP server, you will need to create an individual account for each user.

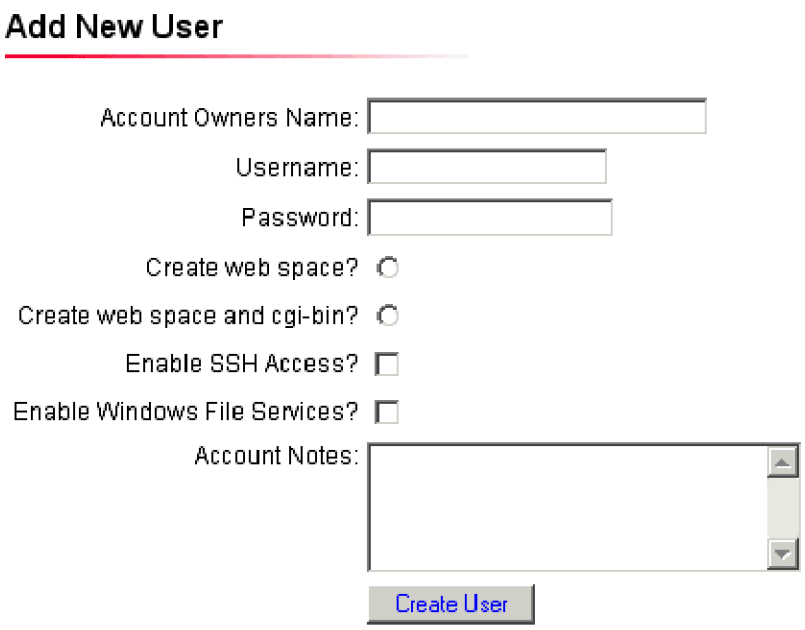
The following topics are covered in this section:

- Add New User
- Modify User
- Delete User

Add New User
To create a new account, click **Add User** under User Management in the FTP Server Control panel. You will see a form with several fields:

Account Owner's Name	Enter the user's full name.
Username	Enter a username that is at least three characters long
Password	Enter a password that is at least three characters long
Create Web Space?	Check the radio button if you would like Web space automatically created for the user
Create Web Space and a cgi-bin?	Check the radio button if you would like both Web space and a cgi-bin automatically created for the user
Enable SSH Access	Enable the user to have access to his or her FTP files via common SSH2 protocol clients
Enable Windows File Services	Enable the user to have access to his or her files via Windows File Services
Account Notes	Enter any administrative notes you would like to save about this user account

To complete account setup, click **Create User**. The selected directory structure will automatically be created and the appropriate permissions configured.



Modify User
To modify an FTP user account, click **Modify User** under the User Management section of the FTP Server Control panel. Click the username of the account you want to modify. In this form you can change the account owner's name, password, and account notes. In addition, you now have the ability to modify the user's home directory or UID. The home directory is the root path the user is moved to when they initially log in to their new server. The UID field is the UNIX owner ID that is associated with file ownership. If you change the UID, you will also need to modify the permissions of this user's account.

Delete User
If you wish to permanently delete an FTP user account, click **Delete User** under the User Management section of the FTP Server Control panel. Click the username of the account you want to delete and review the account information. You can also delete all user files associated to this account by checking the box **Delete home directory? Note:** If you plan on re-creating the user account later, you may want to uncheck the **Delete home directory?** box.

Multiple Server Setup

If you select a Multiple Server setup with several different FTP sites being hosted on your Server Appliance, you will have three additional options within your server configuration. **Note:** If you originally configured for a single FTP server you will not be able to add additional virtual servers.

The following topics are covered in this section:

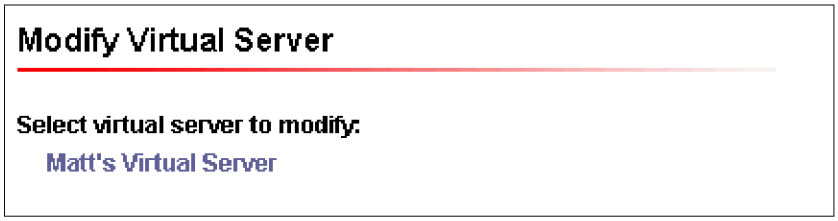
Add Virtual Server
To begin configuring a new virtual server, click **Add Virtual Server** from the FTP Server Control Panel.

Step 1: Select Virtual Server Type
Select either a user-based FTP server or an anonymous FTP server. A user-based FTP server requires each user to supply a username and password to gain access. An anonymous FTP server will allow users to log in without providing a username and password.

Step 2: Add Virtual Server
You will see a form with several fields. Enter your settings and click **Save Changes** to complete configuration.

Setting	Description
Server Name	The FTP server name that will be displayed when a user logs in. An example of a standard FTP server name would be **ftp.yourdomain.com**.
Server Description	The description will help you identify the server if you want to modify its properties at a later time. For example, **Your Company Sales Support FTP Server**.
Listen on IP Address	The IP address the virtual FTP server will listen to for connections. This IP address must be unique.
Port	The port the virtual FTP server will listen on for connections. This must be a unique port.
Idle Timeout	Allows you to set the amount of time in seconds a user will be allowed to stay connected to the server without any activity.
Maximum Connections	Allows you to limit the number of simultaneous user connections.
Umask	Sets the mask applied to the newly created files and directories for the given virtual FTP server.

Modify Virtual Server
To modify a virtual server click **Modify Virtual Server** under Virtual Servers in the FTP Server Control panel. Click the server you wish to modify. You can change any of the settings listed above. Click **Save Changes** to complete.



Delete Virtual Server
To permanently free up an IP address and port or to simply get rid of a virtual server, click **Delete Virtual Server** under Virtual Servers in the FTP Server Control panel. Click the server you wish to delete. The next window will allow you to confirm your selection. This window will also display additional information for the virtual server.

FTP Server Configuration Settings

To review or modify your default FTP server settings, click **Default Server Settings** under Server Configuration on the FTP Server Control panel.

Setting	Description
Server Name	The FTP server name that is displayed when a user logs in
Server Description	A description of the FTP server for your own identification purposes
Port	The port the virtual FTP server will listen on for connections must be a unique port
Idle Timeout	The length of time in seconds users will be allowed to stay inactive on the server before being disconnected
Maximum Connections	The maximum amount of simultaneous connections to the server
Umask	The mask applied to the newly created files and directories for the given virtual FTP server
Reverse DNS	When a user connects, the ability to reverse lookup a user's IP address to find a host and domain name for additional logging. Note: Using this feature will cause a delay in login time.
Ident Lookups	When a user connects, the ability to check for a valid IDENTD client/server relationship and store that data for additional logging. Note: Using this feature will cause a delay in login time.

The following topics are covered in this section:

Configuring Windows File Services

The Windows File Server and the FTP Server share an authentication database, and all of the configuration settings for the Windows File Server can be found under the FTP Server button.

To begin using Windows File Services you'll want to enable the service under **Default File Server Settings**. Please skip to the section *Default File Server Settings* for additional information.

Add File Share

By creating a new file share on your network, you'll be creating a new point of storage under Network Neighborhood on Microsoft Windows desktop machines. The following options are available when creating a new file share:

Setting	Description
Share Name	Name of the file share to appear in Network Neighborhood
Share Description	A description to appear alongside the share name in Network Neighborhood
Share Path	A specific place on the server appliance file system, auto create a path on the appliance, or contained under a specific user account
Browseable Share	Allow a share to appear under Network Neighborhood
Public Share	Available to be opened and accessible to all users as a public drive
Users With Write Permission	Selected users are allowed to both read and write files under this share point
Users With Read Permission	Selected users are allowed to read and view files under this share point but not modify or delete the files

View/Modify File Share

To modify a file share under File Shares in the FTP Server Control panel, click the share you wish to modify. You can change any of the settings listed above. Click **Modify Share** to complete.

Delete File Share

To permanently delete a file share click **Delete File Share** under Virtual Servers in the FTP Server Control panel. Click the share you wish to delete. The next window will allow you to confirm your selection. This window will also display additional information for the file share and ask if you wish to delete the files under the share as well.

Add Computer to Domain
Your Server Appliance with Windows File Services may function as a primary domain controller to authenticate user access. In order to allow workstations to join the domain you'll need to click **Add Computer to Domain** and input the NetBIOS workstation name as well as a brief description.

You only need to add a computer to a domain if you wish to have a person's access granted or denied based upon password access. To act as a simple file server with authentication, you will not need to enable domain services.

Delete Computer from Domain
To remove a workstation's access from the file server simply delete the machine name and the machine will no longer be a member of the domain.

Default File Server Settings

Default file server settings is the basic configuration for your new file server. You may select to enable or disable file services all together as well as server name and user access.

The following options are available:

Setting	Description
Enable Windows File Services	Place a check in the checkbox to enable Windows File Services
Workgroup/Domain Name	The workgroup or domain name to join or be the primary domain controller for
NetBIOS/Server Name	The name of the server; this will be the server's name under Network Neighborhood
Admin Users	Users with administrative privileges. These privileges are required to join and leave the domain name as well as administrative access to all file shares.
Enable Domain Logons	Enable the file server to function as a domain logon authenticator
Enable WINS Server	The WINS server providers NetBIOS resolution for IP addresses to NetBIOS name under Windows
Enable Home Directories	Every user with file server authentication will have a home directory that appears under the server in Network Neighborhood as their personal file store
Enable Printers	Enable USB and Parallel printers attached directly to the system via CUPS

DNS Server Configuration Guide

The following topics are covered in this section:

DNS Server Configuration Wizard

In order for DNS to successfully and authoritatively propagate across the Internet, you will need to register a domain name with a domain registrar. In addition you will need to tell your domain registrar that your Server Appliance will be the authoritative DNS server for that domain name. Once that is complete you will be able to successfully manage DNS for your domain name on your new Server Appliance.

Step 1: Default DNS Domain Name
Set up DNS for your first domain name. Enter a default domain name and an IP address to point to that domain name. The defaults for your current server will be listed as examples.

Step 2: Domain Zone Transfers
The next step will ask you if you would like to authorize other DNS servers to view your DNS data. If you're planning on configuring a secondary or tertiary DNS server in case your primary DNS server is unavailable, you will need to list **Additional DNS Servers** in the text box. These other DNS servers should be listed with their FULL DNS host and domain name as they will be allowed to pull DNS data from that resolvable domain name.

Step 3: Save DNS Server Settings
Review your settings and if OK, click **Save Changes**. Click **OK** in the confirmation dialog box. The configuration wizard will automatically set up DNS records for the default domain name, the sub domain www, the sub domain mail, and appropriate mail and NS records.

Domain Management

The following topics are covered in this section:

Add Domain
To set up a new domain name, click **Add Domain** under Domain Management on the DNS Server Control panel.

Step 1: Decide what kind of role and zone type you will need and click **Next**. If you're simply looking to set up a domain name and manage it from this Server Appliance, we suggest you use the defaults.

Setting	Description

Server Role: Master Zone	This server will be controlling the DNS records for this domain name
Server Role: Slave Zone	This server will be getting its DNS data for this domain name from another server
DNS Zone Type: Forward Zone	This server will be looking up DNS domain names and records to IP addresses
DNS Zone Type: Reverse Zone	This server will be looking up IP addresses to domain names and records

Step 2: Depending on which options you chose in Step 1, you will be asked for additional information before creating a new domain.

Master Zone Domain Options

Domain Name	The name for which to handle DNS
SOA Refresh	The length of time to refresh data
SOA Retry	The length of time to retry for outdated data
SOA Expire	The length of time cached records expire
SOA TTL	The length of time to wait before checking for new data
DNS Maintainers E-Mail	Person responsible for DNS related questions
Create a Mail Zone	Checked if you would like to handle mail for this domain name on the machine as well

Slave Zone Domain Options:

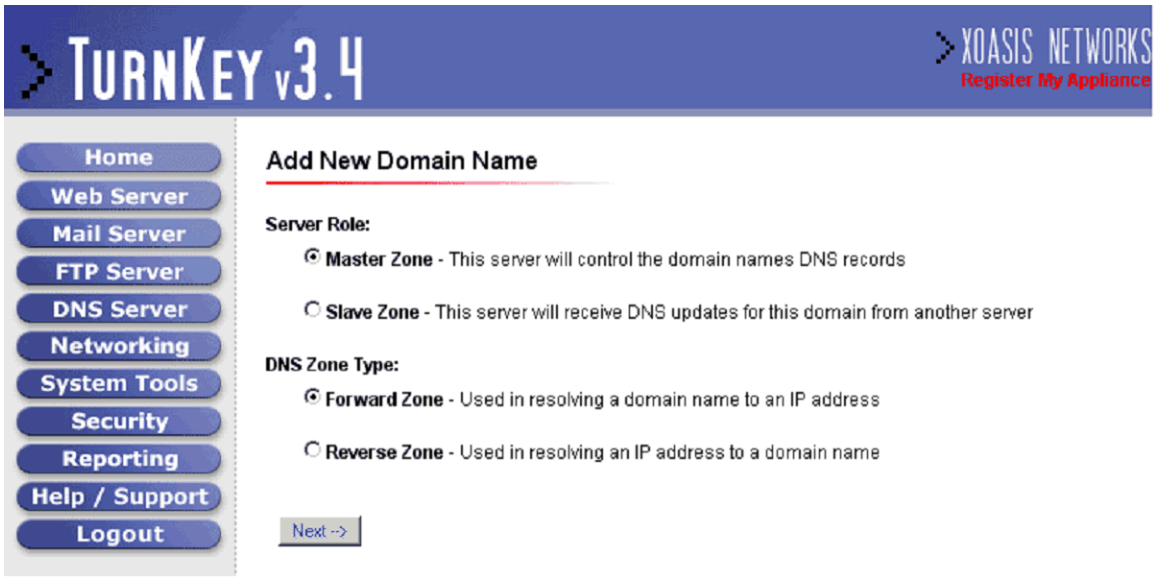
Domain Name	The domain name for which you're going to be running secondary DNS
Primary DNS Servers	The DNS servers to inherit DNS settings from. These servers should be separated by a new line

Forward Zone Domain Options

IP Block	The class C IP block for which to handle DNS
SOA Refresh	The length of time to refresh data
SOA Retry	The length of time to retry for outdated data
SOA Expire	The length of time cached records expire
SOA TTL	The length of time to wait before checking for new data
DNS Maintainers E-Mail	Person responsible for DNS related questions
Create a Mail Zone	Check if you would like to handle mail for this domain name on the machine

Reverse Zone Domain Options:

IP Block	The class C IP block for which you're going to be running secondary DNS
Primary DNS Servers	The DNS servers to inherit DNS settings from. These servers should be separated by a new line



Modify Domain Name
In order to modify a domain name, click **Modify Domain** under Domain Management in the DNS Server Control panel. Click the domain name that you wish to modify. Please refer to the configuration chart under Add Domain (above) for a detailed analysis of the different options associated with different types of domain zones.

Delete Domain Name
To delete a domain name, click **Delete Domain** under Domain Management in the DNS Server Control Panel. Click the domain name you wish to delete. A confirmation screen will appear. You will also have the option of deleting all of the DNS records under the domain name you're deleting.

DNS Record Management

The following topics are covered in this section:

- Add New DNS Record
- Modify DNS Record
- Delete DNS Record

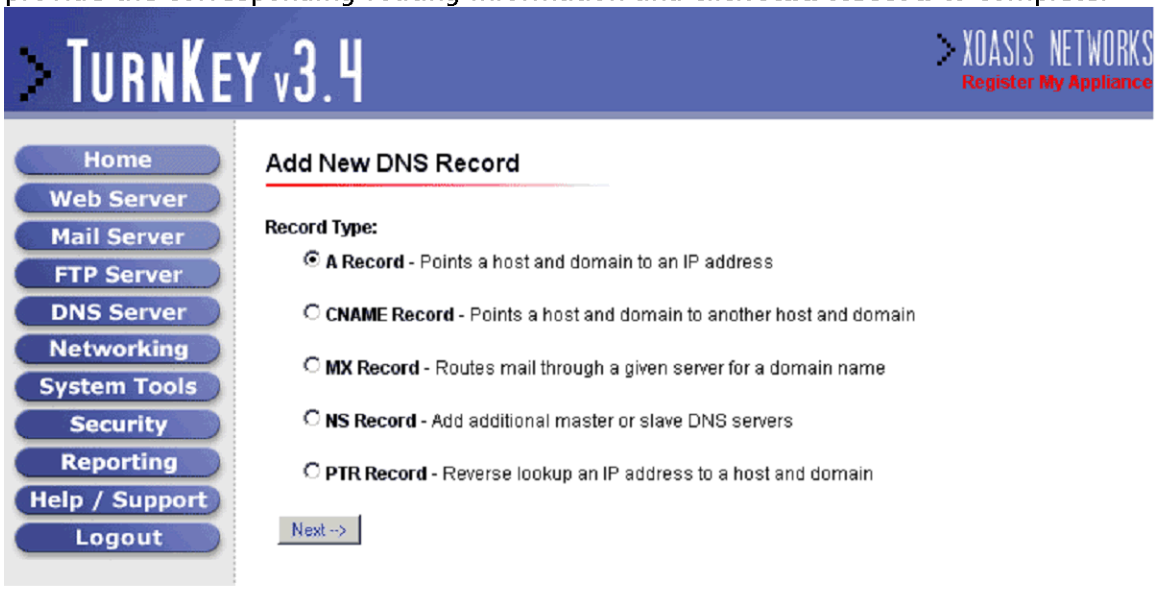
Add New DNS Record
DNS Records contain different feature sets but essentially perform the same action of resolving a name or IP address to another name or IP address. You can configure all common DNS record types by clicking **Add Record** under DNS Record Management in the DNS Server Control panel.

These record types are:

Setting	Description
A Record	Points a host and domain name to an IP address. Example: www.cnn.com resolves to 127.0.0.1
CNAME Record	Points a host and domain name to another host and domain name. Example: www.cnn.com resolves to www-server.cnn.com
MX Record	Routes mail for a domain name through a given server.

	Example: All mail sent to cnn.com routes to mail.cnn.com
NS Record	Adds additional authoritative master or slave DNS server entry. Example: ns2.cnn.com is also a DNS server for cnn.com
PTR Record	Does a reverse lookup from an IP address to a host or domain. Example: 127.0.0.1 resolves to cnn.com

Choose the type of record you want to create and click **Next**. On the next screen, provide the corresponding routing information and click **Add Record** to complete.



Modify DNS Record
To modify a DNS record, click **Modify Record** under DNS Record Management in the DNS Server Control panel. Click the DNS record under the domain name that you wish to modify. Please refer to the configuration chart under Add New DNS Record above for detailed analysis of the different options associated with different types of domain zones.

Delete DNS Record
To delete a DNS record, click **Delete Record** under DNS Record Management in the DNS Server Control panel. Click the DNS record that you wish to delete. A confirmation screen will appear that lists the details of the record. To delete, click **Delete Record**.

DNS Server Settings

Because most DNS zone settings are configured directly with the domain name, there are not very many configuration options for the DNS server. The only option listed under DNS Server Settings in the DNS Server Control panel is **Domain Zone Transfers**. If you plan on having secondary or tertiary DNS servers maintain domains that your Server Appliance is hosting, you will need to list those servers in the text box.

Phone / VoiceIP PBX Configuration Guide

The following topics are covered in this section:

- Managing Phone Extensions
- Managing Dial Plans for Inbound Calls
- Connecting Multiple Units
- Searching and Managing Call Detail Records (CDR)
- PSTN Connections

Managing Phone Extensions

Phone extensions may be thought of as your programming for individual phones on your network. Unlike traditional phone extensions attached to a PBX, Voice over IP handsets generally require you to login with a username and password into the PBX. Multiple users may share a single handset by logging in and out of the handset with separate usernames and passwords.

Add Phone Extension

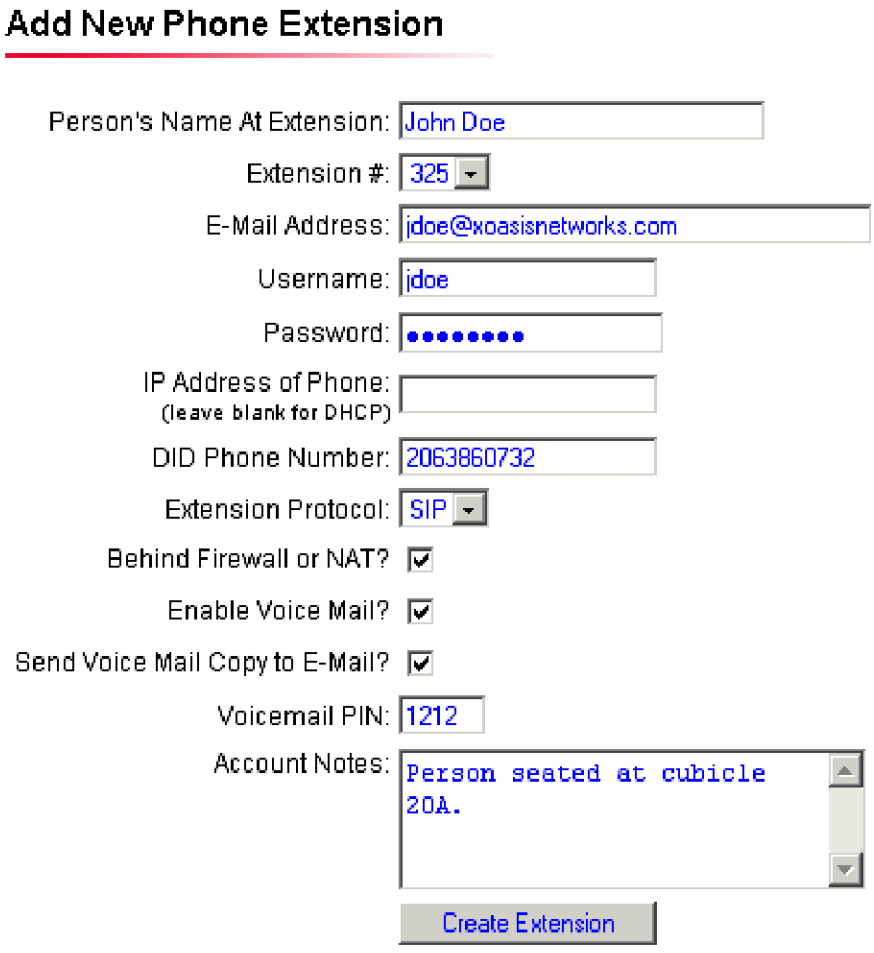
In order to add a new phone to the network you will need to create individual extensions for your phone users. Various types of phone extensions and options may be defined.

These options are:

Setting	Description
Person's Name	Free form text box listings the persons name at the phone extension, the name will be used as caller ID between internal calls.
Extension #	The traditional numeric extension number callers can reach you out when calling from the outside.
E-Mail Address	The persons e-mail address that can be used for things like mailing voicemail copies or sending service notices like full voicemail boxes.
Username	The username the person will use to login to the PBX from the VoIP handset.
Password	The password the person will use to login to the PBX from the VoIP handset.
IP Address of Phone	The IP address of the persons handset, due to network configurations you may have to supply this value to improve voice reliability. If left blank, the phone handset will assumed to be set to DHCP or to a roaming profile. A roaming profile would be multiple users logging in and out of the same handset at different periods.
DID Phone Number	The inbound direct phone number of the person at the above listed extension. This item may be left blank if no DID is required.
Extension Protocol	The type of VoIP phone logging into the PBX. The Xoasis unit will expect to communicate in this protocol with the phone. Available phone protocols

	include SIP, MGCP, H323, and SKINNY.
Behind Firewall or NAT	Select this checkbox if you have multiple handsets located behind a firewall or NAT gateway.
Enable Voice Mail	Select this checkbox if this extension requires a voicemail box.
Send Voice Mail Copy to E-Mail	If voicemail is enabled, you may mail a copy of each voicemail in audio WAV format to the person.
Voicemail PIN	The 4 digit number that will be used to access voicemail services.
Account Notes	Free form text box for account notes.

Example:



View/Modify Phone Extension
To modify a phone extension, click **View/Modify Phone Extension** under **Phone Extensions** in the **Phone Server Control Panel**. Click the phone extension that you wish to modify. Please refer to the configuration chart under **Add New Phone Extension** above for detailed analysis of the different options associated with different types of phone extension options.

Delete Phone Extension
To delete a Phone Extension, click **Delete Phone Extension** under **Phone Extensions** in the **Phone Server Control Panel**. Click the phone extension that

you wish to delete. A confirmation screen will appear that lists the details of the phone extension. To delete, click **Delete Extension**.

Managing Dial Plans for Inbound Calls

Dial plans are how a phone call is handled when placed inbound to one of your phone numbers. How and what should occur when the call is answered by the Xoasis PBX rely on the rules you configure and enable.

Add Dial Plan

To create a new dial plan click **Add Dial Plan** under Dial Plans. You will be asked to select a type of dial plan. The available dial plan types are:

Setting	Description
Ring Multiple Extensions At Once	When an inbound call is received, multiple phones will ring at once. The first person to answer the line will handle the inbound call.
Dial One Extension Then Another	An inbound call will ring one extension, than another, etc. until the call is answered. The order of phones ringing may be defined.
Auto Attendant	Inbound calls will be greeted with a voice recording and options for how to route the call.

Select one of the options above and click the Next button. Depending on the option selected above you will be asked to supply the following:

Setting	Description
Dial Plan Name	Free form description for the dial plan.
Drop Down Extensions	If you selected ring multiple or dial one extension then another you will be asked to provide a list of dropdowns with the existing phone extensions you've previously defined. If you selected to ring multiple extensions at once, you should select each extension you wish to have ring at the same time. If you selected dial one extension then another, select the extensions from top to bottom in which the order you would like the call dialed.
Press 1 For, etc.	If auto attendant was selected, your options will be to "Press 1", "Press 2", etc. Each drop down will have a phone extension listed, these extensions will be dialed when 1, 2, 3, etc. is pressed.
No Answer Voicemail	If no options are selected or a call goes unanswered, this voicemail box will automatically be presented to the caller to leave a message.
Account Notes	Basic free form text box to make notes about each dial plan.

No matter what dial plan you configure, the following two options are defined in every Xoasis PBX. By pressing the * key a user will be presented with a dial by name directory or by pressing the # key the voicemail interface will be brought up for the user to enter their extension and password.

After a dial plan is active you will need to map the dial plan to a number and activate the dial plan. To activate a dial plan, select **Dial Plan Mapper** under **Server Configuration** in the **Phone Server Control Panel.**

While adding a new mapping you will have the following options:

Setting	Description
Name	Free form text to describe the dial plan mapping
Dial Plan	The dial plan you previously defined under "Add Dial Plan"
Inbound Number	The number the dial plan functions with. If no inbound number is defined, the dial plan will apply to all inbound phone numbers on the system.

Once a new dial plan mapping is created, you will need to active the plan. The new mapping will appear in the list of mappings and either say "Yes" or "No" under "Active?". Click the No or Yes link to change the status. If a mapping is listed as "Yes" it is active. New mappings are automatically set to "No".

One dial plan may have multiple mappings. A single dial plan may require multiple mappings depending on the time of day or day in question. After hours a company may wish to use an auto attendant while during business hours a live voice may be desired.

Recording Voice Prompts for Auto Attendants
Voice prompts may be recorded by dialing extension 9000 from any VoIP handset attached to the Xoasis PBX. A beep will be heard and you should begin speaking into the phone to record your prompt. When complete simply hang up the phone. The new voice prompt will be saved on the Xoasis PBX. The recording may be viewed by going to **Voice Prompts** under **Server Configuration** in the **Phone Server Control Panel**. New voice prompts recorded through extension 9000 will be saved as "prompt.gsm". You may rename this file to something more descriptive under this same tool, if you use extension 9000 to record an additional prompt the existing prompt.gsm will be overwritten. The voice prompts are recorded in GSM format. GSM files may be downloaded and uploaded from the same **Voice Prompts** tool. GSM files may be listened to on a PC via the Quick Time audio program.

View/Modify Dial Plan
To modify a dial plan, click **View/Modify Dial Plan** under Dial Plans in the Phone Server Control panel. Click the dial plan that you wish to modify. Please refer to the configuration chart under Add Dial Plan above for detailed analysis of the different options associated with different types of dial plans.

Delete Dial Plan
To delete a dial plan, click **Delete Dial Plan** under Dial Plans in the Phone Server Control panel. Click the dial plan that you wish to delete. A confirmation screen will appear that lists the details of the dial plan. To delete, click **Delete Dial Plan**.

Connecting Multiple Units

Multiple units may be connected through the **Connection Manager** under **Server Configuration** in the **Phone Server Control Panel**. The connection manager tool will list existing connections as well as a tool to add new connections. When creating

a connection between two or multiple units, you will need to create a connection on each unit you plan on connecting.

When creating a new connection the following options are available:

Setting	Description
Local Username	The username that the remote unit will try and authenticate with. The local and remote usernames need to be different.
Remote Username	The username that the local unit will send to authenticate with the remote unit. The local and remote usernames need to be different.
Local Password	The password that the remote unit will try and authenticate with. The local and remote passwords may be the same.
Remote Password	The password that the local unit will send to authenticate with the remote unit. The local and remote passwords may be the same.
IP Address	The IP Address of the remote unit which you're trying to establish a connection with.
Connection Modifier	The connection modifier enables dialing between multiple machines. For example, if you're calling from Seattle to New York and your phone extension is plugged into the Seattle unit and the connection modifier on the New York unit is "2xxx". In order for you to dial extension 100 on the New York PBX from the Seattle PBX you would need to dial "2100". The first "2" will tell the Seattle PBX that the call is destined for New York. Each location should have its own connection modifier.

Once a new connection is created you will need to activate the connection by checking the status under "Active?". If the "Active?" option says "No", click it and it will change to "Yes" and the connection will be active. If the "Active?" option says "Yes", click it and the connection will no longer be active.

The outbound option may be used to pass all traffic destined for the PSTN through a remote unit. For example, if New York is connected via a PRI T-1 circuit with 23 available voice channels, you may adjust the Outbound option to "Yes" under the listed connection to force all Seattle PSTN traffic out the New York connection. You may have only one Outbound connection.

Searching and Managing Call Detail Records (CDR)

Call Detail Records or CDR record and log the calling habits of phone users on the network. The Xoasis PBX keeps track of all phone calls made through the PBX. To search CDR, select **Search Call Detail Recording** under **Server Configuration** in the **Phone Server Control Panel**.

The search options are as follows:

Setting	Description
Source Caller	The call was either placed inbound or outbound, if its placed as an outbound call the phone extension who dialed it will be supplied.

Destination	The destination of the call may either be the phone extension who answered the call or the phone number which was dialed if it was an outbound call.
Caller ID	The caller ID of the person dialing inbound or the name of the person dialing outbound.
Call Status	Whether the call was answered or went unanswered.
Call Application	What type of application the call took, did it go to Voicemail, was it outbound, did it go over a VoIP line, etc.
Start Date Range	Date range to start searching from.
End Date Range	The last date to search from.
Record to Display	The total number of records to display at one time.

Additionally, after searching for CDR you may select to export it. Scroll down to the bottom of the screen one you have some search results and you will see an **Export Results** button which will provide a download prompt. The exported results will appear in comma separated format and may be imported into Microsoft Excel or another application.

PSTN Connections

Units ordered from Xoasis may come with additional ports to connect the PBX to the PSTN phone network. These cards will come from the factory already configured for use based upon card type. PRI T-1 cards may have varying options and might require additional support setup from Xoasis, support is available through your Xoasis Sales Representative or support@xoasisnetworks.com.

Networking

The following topics are covered in this section:

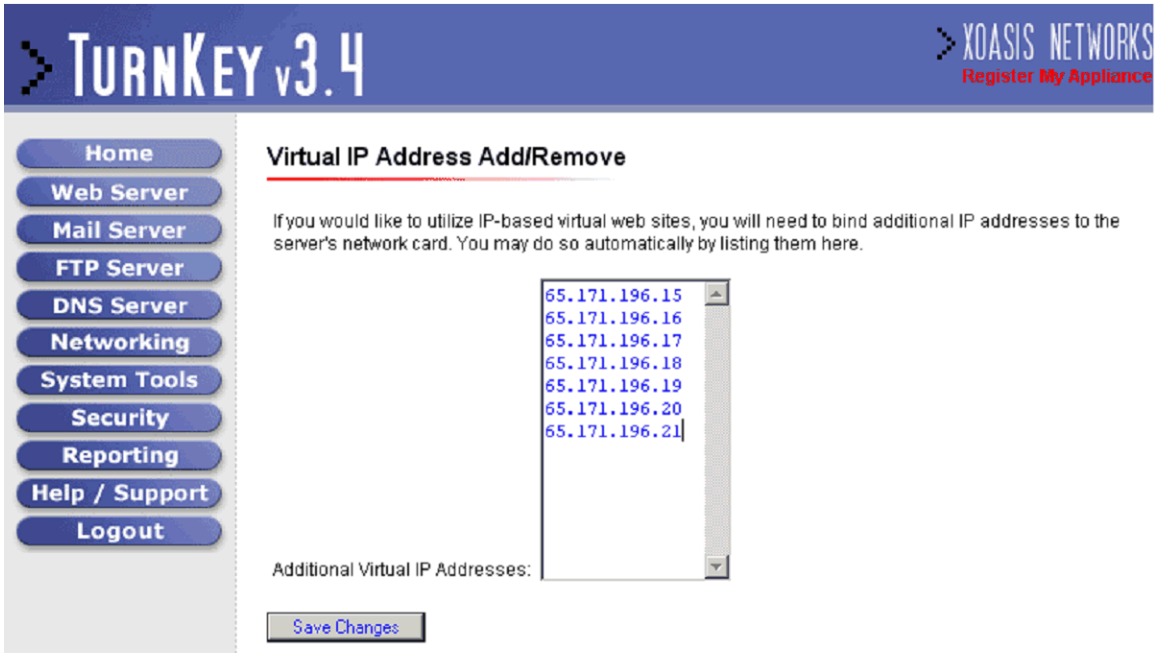
Settings

Network Settings

This form allows you to configure your server on the network. You can change or modify the server name, domain name, IP address, gateway address, subnet mask, and DNS servers. **Note:** If you change any of these options, you will need to restart the server for the changes to take effect.

Virtual IP Address Management

Since you have the ability to bind specific virtual FTP or Web sites to distinct IP addresses and ports, you might need to configure additional IP addresses for the server. You may do that in IP Address Management. List all IP Addresses available to the server in the text box and separate each entry with a new line. All settings will take effect without restarting the server.



Virtual IP Address Permissions

All of your virtual IP addresses may be assigned to a given user for their sole use. For example, if you added an IP address and only wanted "John Doe" to have access to create virtual web and FTP sites on that IP address, you could use the Virtual IP Address Permissions section to define which IP address "John Doe" had complete control over.

Bandwidth Management for Virtual Sites

This feature allows you as systems administrator to control the maximum amount of "bandwidth stream" into each virtual site. For example, you could limit a given virtual web server to a 64,000 byte stream which would cap its monthly usage at about 20GB. This feature will keep users from raking up high bandwidth bills, or slowing the appliance due to a large amount of users downloading large files from a given site.

Note: You can allow users to control their own bandwidth streams as well as mail quotas under the group permissions section.

Services

Manage Router/DHCP Service

Your Server Appliance may function as a gateway router by utilizing the two Ethernet ports on the back of the appliance. The primary interface should be plugged into your public IP network via a DSL router, cable modem, wireless router, or directly out of a switch or hub. The second interface can be plugged into the same private network or a second private network to bridge the traffic between the two interfaces.

The DHCP component can be enabled to assign IP addresses automatically to network clients. You may set the DHCP IP range by specifying a start and stop range under the options menu.

Manage Content/Cache Filter Service

If the router component of the Server Appliance is enabled, you may filter the web traffic that your network users are allowed to view by enabling the Content/Cache Filter Service.

First, select the type of traffic you wish to filter. You may filter traffic three ways: block all traffic but certain specific sites, allow all traffic but certain specific sites, or allow all traffic but certain types of sites.

The content can be filtered by these specific sections:

- Pornography
- Free Mail Sites
- Banner Advertising
- Aggressive
- Audio/Video
- Drugs/Alcohol
- Gambling
- Hacking
- Illegal Software/Music/Movies

Secure Firewall

The secure firewall allows you to block access to various Internet networks or unwanted services running on the machine. For example, you could block a competitor's IP address from accessing your web server, or disable web-site access entirely from all Internet users.

Firewall Configuration Wizard
This simple wizard will ask you a few questions and provide some options for blocking unwanted Internet access. It can block Internet traffic based upon the originating network, destination network, or desired service (port traffic).

Manual Configuration
For advanced users only, manual configuration allows you to write and implement your own custom rule set based upon the BSD-based ipfw command-set. For more information about the ipfw command-set please visit,
http://www.freebsd.org/cgi/man.cgi?query=ipfw&sektion=8

Enable/Disable Firewall
In the event of a misconfiguration, disruption of service, or personal whim you can easily disable or enable the firewall from this utility.

System Tools

Additional settings and helpful tools can be found by clicking **System Tools** on left menu under Configuration.

The following topics are covered in this section:

Settings

Veritas© Backup Client Settings

If you would like to remotely back up your Server Appliance from a Veritas BackupExec server, you may do so by configurating the Veritas Backup Client Settings. Simply specify 1) the Backup Server Name (should be an IP address or resolvable DNS address), 2) a new password that will be required before the server can access your server appliance, and 3) whether the agent is currently enabled or not. From your remote Veritas BackupExec server you will be able to see lists of your files and other vital appliance data.

SQL Query Analyzer

If you wish to have direct access to the database structure, add new users via the database interface, or allow users access to MySQL hosting for their PHP files, you may execute standard MySQL queries through the SQL Query Analyzer.

Virus Scan

To protect your appliance and your users' files, you can fully scan either the entire file system or just the user directories of your appliance for malicious viruses. Xoasis Networks has implemented a full command-line virus scanner with real-time updates from Network Associates and McAffee.

The following options are associated with the virus scan software:

Option	Description
Run Virus Scans	Select how frequently you would like the system scanned for viruses. Whether you select daily, weekly, or monthly, the virus scans will always be run at 2 AM.
Directories to Scan	You can either scan a part of the system or the entire system. It will most likely be more important to scan only the home directory files as users will be frequently uploading files that might contain viruses.
Check For Virus File Updates Before Scanning	To check McAffee for the latest virus data before running your usual scan, select this option. If you're not connected to the public Internet or behind a firewall which restricts FTP traffic you'll need to disable this option.
Clean or Quarantine Infected Files	When the scanner finds an infected virus

	it can clean the file or move it to a safe directory. If you do not select this option, virus-ridden files will only be reported in the usual log file.
Keep Detailed Report of Virus Scan Actions	Every time the scanner runs it will keep a detailed log report for the actions that took place; if you check this option. that log will be kept and will be viewable by clicking on the link.
Virus Scan Enabled	This allows you to disable the virus scan in the middle of its run or stop it from making its usual run until you enable it again.

Restart Server and Shutdown Server
You may directly **restart server** or **shutdown server** by clicking these links. You will be asked for confirmation after you click the link.

Package Update System

The package update system allows you to quickly deploy software fixes, enhancements, and upgrades to your Server Appliance from Xoasis Networks.

Install New Packages
The **Install new packages wizard** will step you through the selection of available software for your system as well as tell you if an update is necessary or optional.

Review Installed Packages
Review installed packages allows you to view currently installed packages, their description, status, and date of installation.

Tools

Ping /Trace Route/DNS Lookup
You have the option to ping, trace route, or look up a DNS entry directly from the Web. Enter either the host name or IP Address and click **Perform Action**.

Security

The following topics are covered in this section:

User Management

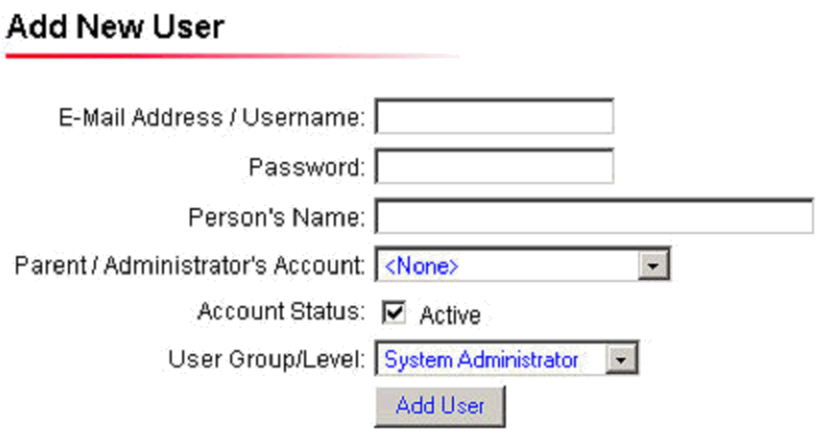
The User Manager utilities allow you to delegate account and server administration. *Note*: The root account is the System Administrator account and may not be deleted under any circumstances.

Add User

To add a new user, click **Add User** under User/Group Manager in the System Settings/Tools Control panel.
1. Select a username for the new account. This may be either a common handle or an e-mail address.
2. Select a password for the new user.
3. For identification purposes, enter the new user's full name in the **Person's Name** box.
4. If the new user's account is going to be a parent account, leave <None> in the Parent/Admin dropdown box. If the account will be managed by another parent account, select that account from the dropdown list.
5. Check **Account Status** to activate account. Account can be disabled at any time without deleting the user.
6. Choose **User Level** from the dropdown list. The following table describes the user levels:

Level	Description
System Administrator	Controls all of the settings and server configurations given permissions. May also control network settings, database access, and restarting and shutting down the server.
Other	A custom defined group with its own permissions and rule-sets. Please read the section on groups for additional information.

7. Click **Add User** to complete the process.



Modify User
To modify a user, click **Modify User** under User/Group Manager in the System Settings / Tools control panel. Click the person's username from the user list. For exact descriptions of the options for modifying a user, please refer to the descriptions listed above in the Add New User section.

Delete User
To delete a user, click **Delete User** under User/Group Manager in the System Settings/Tools control panel. Then click the person's username from the user list. You will be allowed to review the account information. If the person is listed as a parent account, you will have the option of delegating its child accounts to another parent for continued management.

Group Management

Add Group

To add a new group, click **Add Group** under User/Group Manager in the System Settings/Tools control panel.

Groups essentially lays out a user's parameters when performing maintenance, adding mail users, adding web sites, setting up FTP users, etc. For example, you could create an individual account that is only able to add new mail users, but only able to add five new mail users with no other system access.

1. Select and type in a "Group Name" to identify this group; it should be something specific and easily recognizable like "Mail Only Users" or "Mail Administrator Access."
2. Next, if you have any notes or specific descriptive comments for this group you can write them in the "Notes" box.
3. Select the individual portions of the admin web site that the group will be capable of accessing. For items with the "Limit" field next to them, you may specify how many of those items the user of the group is able to add before being stopped from adding additional items. (The limit is for the individual user in the group, not the entire group with multiple entries.)
4. Click **Add Group** at the bottom of the web page.

Modify Group
To modify a group, click **Modify Group** under User / Group Manager in the System Settings / Tools control panel. Then click the group's name from the group list. You will be allowed to review the group information and make adjustments to the permission set. You will not be able to change the Group Name, however.

Delete Group
To delete a group, click **Delete Group** under User / Group Manager in the System Settings / Tools control panel. Then click on the group's name from the group list that you wish to delete. You will be allowed to review the group information before finally deleting the group.

Reporting

Reporting will be the best indicator of what is going on with your Server Appliance. The system automatically records various internal data and creates time-based graphs showing the performance of your appliance. The details of the metrics that are recorded have been listed below. All reporting with the exceptions of the security log warnings and web-server performance are shown in daily, weekly, monthly, and yearly formats.

User CPU Load
Two metrics will be graphed in this percentage: the percent of the processor system that is active and the percent that is completely idle. If you start to see your user percentage averaging above 80 percent on a weekly basis, it might be time to expand your appliance.

Active CPU Load
This metric simply graphs what percent of your system is being completely utilized. If your system climbs above about 50 percent, it might be time to look at expanding your processor.

Disk Usage
The disk usage will show how much space is being fully utilized on your system. Both the /home directory which is where user files are stored, and the / directory where system and log files remain are graphed. If you begin approaching 90 percent of capacity you might consider adding some additional disk space.

Traffic Analysis for Ethernet Interface 0/1
This metric monitors the total bandwidth going through a given interface at a given time. It can show the system administrator or a hosting provider how much bandwidth a given Ethernet interface is using over an extended time period.

Memory Usage
This will list the percentage of total physical and virtual memory being currently used. (Physical memory is memory actually located in the machine, while virtual memory is segmented disk space utilized as memory in the case of physical memory shortages.) If your virtual memory begins to rise to the 75-percent range you might consider adding some additional memory to meet user loads.

Security Log Warnings
The security section is extremely accurate and detailed. In this section various TCP, UDP, and ICMP traffic is logged. If a remote IP address of some kind is attempting to perform malicious activities or check for weaknesses in the system, it will be recorded in a log along with a time stamp and some detailed information about the possible vulnerability. This section does NOT list things wrong with the Server Appliance, it merely shows the system administrator potentially dangerous traffic.

Web Server Status
This is a real-time assessment of requests being processed by the web server as well as active processes and other detailed information. This can help you track file types

being downloaded or information concerning which websites on your server are gathering more traffic than others.

Web, FTP, SQL, SMTP, POP3, DNS, WFS, WINS, Spam Memory/CPU Usage
Each active server process on the appliance outputs both memory and CPU percentage utilization and is graphed in separate reports. The green line always represents the memory and the blue line represents the CPU. Each is tracked as a percentage of 100 percent memory or CPU utilization.

Blackbox Commander Shell

The Blackbox Commander shell allows you to perform several functions that may also be covered from the Web interface. These functions are available in case your only access option is through the console. In addition to being able to log in to the Blackbox account from a direct plug-in to the console server, you may also connect remotely from a fully functional SSH2 client such as Secure CRT from VanDyke Technologies.

The functions available from the commander area are:

Function	Description
Stop Server Process	Stop the Web, Mail, FTP, DNS, or SQL Service
Start Server Process	Start the Web, Mail, FTP, DNS, or SQL Service
Restart Server Process	Stop and start the Web, Mail, FTP, DNS or SQL Service
Exit to Bash Shell	Exit to an ANSI bash shell for system configuration
Restart Server	Reboot the server
Shutdown Server	Shutdown the server entirely
Change Network Settings	Adjust network settings; this should only be used as a last resort for changing network settings
Adjust Time Zone	Adjust the system clock to your time zone
Rebuild Server	Remove your entire configuration and restore the server to its factory shipping settings and defaults
Change System (Root) Password	Modify the systems root password
Change MySQL (Database) Password	Modify the database login password
Change System (BlackBox) Password	Modify the system shell (blackbox) password
Disable IP Firewall	Reset and disable a bad or too restrictive firewall configuration

```
-------------------------------------------------------
      Xoasis Networks Black Box Shell Commander
-------------------------------------------------------
Welcome to the system configuration shell.

      1) Stop Server Process
      2) Start Server Process
      3) Restart Server Process
      4) Exit to Bash Shell
      5) Restart Server
      6) Shutdown Server
      7) Change Network Settings
      8) Adjust Time Zone
      9) Rebuild Server
      10) Change System (Root) Password
      11) Change MySQL (Database) Password
      12) Change System (BlackBox) Password
      13) Disable IP Firewall

Command?
```

SSH Shell Access

If you need to perform additional maintenance to the server; add, remove, or modify software; or perform any other routine maintenance, you may do so by connecting to the server over the SSH2 protocol. The SSH2 protocol is supported in such common programs as Secure CRT available at www.vandyke.com. Additionally, a free SSH2 client known as PuTTy may be obtained as well.

Both the blackbox and root passwords are supplied on the Security Pass card included in your original server box. You're encouraged to only use the blackbox account for security reasons. However, if you do need to log in as root, you may do so by first logging in via SSH2 to the blackbox account. Then use the su or sudo commands to gain access to the root shell.

If for some reason you have lost access to the root account password but still have the blackbox account password you may modify the root account password by issuing the command `sudo passwd root` at the command prompt of the blackbox account.

License Agreement

LICENSE AGREEEMENT
XOASIS NETWORKS, INC.
Black Box Server Appliance

IMPORTANT-READ CAREFULLY: This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Xoasis Networks, Inc. ("Xoasis") regarding the Black Box Server Appliance ("System") you acquired, which includes certain Xoasis software product(s) installed on the System and/or included in the System package ("Software"). The Software includes computer software, the associated media, any printed materials, and any "online" or electronic documentation. By installing, copying or otherwise using the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, Xoasis is unwilling to license the Software to you. In such event, you may not use or copy the Software, and you should promptly contact Xoasis for instructions on return of the unused product(s) for a refund.

SOFTWARE LICENSE

The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold.

i) GRANT OF LICENSE. Software includes software already installed on the System ("System Software") and software contained on the CD-ROM disk and/or floppy disk(s) ("Additional Software"). This EULA grants you the following rights to the Software:

(1) System Software. You may use the System Software only as installed in the System.

b. Additional Software. Additional Software might not be included with your System. If Additional Software is included with your System, you may install and use the component(s) of the Additional Software in accordance with the terms of the end user license agreement provided with such component(s). In the absence of a separate end user license agreement for particular component(s) of the Additional Software, you may install and use only one (1) copy of such component(s) on a single computer with which you use the System.

ii) DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

(1) Limitations on Reverse Engineering, Decompilation and Disassembly. You may not reverse engineer, decompile, or disassemble the System Software, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

(2) Single System. The System Software is licensed with the System as a single integrated product. The System Software installed in Read Only Memory ("ROM") of the System may only be used as part of the System.

(3) Single EULA. The package for the System Software may contain multiple versions of this EULA, such as multiple translations and/or multiple media versions (e.g., in the user documentation and in the software). Even if you receive multiple versions of the EULA, you are licensed to use only one (1) copy of the System Software.

(4) Rental. You may not rent or lease the Software.

(5) Software Transfer. You may permanently transfer all of your rights under this EULA only as part of a sale or transfer of the System, provided you retain no copies, you transfer all of the Software (including all component parts, the media, any upgrades or backup copies, this EULA and, if applicable, the Certificate(s) of Authenticity), and the recipient agrees to the terms of this EULA. If the Software is an upgrade, any transfer must include all prior versions of the Software.

(6) Termination. Without prejudice to any other rights, Xoasis may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the Software and all of its component parts.

iii) UPGRADES AND RECOVERY MEDIA. If the System Software and this EULA are provided separate from the System by Xoasis and the System Software is on a ROM chip, CD ROM disk(s) or floppy disk(s), and labeled "For ROM Upgrade Purposes Only" ("ROM Upgrade"), you may install one copy of the ROM Upgrade onto the System as a replacement copy for the System Software originally installed on the System and use it in accordance with Section 1 of this EULA. You may also install additional copies of the ROM Upgrade as replacement copies onto additional systems which are the same brand and model as the System and contain a duly licensed copy of the same version and language release of the Software ("Additional Systems"), provided that (1) Xoasis has supplied a corresponding serialized sticker for each additional copy of the ROM Upgrade, and (2) you affix a serialized sticker per Xoasis' instructions for each unit of ROM Upgrade you install. If the System Software is provided by Xoasis on separate media and labeled as "Recovery Media", you may not make a copy of the Software as described in Section 1 for archival purposes. Instead, you may use the Recovery Media solely to restore or reinstall the same version and language release of the Software as originally installed on the System and thereafter use the Software as restored or reinstalled in accordance with Section 1 of this EULA. A single unit of Recovery Media may be used by you to restore or reinstall the Software on Additional Systems.

iv) COPYRIGHT. All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets," incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Xoasis or its suppliers. You may not copy the printed materials accompanying the Software. All rights not specifically granted under this EULA are reserved by Xoasis and its suppliers.

v) PRODUCT SUPPORT. Product support for the Software and the System includes 24 months of e-mail and phone support provided by Xoasis. You

may purchase a support contract from Xoasis for additional support after 24 months from your original purchase date of the System or other Xoasis server appliance products. For product support, please refer to Xoasis' support number provided in the documentation for the System. Should you have any questions concerning this EULA, or if you desire to contact Xoasis for any other reason, please refer to the address provided in the documentation for the System.

vi) EXPORT RESTRICTIONS. You agree that you will not export or re-export the Software to any country, person, or entity subject to U.S. export restrictions. You specifically agree not to export or re-export the Software: (i) to any country to which the U.S. has embargoed or restricted the export of goods or services, which as of March 1998 include, but are not necessarily limited to Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria, or to any national of any such country, wherever located, who intends to transmit or transport the products back to such country; (ii) to any person or entity who you know or have reason to know will utilize the Software or portion thereof in the design, development or production of nuclear, chemical or biological weapons; or (iii) to any person or entity who has been prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. If Software is labeled "North America Only Version" on the Product Identification Card, or on the Software packaging or other written materials, then the following applies: The Software is intended for distribution only in the United States, its territories and possessions (including Puerto Rico, Guam, and U.S. Virgin Islands) and Canada. Export of the Software from the United States is regulated under "EI controls" of the Export Administration Regulations (EAR, 15 CFR 730-744) of the U.S. Commerce Department, Bureau of Export Administration (BXA). A license is required to export the Software outside the United States or Canada. You agree that you will not directly or indirectly, export or re-export the Software (or portions thereof) to any country, other than Canada, or to any person or entity subject to U.S. export restrictions without first obtaining a Commerce Department export license. You warrant and represent that neither the BXA nor any other U.S. federal agency has suspended, revoked or denied your export privileges.

vii) LIMITED WARRANTY.

(1) Limited Warranty. Subject to Section 7(c) below, Xoasis warrants that the Software will perform substantially in accordance with the accompanying written materials for a period of twenty-four (24) months from the date of receipt. Any implied warranties on the Software are limited twenty four (24) months. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

(2) Customer Remedies. Xoasis's and its suppliers' entire liability and your exclusive remedy shall be, at Xoasis's option, either (a) return of the price paid, or (b) repair or replacement of the Software that does not meet the above Limited Warranty and which is returned to Xoasis with a copy of your receipt. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplication. Any replacement Software will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(3) No Other Warranties. EXCEPT AS EXPRESSLY PROVIDED IN THE LIMITED WARRANTY SECTION ABOVE, THE SOFTWARE IS PROVIDED TO THE END USER "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF NON-INFRINGEMENT,

MERCHANTABILITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK OF THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU.

(4) No Liability for Consequential Damages. XOASIS OR ITS SUPPLIERS SHALL NOT BE HELD TO ANY LIABILITY FOR ANY DAMAGES SUFFERED OR INCURRED BY THE END USER (INCLUDING, BUT NOT LIMITED TO, GENERAL, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES INCLUDING DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION AND THE LIKE), ARISING FROM OR IN CONNECTION WITH THE DELIVERY, USE OR PERFORMANCE OF THE SOFTWARE.

(5) Effect of Modifications. Removing, replacing or adding component hardware will void any and all hardware and software warranties unless such removal, replacement or addition is specifically authorized in writing by Xoasis and has been delivered by Xoasis for the repair or upgrade of the System. Any addition or modification to the System Software, without written authorization from Xoasis, will void any and all warranties, express or implied, with respect to software performance and stability warranties.

If you acquired this EULA in the United States, this EULA is governed by the laws of the State of Washington and each of the parties hereto irrevocably attorns to the jurisdiction of King County, Washington and further agrees to commence any litigation which may arise hereunder in the courts located in King County, Washington. If you acquired this EULA in Canada, this EULA is governed by the laws of the Province of Ontario, Canada and each of the parties hereto irrevocably attorns to the jurisdiction of the courts of the Province of Ontario and further agrees to commence any litigation which may arise hereunder in the courts located in the Judicial District of York, Province of Ontario. If this EULA was acquired outside the United States, then local law may apply. Should you have any questions concerning this EULA, please contact Xoasis.

viii) U.S. GOVERNMENT RESTRICTED RIGHTS. The Software and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.