



Chapter 1 - Introduction

- [Introduction](#)
- [Services on the OSPanel server appliance](#)
- [Documentation](#)
- [Customer Service and Technical Support](#)
- [Before contacting Technical Support](#)
- [Further resources and information](#)

Chapter 2 - Initial Setup

- [Setting up the OSPanel server appliance](#)
- [Configuring the OSPanel server appliance with the Setup Wizard](#)
- [Network Settings](#)
- [Password Guidelines](#)
- [Time Settings](#)
- [Completing configuration with the Setup Wizard](#)
- [Logout icon](#)

Chapter 3 - Services

- [Services](#)
- [Managing your Personal Profile](#)
- [Using email on the server appliance](#)
- [Email relaying](#)
- [POP-before-SMTP feature](#)
- [Mailing lists](#)
- [Developing Web pages](#)
- [CGI scripts](#)
- [Server Side Scripting Languages](#)
- [Publishing Web pages using FTP](#)
- [Domain Name System \(DNS\)](#)
- [RAID](#)
- [System Health Monitoring](#)
- [Secure sockets layer \(SSL\)](#)
- [Simple Network Management Protocol \(SNMP\)](#)

Chapter 4 - Server Management

- [Server Management](#)
- [Accessing Server Management](#)
- [Server Administrators](#)
- [Network Services](#)
- [Web Server Settings](#)
- [FTP Server Settings](#)
- [Email Servers](#)

- [Email Servers Settings \(Basic\)](#)
- [Email Servers Settings \(Advanced\)](#)
- [DNS The Domain Name System](#)
- [SNMP](#)
- [Shell](#)
- [SSL](#)
- [System Settings](#)
- [TCP/IP](#)
- [IP Address Allocation](#)
- [Power](#)
- [Time](#)
- [Maintenance](#)
- [Server Appliance UI](#)
- [Usage Information](#)
- [Network Usage Information](#)
- [Configure Web Reporting Options](#)
- [Configure FTP Reporting Options](#)
- [Configure Email Reporting Options](#)
- [Configure Disk Reporting Options](#)
- [Active Monitor](#)
- [Active Status Overview screen](#)

Chapter 5 - Site Management

- [Site Management](#)
- [Administrator privileges](#)
- [Site Management screen \(for Server Administrator\)](#)
- [Search Virtual Sites](#)
- [Site Management screen \(for Server Administrator\)](#)
- [Editing the virtual site template](#)
- [Managing Virtual Sites](#)
- [User Management](#)
- [Creating a TSV text file](#)
- [Importing Users](#)
- [Exporting Users](#)
- [Mailing Lists](#)
- [General Settings](#)
- [Services](#)
- [Services - Web](#)
- [Services - Anonymous FTP](#)
- [Services - Email](#)
- [Services - Shell](#)
- [Services - SSL](#)
- [Usage Information](#)

Chapter 6 - Installing Software and Updates

- [Updates](#)
- [Installed Software](#)
- [Settings](#)

Chapter 7 - Personal Profile

- [Personal Profile](#)
- [Email Formats](#)
- [Enabling the vacation message](#)
- [Disabling the vacation message](#)
- [Disk Usage](#)

Chapter 8 - Advanced Usage

- [Serial console port](#)
- [Powering down the server appliance remotely](#)
- [Development tools](#)
- [Configuration files](#)
- [Directory structure](#)
- [Customised error Web pages](#)
- [Site User Home Page](#)

Chapter 9 DNS - The Domain Name System

- [Domain Name System](#)
- [Advanced DNS](#)
- [Domain administrator email address](#)
- [Retry interval](#)
- [Forwarding server](#)
- [Zone transfer](#)
- [Zone Format](#)
- [Primary services](#)
- [Modifying the SOA record](#)
- [Deleting all DNS records](#)
- [Configuring a Forward Address \(A\) record](#)
- [Configuring a Reverse Address \(PTR\) record](#)
- [Configuring a Mail Server \(MX\) record](#)
- [Configuring an Alias \(CNAME\) record](#)
- [Adding a Subdomain Delegation](#)
- [Adding a Subnet Delegation](#)
- [Secondary services](#)
- [Sample setup of DNS service](#)
- [Brief history of the Domain Name System \(DNS\)](#)
- [How does DNS work?](#)



Chapter 1

Introduction

The OSPanel Server Appliance is a powerful and versatile network server. It fits easily within an existing network, and provides virtual hosting capabilities for email and Web hosting. The OSPanel Server Appliance is primarily an Internet Web, mail, FTP and DNS server with extensive virtual hosting and dynamic content generation capabilities. After initial setup using the server's LCD or serial console, all server administration is done through a secure browser connection through either an intranet or Internet connection. Server-wide service offerings are configured through a Web administration facility. This gives the administrator the ability to:

- Administer virtual sites
- Configure email, FTP, Telnet, SNMP, ASP and DNS services
- Install and upgrade software
- Configure network parameters
- Configure uninterruptible power supply (UPS) operation
- Configure wake options
- Monitor system services and resources

The administration Web pages allow the addition, configuration and monitoring of virtual sites, either based on name or IP address. Configuration options for virtual sites include:

- Adding users
- Creating mailing lists
- Configuring CGI, SSI, PHP, Telnet, Frontpage, FTP

Assigning bandwidth limits Additionally, the server administration interface gives status on sites, including traffic reports and disk usage information. Individual users on a virtual site have access to the Web administration facility where they can access the following:

- Email settings
- Personal preferences
- Usage data

Services on the OSPanel Server Appliance

Here is a sample of what you can do with the OSPanel Server Appliance:

- Web publishing
- Email

The Server Appliance's email service allows you to communicate internally and externally to individuals. It includes auto-forward and auto-response capabilities for each personal site. You can also create mailing lists

that include external users. To access your email on the OSPanel Server Appliance, you can use any standard email client software. These services can be used within an extranet or an intranet environment, or across the Internet.

Documentation

You can access the user manual in PDF format from the browser-based user interface. If you have installed third-party software on the OSPanel Server Appliance, the relevant documentation is available on the browser screen. To access the PDF file for the user manual, click on the "question mark" help icon in the top right corner. A separate browser window opens displaying a list of PDF files in the languages available. Click the link for the PDF in your preferred language; you can open the PDF file in the browser window or save it to your personal computer.

Customer Service and Technical Support

You can use the OS Office discussion forum to find answers, post problems and read responses to posted problems. Our discussion forum is moderated by OS Office Support staff.

Before contacting Technical Support

Take note of all actions you perform and any error messages so that, if necessary, you can describe them to a member of the Technical Support team. Refer to the user manual and to the Web-based resources, such as the OS Office Forum.

Further resources and information

To speed up your support call When contacting Technical Support, the more information you can provide, the better. Before you call or email, have the following information ready:

- Any additional software installed on your system
- Any peripherals connected to your system
- Any error messages you have received and the time when they occurred
- The process you were running or the changes you had made when the error occurred
- The steps you have taken to resolve the problem



Chapter 2

Setting up the OSPanel Server Appliance

To use the browser to set up the OSPanel Server Appliance, follow these steps:

1. Launch a standard Web browser on a computer connected to the network.
2. Enter the IP address of the Server Appliance in the URL field of your browser
3. Press Return (or Enter) on your keyboard. If you configured the network settings successfully, the OSPanel Welcome screen appears; see Figure 6.

Figure 6. Welcome Screen

Welcome and thank you for installing BlueQuartz, the open source server appliance platform for web hosting. Within minutes, you will be able to host multiple domains, each with complete web, email, and FTP services - all easily administered from your browser.

Click the Start button below to begin the Setup Wizard, which will guide you through the process of setting up your new server interface.

[Start](#)



Configuring the OSPanel Server Appliance with the Setup Wizard

If the browser is set up to display a specific language, the Setup Wizard synchronizes with that language preference (if it is available in the software for OSPanel Server Appliance).

The default language is English. The browser then displays the Welcome screen in the selected language. If the language selected in the browser preferences is not available on the Server Appliance, the server defaults to the Administrator's choice of language.

To configure the Server Appliance, enter information into the fields on the Setup Wizard screens. These fields are described in the sections that follow.

The Setup Wizard is a series of screens that guide you through the setup process. After completing each step, click on the right arrow at the bottom to apply the changes and move on to the next step. You can click on the left arrow to return to a previous screen.

The OSPanel Server Appliance performs automatic checks on the information entered and alerts you when an illegal value or a problem is encountered. When the information is entered correctly at each stage, the Server Appliance enters the changes in its configuration files before proceeding to the next step. Changes may take several seconds to complete.

Click Start on the Welcome screen to begin the Setup Wizard.

Note: You cannot use accented characters (for example, a", e', n~) in the following items:

- User names
- Email addresses and email aliases
- Host names and domain names You can use accented characters in descriptive fields, for example, in the Full Name field for a user.

Note: For help with a particular item in the Setup Wizard, move the pointer over the item on the screen; help text appears at the bottom of the screen.

At this stage, you should see the System Settings Screen

Figure 8. System Settings

System Settings

Network Settings

Host and Domain Name
Host Name Domain Name

DNS Servers (optional)

Gateway (optional)

Primary Interface

IP Address

IP Network Mask

MAC Address 00:10:E0:01:8D:94

Administrator Settings

User Name admin

Password
 (Enter Again)

Preferred Language

Select Your Preferred Language ▾

Time Settings

Date ▾ ▾ ▾
 ▾ : ▾ ▾

Time Zone ▾
 ▾
 ▾

Network Settings

On the Network Settings portion of the screen, you can do the following:

- Assign a host name (for example, bq1) to the Server Appliance.
- Enter your domain name. The domain name is either the official domain name that is registered with an ICANN-accredited registrar (for example, "mydomain.com") or an intranet domain name specific to your network.

- Coordinate the host name and domain name with your Internet service provider (ISP) to ensure the integrity of your network. If your OSPanel Server Appliance is integrated into a larger network, consult with your network administrator for this information. This allows you to access your Server Appliance by host name and domain name, rather than only by IP address.
- Enter the IP address of your Domain Name System (DNS) server. A DNS server maintains a list of computer names and their IP addresses. The OSPanel Server Appliance needs access to this list on the DNS server in order to convert between IP addresses and names. This conversion is essential for sending and receiving email external to the Server Appliance. For more information on DNS, see [Domain Name System](#).

Note: There are no spaces allowed in the host name.

The OSPanel Server Appliance Administrator is responsible for the following:

- Setting up and maintaining the users and services on the Server Appliance
- Responding to email alerts from the Server Appliance in order to forestall potential problems
- To set up the OSPanel Server Appliance for the Administrator, you must enter a Password in this field. For guidelines on choosing a password, see "Password Guidelines"

Be sure to remember the password to access the Administration features in the future.

If you forget the password or want to reset the password, see "Resetting the Administrator password"

If you want to change the password for the Administrator, see "Account"

Note: We recommend that you reserve the email account admin for system messages and alerts only and that you do not publicize this admin account.

Password Guidelines

Use the following guidelines when choosing a password:

The valid characters include: a-z A-Z 0-9 % ! @ \$ ^ & * - _ = \ | . , / ? ; : +

1. Use between three and sixteen alphanumeric characters.
2. Use both upper- and lower-case letters.

Note: A password is case-sensitive.

3. Do not use a proper name.
4. Do not use a word found in a dictionary.
5. Do not use a date.
6. Do not use a command word.
7. Do not use a string of consecutive keys on a keyboard (for example, "qwerty").

Time Settings

On the Time Settings portion of the screen, you can set the day, date, time and time zone.

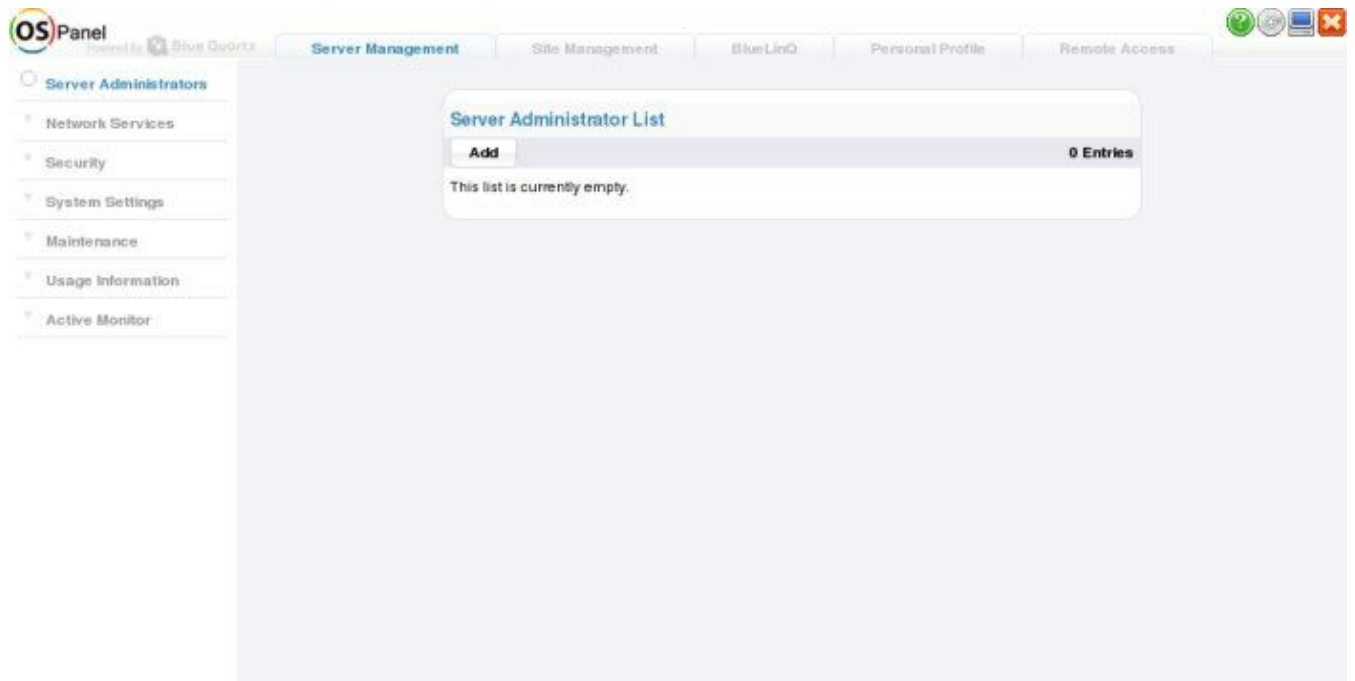
Click the right arrow at the bottom to move to the next screen.

Completing configuration with the Setup Wizard

When you complete the Product Registration screen, click the right arrow at the bottom.

Once the OSPanel Server Appliance has been configured, the screen shown in Figure 11 appears.

Figure 11. Server Management on the user interface



There are four tabs at the top of the screen:

- Server Management - for details, see [Chapter 4 Server Management](#)
- Site Management - for details, see [Chapter 5 Site Management](#)
- BlueLinQ - for details, see [Chapter 6 Installing Software and Updates](#)
- Personal Profile - for details, see [Chapter 7 Personal Profile](#)

The buttons on the left side of user interface provide access to the information and functions on this site. Move the mouse pointer over the menu buttons and a description of the user interface features appears in the help text frame at the bottom.

Note: If you changed the system time in the System Settings screen, you may be presented with the login screen.

The icons in the upper right-hand corner of the screen are described below: Help icon

You can access the user manual in PDF format from the user interface. If you have installed third-party software on the OSPanel Server Appliance, the relevant documentation is available on this screen.

To access the PDF file for the user manual, click on the help icon in the top right corner. A separate browser window opens displaying a list of PDF files in the languages available. Click the link for the PDF in your preferred language; you can open the PDF file in the browser window or save it to your personal computer.

The Active Monitor icon allows you to view system and services status information. The icon turns red and blinks if any of the components monitored by Active Monitor have severe problems.

For more information on the Active Monitor feature, see "Active Monitor"

Logout icon

Click this icon to log out of the system.



Chapter 3

Services

This chapter offers a brief overview of the services available on the OSPanel Server Appliance.

These services include:

- [Publishing Web pages using FTP](#)
- [RAID1 support](#)
- [Secure sockets layer \(SSL\)](#)
- [Simple Network Management Protocol \(SNMP\)](#)
- [Managing virtual sites, each with their own Web, mail, usage statistics and FTP settings](#)
- [Enabling PHP scripting, Common Gateway Interface \(CGI\) and FrontPage Extensions](#)
- [Installing software](#)
- [Domain Name System \(DNS\) server](#)

Managing your personal profile

Registered users on the OSPanel Server Appliance can manage their own Personal Profile, including changing their password, using a standard Web browser

The features accessible from the Personal Profile screen are:

- Account
- Email
- Disk usage For more information, see [Personal Profile](#)

Using email on the Server Appliance

To use all of the email capabilities on the OSPanel Server Appliance, you must configure the email settings correctly. You must also configure your email client to send email to and retrieve email from the Server Appliance.

Email aliases

Each registered user on the OSPanel Server Appliance must have a unique user name (for example, mary or john.smith or khoward). This user name is used to send or retrieve email.

The Email Alias feature allows you to create an arbitrary email address without creating a user account on the Server Appliance. An email message addressed to the alias is forwarded to an existing email address.

If you add more than one alias for a user, enter one alias per line. You can only use lowercase alphanumeric characters, periods (.), hyphens (-) and underscores (_) in the alias.

Let us say that the XYZ Company has an OSPanel Server Appliance and that the company's domain name is xyz.com. The email addresses for the users of the Server Appliance is @xyz.com. Employee Andrew Bose has a user name of "abose"; his email address is "abose@xyz.com".

Users can have several email aliases that point to their user name. For example, Andrew Bose can have the aliases "andrew@xyz.com" and "andrew.bose@xyz.com". If he were an avid soccer player, he might want to use the alias "striker@xyz.com". All of these aliases point to his user name at xyz.com. Email messages addressed to any of these aliases are forwarded to "abose@xyz.com".

However, having a large number of aliases for each user can cause problems. If a new user is added and the user name that is automatically generated by the Server Appliance is already in use, a warning appears in the help text at the bottom of the screen, stating that has already been taken by another person. In this case, the Server Appliance does not accept the New User entry.

Following the previous example, let us say that Andrew Boisvert is a new employee at the XYZ Company. If he wanted to have "andrew" as his user name, the Server Appliance help text displays:

"Sorry, you have entered a value for User Name that has already been taken by another person on this system. Please enter another value for User Name."

The system suggests an alternate user name. The OSPanel Server Appliance verifies the alias that you enter. If the alias is already in use as a user name, as another user's alias or as the name of a mailing list, the Server Appliance does not allow the new alias.

An Administrator can also set up aliases such as webmaster@xyz.com, info@xyz.com, sales@xyz.com, comments@xyz.com or support@xyz.com that point to a specific user name.

Email relaying

Simple Mail Transfer Protocol (SMTP) service is different from Post Office Protocol (POP), telnet and File Transfer Protocol (FTP) services in that SMTP does not try to authenticate a user when an SMTP connection is made. Every email server on the Internet has to be able to deliver email to you, so the email servers must be able to connect freely to send the email.

The OSPanel Server Appliance accepts email if the recipient has a user account or an alias email account, or if the sending host (your client computer) is trusted to relay outgoing email messages to another domain. These trusts are defined by host or domain names, as well as by IP addresses and networks. A network is a range of IP addresses; a network can be as small as one IP address, but that is not very practical.

Caution: Some users advise you to open relay to all com, edu, net and other top-level domain addresses. However, doing so allows hosts belonging to com, edu, net and others to relay email through your OSPanel Server Appliance; this relayed mail is often known as spam mail. Spam mail can appear as though it originated from your Server Appliance and as a result, others may blacklist your Server Appliance as a known spam site. If your Server Appliance is blacklisted, many mail servers will not relay your email and your customers will not receive a large amount of their email messages.

OSPanel Server Appliance "209.48.0.0" to the "Relay email from these hosts/domains" field of the Email Parameters menu. If your ISP gives you a list of 30 networks used by 30 points-of-presence (which are regional ISP offices) across the country and your clients can dial in from any of them, then you must trust all

30 networks or these users cannot send email through your Server Appliance.

POP-before-SMTP feature

The OSPanel Server Appliance provides an option to allow POP authentication before SMTP.

Normally, you only permit email relaying from within your own network. But some users travel and connect from other places (for example, sales people or field engineers) and you want to let those users relay email through your server. The way to allow this and still protect your Server Appliance from being used to relay spam mail is to authenticate the user through POP before establishing an SMTP connection.

When a user logs in for POP3 email, the OSPanel Server Appliance notes the IP address from which the connection was made and permits relay from that IP address for a limited time. Travelling users need only check their email to "unlock" the mail server; no changes to the client mail software are necessary.

The POP-before-SMTP implementation causes the IP addresses to expire after 30 minutes.

Mailing lists

A mailing list allows you to send messages to a certain group of people without having to address them individually. You can create a mailing list comprising users registered on the OSPanel Server Appliance as well as email addresses external to the Server Appliance. See [Mailing Lists](#) for more details on how to set up and use mailing lists.

Note: By default, the domain name for the OSPanel Server Appliance is allowed to relay email.

If you do not want to allow email originating from the domain to which your Server Appliance belongs to be relayed through your Server Appliance, enter the domain name of your Server Appliance in the "Block Email From Hosts/Domains" field.

You will be then able to download email but not be able to send outgoing email messages through OSPanel Server Appliance.

Developing Web pages

The OSPanel Server Appliance automatically provides a default home page for each individual user. It also supports a broad range of Web publishing capabilities that allow both novice and expert users to build and publish custom Web pages.

Note: To access your home page, enter the URL <http://hostname/~username/>, where hostname is the fully qualified domain name of your OSPanel Server Appliance and username is your user name on the Server Appliance.

You must include the tilde mark (~) before your user name.

Using an HTML editor

You can create Web pages using any of the standard HTML editors and the HTML publishing capabilities of many popular desktop productivity applications. You can create and link the Web pages themselves on your desktop computer, and then move them to the appropriate subdirectory in the OSPanel Server Appliance through an FTP application; see [Publishing Web pages using FTP](#).

CGI scripts

The OSPanel Server Appliance supports common gateway interface (CGI) scripts, such as those written in Perl or C, as well as UNIX(R) shell scripts.

CGI scripts allow you to develop highly interactive, powerful Web-based applications by building server-side CGI scripts that generate Web pages in response to specific user inputs. These applications range from simple scheduling and conferencing applications to sophisticated electronic commerce solutions.

You can develop CGI scripts on your desktop machine and then transfer them to the Server Appliance through an FTP-based application that allows the permissions to be set to "Executable".

CGI scripts must use .pl or .cgi filename extensions in order to be executed by the Web server.

Use FTP to upload .cgi and .pl files; use ASCII mode to upload CGI files. Once the file is on the OSPanel Server Appliance, use your FTP program to make the script executable. You can also use the telnet command:

```
chmod 775 .cgi  
The path to Perl is  
/usr/bin/perl/
```

Server Side Scripting Languages

The OSPanel Server Appliance supports both the Active Server Pages (ASP) and PHP scripting languages. These features are enabled on a per-site basis (see the "Web Settings" table under Site Management > Services > Web).

Like CGI scripts, you can develop ASP and PHP scripts on your desktop machine and then transfer them to the Server Appliance by means of an FTP-based application. Unlike CGI scripts, ASP and PHP do not require execute permissions to work correctly. However, ensure that the Web server process can read the scripts; you can use the telnet command:

```
chmod 664 .asp or chmod 664 .php
```

 For the Web server to run the scripts correctly, PHP scripts must use the .php filename extension.

The OSPanel Server Appliance is pre-configured with support for embedded PHP scripts. You can save PHP files in any directory on your site, provided that the file ends with a .php extension, as previously mentioned.

Publishing Web pages using FTP After creating your Web pages, you can publish them on the OSPanel Server Appliance using an FTP-based application.

Make sure you have the following information:

- The host name or the IP address of your Server Appliance
- Your user name and password
- A filename of your choice to save as your main page (the default is index.html)

Launch your FTP software and establish an FTP link to the Server Appliance. Upload your HTML files. If you need help, consult the instructions for your FTP application.

Publishing Web pages using FTP

After creating your Web pages, you can publish them on the OSPanel server appliance using an FTP-based application.

Make sure you have the following information:

1. The host name or the IP address of your server appliance
2. Your user name and password
3. A filename of your choice to save as your main page (the default is index.html)

Launch your FTP software and establish an FTP link to the server appliance.

Upload your HTML files. If you need help, consult the instructions for your FTP application.

By default, the files you upload using an FTP-based application are stored in your personal directory; the directory path is:

`/home/sites/sitename/users/username`

where sitename is the fully qualified domain name of your virtual site and username is your user name.

Note to the Site Administrator: To post Web pages for your site, you must upload to the directory:

`/home/sites/sitename/web`

Only Site Administrators or the Server Administrator can upload to this directory. If you do not specify this directory, your Web pages are stored in your personal directory which is not accessible from the Web.

The Site Administrator can access and update the site root content in the directory `/web` during an FTP session. The site Web root is accessible on the Web at `http://sitename/`.

Site Administrators can update their personal Web pages in the directory: `/users/username/web` during an FTP session. Personal Web sites are accessible on the Web at : `http://sitename/~username/`

Users who are not Site Administrators can update their personal Web sites in the directory `/web` during an FTP session.

Domain Name System (DNS)

Domain Name System (DNS) The Domain Name System (DNS) is a vital and integral part of the Internet. Setting up DNS correctly on your OSPanel Server Appliance is very important. For this reason, please read the section solely devoted to explaining DNS: [Domain Name System](#)

The appendix covers the following items:

- Basic DNS issues
- Advanced DNS issues
- A quick start guide detailing a sample setup of DNS for an OSPanel Server Appliance

RAID

A redundant array of independent disks (RAID) is a way of storing the same data in different places (thus, redundantly) on multiple hard disks. A RAID appears to the operating system to be a single logical hard disk.

There are a variety of different types and implementations of RAID, each with its own advantages and disadvantages. The OSPanel Server Appliance implements RAID Level 1 (RAID-1), also known as disk mirroring, which consists of a primary hard disk and a secondary hard disk; the secondary hard disk is an

exact copy or "mirror image" of the primary hard disk. RAID-0 is also available.

RAID-0 stripes data across two disks, making the two disks appear as one large disk (about the size of the two disks combined). While this gives you more disk size, if either disk fails, data will be lost.

Although RAID can protect against disk failure, it does not protect against operator and administrator (human) error, or loss due to system errors.

The Server Appliance configuration uses Software RAID, meaning that it implements RAID in the software and requires no extra hardware.

RAID-0 must be enabled through the Setup Wizard. RAID-1 is enabled by default if your server contains two hard disk drives.

Hard disk drive failure When RAID-1 is implemented, if one of the hard disk drives fails, the OSPanel Server Appliance can function with one drive, but the server can no longer provide disk mirroring. To restore RAID service, you must shut down the Server Appliance and replace the failed drive. If RAID-0 is implemented and a hard disk drive fails, there is no recovery.

Caution: The hard disk drives in the Server Appliance are not hot-swappable; the system must be powered off before removing and replacing drives.

When a drive fails, Active Monitor indicates which drive has failed (Drive 1 or Drive 2). As viewed from the front, Drive 1 (known in Linux as hda) is closest to the front of the Server Appliance and Drive 2 (known in Linux as hdc) is behind it.

System health monitoring

Through a combination of software and hardware monitoring techniques, the OSPanel Server Appliance monitors the events described in this section.

Fan, voltage and temperature monitoring Through the use of built-in sensors, the Server Appliance monitors internal voltage and temperature levels as well as fan operation. If inappropriate behavior is observed, action is taken to protect the system.

Secure sockets layer (SSL)

The Administrator can administer the OSPanel Server Appliance through secure sockets layer (SSL). SSL is provided in 128-bit encryption code and offers a secure Web connection to the end user. The implementation of SSL on the Server Appliance is based on mod_ssl and includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)

A secure connection means two things: encryption and authentication. Encryption ensures that no one can snoop the connection between the browser and the OSPanel Server Appliance; authentication ensures the client, through a certificate, that the server is who they say they are. The security is assured on two levels.

At the network level, the first time the browser connects to a server, the browser stores the server's certificate. This is the encryption part of the secure connection. Each time the browser "thinks" that it is communicating with this same server, it verifies that this same certificate is used to assure the secure connection.

At a higher level, a server's certificate is "signed" by a trusted external authority that the browser knows about, such as VeriSign. This is the authentication part of the secure connection. The server information (country, state, city, organization) is encoded into the certificate and certificate request. The external authority signs your request and guarantees that your server information is legitimate.

For example, if a Web site sends a signed certificate saying that it comes from Sun Microsystems in Palo Alto, California, United States, the end user can trust (due to the signed certificate from the external authority) that this Web site is indeed run by this company located in this city.

A self-signed certificate is a certificate that has not been signed by an external authority. A self-signed certificate simply ensures that an encrypted Web connection is in place; it does NOT provide authentication to a user that the server is who they say they are.

On the OSPanel Server Appliance, a self-signed certificate is generated by the Server Appliance during configuration.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance and security on a network. See [SNMP](#) for more details on how SNMP is used to access the OSPanel Server Appliance.



Chapter 4

Server Management

This chapter describes the server management functions that only the Administrator of the OSPanel Server Appliance is allowed to perform. The Administrator, with the user name admin, has full control of the Server Appliance.

The Administrator of the OSPanel Server Appliance:

- Creates other server administrators
- Enters the network settings
- Enables or disables the various services
- Adds and deletes sites
- Adds and deletes users and mailing lists
- Performs maintenance functions
- Receives system alerts and warnings by email

Note: In most of the short procedures in this chapter, the first step is to click the Server Management tab in the top menu bar and the second step is to click on a selection from the left menu bar.

To reduce the number of steps in each procedure, the menu commands are grouped together and shown in bold type face. Right angle brackets separate the individual items.

For example, select **Server Management > System Settings > TCP/IP** means to click the Server Management tab in the top menu bar, click the System Settings menu category in the left menu bar and finally click the TCP/IP sub-menu item.

Server Management on the user interface is available only when you log in under the user name admin. Besides the options on the standard user interface, there are two other options: the Administration menu and the BlueLinQ.

Resetting the Administrator password If you simply want to change the Administrator password for the Server Appliance, you can do so through the Server Appliance UI.

Accessing Server Management

To access the Server Management: tab on the OSPanel Server Appliance:

1. Enter the following URL into your browser:

`http://.login/`

2. At the login screen that appears, enter the user name: admin

Only this user name and the server administrators added by the Administrator can access the Server

Management section.

Any other user name brings up the normal Server Appliance UI.

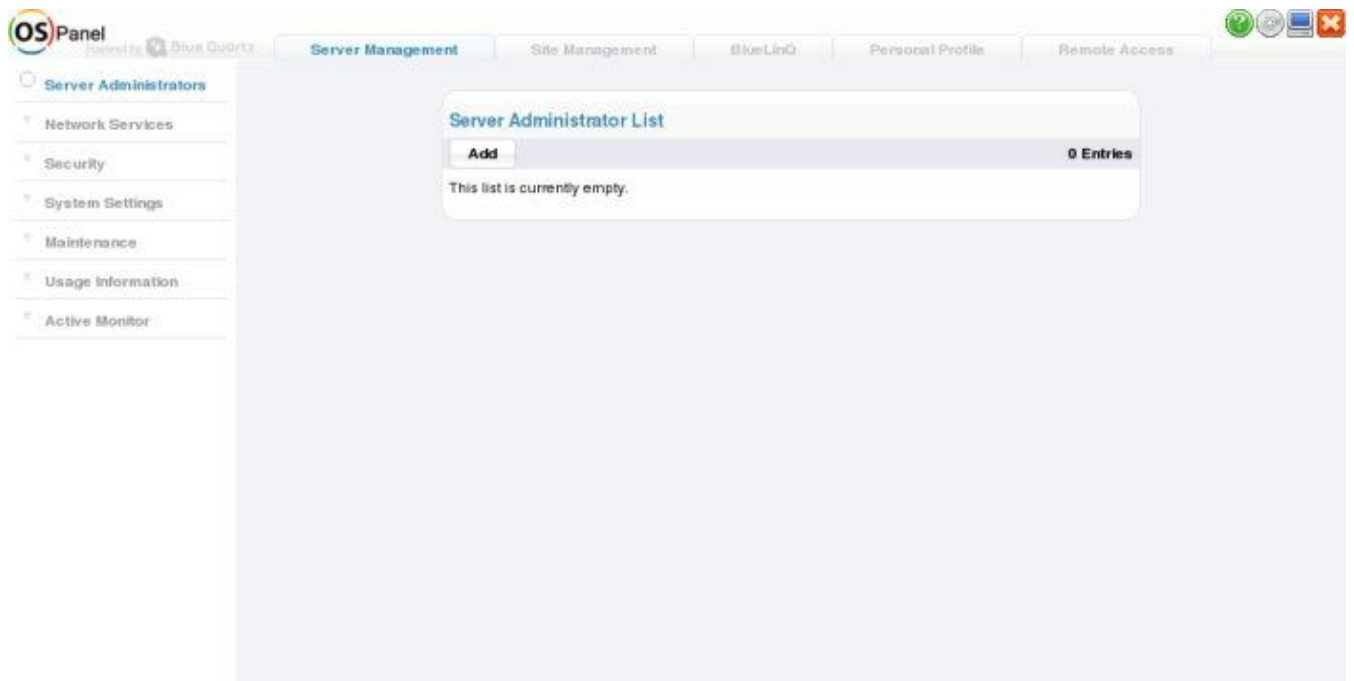
A server administrator can be given different levels of access by the Administrator.

3. Enter the admin password.
4. If you want to establish a secure connection when you log in to the Server Appliance, click the Secure Connect check box.

This establishes a Secure Sockets Layer (SSL) connection between your browser and the Server Appliance. We recommend that you enable the secure connection so that any data sent to or received from the OSPanel Server Appliance is encrypted. If your browser does not support SSL or has problems accessing the Server Appliance, try connecting without enabling the secure connection. Some browsers do not handle SSL properly and the only option is not to use SSL.

5. Click Login. If you enabled the Secure Connect option, your browser may prompt you to accept a self-signed certificate. This certificate is generated automatically for you and is required for SSL encryption. If you do not accept the certificate, you cannot use the Secure Connect option.
6. The Server Management screen of the user interface appears; see Figure 13.

Figure 13. Server Management screen



Note: The OSPanel Server Appliance generates a self-signed certificate during configuration. A self-signed certificate encrypts the data but it does not authenticate the identity of the server at the other end of the connection.

The following bullet items represent the fully expanded menu items on the left side of Server Management screen.

These are the functions and services that the Administrator can manage from the Server Management screen.

They are explained in this chapter.

- Server Administrators
- Network Services
- Web
- FTP
- Email
- DNS
- SNMP
- Shell
- Security
- SSL
- System Settings
- TCP/IP
- IP Address Allocation
- Bandwidth Limits
- Power
- Time
- Information
- Maintenance
- Server Appliance
- Usage Information
- Network
- Web
- FTP
- Email
- Disk
- Active Monitor
- Status
- Settings

Server Administrators

The Server Administrators section is where you create and manage server administrator accounts. Creating separate server administrator accounts other than the admin account allows the Administrator to allow trusted third parties to manage the server. Server administrator accounts can be created to have all the same powers, except for managing the administrator accounts controlled from the admin account. Server administrator accounts can also be created with more limits on which aspects of the Server Appliance they are allowed to control.

Click Add to add a new server administrator account.

The screen shown in Figure 14 appears.

Figure 14. Add New Server Administrator screen

There are two areas within the Add New Server Administrator main screen:

- User Information
- Administrator Options Configure the User Information fields:

1. Enter the full name, user name and password of the new Server Administrator.
2. Enter the maximum amount of disk space in megabytes (MB) that this user

should be allowed to use on this server. Leave the field blank to give the user access to an unlimited amount of disk space. Configure the Administrator Options:

1. Move extra abilities that this server administrator account should be allowed from the Available Abilities column to the Extra Abilities column.
 - ◆ IP Address Allocation: used to specify acceptable IP address ranges for this server.
 - ◆ Control Power: used to specify how the system reacts to power outages.
 - ◆ Root Access: used to allow Server Administrators to have root access to the server over a telnet connection.
2. Click Save.

Note: This optional area of the screen allows restoration of certain abilities to a Server Administrator that are normally reserved for the admin user alone.

Network Services

This section allows you to control the server's services. The following submenus are available:

- Web
- ASP
- FTP
- Email
- DNS
- SNMP
- Shell

Web Server Settings

Figure 15. Web Settings screen

The screenshot shows a 'Web Settings' configuration window. It contains four settings:

- Hostname Lookups:** A checkbox that is currently unchecked.
- Maximum Simultaneous Connections:** A text input field containing '125' with a range '(1 - 314)' to its right.
- Minimum Spare Servers:** A text input field containing '10' with a range '(1 - 50)' to its right.
- Maximum Spare Servers:** A text input field containing '25' with a range '(1 - 100)' to its right.

At the bottom center of the window is a 'Save' button.

Configure the settings in the table:

- **Hostname Lookups.** Use this to turn on host name lookups for the Web server.
 This causes the Server Appliance to do a DNS lookup on the client IP address when it connects to the server and record it in the log files.
 This host name information is then available in the Server Appliance usage Web reports.
 Without this feature, only client IP addresses are reported in the Web server usage domain report.
- **Maximum Simultaneous Connections.** This is the maximum number of requests that can be made to the server at any instance.
 Each connection requires its own Web server process.
 If this number is exceeded, clients will receive a message that the server is busy and will be asked to try again later.
 This setting is useful for controlling the load on your server.
 The maximum number of Web servers is limited by the amount of RAM installed in this server.
- **Minimum Spare Servers.** When the Web server starts or is in an idle state, this is the minimum number of Web server processes available for serving Web requests.
 The maximum number of Web servers is limited by the amount of RAM installed in this server.
- **Maximum Spare Servers.** The Web server will launch additional processes, as needed, to service additional load.

This number is the maximum number of processes the system will launch.

High traffic sites should increase this number for better performance.

The maximum number of Web servers is limited by the amount of RAM installed in this server.

FTP Server Settings

Selecting the FTP menu item brings up the File Transfer Protocol (FTP) Settings screen shown in Figure 17.

Figure 17. FTP Settings screen



The screenshot shows the 'File Transfer Protocol (FTP) Settings' window. It contains three configuration options: 'Enable Server' (checkbox), 'Hostname Lookups' (checkbox), and 'Maximum Connection Rate' (input field with value 80 and range 1-1,024). A 'Save' button is located at the bottom.

Configure the settings in the table:

- **Enable Server.** Use this to turn File Transfer Protocol (FTP) functionality on or off. Anonymous FTP access is configured by going to guestShare.
- **Maximum Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.

Email Servers

This section describes how the Administrator configures the email settings on the OSPanel Server Appliance. For additional information about setting up your email client to access email on the Server Appliance, see "Using email on the Server Appliance".

The Server Appliance supports email for entire domains such as www.mydomain.com. By default, each registered user has an email account created on the Server Appliance.

The Server Appliance supports multiple client and server email protocols but does not implement virtual email users. This means that for the entire Server Appliance, each user must have a unique username.

The Server Appliance can act as a Simple Mail Transfer Protocol (SMTP) server for sending and receiving Internet email.

Users can retrieve their email using the Post Office Protocol 3 (POP3) and the Internet Message Access Protocol 4 (IMAP4). Users can send mail using the Simple Mail Transfer Protocol (SMTP).

Selecting the Email Servers menu item brings up the Email Servers Settings screen shown in Figure 18.

Figure 18. Basic Email Servers Settings (Basic Tab) screen

Email Servers Settings	
Basic Advanced	
SMTP Service	
Enable SMTP Server	<input checked="" type="checkbox"/>
Enable SMTPS Server	<input type="checkbox"/>
Enable SMTP Auth	<input type="checkbox"/>
Enable Submission Port	<input type="checkbox"/>
IMAP Service	
Enable IMAP Server	<input checked="" type="checkbox"/>
Enable IMAPS Server	<input type="checkbox"/>
POP Service	
Enable POP Server	<input checked="" type="checkbox"/>
Enable POPS Server	<input type="checkbox"/>
<input type="button" value="Save"/>	

Important: If your Internet service provider (ISP) also provides your Domain Name System (DNS) service, the ISP must create a Mail Server (MX) record specifying your OSPanel Server Appliance as the mail server for your registered domain in order for the Server Appliance to receive email.

If your Server Appliance is integrated into a larger network, consult with your network administrator for this information.

The IP address of the DNS server must be entered in the network settings for the Server Appliance or the SMTP protocol will not work.

If you are providing your own DNS service through the OSPanel Server Appliance, you need to create an MX record for the Server Appliance. For more information on DNS, see Appendix B, "Domain Name System,".

Email Servers Settings (Basic)

1. Fill in the Basic tab settings on the Email Servers Settings table:
 - ◆ Enable SMTP Server. Use this checkbox to turn the Simple Mail Transfer Protocol (SMTP) service on or off.
Enabling SMTP allows this Server Appliance to act as an SMTP server for sending and receiving Internet email between other servers.
SMTP also allows users to use this Server Appliance for sending email.

- ◆ **Enable IMAP Server.** Use this checkbox to turn the Internet Message Access Protocol (IMAP) service on or off.
Enabling this service allows users to retrieve email from this Server Appliance using email clients that support IMAP.
IMAP allows users to store email on the server but requires continuous access to the server during the time the user is working with their mail.
- ◆ **Maximum IMAP Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.
- ◆ **Enable POP Server.** Use this check box to turn the Post Office Protocol (POP) mail retrieval service on or off. Enabling this service allows users to retrieve email from this Server Appliance using most standard email clients.
- ◆ **Maximum POP Connection Rate.** Enter the maximum number of allowed connections per minute. New connections will be denied if the connection rate has reached this limit.

2. Click Save to save the settings.

Email Servers Settings (Advanced)

Clicking the Advanced tab brings up the screen shown in Figure 19.

Figure 19. Email Servers Settings (Advanced Tab) screen

Email Servers Settings

Basic
Advanced

Delivery Schedule Immediate

Maximum Email Size (MB)
(optional)

Force Sender Domain
(optional)

Smart Relay Server *(optional)*

POP Authenticated Relaying

Relay Email From
Hosts/Domains/IP Addresses
(optional)

Block Email From
Hosts/Domains *(optional)*

Block Email From Users *(optional)*

Save

1. Fill in the Advanced tab fields in the Email Servers Settings table.

- ◆ **Delivery Schedule.** This setting specifies how frequently email is delivered by the email server on the OSPanel Server Appliance. The Server Appliance queues the messages, sending them at the specified frequency.
If you connect to the Internet through a dedicated phone line or by Ethernet (through the secondary network interface, labeled II on the back panel), then you can choose to have your email delivered and retrieved more often.
- ◆ **Maximum Email Size (MB).** Sets the maximum size of email messages this email server will send or receive. Enter an integer greater than 0. The default value is to leave this field empty, which allows this server to send and receive email messages of any size.
- ◆ **Force Sender Domain.**
An optional domain name can be specified to override the From: address of mail sent by users of this server. This feature is also called Domain Masquerade.

- ◆ **Smart Relay Server.** You can enter an optional host name in this field. With this feature, you can configure the OSPanel Server Appliance to send Internet email to a specific email server. Enter the host name of the email server through which you want to relay your email. This feature is useful if the Server Appliance does not have direct Internet access, but can communicate with an email server that has direct Internet access.
- ◆ **POP Authenticated Relaying.** Check this box to enable SMTP relay trusts by POP authentication. If checked, any user who successfully uses POP to check mail is trusted for 30 minutes to send email using the SMTP service. This feature is useful for users who frequently travel.
- ◆ **Relay Email from Hosts/Domains/IP Addresses.** Enter the IP addresses, host names or domain names that are allowed to relay email through this OSPanel Server Appliance. For more information, see "Email relaying".

A user cannot send outgoing email through this server unless the IP address, host name or domain name of the machine from which they are connecting is entered in this field. Networks may be specified in addition to IP addresses. For example, to allow relaying for a network 192.168.1.1 with subnet mask 255.255.0.0, specify the address 192.168.0.0.

Caution: Some users advise you to open relay to all com, edu, net and other top-level domain addresses. However, doing so allows hosts belonging to com, edu, net and others to relay email through your Server Appliance; this relayed mail is known as spam mail.

Spam mail can appear as though it originated from your Server Appliance and as a result, others may blacklist your Server Appliance as a known spam site. If your Server Appliance is blacklisted, many mail servers will not relay your email and your customers will not receive any email messages.

The entries you add to this field serve as part of a pattern match against the email that the client is sending. As a result, some handy shortcuts are possible. If you have a number of hosts in the same network block, you can, as a shortcut, simply enter the number of the network block.

For example, specifying a network such as 192.168.1.0 in the "Relay email from these hosts/domains" field trusts all IP addresses from 192.168.1.0 through 192.168.1.254.

If you want to allow connections from a host that ends, for example, in mydomain.com, add the string mydomain.com in the text area.

- ◆ **Block Email from Hosts/Domains.** In this field, enter email addresses or domains from which you want to block any email. Anyone trying to send you messages from one of these addresses or domains will receive an error message in return.
- ◆ **Block Email from Users.** In this field, enter email addresses of users from which you want to block any email. Anyone trying to send you messages from one of these addresses will receive an error message in return.

2. Click Save in the Email Servers Settings table.

Note: By default, the domain name for the OSPanel Server Appliance is allowed to relay email. If you do not want to allow email originating from the domain to which your Server Appliance belongs to be sent through your Server Appliance, enter the domain name of your Server Appliance in the "Block Email From Hosts/Domains" field. You will be able to download email but not be able to send outgoing email messages through OSPanel Server Appliance.

Note: If you are entering a domain name or part of a domain name in the text box, you must have reverse DNS working on your clients.

DNS The Domain Name System

(DNS) is a vital and integral part of the Internet.

Setting up DNS correctly on your OSPanel Server Appliance is very important.

The section covers the following items:

- Basic DNS issues
- Advanced DNS issues
- Zone format
- A quick start guide detailing a sample setup of DNS for an OSPanel Server Appliance
- A brief history of the DNS service

SNMP

If the SNMP agent is enabled, you can use SNMP software to remotely monitor server information such as CPU utilization and network traffic. You can specify the Simple Network Management Protocol (SNMP) communities that can have read-only and read-and-write access to this SNMP agent. The default read-only access community is "public." The default read-and-write access community is "private." To specify the SNMP communities:

Select Server Management > Network Services > SNMP. The SNMP Settings table appears; see Figure 20.

Figure 20. SNMP Settings table

Configure the following settings:

- Enable Server. Turns the Simple Network Management Protocol (SNMP) server on or off.
- Read Only SNMP Community. Enter the Read Only SNMP Community to which this OSPanel Server Appliance server belongs. The Read Only SNMP Community you enter can only contain alphanumeric characters along with '-' and '_'.
- Read and Write SNMP Community. Enter the Read and Write SNMP Community to which this Server Appliance server belongs. The Read and Write SNMP Community you enter can only contain alphanumeric characters along with '-' and '_'.
- Click Save.

Note: We recommend that you change the default string for the Read and Write SNMP Community to a unique value.

Shell

The Shell menu allows you to configure services, such as telnet and ssh, that users with shell access can use to connect to this Server Appliance.

To specify the Shell settings:

Select Server Management > Network Services > Shell. The Shell table appears; see Figure 21.

Figure 2 Shell table

Configure the selections as follows:

- Enable Telnet Server.

Enabling telnet allows users with shell access to connect to this server using telnet client software.

Enter the maximum number of allowed connections per minute.

New connection requests will be denied if the connection rate has reached this limit.

- Enable SSH Server.

Enabling the SSH server allows users with shell access to connect to this server using SSH client software.

Use of SSH is generally considered more secure than use of telnet because SSH encrypts all data, including passwords, that are sent between the client and the server.

SSL

The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. The SSL menu allows you access information about the SSL certificate used for secure access to the Server Appliance UI.

To specify the SSL settings:

Select Server Management > Security > SSL. The Certificate Information for Server Appliance screen appears along with its associated buttons; see Figure 24. >br /> Figure 24. Certificate Information for Server Appliance screen



To create a new self-signed certificate, click **Create Self-Signed Certificate** and configure the selections as follows:

- **City.** The city in which the organization is located or registered. It is important that this information is correct and can be verified with a local, regional, or national government, or other official organization.
- **State or Province.** The state, province, or region in which the above city is located. It is important that this information is correct and can be verified with a local, regional, or national government or other official organization.
- **Country.** Select the country in which the organization that will use this certificate is located or registered. It is important that this information is correct and can be verified with a local, regional, or national government or other official organization.
- **Organization.** The official name of the organization owning this certificate. In order to obtain a signed certificate from a certificate authority, the organization name and location must be verifiable with a local, regional, or national government or other official organization. In addition, the certificate authority must be able to verify that the person requesting the certificate is the owner or employee of the named organization.
- **Organization Unit.** The division or unit of the organization that is using this certificate. This is optional, but may be useful if the person applying for a signed certificate is an employee of a subsidiary of a larger organization.
- **Contact Email.** The email address to be contacted for information about this certificate.
- **Certificate Expiration Date.** The date after which the certificate should no longer be considered valid by client software attempting to connect to this server.

Click **Create Signing Request** to create a certificate signing request. The **Signing Request Information for Server Appliance** screen appears; see Figure 25.

Note: In some cases, the state and province information does not apply, depending on the country and how it is divided into different areas.

Figure 25. Signing Request Information for Server Appliance

Signing Request Information for Server Desktop

Generate Self-Signed Certificate

Location

City

State or Province

Country

Organization Information

Organization

Organization Unit *(optional)*

Other Information

Contact Email *(optional)*

Valid Period year(s)

Create Signing Request **Cancel**

After the fields are filled in, activate the Generate Self-Signed Certificate checkbox. This allows you to generate a self-signed certificate along with the signing request. The self-signed certificate can be used temporarily while you wait for the Certificate Authority to process your signing request. The certificate signing request can be submitted to a Certificate Authority to create a signed certificate that Web browsers can verify as authentic.

Click Manage Certificate Authorities to add or remove secondary certificate authorities for this site. The Certificate Authority Management for Server Appliance screen appears; see Figure 26.

Figure 26. Certificate Authority Management for Server Appliance screen

Certificate Authority Management for Server Desktop

Add

Management Actions

Certificate Authority Name

Select Certificate **Browse...**

Save **Cancel**

Note: Secondary certificate authorities are usually not needed, but certain authorities issue an extra certificate to be used for client authentication in addition to the usual server certificate that most certificate authorities issue.

Configure the settings as follows:

- Certificate Authority Name. Enter a unique name to identify this secondary certificate authority.
- Select Certificate. Click Browse to select the file that contains the certificate authority's certificate.

The certificate should be the only thing in the file. Click Import to import a signed certificate; see Figure 27.

Figure 27. Import Certificate for Server Appliance screen



Click Browse to select the text file containing the certificate to import.

The certificate file must contain both the private key and certificate sections if you are transferring it from another server.

If the certificate is from a certificate authority to which you submitted a certificate signing request generated by this server, only the certificate is necessary, but it is okay if a private key is included with the signed certificate.

Click Export to download the current private key and certificate, so the certificate can be transferred to another server.

System Settings

The System Settings section allows you to configure the Server Appliance's network, bandwidth and time settings.

The following submenus are available:

- TCP/IP
- IP Address Allocation
- Bandwidth Limits
- Power
- UPS
- Time
- Information

TCP/IP

To specify the TCP/IP settings:

1. Select Server Management > System Settings > TCP/IP. The TCP/IP Settings table appears; see Figure 28.

Click the Primary Settings tab and configure the selections as follows:

- ◆ **Host Name.** Enter the host name of this OSPanel server appliance. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes, or periods. For example, www is a valid entry.
- ◆ **Domain Name.** Enter the domain name of this OSPanel server appliance. The host name and the domain name combined together should uniquely identify this server. Enter only lowercase alphanumeric characters, dashes or periods. For example, osoffice.co.uk is a valid entry.

Figure 28. TCP/IP Settings screen

- ◆ **DNS Servers.** Enter the IP address or addresses of your local domain name server or servers. A domain name server translates textual host names and domain names into numerical IP addresses and vice-versa. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.

2. Leaving this field empty will prevent this machine from finding other machines by host name or domain name and will cause networking difficulties.

Note: Be sure to enter the IP address of your DNS server(s) here. Otherwise, the Simple Mail Transfer Protocol (SMTP) will not work. SMTP is used for transferring electronic mail messages.

For more information, see "Domain Name System".

- ◆ **Server Gateway.** Enter the IP address of the local network gateway for this Server Appliance. This is the gateway for both the primary and secondary interfaces. A network gateway allows your server to connect to the world outside of your local network area. Please enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
- ◆ **IP Address (Primary Interface).** Enter the IP address of the primary interface. If you are using only one network interface connection to the Server Appliance, use the primary Ethernet interface (labeled I on the back panel) and leave the secondary Ethernet interface (labeled II on the back panel) empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
- ◆ **IP Network Mask (Primary Interface).** Enter the network mask of the primary interface. If you are using only one network interface connection to the Server Appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- ◆ **MAC Address (Primary Interface).** The Media Access Control (MAC) address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.
- ◆ **IP Address (Secondary Interface).** Enter the IP address of the secondary interface. If you are using only one network interface connection to the Server Appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 209.43.21.5 is a valid entry.
- ◆ **IP Network Mask (Secondary Interface).** Enter the network mask of the secondary interface. If you are using only one network interface connection to the Server Appliance, use the primary interface and leave the secondary interface empty. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- ◆ **MAC Address (Secondary Interface).** The MAC address is the hardware address of the network interface card. This hardware address is a unique identifier and cannot be changed after manufacture.

3. Click **Modify Static Routes**. The **Static Route List** table appears; see Figure 29.

If you have more than one router or gateway on a local area network (LAN), you need to configure the static routes so that TCP/IP traffic is delivered correctly.

Figure 29. Static Route List table



4. Click Add. The Add Static Route table appears; see Figure 30.

Figure 30. Add Static Route table

5. Configure the Add Static Routes table fields:

- ◆ Target Subnet. Enter the IP address of the subnet to be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.0 is a valid entry.
- ◆ Target Network Mask. Enter the network mask of the subnet to be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 255.255.255.0 is a valid entry.
- ◆ Gateway. Enter the IP address of the network gateway through which the target subnet's packets will be re-routed. Enter a series of four numbers between 0 and 255 separated by periods. For example, 192.168.1.1 is a valid entry.
- ◆ Network Interface. Select the network interface through which the target subnet's packets will be re-routed. If no device is specified, a device will be selected based on the IP address of the network gateway. Your choices are Primary Ethernet Interface and Secondary Ethernet Interface

6. Click Save.

You can use a TCP/IP alias to establish an additional network address for the same network interface. This can be useful in permitting a single physical interface to accept packets addressed to several different addresses such as when you are changing network numbers and you wish to accept packets addressed to the old interface. Another case is when you would like to have multiple addresses assigned to a single network interface.

1. Return to the main screen and click the Interface Aliases tab; see Figure 31.

Figure 31. Interface Aliases Tab



2. Click Add to display the Add Alias table; see Figure 32.

Figure 32. Add Aliases table

3. Configure the table as follows:
 - ◆ Interfaces. The interface field is changeable if there is more than one interface configured on the TCP/IP > Primary Settings page. For example, if the primary and secondary interface are set up, then on the Add Alias page you can select either interface.
 - ◆ IP Address. The IP address on which this alias should listen.
 - ◆ Netmask. The netmask for this alias.

IP Address Allocation IP address allocation provides a way to select from allowable IP addresses for the server.

This is a convenience feature for assigning IP addresses for sites on the machine and is also intended to help prevent incorrect assignments and potential conflicts or misuse.

Increasing numbers of supportable sites per server makes this scaling feature all the more important and useful.

The IP Address Allocation menu is used to specify an acceptable IP address range for the Ethernet ports for the server.

Later, when an IP address is assigned to a virtual site, it must fall within this range to be accepted (see Figure 67, Edit Virtual Site Template - Basic Settings tab). To specify the IP Address Allocation settings:

Select Server Management > System Settings > IP Address Allocation. The IP Address Allocation screen appears; see Figure 33.

Figure 33. IP Address Allocation screen

IP Address Allocation	
Enabled	<input checked="" type="checkbox"/>
<input type="button" value="Save"/>	
Acceptable Ranges	
<input type="button" value="Add"/>	2 Entries
Beginning of Range	End of Range

Make sure the Enabled checkbox is not checked. If you check it before you enter an acceptable IP

address range, the system will send you an error message.

Click Add in the Acceptable Ranges table to add an address range. The resulting screen is shown in Figure 34.

Figure 34. Acceptable Ranges screen

The screenshot shows a web interface for IP address management. At the top, there is a section titled "IP Address Allocation" with a "Save" button and a checked "Enabled" checkbox. Below this is a section titled "Acceptable Ranges" which contains a table with two columns: "Beginning of Range" and "End of Range". The table currently has no entries. To the right of the table, it says "3 Entries". At the bottom of the table, there are two input fields for the range, a "Save" button with a red trash can icon, and a "Cancel" button.

Enter the starting and ending IP address ranges in the table and click Save to save the changes made to the range.

Check the Enabled checkbox to enable IP Address Allocation. Only IP addresses within the ranges listed in the Acceptable Ranges table will be allowed for use by virtual sites.

Use the red trash can icon to delete an entry in the table.

Power

This menu is used to configure remote booting (Wake On LAN with Magic Packet) and power up options.

To specify the Power Options settings:

1. Select Server Management > System Settings > Power. The Power Options screen and its associated buttons appear; see Figure 38.

Figure 38. Power Options screen



2. Click Shutdown. This screen lists the steps for powering down
3. Click Reboot Now in the Power Options screen to reboot the Server Appliance. A confirmation dialog appears
4. 6. Once the Server Appliance reboots, the Server Management screen will be available again.

You can also reboot the OSPanel Server Appliance through the LCD console; refer to "Power menu"

Note: Rebooting the OSPanel Server Appliance sometimes cures problems with certain services. The Active Monitor software recommends when a reboot is necessary.

Time

This menu is used to configure the server time settings. To specify the Time settings:

1. Select Server Management > System Settings > Time. The Time Settings screen appears; see Figure 42.
2. Configure the Time Settings fields.
 - ◆ Date and Time. Set the current date and time.
 - ◆ Time Zone. Set the proper time zone.
 - ◆ NTP Server Address (optional).
3. Enter the network address or fully qualified domain name of a Network Time Protocol (NTP) server to which your system date and time will be periodically synchronized. You can find a list of other publicly available NTP servers at: <http://www.eecis.udel.edu/~mills/ntp/servers.htm>.
4. Information Click this menu item to display system information for the Server Appliance, such as serial numbers and MAC addresses.

Note: If you have manually entered time settings, the Server Appliance time is updated to those values as soon as you click Save. If you have entered an NTP server address only and no manual data and time settings, after you click Save, the time settings on the Server Appliance are synchronized to the NTP server at the next scheduled NTP server update.

Maintenance

The Maintenance section allows you to lock the server appliance UI for maintenance

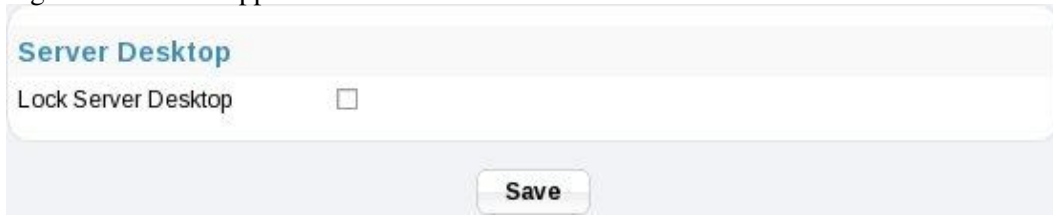
Server Appliance UI

A server administrator or third-party backup software may lock the Server Appliance UI during backup to prevent modification of server configuration parameters while they are being backed up.

To specify the Server Appliance UI settings:

1. Select Server Management > Maintenance > Server Appliance. The Server Appliance table appears; see Figure 43.

Figure 43. Server Appliance screen



2. Configure the Server Appliance settings.
 - ◆ Lock Server Appliance. This option gives the ability to make the administrative user interface (Server Appliance) read-only. Locking the Server Appliance during the backup and restore process will help guarantee that server configuration is properly saved and restored.
3. Click Save to save the settings.

Usage Information

The Usage Information section allows you to browse server and network service usage statistics. The following submenus are available:

Network

- Web
- FTP
- Email
- Disk

Network Usage Information

To configure Network usage information for display:

1. Select Server Management > Usage Information > Network. The Configure Network Reporting Options screen appears; see Figure 49.

Figure 49. Configure Network Reporting Options screen



2. Enter the start and end dates for network activity to be included in the report.
3. Click Generate Report.
4. Use the drop down box to display the data in various ways.
5. Click Generate New Report to return to the screen shown in Figure 49.
6. Click Download Log to download a log file of the network activity.

Configure Web Reporting Options

To configure Web usage information for display:

1. Select Server Management > Usage Information > Web. The Configure Web Reporting Options screen appears; see Figure 51.
2. Enter the start and end dates for Web activity to be included in the report.
3. Click Generate Report to display a summary of the Web activity.

Figure 51. Configure Web Reporting Options screen



Configure Web Reporting Options

Starting From February 12 2009

Ending On February 12 2009

Generate Report **Back**

Configure FTP Reporting Options

To configure FTP usage information for display:

1. Select Server Management > Usage Information > FTP. The Configure FTP Reporting Options screen appears; see Figure 52.
2. Enter the start and end dates for FTP activity to be included in the report.
3. Click Generate Report to display a summary of the FTP activity.

Figure 52. Configure FTP Reporting Options screen



Configure FTP Reporting Options

Starting From February 12 2009

Ending On February 12 2009

Generate Report

Configure Email Reporting Options

To configure email usage information for display:

1. Select Server Management > Usage Information > Email.

The Configure Email Reporting Options screen appears; see Figure 53.

2. Enter the start and end dates for email activity to be included in the report.
3. Click Generate Report to display a summary of the email activity.

Figure 53. Configure Email Reporting Options screen

Configure Email Reporting Options

Starting From: February 12 2009

Ending On: February 12 2009

Generate Report

Configure Disk Usage Reporting Options

To display the statistics for disk usage on a virtual site, follow these steps:

1. Select Server Management > Usage Information > Disk. The Disk Usage screen appears; see Figure 54.

Figure 54. Disk Usage screen

Disk Usage

Summary | Sites | All Users | Notification Settings

4 Entries

Partition	Disk Usage (MB)	Total Size (MB)	Percentage Used
/	1476.57	1883.77	78%
/home	24156.92	68501.38	35%
/tmp	45.54	1883.77	2%
/var	735.17	1883.77	39%

2. Click the Summary tab.

The Disk Usage table displays the disk usage by partition name; see Figure 54.

3. Click the Sites tab.

The Disk Usage table displays the disk usage by site host name; see Figure 55.

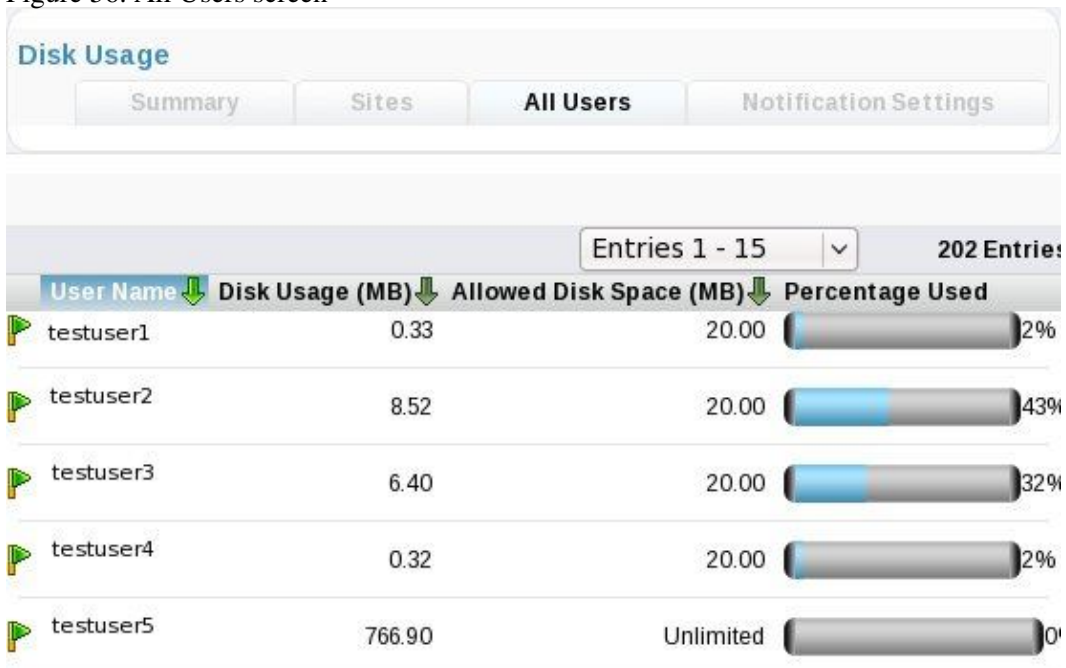
Figure 55. Disk Usage screen



4. Click the All Users tab.

The Disk Usage table displays the disk usage by user; see Figure 56.

Figure 56. All Users screen



5. Click the Notification Settings tab.

The Disk Usage table lists the types of notifications to be sent when the user or the site exceed the allocated disk space; see Figure 57.

Figure 57. Notifications Settings screen

Note: Refer to [Active Monitor](#) for information on how to set up an email address for alert notification.

Active Monitor

The OSPanel Server Appliance uses Active Monitor software, a utility that runs on a Server Appliance and updates key system and service status every 15 minutes. This section describes how to use the Active Monitor.

Active Monitor icon

The Active Monitor icon in the top right corner of the user interface allows you to view status information. The icon turns red if any of the components monitored by Active Monitor have severe problems. The amber System Fault LED on the front panel is illuminated for any hardware failure detected by Active Monitor.

The Active Monitor section allows you to check for correct operation of system components.

The following submenus are available:

- Status menu selection. Brings up the Overview screen (System Status, Service Status and Other Status)
- Settings menu selection. Brings up the Active Monitor Settings screen

This menu item displays the Check Status Now button and three screens. A colored dot at the left of each item indicates its status.

1. To view detailed status information for a particular system component or service, click the colored circle to the left of the item's name in the table or click the magnifying glass in the Action column that corresponds to the name of the item. See Figure 58.

Figure 58 System Status Overview

















System Status - Overview		7 Entries
Component Name		Action
 CPU Usage		
 Disk Integrity		
 Disk Usage		
 Fans		
 Memory Usage		
 Network Status		
 Temperature		

Note: System software events are triggered in the event of serious system conditions that may damage the Server Appliance (for example critical overtemperature or overvoltage). See [System health monitoring](#) for more details.





The status of each of the above items is indicated by a green, yellow, red or grey circle beside each item. The colors have the following significance:

- ◆ Grey. No information is available or monitoring is not enabled
 - ◆ Green. Normal functioning
 - ◆ Yellow. A problem exists that should be investigated by the Administrator (for example, low disk space)
 - ◆ Red. A severe problem exists that needs immediate attention by the Administrator.
2. Click the Check Status Now button to retrieve the current status of the server.
 3. View the System Status - Overview screen. This screen displays server hardware and environmental status; see Figure 58.
 4. View the Service Status - Overview screen. This screen displays status of the various servers (DNS, FTP, Email, Telnet, Web and SNMP), status of pages (ASP and JSP), Buffer Overflow Protection, Scan Detection and Server Appliance; see Figure 59.

Figure 59 Service Status Overview

Service Status - Overview		8 Entries
Component Name		Action
 Domain Name Service (DNS) Server		
 Email Servers		
 File Transfer Protocol (FTP) Server		
 MySQL Server		
 Server Desktop		
 Simple Network Management Protocol (SNMP) Server		
 Telnet Server		
 Web Server		

Key:

-  No Information Available or Monitoring Not Enabled
-  Normal
-  Problem
-  Severe Problem

Note: When a condition that results in the activation of a red or yellow indicator is corrected, the indicator will not change color until Active Monitor is run manually or automatically (every 15 minutes).

Thus, after a defective fan is replaced, for example, both the Active Monitor status indicator and the amber System Fault LED remain active until Active Monitor runs.

Note: Clicking this button immediately begins the process of updating system and service status information. This may take as long as several minutes and will proceed in the background.

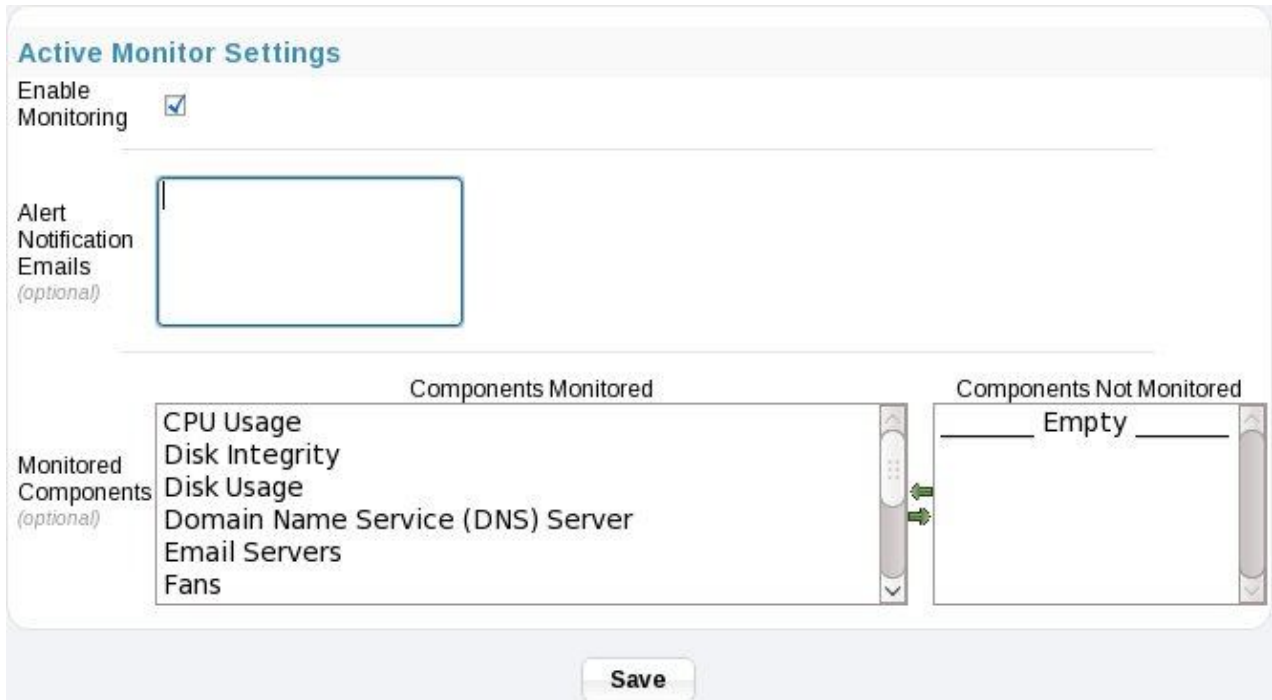
Note: Clicking the magnifying glass icon for a status item displays more details and, in some cases (fan and DIMM status, for example), provides graphical illustrations to help identify, locate and correct a fault condition.

Active Status Overview screen

This menu item allows you to configure Active Monitor Settings. To configure Active Monitor settings:

1. Select Server Management > Active Monitor > Settings. The Active Monitor Settings screen appears; see Figure 61.

Figure 61. Active Monitor Settings screen



2. Configure the Active Monitor Settings fields:

- ◆ **Enable Monitoring.** Turn Active Monitor on or off. Enabling this functionality allows specific system components to be regularly checked for proper operation. These system components can be selected in the other portion of the screen.
- ◆ **Alert Notification Emails (optional).** Enter the list of email addresses to which Active Monitor will send alert messages.
Each email address must be on an individual line, separated by a carriage return.
- ◆ **Monitored Components (optional).** Select the specific system components to be regularly checked by Active Monitor. The left column shows the system components that are currently being monitored. The right column shows the system components which could possibly be monitored. To add a system component to be monitored, select the component and use the left arrow to move the system component from the right column to the left column.



Chapter 5

Site Management

This section describes the features available to a Server Administrator and a Site Administrator on the OSPanel Server Appliance.

A Site Administrator is allowed to do the following:

- Setup and manage users
- Import and export users
- Create and manage mailing lists
- Use Web deployment
- Manage SSL (for this vsite)
- Generate usage reports

A Server Administrator is allowed to do all of the Site Administrator functions as well as the following:

- Search for virtual sites by host name or IP address
- Edit the virtual site template
- Add virtual sites

A Site Administrator, can access all of the features described for the site user in [Chapter 7 - Personal Profile](#).

The Server Administrator designates the Site Administrator for each site. The Site Administrator has control only over this virtual site (unless he or she is also the Server Administrator).

The Site Administrator can also designate other site users as a Site Administrator.

Note: If desired, all of the virtual sites may be removed and the Server Appliance may be used as a dedicated DNS server or email server.

Note: If the Site Administrator for a virtual site is also the Server Administrator, he or she has access to all of the server administration functions as well by logging in as the user admin.

Administrator privileges

A Site Administrator, can manage a virtual site using any standard Web browser. To access the Site Management () screen for your site, type the URL `http://login/` into your browser. The browser-based user interface (UI), known as the Server Appliance, prompts you for a user name and password. You can log in as a regular user or as a Site or Server Administrator.

Once you have responded to the prompts, if you are an authorized Site Administrator, the Site Management () screen appears.

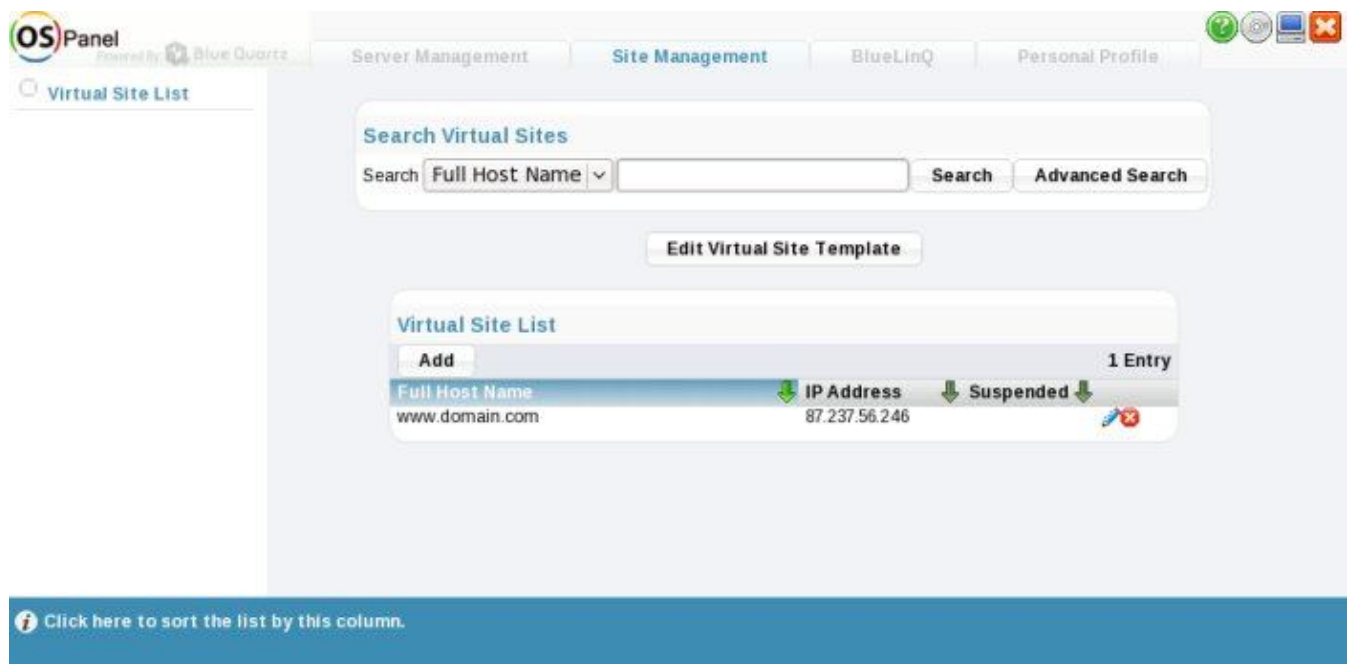
Note: The Site Management screen can only be accessed using the fully qualified domain name for the virtual site in the Web browser. The Site Management screen is not accessible if an incomplete or aliased site name is specified.

You cannot access the Site Management screen for a name-based virtual site by the URL <http://siteadmin/> unless a DNS record has been properly set up to point to your server. However, the Server Administrator can always access the Site Management screen for a virtual site through the Server Management screen.

Site Management screen (for Server Administrator)

When you log in as a Server Administrator and go to Site Management, the Site Management screen appears with the Virtual Site List menu item highlighted, as shown in Figure 62.

Figure 62. Site Management screen for Server Administrator



As shown above, a Server Administrator can search for virtual sites, edit the virtual site template, or add virtual sites. Only a Server Administrator can perform these functions. After performing these functions, the Server Administrator can click the green pencil icon on the Virtual Site List to bring up the screen shown in Figure 71. This screen shown in Figure 71 is the one that either a Site Administrator or a Server Administrator can use to manage virtual site users.

There are three main areas on the Site Management main screen (see Figure 62) that are available to Server Administrators:

- Search Virtual Sites dialog box
- Virtual Site List dialog box
- Edit Virtual Site Template button

Search Virtual Sites

The Search Virtual Sites dialog box, shown in Figure 63, allows you to search for virtual sites that match the properties entered in the dialog box.

These functions are useful if you have a large number of virtual sites on your Server Appliance and you want to restrict the display to certain virtual sites.

You can search the list of virtual sites according to the following criteria:

- by host name (whether the host name is equal to, is contained in or is not contained in the search string)
- by IP address (whether the IP address is equal to, is within or is not within a specified subnet)
- by a specific service enabled on a site

Figure 63. Search Virtual Sites screen

The screenshot shows a dialog box titled "Search Virtual Sites". On the left, there is a label "Search" followed by a dropdown menu showing "Full Host Name" with a downward arrow. To the right of the dropdown is a text input field. Further right are two buttons: "Search" and "Advanced Search".

1. Configure the settings shown in the screen:
 - ◆ Search. The Search drop down box allows you to choose the site property on which to search (full host name or IP address). Sites with names or IP addresses that contain the text entered in the field to the right of the drop down box for the chosen property will be listed when you click Search.
 - ◆ Advanced Search. An advanced search allows you to perform a more refined search on site properties. When you click Advanced Search, the dialog box shown in Figure 64 appears. Choose the search criteria that you desire to make your search more refined.
2. Click Search to begin the search.

Figure 64. Advanced Search screen Virtual Site List

The Virtual Site List dialog box, shown in Figure 65, displays the existing virtual sites and allows you to add or delete them.

Figure 65. Virtual Site List screen

Full Host Name	IP Address	Suspended
www.domain.com	87.237.56.246	

Site Management screen (for Server Administrator)

The settings shown in the screen are:

- Full Host Name.
The Full Host Name is the complete name of the site and is also known as the fully qualified domain name.
This is a combination of the host name and the domain name.
- IP Address. This is the IP address of the site.
- Suspended. This indicates if the site is suspended. If a site is suspended, access for users of the site as well as the Web and FTP site associated with it will be disabled.
Click the green pencil icon to modify an item in the Virtual Site List (see "Managing Virtual Sites")

for more details) or the red trash can icon to delete an item in the list.

- Click Add to add a new item to the Virtual Site List. The screen shown in Figure 66 appears.

Figure 66. Add a new virtual site.

Add New Virtual Site

IP Address
Valid Ranges: 87.237.56.253 - 87.237.56.253
92.63.134.161 - 92.63.134.178

Host and Domain Name .
Host Name Domain Name

Web Server Aliases
(optional)

Disable Email for Domain

Email Server Aliases
(optional)

Catch-All Email Address
(optional)

Maximum Allowed Disk Space (MB) (1 - 68,501)

Maximum Allowed Number of Users

Automatic DNS Configuration

Preview Site Configuration

Services and Features

Enable

Anonymous FTP Enable
Maximum Allowed Upload Disk Space (MB)
Maximum Simultaneous Connections

Enable PHP Scripting

Enable Common Gateway Interface (CGI)

Enable Server-Side Includes (SSI)

Enable

webmaster Password
 (Enter Again)

Site Management screen (for Server Administrator)

Fill in this dialog box as needed to create a new virtual site.

Note: Automatic DNS configuration manages DNS records for this site. Web and Email server aliases are supported only if they share the site domain name. This service does not register the domain name with a top-level registrar.

Editing the virtual site template

There are many advantages for setting defaults for the virtual sites.

For example, since multiple sites can share an IP address, a default IP address can be set for all new virtual sites added. Also, since it is common for many sites to share a common domain name, it can be desirable to set a default domain name for your virtual sites.

The same is true for all of the options for a virtual site; it is best for you to decide the needs of your typical virtual site before assigning these values.

Site defaults and site settings can only be configured by the Server Administrator.

If you (as the Server Administrator) enable FrontPage Server Extensions service Shell Accounts service, or APOP service, the Site Administrators can enable or disable FrontPage user webs, enable or disable individual (per-user) shell access, or APOP per user.

Follow these steps to edit the virtual site template:

1. Click the Edit Virtual Site Template button to edit the settings that are automatically filled in when adding a virtual site.

When you click this button, the Virtual Site Template table appears, see Figure 67.

Figure 67. Edit Virtual Site Template--Basic Settings tab

Virtual Site Template

Basic Settings | Services and Features | Web | Anonymous FTP

IP Address

Domain Name

Maximum Allowed Disk Space (MB)

Maximum Allowed Number of Users

Disable Email for Domain

Catch-All Email Address

Automatic DNS Configuration

Preview Site Configuration

Save **Cancel**

2. Use the Basic Settings tab to configure the default network, user and disk limits, and email settings for new virtual sites.
 - ◆ **IP Address.**
The default IP address that will be filled in when adding a site. To use the Server Appliance, you require an IP address or range of IP addresses.
 - ◆ **Domain Name.** The default domain to which new sites will belong.
Each virtual site also requires a domain name (for example, efg.com or xyz.com). You must register the domain name. Visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org>. for a list of accredited domain-name registrars.
 - ◆ **Maximum Allowed Disk Space.**
The maximum disk space on the Server Appliance in megabytes (MB) available to a site for files.
 - ◆ **Maximum Allowed Number of Users.**
The maximum number of user accounts that a site can have.
 - ◆ **Catch-All Email Address.**
Specify an email address to receive messages that are addressed to unknown users and mailing lists.
If left blank, email addressed to unknown users or mailing lists will not be accepted.
If the specified address does not exist, mail to unknown users and mailing lists may be rejected just as if no address was specified.
Note: The OSPanel Server Appliance supports name-based virtual sites, allowing many sites to share a single IP address. You can create many virtual sites using the same IP address (for example, 192.168.25.77) as long as the fully qualified domain name for each site is different (for example, both www.efg.com and www.xyz.com can use 192.168.25.77 as their IP

address).

Note: The OSPanel Server Appliance can serve as the DNS server and provide the host name.

◆ Automatic DNS Configuration

Automatic DNS configuration manages DNS records for this site.

Web and Email server aliases are supported only if they share the site domain name.

This service does not register the domain name with a top level registrar.

You can have the Server Appliance automatically create DNS records for this virtual site.

If enabled, the Server Appliance acts as the primary DNS server for this site.

The default setting for this feature is OFF.

If the Web server aliases or email server aliases have the same domain name as this site, DNS records are created for these aliases as well.

3. Use the Services and Features tab to enable or disable various services. See Figure 68.

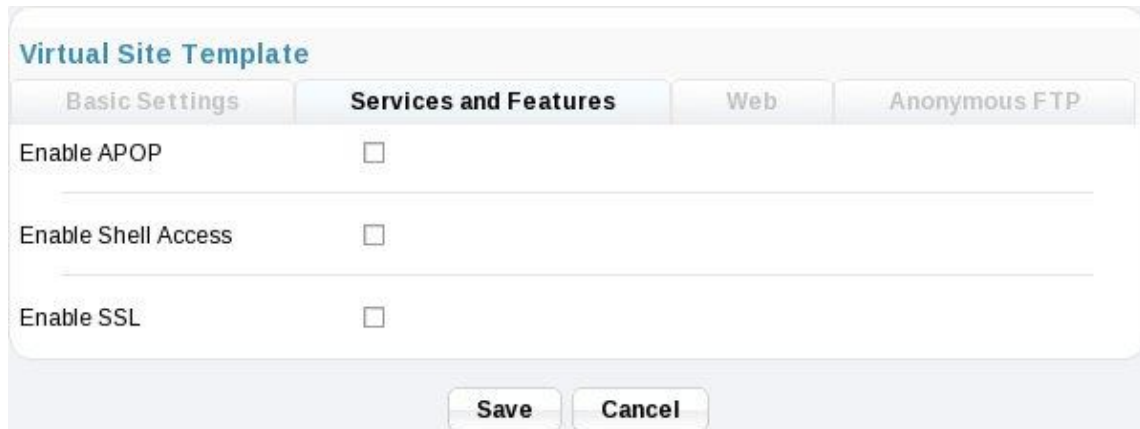
◆ Enable APOP. Enable authenticated POP (APOP). See [Email](#) for more detailed information.

◆ Enable SSL. Enable SSL to allow secure access to the Web server for the site. See [SSL](#) for more detailed information.

◆ Enable Shell Access. Enable shell access to allow the creation of users who can connect to the server using services such as telnet and ssh.

See [Shell](#) for more detailed information.

Figure 68. Edit Virtual Site Template--Services and Features tab



Note: This feature does not register the new site name with a top-level domain name registrar. You must register the new site name.

Visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org> for a list of accredited domain-name registrars.

Note: If any of these are enabled for a site, they may be enabled or disabled on a per user basis.

4. 4. Use the Web tab to configure Web options, such as scripting languages. See Figure 69.

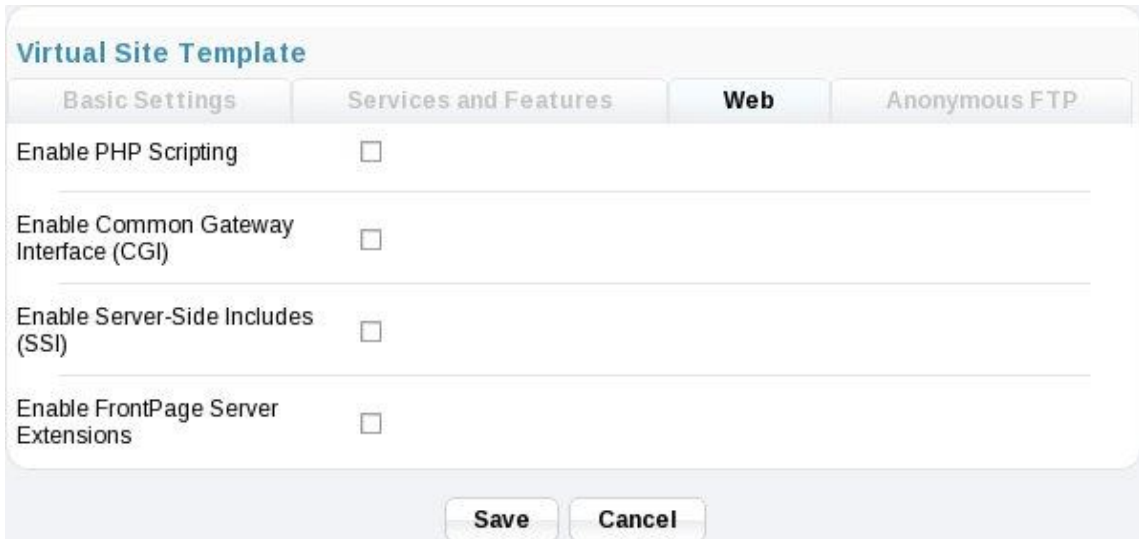
The following items are explained more fully in the [Web Section](#).

◆ Enable PHP Scripting. Enable the use of PHP scripts.

◆ Enable Common Gateway Interface (CGI). Enable the use of CGI applications.

◆ Enable Server-Side Includes. Enable the use of Server-Side Includes.

Figure 69. Edit Virtual Site Template Web tab

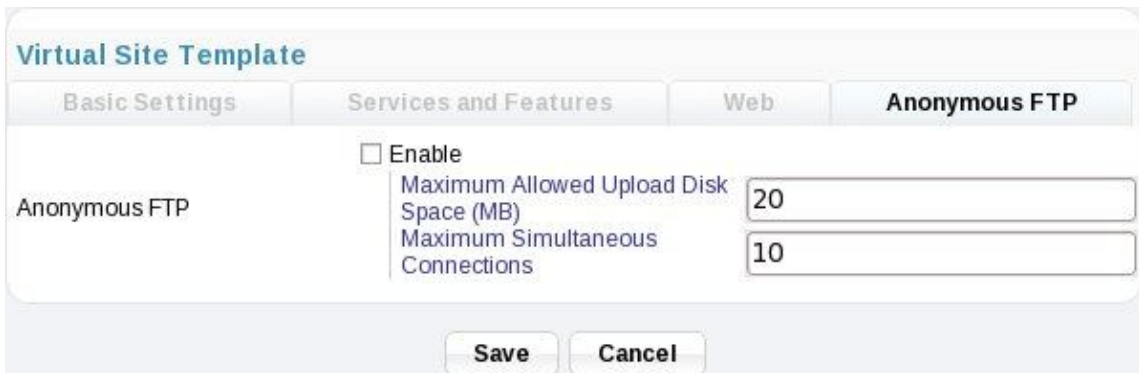


Use the Anonymous FTP tab to modify settings for anonymous FTP.

Anonymous FTP is explained more fully in the section titled "Anonymous FTP"

- ◆ Activate the Enable checkbox to enable anonymous FTP for the site.
- ◆ Maximum Allowed Upload Disk Space. Enter the limit in megabytes (MB) for anonymous FTP uploads.
- ◆ Maximum Simultaneous Connections. Enter the maximum number of anonymous FTP users that can be connected to the server at one time.

Figure 70. Edit Virtual Site Template--Anonymous FTP tab

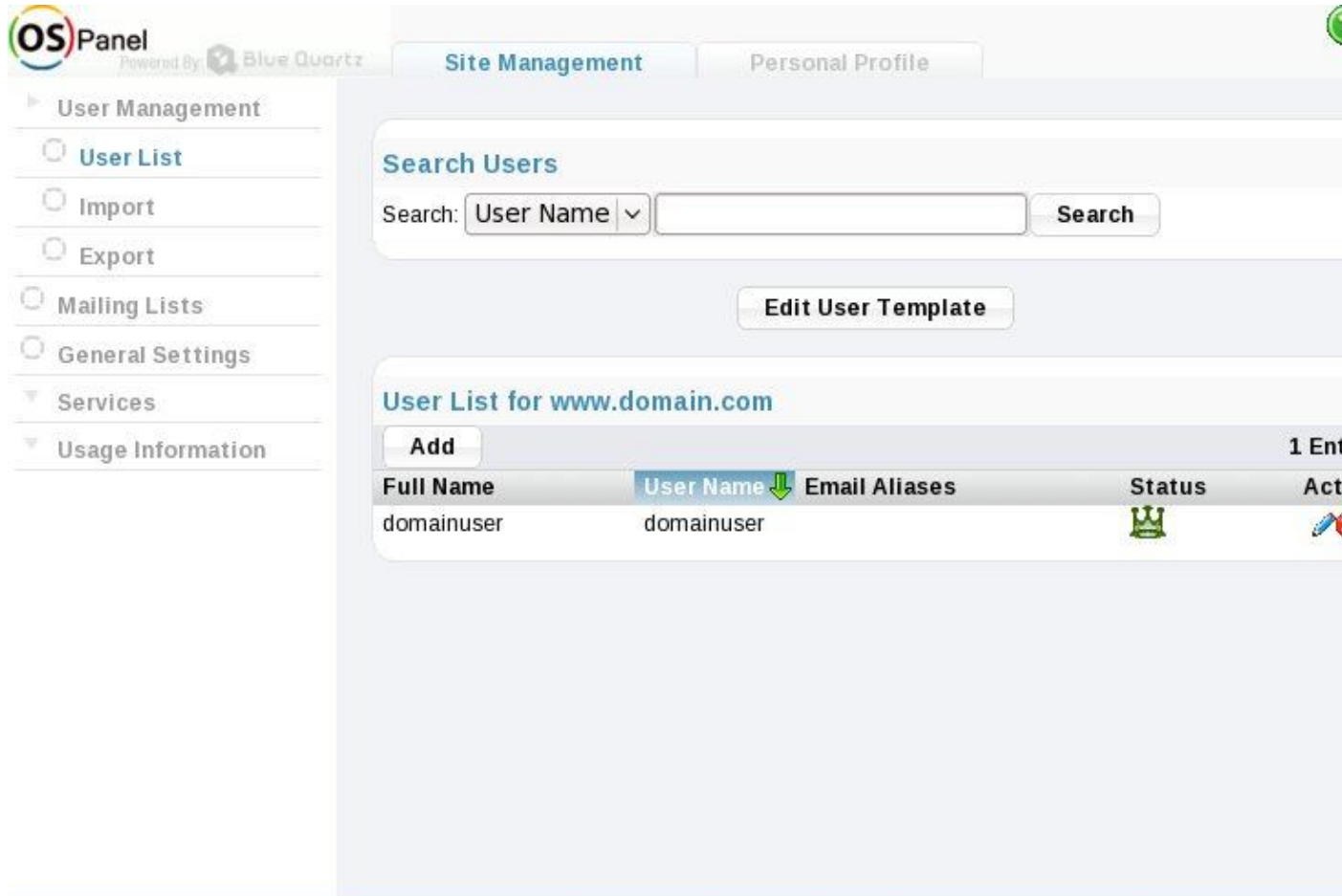


5. Click Save.

The information now appears filled in on the Add Virtual Site screen each time you click Add to add a new item to the Virtual Site List.

When you log in as a Site Administrator and go to Site Management, the Site Management screen appears as shown in Figure 71. Notice that the screen shown in Figure 62, which is restricted to Server Administrators, is not available to the Site Administrator.

Figure 71. Site Management screen for Site Administrator

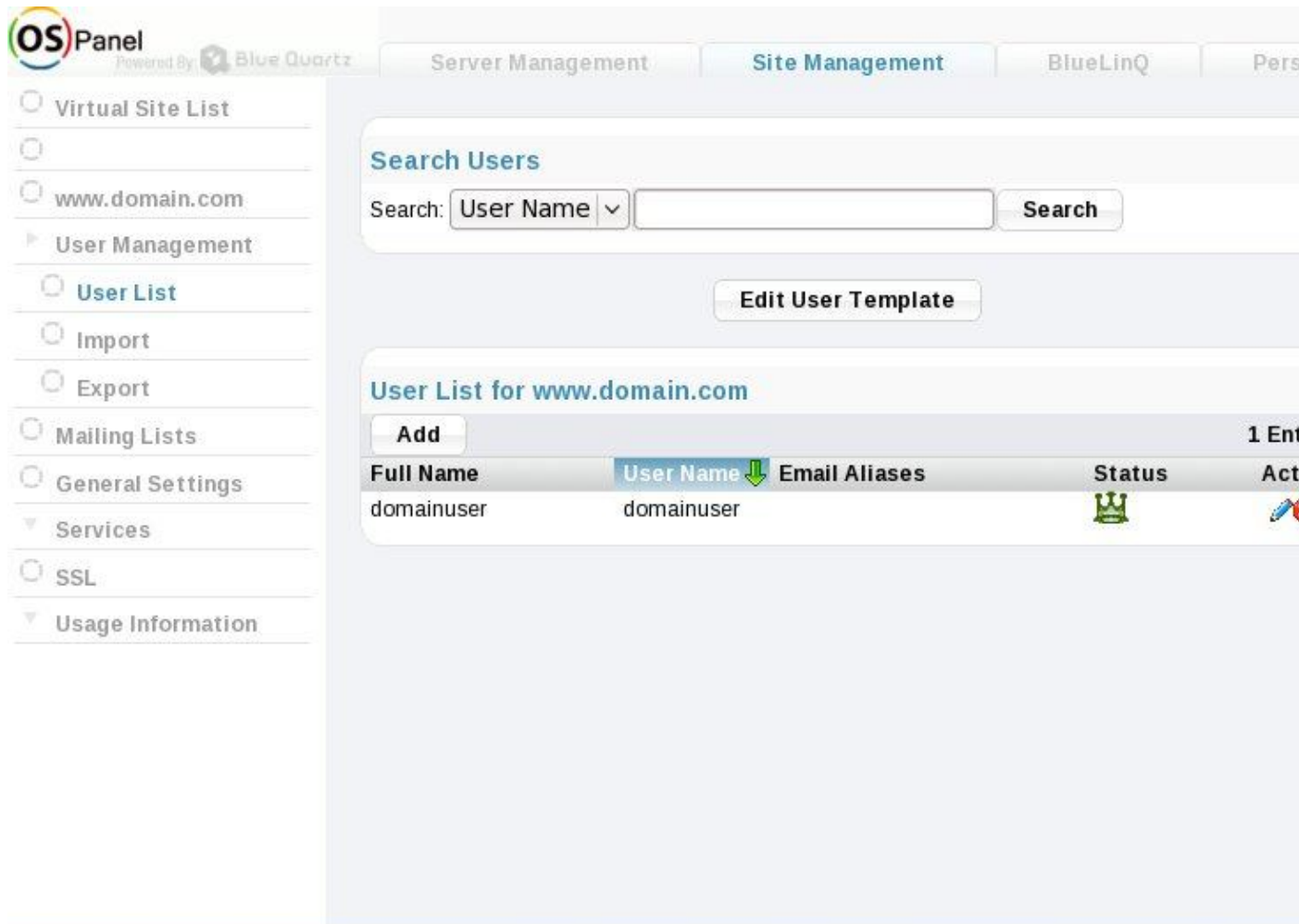


As shown above, a Site Administrator (and Server Administrator) has access to all the menu items shown at the left of the screen. However, in the User List menu (which is active in the screen), the Site Administrator can only search for users, edit the user template and add users. A Site Administrator cannot search for virtual sites, edit the virtual site template, or add virtual sites. Only a Server Administrator can perform these functions.

Managing Virtual Sites

When you click the crayon icon in the Virtual Site List screen as a Server Administrator (see [Figure 65](#), "[Virtual Site List screen](#)"), or when you come to Site Management as a Site Administrator, the screen shown in [Figure 72](#) appears, which allows you to modify the virtual site selected.

Figure 72. Virtual Site Management screen (for Server Administrator)



i This is the complete name of the site and is also known as the fully-qualified domain name. The full host name is sorted by domain and then by host name.

Note: The Virtual Site Modification screen for Site Administrators has only two tabs at the top: Site Management and Personal Profile. The other two tabs (Server Management and BlueLinQ) are available only to Server Administrators.

The following bullet items represent the fully expanded menu items on the left side of the Virtual Site Modification screen. These are the functions and services that the Administrator can manage. They are explained in this section.

- User Management
- User List
- Import
- Export
- Mailing Lists
- General Settings
- Services
- Web

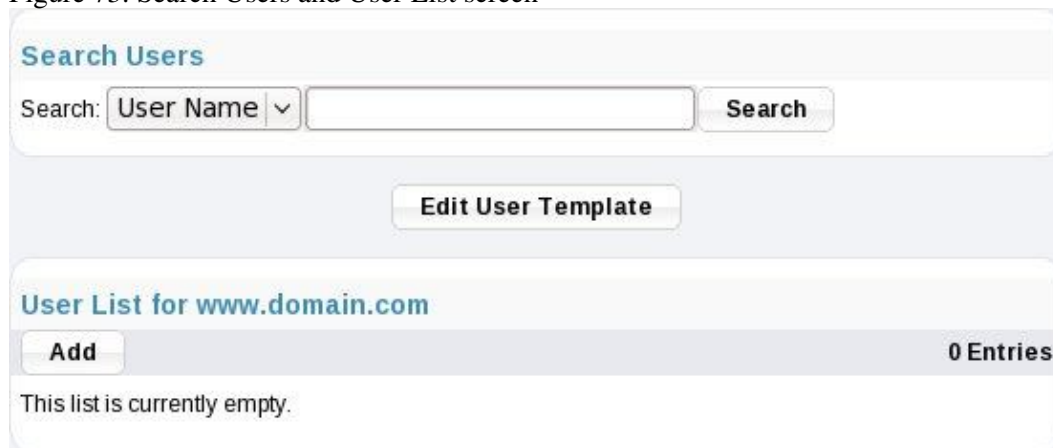
- Anonymous FTP (only available to Server Administrator)
- Email
- Shell only available to Server Administrator)
- Web Deployment
- SSL (only available to Server Administrator)
- Usage Information
- Web
- FTP
- Email
- Disk
- Settings

User Management

The User Management menu item is used to add, modify, or remove users.

User List Selecting the User List menu item brings up the Search Users and User List screens; see Figure 73.

Figure 73. Search Users and User List screen



The screenshot shows a web interface for user management. At the top, there's a section titled "Search Users" with a search form. The form includes a dropdown menu currently set to "User Name", an empty text input field, and a "Search" button. Below the search form is a button labeled "Edit User Template". The main content area is titled "User List for www.domain.com" and contains an "Add" button on the left and "0 Entries" on the right. Below the table area, a message states "This list is currently empty."

1. Configure the settings in the Search Users table:
 - ◆ Search. You can use the search tool to find users based on the criteria you specify using the dropdown box. Select the field on which to search and choose how the text you enter should be compared against the field.
2. In the User List table, click Add to add a new user. The Add New User screen appears; see Figure 74.

Figure 74. Add New User screen

Add New User to www.domain.com

Full Name

User Name

Password
 (Enter Again)

Maximum Allowed Disk Space (1 - 500)

Site Administrator

DNS Administrator

Disable User's Email

Email Aliases (optional)

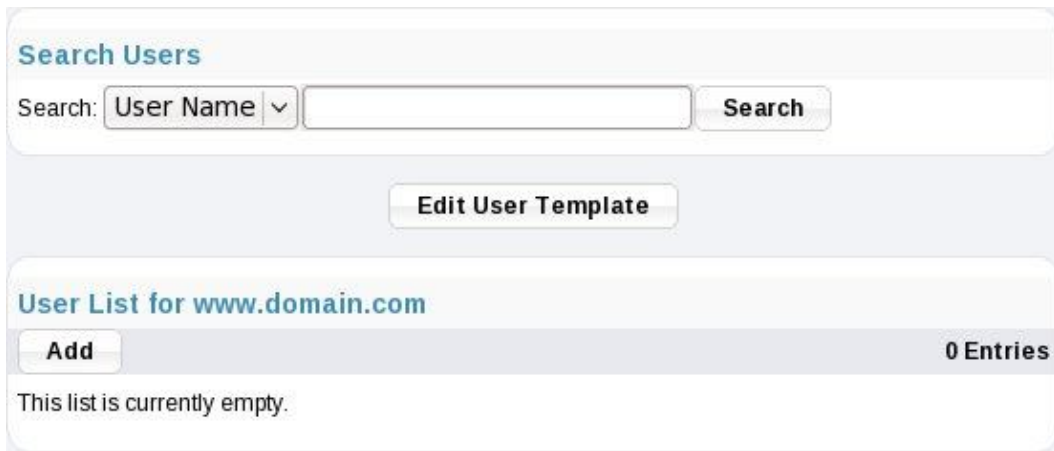
Remarks (optional)

3. Configure the settings on the Add New User table:

- ◆ Full Name. Enter the full name of the user. Please enter any characters except colons. For example, John Doe is a valid entry.
- ◆ User Name. Enter the name to be used by the system to identify the user. Please enter no more than 12 characters containing only lowercase alphanumeric characters, periods, hyphens and underscores. The first character must be a letter. For example, john.doe is a valid entry
- ◆ Password. Enter the password to be used by the system to identify this user. The password should be between 3 and 16 characters long. A good password should contain at least 5 characters with a mix of uppercase and lowercase letters as well as numbers and punctuation. It should not spell out any words found in the dictionary. Passwords are case sensitive.
- ◆ Maximum Allowed Disk Space. Set the disk quota of this user. This is the maximum disk space available to this user for the storage of Web pages, email messages and all other user files. The quota can not be smaller than 1 MB. The default value for new users is set in the User Template. For site level accounts, you cannot leave the Maximum Allowed Disk Space (MB) field blank. You must enter a number in this field.

- ◆ Site Administrator. Site administrators are users who are capable of configuring settings for a site, adding and removing users, and so on.
 - ◆ Email Aliases (optional). Enter additional names under which the user will receive email. Enter characters containing only lowercase alphanumeric characters, periods, hyphens and underscores. The default value is the lowercase first and last name of the user separated by a period. For example, john.doe is a valid entry.
 - ◆ Remarks (optional). Enter additional information or comments about the user here.
4. 4. Click Save to save the settings. After a user has been added, the new user is listed in the User List screen (see Figure 75).

Figure 75. User List screen



Use the green pencil icon to modify the user settings or the red trash can icon to delete the user.

When you click the green pencil icon to modify user settings, the Modify User Settings screen appears (see Figure 76).

Figure 76. Modify User screen

Modify User Settings for mick

Account | Email | Spamassassin

Full Name:

New Password (optional): (Enter Again)

Maximum Allowed Disk Space: (1 - 500)

Site Administrator:

DNS Administrator:

Suspended:

Remarks (optional):

Save Cancel

Configure the settings in the Modify User Settings screen (Account tab).

- ◆ Full Name. Enter the full name of the user. Please enter any characters except colons. For example, John Doe is a valid entry.
 - ◆ New Password. Enter the password to be used by the system to identify this user. The password should be between 3 and 16 characters long. A good password should contain at least 5 characters with a mix of uppercase and lowercase letters as well as numbers and punctuation. It should not spell out any words found in the dictionary. Passwords are case sensitive.
 - ◆ Maximum Allowed Disk Space. Set the disk quota of this user. This is the maximum disk space available to this user for the storage of Web pages, email messages and all other user files. The quota can not be smaller than 1 MB. The default value for new users is set in the User Template. For site-level accounts, you cannot leave the Maximum Allowed Disk Space (MB) field blank. You must enter a number in this field.
 - ◆ Site Administrator. Site administrators are users who are capable of configuring settings for a site, adding and removing users, and so on.
 - ◆ Suspended. Suspending a user will prevent that user from accessing system services associated with that account such as telnet, FTP, mail and Web access to their files. Email sent to this account will be rejected and the sender will receive an error message.
 - ◆ Remarks (optional). Enter additional information or comments about the user here.
5. Configure the settings in the Modify User Settings screen (Email tab).
- ◆ Email Aliases (optional). Enter additional names that the user will receive email as. Please enter characters containing only lowercase alphanumeric characters, periods, hyphens and

underscores. The default value is the lowercase first and last name of the user separated by a period. For example, john.doe is a valid entry.

- ◆ **Email Forwarding.** Enabling email forwarding causes email received in the future to be automatically forwarded to the email addresses specified.

In the Email Addresses area, enter the email addresses to which you would like your email forwarded. The values entered must be valid email addresses such as user@example.com. To specify multiple addresses, separate the addresses with a comma, or put each address on a separate line.

- ◆ **Save Copy.** Checking Save Copy saves a copy of every email received to the mailbox in addition to forwarding a copy to the email addresses specified.
- ◆ **Vacation Message.** Vacation Message allows you to automatically send a custom message to everyone who sends you email. This is useful if you are unable to read your email, or want to send an automatic response message to the sender.
- ◆ **Auto Reply.** Enter the message that will be sent automatically as a reply to the sender of every email you receive. 3. Click the Edit User Template button (see Figure 73) to configure default settings to use when adding other new users.

Importing and exporting site users The purpose of importing and exporting users is to provide an easy way to migrate users from one virtual site to another or from one Server Appliance to another.

A Site Administrator can import a list of users to a virtual site by uploading a specially formatted text file containing the names of the users and their settings. The list of users can also be exported on the virtual site to a text file that is compatible with the import function.

These two functions allow you to rapidly create and maintain accounts for large numbers of site users.

Note: The following features, if enabled for the site, can also be enabled or disabled on a per user basis:

- ◆ FrontPage Server Extensions (see [Web](#))
- ◆ APOP (see [Email](#))
- ◆ Shell Access (see [Shell](#))

Creating a TSV text file

The first step in importing a list of users is to generate a text file in the required format. The file format used is called tab-separated-value (TSV) format and contains a separate line for each user you want to add. Each line contains the parameters for the user; a tab character separates each parameter.

The parameter order is the following: To specify multiple email aliases for a user, separate each alias with a space character.

Other parameters for a site user, such as the user's maximum allowed disk space and site administrator privileges cannot be specified in the file for individual users. However, the settings specified in the User Templates page are applied to each user imported. Thus, for example, if you wanted all the users in your text file to have FrontPage enabled, you could configure FrontPage "enabled" by default in the User Templates table.

An example file with two users might look like this: dwestDoug West4ng3lf1r3doug douggie dw
tdurdenTyler Durdens04ptyler td fighter

Note: The Server Administrator must enable a particular service for the virtual site before the Site Administrator can enable that service for a site user.

Note: The indicator represents the tab key on your keyboard.

Importing Users

Selecting the Import menu item brings up the Import User List screen; see Figure 77.

Figure 77. Import User List screen



1. Configure the settings on the Import User List screen:

- ◆ Source File. Enter the location from which to obtain the TSV (Tab Separated Value) format file containing a list of users to be uploaded to the system. Enter a URL beginning with either http:// or ftp:// to download the file from a location on the internet, or enter the full path to a file to upload. Click Browse to choose a file on your local hard drive.
- ◆ Click Import Now. The server prompts you with a confirmation dialog.

If you agree to continue, the server returns a status screen showing you how many lines of the text file have been processed and how many of the users have been successfully added (and not added).

After all the lines in the file have been processed, if errors were encountered, the system displays a summary report. The summary report explains why a particular line failed to add a user.

If no errors were encountered, the system returns you to the "User List" table, displaying the newly added users.

Exporting Users

You can export the list of users on the virtual site to a text file that is compatible with the Import feature described above. The file is downloaded to your local machine.

Passwords for users are stored in an encrypted format that does not allow for the recovery of the actual password. Therefore, you have two options for the creating a temporary password for each exported user.

Click Export to export users from the server. The export function returns a TSV (Tab Separated Value) format file that is compatible with the user import function.

Selecting the Export menu item brings up the Export User List screen; see Figure 78.

Figure 78. Export User List screen



1. Configure the settings on the Export User List screen:
 - ◆ Password Format. Due to the encryption algorithm used to store user passwords, the user's actual password cannot be exported. If you choose to use User Names, users will be able to use their login name as their password. Choosing Random Strings prevents other users from being able to easily guess another user's password.
 - ◆ Click Export Now. The server sends the text file to your local machine.

Mailing Lists

This menu item is used to manage mailing lists. A mailing list allows a discussion by email between a group of people; the email addresses of the people in the group make up the list.

The mailing list is given a name, for example new_project. The mailing list can include users on the OSPanel Server Appliance as well as external users.

A message addressed to the name of the mailing list is delivered to each person on the list.

When replying to a mailing-list message, you can reply either to the original sender only or to the entire mailing list. This function depends on the email client that you are using.

Selecting the Mailing List menu item brings up the Mailing Lists screen; see Figure 79.

Figure 79. Mailing Lists screen



1. Click Add to add a mailing list; see Figure 80.

Use the Basic, Subscribers and Advanced tabs to configure the mailing lists.

Figure 80. Add Mailing Lists screen (Basic tab)

Add Mailing List to www.domain.com

Basic Subscribers Advanced

List Name

Remarks

Save Cancel

2. Click the Basic tab and configure the settings:
 - ◆ List Name. Enter the name of the mailing list. Please enter only lowercase alphanumeric characters, hyphens and underscores. For example, sales is a valid entry.
 - ◆ Remarks. Enter additional information or comments about the mailing list here.
3. Click the Subscribers tab.

The dialog box shown in Figure 81 appears.

Add Mailing List to www.domain.com

Basic **Subscribers** Advanced

Local Subscribers 0 Local Subscribers Edit

Remote Subscribers

Save Cancel

Figure 81. Add Mailing Lists screen (Subscriber tab)

4. Configure the settings:
 - ◆ Local Subscribers. Click the Edit button to select the local users that are subscribers to this mailing list. The dialog boxes shown in Figure 82 appear. They allow you to search for and add users to the mailing list.
 - ◆ Remote Subscribers. Enter the remote users (Figure 81) that are subscribers to this mailing list. Remote users are users who do not have accounts on this Server Appliance. Please enter a properly formatted email address. For example, user@example.com is a valid entry.

Figure 82. Search and Add Users to Mailing List

Search User List

Search

All Users on www.domain.com

1 Entry

	User Name	
<input type="checkbox"/>	mick2	

5. Click the Advanced tab and configure the settings:

The dialog box shown in Figure 83 appears.

Figure 83. Mailing List Advanced Tab

Add Mailing List to www.domain.com

Owner/Moderator

Password

Policies

Posting Policy

Subscription Policy

Maximum Message Length

Reply Policy

- ◆ Owner/Moderator. Enter the email address of the user performing all administrative duties (for example, approving subscriptions or moderating messages) for the mailing list. Please enter a properly formatted email address or the user name of a valid user on this Server

Appliance. The default value is admin. For example, user@example.com and admin are valid entries.

- ◆ Password. Enter an administrative password for this mailing list. This password is used when performing certain list administration tasks via email. If you do not plan on using these features, you may leave this field blank.
- ◆ Posting Policy. Select a posting policy for this mailing list.
- ◆ Only Subscribers Can Post Messages. Only subscribers to this mailing list are allowed to post messages.
- ◆ All Users Can Post Messages. Any user, subscriber or not, can post messages.
- ◆ Moderator Confirms All Messages. Every message will require approval from the list owner/moderator.
- ◆ Subscription Policy. Select a subscription policy for the mailing list.
- ◆ Open. Any user may subscribe.
- ◆ Confirm. An email confirmation is required to subscribe.
- ◆ Closed. The approval of the list owner is required before subscribing.
- ◆ Maximum Message Length. Select the maximum size in kilobytes or megabytes allowed for messages sent to this mailing list. Messages exceeding this size will be rejected.
- ◆ Reply Policy. Set the reply policy for this mailing list. If you choose Reply to List, replies will go to the list. Otherwise, replies will go only to the original author of the message.

Note: Users can subscribe or unsubscribe from the list by sending mail to majordomo@thishost.thisdomain.com with the words `subscribe list' or `unsubscribe list' (list is the mailing list name) in the body of the message. If the policy is `Closed', the message is sent to the list owner for approval before the subscription is allowed. Approval is never required to unsubscribe.

General Settings

This menu item is used to modify settings for this site and configure some services.

Selecting the General Settings menu item brings up the Virtual Site Settings screen; see Figure 84.

Figure 84. Virtual Site Settings screen

Figure 85. Web Settings screen

Web Settings for www.domain.com

Enable PHP Scripting

Enable Common Gateway Interface (CGI)

Enable Server-Side Includes (SSI)

Enable

webmaster Password (Enter Again)

License Agreement

END USER LICENSE AGREEMENT FOR MICROSOFT VERSION 2002

IMPORTANT-READ CAREFULLY: This End-User a legal agreement between you (either an legal entity, who will be referred to in Licensor for the Microsoft software tech including any associated media, printed documentation (the "Software"). The Sof software updates, add-on components, web

Accept License Agreement

Web Server Aliases (optional)

Save

1. Configure the settings:

- ◆ Enable PHP Scripting.

Enable the use of PHP scripts.

In Web programming, PHP is a script language and interpreter that is freely available. PHP is an alternative to Microsoft's Active Server Page (ASP) technology. As with ASP, the PHP script is embedded within a Web page along with its HTML. Before the page is sent to a user that has requested it, the Web server calls PHP to interpret and perform the operations called for in the PHP script. An HTML page that includes a PHP script is typically given a file name suffix of ".php" ".php3," or ".phtml". Like ASP, PHP can be thought of as "dynamic HTML pages," since content will vary based on the results of interpreting the script.

- ◆ Enable Common Gateway Interface (CGI). Enable the use of CGI applications. CGI programs are the most common way for Web servers to interact dynamically with users. Many HTML

pages that contain forms, for example, use a CGI program to process the form's data once it is submitted. Another increasingly common way to provide dynamic feedback for Web users is to include scripts or programs that run on the user's machine rather than the Web server. These programs can be Java(TM) applets, Java scripts, or ActiveX controls. These technologies are known collectively as client-side solutions, while the use of CGI is a server-side solution because the processing occurs on the Web server.

- ◆ Enable Server-Side Includes (SSI). SSIs are directives that are placed in HTML pages and evaluated on the server while the pages are being served. They let you add dynamically generated content to an existing HTML page, without having to serve the entire page via a CGI program, or other dynamic technology. The decision of when to use SSI and when to have your page entirely generated by some program is usually a matter of how much of the page is static, and how much needs to be recalculated every time the page is served. SSI is a great way to add small pieces of information, such as the current time. But if a majority of your page is being generated at the time that it is served, you need to look for some other solution.
- ◆ Web Server Aliases (optional). Enter additional host or domain names for which this virtual site should accept Web requests. Separate multiple entries with a comma. Example: example.com, www.example.com. Note that DNS must be configured to resolve alias addresses in addition to the site name. You can add aliases for Web servers; you are not restricted to receiving Web requests only on the domain name entered in the site settings.

2. Click Save to save the settings.

Services - Anonymous FTP

This menu item is used to change File Transfer Protocol (FTP) Settings and is only available to Server Administrators.

The Server Administrator can enable the anonymous FTP server for the site, set limits on the size of files that can be uploaded and set the number of simultaneous anonymous users. This feature allows users without passwords to download and upload files through an FTP-based application, up to the specified amount of space allocated on the hard disk drive.

You can only enable anonymous FTP on one name-based virtual site per IP address. The UI does not allow you to enable anonymous FTP on a second name-based virtual site that shares the same IP address.

Selecting the Anonymous FTP menu item brings up the Web Settings screen; see Figure 86.

Figure 86. Anonymous FTP Settings screen

The screenshot shows a web interface for configuring Anonymous FTP settings for the domain 'www.domain.com'. At the top, the title is 'Anonymous FTP Settings for www.domain.com'. Below this, there is a section labeled 'Anonymous FTP' which includes an unchecked checkbox for 'Enable'. To the right of the checkbox are two input fields: 'Maximum Allowed Upload Disk Space (MB)' with a value of '20' and a range indicator '(1 - 500)', and 'Maximum Simultaneous Connections' with a value of '10'. At the bottom center of the form is a 'Save' button.

- Configure the settings:
- Enable. Check this box to allow anonymous FTP for the user.
- Maximum Allowed Upload Disk Space (MB). This sets the limit in megabytes (MB) for anonymous FTP uploads.
- Maximum Simultaneous Connections. The maximum number of anonymous FTP users that can be connected to the server at one time. 2. Click Save to save the settings. To download files by anonymous FTP, log on to the virtual site with the user name guest or anonymous--you do not need to enter a password. When you log on with one of these user names, you enter the directory /home/sites//ftp/. The Site Administrator can post files here for downloading through FTP client software or a Web browser.

Site Administrators can access the anonymous FTP directory as "/ftp" during an FTP session.

To upload files, you must use FTP client software (for example, Fetch) and access the directory /home/sites//ftp/incoming/. Once you have uploaded a file, you (as a guest) cannot see it or access it on the FTP site. All registered site users with telnet/shell privileges can access the file, but only the Site Administrator can access the file through FTP.

The size limit specified for FTP uploads is the total amount of space allocated on the hard disk drive for FTP uploads.

Services - Email

This menu item is used to configure email options for a virtual sites. Selecting the Email menu item brings up the Email Settings screen; see Figure 87.

Figure 87. Email Settings screen

The screenshot shows the 'Email Settings for www.domain.com' interface. It features four main sections: 'Enable APOP' with an unchecked checkbox, 'Disable Email for Domain' with an unchecked checkbox, 'Email Server Aliases (optional)' with a text input field containing 'domain.com', and 'Catch-All Email Address (optional)' with an empty text input field. A 'Save' button is located at the bottom center of the form.

1. Configure the settings:
 - ◆ Enable APOP. Check this box to enable authenticated POP (APOP). APOP prevents your popmail password from traveling over the network, instead using it to encrypt a session password which can be checked against one encrypted by the popmail server also using your

password. This means that a hacker using a network sniffer can only capture your session password, which cannot be used on a second session to read your electronic mail or do any other damage. Using APOP means that your email password is less able to be electronically "stolen" and used by someone else.

- ◆ Email Server Aliases (optional). Enter additional host or domain names for which this virtual site should accept email [SMTP port 25] connections. Separate multiple entries with a comma. Example: example.com, mail.example.com. You can add aliases for email servers; you are not restricted to receiving email messages only on the hostname.domainname as entered in the site settings.
- ◆ Catch-All Email Address (optional). Specify an email address to receive messages that are addressed to unknown users and mailing lists. If left blank, email addressed to unknown users or mailing lists will not be accepted.

2. Click Save to save the settings.

Services - Shell

This menu item is used to configure shell settings for this site and is only available to Server Administrators. Selecting the Shell menu item brings up the Shell Settings screen; see Figure 88.

Figure 88. Shell Settings screen



The screenshot shows a web interface for configuring shell settings. At the top, it says "Shell Settings for www.domain.com". Below that, there is a checkbox labeled "Enable Shell Access" which is currently unchecked. At the bottom of the form, there is a "Save" button.

1. Click the Enable Shell Access checkbox to enable shell access. This allows the creation of users who can connect to the server using services such as telnet and ssh.
2. Click Save to save the setting.

Services - SSL

This menu item is used to access information about the SSL certificate used to provide secure access to your site using https on port 443 and is only available to Server Administrators. For example, SSL allows users to access your site by going to https://www.example.com:443.

Selecting the SSL menu item brings up the Certificate Information screen with its associated buttons; see Figure 91.

Figure 91. Certificate Information screen



Check the Enable SSL checkbox to allow secure access to the Web server for the site.

Usage Information

Use this menu item to view information about resource usage for this site.

Web This menu item is used to configure Web usage information for display.

1. Selecting this menu item brings up the Configure Web Reporting Options screen; see Figure 92.

Figure 92. Configure Web Reporting Options screen



2. Enter the start and end dates for Web activity to be included in the report.
3. Click Generate Report to display a summary of the Web activity.

FTP

This menu item is used to configure FTP usage information for display.

1. Selecting this menu item brings up the Configure FTP Reporting Options screen; see Figure 93.

Figure 93. Configure FTP Reporting Options screen

Configure FTP Reporting Options for www.domain.com

Starting From February 12 2009

Ending On February 12 2009

Generate Report

2. Enter the start and end dates for FTP activity to be included in the report.
3. Click Generate Report to display a summary of the FTP activity.

Email

This menu item is used to configure email usage information for display.

1. Selecting this menu item brings up the Configure Email Reporting Options screen; see Figure 94.

Figure 94. Configure Email Reporting Options screen

Configure Email Reporting Options for www.domain.com

Starting From February 12 2009

Ending On February 12 2009

Generate Report

2. Enter the start and end dates for email activity to be included in the report.
3. Click Generate Report to display a summary of the email activity.

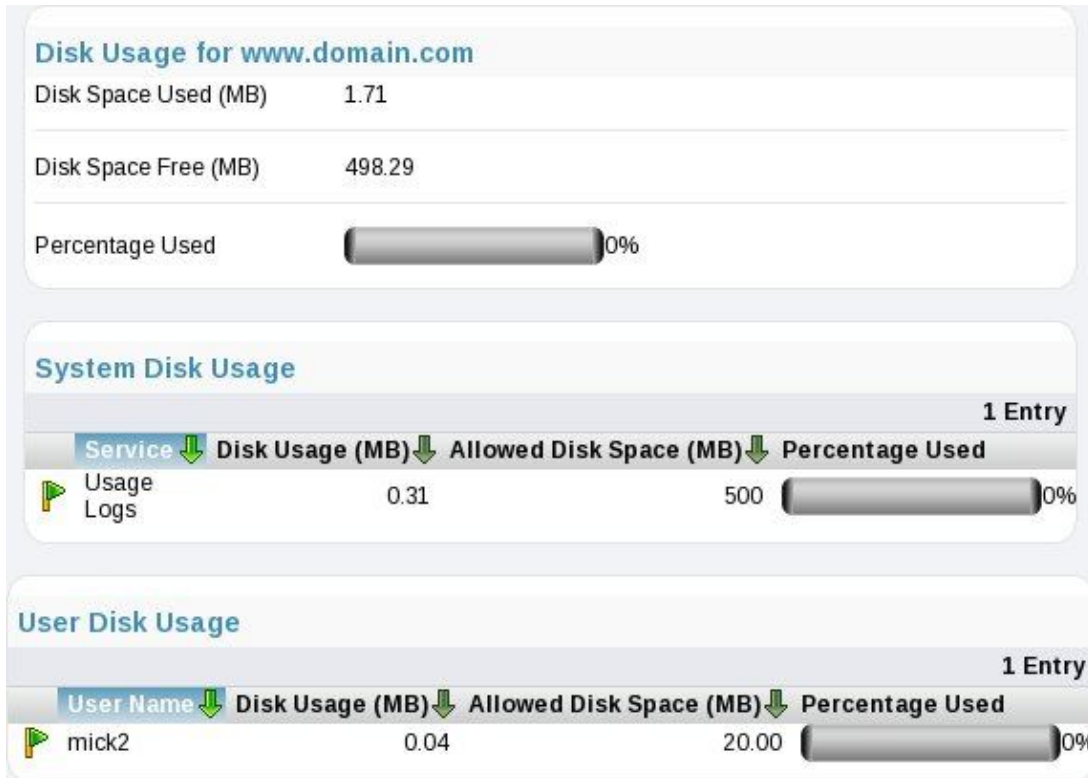
Disk

This menu item is used to display disk usage information.

1. Selecting this menu item brings up the Disk Usage screen; see Figure 95.

The Disk screen displays the disk usage by site host name, by system and by user.

Figure 95. Disk Usage screen



Statistics

This menu item is used to configure usage information and statistics generation for this site.

1. Selecting this menu item brings up the Settings screen; see Figure 96.

Figure 96. Settings screen

Usage Information Settings for www.domain.com

Enable Statistics Generation

Detail Level Daily ▾

Statistics History Forever ▾

Save

2. Use the Enable Statistics Generation checkbox to enable Virtual Site web, FTP and email usage statistics.
3. Use the Detail Level drop-down box to determine whether daily statistics information files are combined into one monthly statistics information file per month. This does not affect statistics information for the current month. If Daily is selected, you can generate reports containing less than

one month's worth of statistics for months prior to the current month. If Monthly is selected, you can only generate reports containing the statistics for whole months for months prior to the current month. Statistics combination cannot be undone for months that have been combined already. Selecting Monthly will consume less disk space compared to Daily.

4. Use the Statistics History drop-down box to determine how far back in time you will be able to cover in statistics reports. A longer period of time allows you to generate reports with a longer history at the expense of disk space.



Chapter 6

Updates

This chapter describes how to use BlueLinQ to check for and install new or updated software packages. When you log into the OSPanel server appliance as admin, the BlueLinQ tab appears in the top menu bar of the Server Desktop user interface (UI). When you select BlueLinQ, the left menu bar presents commands that allow you to update the OSPanel server appliance software, add new software and view the installed software. This section describes how to use these commands.

Installing New Software

1. Select BlueLinQ > Updates or BlueLinQ > Third Party Updates

Figure 99. Install Software table 4.



Click Install Manually. The Install Manually table appears; see Figure 100.

Figure 100. Install Manually table



2. Enter a URL in the URL field or enter a path and filename to load the software package from your computer. You can also click Browse to locate the software package.
3. Click Prepare. The system verifies that the file you are loading is in the correct.pkg format. The system then begins to load the software.

Installed Software

The following packages are critical to the operation of OSPanel; you cannot un-install these packages.

- BlueQuartz Base
- RAID

It is not usually possible to un-install various updates and additions that have been made to your Server Appliance through BlueLinQ. To view the software installed on the Server Appliance:

1. Select BlueLinQ > Installed Software. The Installed Software List table appears; see Figure 101.
2. Click the icon in the Uninstall column if you wish to uninstall a particular software. A confirmation dial appears to proceed with the uninstall procedure.
3. Click OK.

Figure 101. Installed Software List table

Installed Software List					10 Entries
Name	Version	Vendor	Description	Uninstall	
BlueQuartz	1.20071210	Project BlueQuartz	The BlueQuartz is the base software for the BlueQuartz 5100R Series. This software package is required in order for your server appliance to function.		
Mindterm SSH Client	1.0	NuOnce Networks	Mindterm SSH Client		
NuOnce - Hosts Fix	1.1	NuOnce Networks	Small fix will add all IPs on your system to /etc/hosts		
NuOnce - Installer Upgrade	1.0	NuOnce Networks	Installer Updates provided via Yum		
NuOnce - Mod_Auth_Ext	2.1	NuOnce Networks	mod_auth_external for Apache. Includes external PAM authentication hooks		
NuOnce - MySQL GUI	1.2	NuOnce Networks	MySQL GUI - Change passwords, disable SQL Server and make backups		
NuOnce - Yum Conf	1.0	NuOnce Networks	Updates for software controlled by NuOnce Networks, Inc.		
oso_php	5.02	osoffice.co.uk	PHP 5.02 for Strongbolt, OS Panel and Blue Quartz		
ospanel	1.0	osoffice.co.uk	OSPanel theme for BlueQuartz GUI		
spamassassin-3.1.4	3.1.4	nuonce.net	Spamassassin v3.1.4 for Blue Quartz		



Personal Profile

This chapter describes how to view your user account information. When you log into the OSPanel server appliance, the Personal Profile tab appears in the top menu bar of the Server Desktop user interface (UI). When you select Personal Profile, the left menu bar presents commands that allow you to manage your account. This section describes how to use these commands.

The menu items for your account appear on the left.

- Account
- Email
- Disk Usage

Account In the Account section, you can change the full name, select a language and change your password. To modify your account information:

1. Click Personal Profile at the top.
2. Click Account on the left. The Account Settings - table appears; see Figure 104.

Figure 104. Account Settings table

 The screenshot shows a web form titled "Account Settings for admin". It contains several input fields:

- "Full Name" with a text box containing "Administrator".
- "Language Preference" with a dropdown menu showing "English".
- "Style" with a dropdown menu showing "OSPanel".
- "New Password (optional)" with two stacked text boxes. The second box is labeled "(Enter Again)".

 At the bottom of the form is a "Save" button.

3. Modify any of the following fields:
 1. Full Name. This field is mandatory. Modify the real name associated with your login account.
 2. Language Preference. The OSPanel server appliance uses the language option selected in your browser software (as long as the text strings for that language are available on the server appliance). If the language selected in your browser is not available, the server appliance defaults to English.
 3. Style. Change the default look and feel of the OSPanel interface

4. New Password. (optional) You can change your password. Enter the password twice for confirmation.

For more information on choosing a password, see [Password Guidelines](#).

4. Click Save.

Email There are two options available in the Email section: Email Forwarding and Vacation Message; see Figure 105.

Figure 105. Email table

The screenshot shows the 'Email Settings for admin' interface. It is divided into two main sections: 'Email Forwarding' and 'Vacation Message'.
In the 'Email Forwarding' section, there is an 'Enable' checkbox, a text input field labeled 'Email Addresses', and a 'Save Copy' checkbox.
In the 'Vacation Message' section, there is an 'Enable' checkbox and a text input field labeled 'Auto-Reply'.
At the bottom center of the interface is a 'Save' button.

Email Formats

The Forwarding feature allows you to forward incoming messages to another email address.

Enabling email forwarding To enable email forwarding:

1. Click the Enable check box in the Email Forwarding area.
2. In the scrolling text window labeled Email Addresses, enter an email address in the format (xxxxx@yyy.zzz).

For more than one email address, separate the addresses with a comma or enter each address on a separate line.

3. You can save a copy of the email messages that you forward by clicking the Save Copy check box.
4. Click Save.

Disabling email forwarding To disable email forwarding:

1. In the Email Forwarding section of the table, uncheck the Enable check box.
2. Click Save.

Vacation message The Vacation Message feature allows you to enter a vacation-reply message that is automatically sent to each person who sends you email. This feature is useful when you know that you will not be reading or responding to incoming email messages for a period of time.

A vacation-reply email is sent only once a week to each sender.

Enabling the vacation message

To enable the vacation message:

1. In the Vacation Message section of the table, click the Enable check box.
2. In the scrolling text window labeled Auto-Reply, type the text of the message you want to send to users while you are away.
3. Click Save.

Disabling the vacation message

To disable the vacation message:

1. In the Vacation Message section of the table, uncheck the Enable check box.
2. Click Save.

Disk Usage

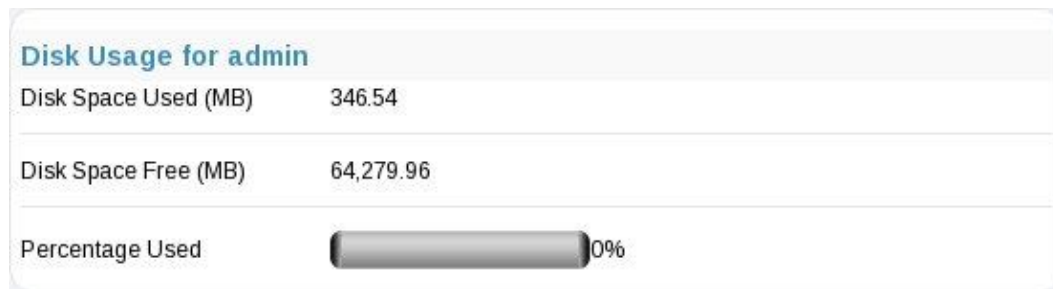
In the Disk Usage section, you can view the amount of disk space in use, the amount of disk available and the percentage of the disk in use.

Viewing the disk usage statistics To view the Disk Usage statistics:

1. Click Personal Profile at the top.
2. Click Disk Usage on the left. The Disk Usage table appears with the usage statistics; see Figure 106.

The table displays the amount of disk space used (MB), the amount of disk space free (MB) and the percentage of disk space used.

Figure 106. Disk Usage table



Caution: The features described in this appendix are intended for advanced users who want to run shell scripts or use shell commands. An advanced user is someone who is proficient in the internal workings of the Linux

operating system.

You can adversely affect the operation of your OSPanel server appliance if you modify system configuration files.

To log in via a shell, use a client such as putty to connect to the server. Enter the users username and press Enter. Enter the password for the account used to login to the machine at the password prompt. Only the admin account and server administrators who are allowed root access can `su' to root.

Note: Only the admin user or server administrators can su - to root.



Serial console port

You can connect a console terminal to the DB-9 connector on the back panel of the OSPanel server appliance. The terminal can be either an ASCII terminal or a PC running terminal software. The console terminal should have the following communications parameters - 115 200 baud, 8 data bits, no parity and one stop bit.

Initializing the server appliance through the serial console port Instead of assigning the initial network settings for the server appliance through the LCD console, you can connect the server to a terminal and assign the network settings through the serial console port.

This feature allows the assignment of network parameters only (IP address, netmask, gateway).

To initialize the OSPanel server appliance through the serial console port:

1. Connect a null modem serial cable to the serial console port on the back panel of the server appliance. See the following figure.

Figure A-1. Serial console port location

2. Configure your terminal software to the following parameters:
 - ◆ 115 200 Baud
 - ◆ 8 data bits
 - ◆ no parity
 - ◆ 1 stop bit
3. Power on the server appliance with the power switch on the front panel. A number of boot messages are displayed on your terminal screen.
4. If there is more than one language available on the system, you will be prompted to select the default system language to use. This language is also used as the admin user's language.

Powering down the server appliance remotely

Caution: This feature requires you to access the server appliance through an ssh or telnet session. Only advanced users of Linux should undertake these changes.

Note: You cannot power up a OSPanel server appliance remotely. Someone must physically power up the server.

You can power down the server appliance remotely through an ssh or telnet session. To obtain a root shell:

1. Connect to the server appliance using ssh or telnet and log in as the user admin or using a server administrator account that has root access enabled.
2. From the command prompt, if logged in as the admin user, enter:
 - su - If logged in as a server administrator, enter: su - root- where `` is the login name for the server administrator account used to connect.
3. Press Enter. A password prompt appears.
4. Enter the password for the account used to connect to the server appliance in
5. Enter the command:

shutdown -h now The system proceeds through its shutdown sequence and powers down.

Note: Only the admin user or server administrators can su - to root.

Development tools

The OSPanel server appliance provides a collection of utilities to support applications development and server administration. These tools include:

- GNU Bourne Again Shell (bash)
- Text editors (emacs, vi, pico)
- File system utilities (ls, mv, cp, ln, rm, chmod, chown, chgrp, du, df)
- File parsing utilities (sed, awk, diff)
- File display utilities (cat, more, less)
- Search utilities (find, grep, which)
- Archive utilities (gzip, tar, cpio, rpm)
- Network utilities (FTP, telnet, netstat, ping, finger, mail, pine)
- Programming languages (perl, python, tcl/tk)

These utilities can be found in one of the following directories:

/sbin /bin /usr/sbin /usr/bin /usr/local/bin

Configuration files

If necessary, you can change some of the configuration files for the services on the OSPanel server appliance for development purposes.

The services and some of their associated configuration files and directories are the following:

- Email : /etc/inetd.conf /etc/mail/
- Domain Name Service (DNS): /etc/named/
- File transfer protocol (FTP):/etc/proftpd.conf
- Web : /etc/httpd/conf/*.conf
- Mailing lists : /usr/local/majordomo/

Caution: Changing any of the following configuration files can dramatically affect the operation of the services configured by means of the server appliance's browser-based administration service or the administration service itself.

Only advanced users of Linux should undertake these changes.

Directory structure

The hard disk drive on the server appliance is partitioned into four segments. Most of the available space on the disk drive is on the partition mounted from / home. It is recommended to do most of your work under this partition. By default, quotas are turned on in this partition and are used extensively by the system software.

Virtual site home page The document root for the virtual sites' Web page content is:

/home/sites/sitename/web For example, www.osoffice.co.uk would have a document root of /home/sites/www.osoffice.co.uk/web Only the Server Administrator or the Site Administrator can upload to this directory.

Web content in this directory is associated with the URL `http://sitename/`. For example, a file saved as:

`/home/sites/sitename/web/testdir/test.html` is accessed through the URL `http://sitename/testdir/test.html`

The home directory for the admin user and the server administrator accounts can be accessed as:

`/home/users/username` where `username` is the login name for the account. Also, the admin user and server administrator accounts have no Web directory that is accessible through the Web server.

Note: `Sitename` refers to the `hostname.domainname` of the corresponding virtual site.

Customised error Web pages

The Server Administrator or a Site Administrator can replace the default error Web pages for a virtual site on the OSPanel server appliance with customised error pages for four common Web server errors.

The errors the server appliance specifically handles with custom files for a virtual site are:

- 401: Authorization Failed - This error page is displayed when you have protected a directory with an `.htaccess` file and the user does not authenticate correctly.
- 403: Forbidden - This error page is displayed when you have changed the permissions of a file or directory so that the Web server cannot access it.
- 404: File Not Found - This error page is displayed a request has been made for a file or directory that the Web server cannot find.
- 500: Internal Server Error - This error page is usually displayed when a dynamic CGI page does not return data to the Web server correctly or cannot be executed properly.

The default error pages for these four errors are located in the Web directory for a virtual site under the error subdirectory. The full path to this directory is:

`/home/sites//web/error`

For example, for a site named `www.osoffice.co.uk`, the error pages would be located in:

`/home/sites/www.osoffice.co.uk/web/error` The filenames for each error begin with the corresponding error code mentioned above. For example, error 404 is handled by the file `"404-file-not-found.html"` in the error subdirectory.

Site user home page

When a user on a virtual site is added through the Server Desktop UI, the home directory for that site user is created in:

`/home/sites/sitename/users/username` The user's default Web page is located in:

`/home/sites/sitename/users/username/web` The content of their Web pages can be viewed at `http://sitename/~username/`.



Domain Name System

The Internet uses a distributed naming system called the Domain Name System (DNS). DNS allows us to refer to computers by host names as well as by Internet Protocol (IP) addresses.

IP addresses are hard to remember and are inconvenient to use. DNS allows us to use host names and domain names which can be resolved to IP addresses. DNS servers translate host names and domain names (for example, www.sun.com) to an associated IP address (for example, 192.168.10.10) and vice-versa.

For example, OS Office has registered the domain name "osoffice.co.uk" for use by our servers "mail.osoffice.co.uk", "www.osoffice.co.uk" and others. The host names "mail" and "www" represent different servers registered in the same domain.

A domain name is a computer name suffix shared by a group of computers in the same organization. A domain name should be associated with an IP address through a Forward Lookup record. Domain names are organized in a hierarchy; this hierarchy includes your company or server name, and a country code (for example, .uk or .ca) or a top-level domain (for example, .com or .edu).

A Web site on the server appliance is created with one IP address, one host name and one domain name that together establish the identity of that Web site on the Internet.

Each domain name requires a primary domain authority on one DNS server. A secondary DNS server acts as a backup to the primary. DNS information is configurable only on the primary server, and not on the backup server.

There are three tabs in the DNS Settings table. The active tab is a light shade of gray; the inactive tab is a dark shade of gray.

- **Basic.** You can enable the DNS server feature.
- **Advanced.** You can configure the Start of Authority (SOA) default values and the server settings.
- **Zone Format.** You can create and select a zone file format for delegating subnets on non-octet boundaries.

There are also two buttons on the DNS screen, available under all three tabs.

- **Edit Primary Services.** You can configure the primary DNS server.
- **Edit Secondary Services.** You can configure the secondary DNS server.

Basic DNS Enabling the DNS server feature To enable the DNS server on the OSPanel server appliance:

1. On the user interface, select **Server Management > Network Services > DNS**.

The Basic Settings section of the Domain Name System (DNS) Settings table appears; see Figure B-1.

2. Click to enable the check box for **Enable server** (if it is not already enabled).
3. Click **Save**.

Figure B-1. Basic DNS table



Note: DNS service is automatically enabled if 127.0.0.1 or another local IP address is specified as a DNS server in the Setup Wizard.

Advanced DNS

Configuring SOA default values You can fine tune the primary domain and network authority settings - known as the Start of Authority (SOA) settings independently of each other.

To modify the SOA settings, see [Modifying the SOA record](#).

To configure the default values for the SOA settings:

1. On the user interface, select Server Management > Network > DNS. The Advanced Settings section of DNS Settings table appears; see Figure B-2.

Figure B-2. Advanced DNS table

Edit Primary Services Edit Secondary Services

DNS Settings

Basic
Advanced
Zone Format
Auto DNS

Start of Authority (SOA) Default Values

Default DNS Administrator Email Address <i>(optional)</i>	<input type="text"/>
Default Refresh Interval (Seconds)	<input type="text" value="10800"/>
Default Retry Interval (Seconds)	<input type="text" value="3600"/>
Default Expire Interval (Seconds)	<input type="text" value="604800"/>
Default Time-To-Live Interval (Seconds)	<input type="text" value="86400"/>

Server Settings

Cache Record Lookups	<input checked="" type="checkbox"/>
Forwarding Servers <i>(optional)</i>	<input type="text"/>
Zone Transfer Access by IP Address <i>(optional)</i>	<input type="text"/>
Query Request Recursion Access by IP Address <i>(optional)</i>	<input type="text"/>

Save

2. Click Advanced on the right side of the table. The fields for the SOA default values and server settings appear. You can configure the values for the following parameters. The parameters are explained in the following paragraphs.

- Domain administrator email address (optional)
- Refresh interval (in seconds)
- Retry interval (in seconds)
- Expire interval (in seconds)

- Time-to-live (TTL) interval (in seconds)
- Enter the IP address(es) of any forwarding DNS server(s).
- Enter the IP address(es) for zone transfer access.
- Click Save.

Important: Always click Save after modifying the settings in the Advanced section. If you do not, the changes will not take effect.

Domain administrator email address

The email address defaults to the user name admin of the OSPanel server appliance. This email address is publicly available and is the administrative contact for the domain or network served. The form my.name@xyz.com is not acceptable in this field (there can be no "dot" in the user name).

Refresh interval You can configure the refresh interval between updates from a secondary DNS server.

- If DNS record changes occur infrequently, increase the default value
- If DNS record changes occur often, decrease the default value Tune the refresh interval to avoid wasting bandwidth and to ensure the content on the secondary server is accurate at all times.

Retry interval

Due to a connection or service failure, a secondary DNS server may be unable to refresh data from the primary server. The secondary DNS server attempts to refresh data after the interval specified for trying again.

Expire interval A secondary DNS server may be unable to refresh data from the primary server for a prolonged period of time. After the interval specified for expiry, the secondary server stops serving name requests.

Time-to-live period (TTL) A caching DNS server other than the primary and secondary DNS servers for this domain or network can cache record lookups for the TTL period. During the TTL period, a caching DNS server does not poll the primary or secondary DNS servers for repeated lookups of the same record.

Configuring the server settings You can also configure the server settings and the zone transfer access control for the DNS server. on the OSPanel server appliance.

Cache record lookups Enabling caching, also called recursion, allows resolution of domains and network zones that other name servers are authoritative for. Disabling caching is useful when operating this server on a private network.

Forwarding server

If the OSPanel server appliance is being used on a private network or in conjunction with a restrictive firewall, you can specify a forwarding DNS server(s) by IP address. If a DNS server cannot answer a DNS query, it forwards the query to the forwarding DNS server to get the needed response, then answers back to the client.

Zone transfer

A zone transfer allows another DNS server to download the complete list of hosts maintained by your DNS server. Zone transfers are used by secondary domain name servers to synchronize their records with primary

domain name servers.

By default, zone transfers are not allowed to any domain. You must explicitly enter any domain names that are allowed to perform zone transfers, or no domain will be able to perform zone transfers.

Note: If you have a primary or secondary DNS entry in a given domain provided by the OSPanel server appliance, no requests in that domain will be forwarded to the forwarding server.

Zone Format

You can create and select a zone file format for delegating subnets on non-octet boundaries that is compatible with your local reverse-delegation method. RFC2317 is the international standard format. Consult your ISP to determine the type of subnet DNS delegation they are using.

The DNS server on the OSPanel server appliance can support user-defined network-delegation formats. If your company uses a proprietary zone file format, you can enter the format parameters in the table on this page.

The symbols in the fields are defined as follows:

- %1 represents the first octet of a four-octet IP address.
- %2 represents the second octet of a four-octet IP address.
- %3 represents the third octet of a four-octet IP address.
- %4 represents the fourth octet of a four-octet IP address.
- %n represents the size of the network (in bits)

For example, if the IP address is 192.168.10.19/0-31:

%1 is 192. %2 is 168. %3 is 10. %4 is 19. %n is an integer number from 0 to 31.

Note: If you select the option "User-defined", you must fill in all four fields in the table.

Important: Consult your network administrator or ISP for the correct order of the data in the proprietary format they are using.

To configure the Zone Format settings:

1. On the user interface, select Server Management > Network > DNS. The Domain Name System (DNS) Settings table appears.
2. Click Zone Format on the right side of the table. The fields and default values for the Zone File Formats appear; see Figure B-3.

Figure B-3. Zone Format table

DNS Settings

Zone File Format Settings

Zone File Format

User Defined Zone File Format Settings

Zone File Format for > 24-bit networks. *(optional)*

Zone File Format for > 16-bit networks. *(optional)*

Zone File Format for > 8-bit networks. *(optional)*

Zone File Format for > 0-bit networks. *(optional)*

3. Select a zone file format.

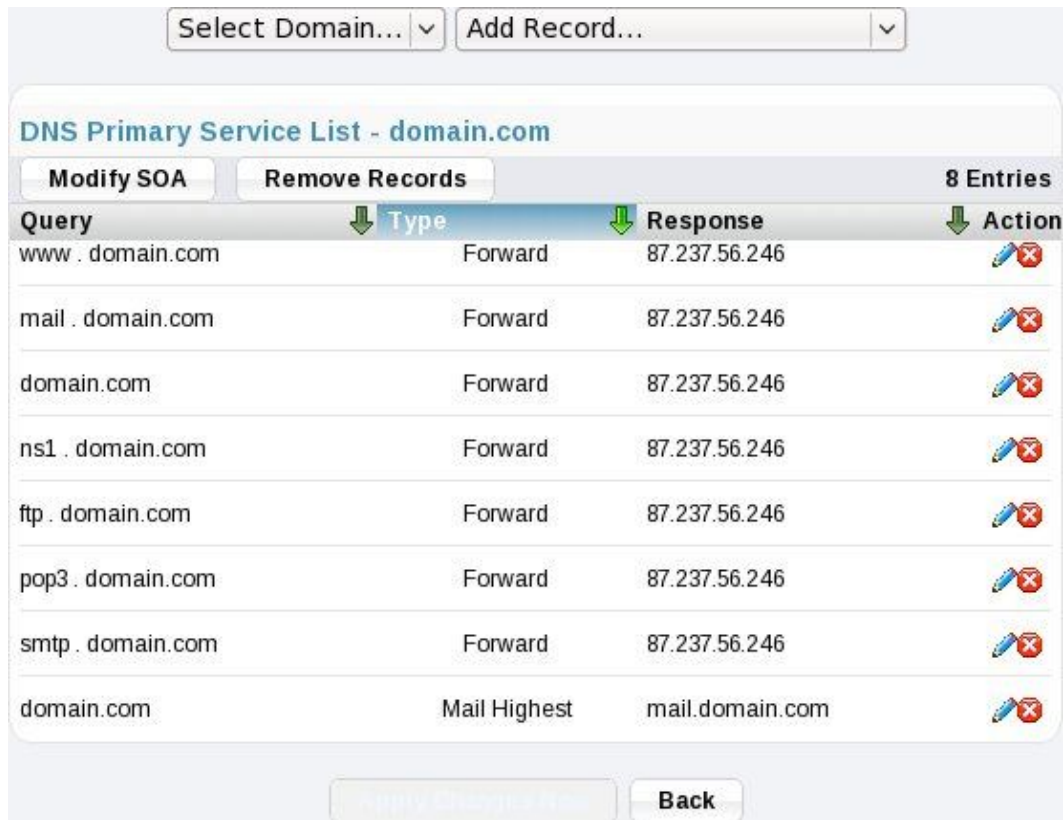
RFC2317 is the international standard format. You can also select the option "User-defined". If you select the option "User-defined", fill in the four fields.

4. Click Save.

Primary services

A primary DNS server maintains a list of name records and their associated IP addresses. This list is made available to other DNS servers if your domain is registered with your country-specific domain-naming organization. Your Internet service provider (ISP) can help you register your Internet server.

Figure B-4 shows some sample entries in the Primary Service List table.



To set up the primary DNS server on the OSPanel server appliance, you need to use the Add Record... pulldown menu to configure the following DNS records.

- Forward Address (A) record
- Reverse Address (PTR) record
- Mail Server (MX) record
- Alias (CNAME) record
- Subdomain Delegation
- Subnet Delegation

If there are no records defined, there are no authority selection options available. If there are records defined, the Select Domain ... menu is available at the top of the screen. There are also two buttons available at the top of the Primary Service List table: Modify SOA and Remove Records. OSPanel server appliance Selecting a domain To display the DNS records for a particular domain, click on the Select Domain... pull-down menu and select the domain.

The screen refreshes and the Primary Service List table displays the DNS records for that domain. The domain name shows up in the title bar.

Modifying the SOA record

Modifying the SOA record You can modify the SOA record for a particular domain or network. For an explanation of the fields you can modify, see "Configuring SOA default values"

1. From the pull-down menu, select the domain for which you want to modify the SOA record. The defined records for that domain appear in the Primary Service List table.

2. Click **Modify SOA** at the top of the **Primary Service List** table. The **Modify SOA Record** table appears. The first field displays either the domain name or the network authority that you selected.

- ◆ **Primary Name Server**

Enter the fully qualified domain name of the primary name server for the selected domain or network authority.

- ◆ **Secondary Name Server**

Enter the fully qualified domain name(s) of the secondary name server(s) for the selected domain or network authority. If you want to specify more than one secondary name server, separate the names with a space.

- ◆ **DNS Administrator email address**

- ◆ **Refresh interval**

- ◆ **Retry interval**

- ◆ **Expire interval**

- ◆ **Time-to-live interval**

3. Click **Save**. The screen refreshes and the **Primary Service List** table appears.

Deleting all DNS records

You can delete all the DNS records for a particular domain name from the **Primary Service List** table.

1. From the pull-down menu, select the domain for which you want to modify the SOA record. The defined records for that domain appear in the **Primary Service List** table.
2. Click **Remove Records** at the top of the **Primary Service List** table. A confirmation dialog appears, asking you if you want to remove all of the DNS records displayed in the table.
3. Click **OK**. The screen refreshes and the **Primary Service List** table is now empty.

Modifying a specific DNS record To modify an individual entry in the **Primary Service List** table, click on the green pencil icon next to that entry. The **Modify Record** table appears.

4. Click **Save**. The screen refreshes.

Deleting a specific DNS record To delete an individual entry from the **Primary Service List** table, click on the red trash can icon next to that entry. A confirmation window appears, asking if you want to delete the record.

5. Click **OK**. The screen refreshes and the **Primary Service List** table no longer display that record.

Configuring a Forward Address (A) record

A **Forward Address (A)** record translates a fully qualified domain name into an IP address.

To configure a **Forward Address (A)** record for your server appliance:

1. Select **Server Management > Network Services > DNS**. The **DNS Settings** table appears.
2. Click **Edit Primary Services** above the table. The **Primary Service List** table appears.
3. Select **Forward Address (A) Record** from the **Add Record...** pull-down menu. The **Add New Forward Address (A) Record** table appears.
4. Enter the host name (optional) and domain name you want to serve (for example, **www** and **mydomain.com**).

5. Enter the IP address (for example, 192.168.10.10) that is used by the host and domain names entered in the first two fields.
6. Click Save. The Primary Service List table reappears with the new entry.
7. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

Configuring a Reverse Address (PTR) record

A Reverse Address (PTR) record translates an IP address into a fully qualified domain name.

To configure a Reverse Address (PTR) record for your server appliance:

1. Select Server Management > Network Services > DNS.

The DNS Settings table appears.

2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Reverse Address (PTR) Record from the Add Record... pull-down menu. The Add New Reverse Address (PTR) Record table appears.
4. Enter the IP address (for example, 192.168.10.10) that you want to resolve to a fully qualified domain name.
5. The Subnet Mask field holds the default value of 255.255.255.0. You can edit this value if necessary.
6. Enter the host name (optional) and domain name (for example, www and mydomain.com) to which the IP address in the first field resolves.
7. If you have not already created a Forward Address (A) record to resolve this host name and domain name to the specified IP address, you can automatically generate one. To do so, click the check box Generate Forward Address (A) Record.
8. Click Save. The Primary Service List table reappears with the new Reverse Address (PTR) entry. If you generated a Forward Address (A) record, that entry appears as well.
9. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

Configuring a Mail Server (MX) record

To receive mail for your domain name (for example, mydomain.com), you need to create a Mail Server (MX) Record.

A Mail Server (MX) record identifies the mail server responsible for delivering email messages to a specified host name (optional) and domain name. An MX record is similar to an A record but resolves to a fully qualified domain name rather than an IP address.

To configure a Mail Server (MX) record for your server appliance:

1. Select Server Management > Network Services > DNS. The DNS Settings table appears.
2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Mail Server (MX) Record from the Add Record... pull-down menu. The Add New Mail Server (MX) Record table appears.
4. Enter the host name (optional) and domain name (for example, www and mydomain.com) to be served by the mail server.

5. Enter the fully qualified domain name of the mail server (for example, mail.mydomain.com) that serves the domain name entered in the second field.
6. Under the Delivery Priority pull-down menu, select the priority for mail delivery to the mail server: very high, high, low, very low.

The value of the delivery priority specifies the order in which a series of mail servers is contacted for mail delivery. The Delivery Priority setting is useful only if more than one MX record is configured for a domain or network.

7. Click Save. The Primary Service List table reappears with the new entry.
8. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

Important: It is critical that the MX record resolve to a fully qualified domain name that has a corresponding A record.

Configuring an Alias (CNAME) record

An Alias (CNAME) record provides the translation from one fully qualified domain name to another fully qualified domain name.

The source domain name is known as the alias and the target domain name is known as the canonical name or real name. The target host name does not need to be a member of the local domain. For example, you can create an Alias (CNAME) record of "news.domain.com" resolving to "uucp.isp.net".

To configure an Alias (CNAME) record for your server appliance:

1. Select Server Management > Network Services > DNS. The DNS Settings table appears.
2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Alias (CNAME) Record from the Add Record... pull-down menu. The Add New Alias (CNAME) Record table appears.
4. Enter the host name (optional) and domain name (for example, news and mydomain.com) of the alias.
5. Enter the host name (optional) and domain name (for example, news and otherplace.com) of the real domain name.
6. Click Save. The Primary Service List table reappears with the new entry.
7. To add another record, select a record type from the pull-down menu again.

To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

Important: Do not use an Alias (CNAME) record to cause a domain name to resolve to a host name. For example, do not create an Alias (CNAME) record for mydomain.com that resolves to www.mydomain.com. Instead, add a Forward Address (A) record for mydomain.com to the IP address used by www.mydomain.com. See [Configuring a Forward Address \(A\) record](#)

CNAME host names must be unique. A and MX records must not share host names with a CNAME record.

Adding a Subdomain Delegation

Select Subdomain Delegation from the Add Record... pull-down menu. The Add a Subdomain Delegation screen is shown in Figure B-5.

Figure B-5. Subdomain Delegation screen

To configure the Add a Subdomain settings:

1. Parent Domain Name. Select the Parent Domain Name. For example, to delegate the subdomain remote.example.com, select example.com.
2. Subdomain Name. Specify the unqualified Subdomain Name. For example, to delegate the subdomain remote.example.com, this server must be authoritative for the domain example.com. Specify only the subdomain name, remote.
3. Name Server. Specify a comma-separated list of fully qualified host names that are authoritative for the specified subdomain. At least one name server must be specified.

Adding a Subnet Delegation

To add a subnet delegation, you must first add a Reverse PTR Record (see [Configuring a Reverse Address \(PTR\) record](#)).

After you add the record and apply the changes, the DNS Primary Service List appears similar to the screen shown in Figure B-6.

Figure B-6. DNS Primary Service List (after adding Reverse PTR Record)

Query	Type	Response	Action
192.168.5.10	Reverse	domain.com	

To configure the Add a Subnetwork settings:

1. Select Subnet Delegation from the Add Record... pull-down menu. The Add a Subnet Delegation Screen appears; see Figure B-7.

Figure B-7. Add a Subnet Delegation Screen

2. Parent Network. This is the parent network for which this server is authoritative. All IP addresses in the specified subnet must belong to this parent network.
3. Subnet IP Address. Specify an IP address within the desired subnet that will be delegated to another DNS server.
4. Subnet Network Mask. Specify the subnet network mask in dot-quad notation.
5. Name Servers. Specify a comma-separated list of fully qualified host names that are authoritative for the specified subnet. At least one name server must be specified.
6. Click Save to save the subnet delegation.

Secondary services

The Administrator can configure a secondary DNS server to provide redundant DNS service to your computers. If the primary DNS server is unavailable, the secondary DNS server takes over.

Figure B-8 shows some sample entries in the Secondary Service List table.

Secondary service for a domain

To add a secondary name-server authority for a domain:

1. Select Server Management > Network Services > DNS. The DNS Settings table appears.
2. Click Edit Secondary Services above the table. The Secondary Service List table appears.
3. Select Domain Secondary Service for a domain from the Add Secondary Service... pull-down menu. The Add Secondary Service table appears; see Figure B-9.

Figure B-9. Add Secondary Service table

The screenshot shows a web form titled "DNS Add Secondary Service". It has a light blue header with the title. Below the header, there are two input fields. The first is labeled "Domain Name" and the second is labeled "Primary DNS Server IP Address". At the bottom of the form, there are two buttons: "Save" and "Cancel".

4. In the first field, enter the domain name for which DNS information is served by the IP address in the second field.
5. In the second field, enter the IP address of the primary DNS server for the domain name specified in the first field.
6. Click Save. The Secondary Service List table reappears with the new entry.
7. To add another secondary service, select a service from the pull-down menu again. To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

To add a secondary name-server authority for a network:

1. Select Server Management > Network > DNS. The DNS Settings table appears.
2. Click Edit Secondary Services above the table. The Secondary Service List table appears.
3. Select Network Secondary Service from the Add Secondary Service pull-down menu. The Add Secondary Service table appears; see Figure B10.
4. In the first field, enter the IP address of a member on the network (for example, 192.168.1.1) whose DNS information is served by the IP address in the third field.
5. In the second field, enter the subnet mask corresponding to the IP address for the specified network authority.
6. In the third field, enter the IP address of the primary DNS server for the specified network.
7. Click Save. The Secondary Service List table reappears with the new entry.
8. To add another secondary service, select a service from the pull-down menu again.

To apply the changes to the DNS settings, click Apply Changes Now. The DNS Settings table appears.

Figure B-10. Add Secondary Network table

DNS Add Secondary Service

Network

Network Subnet Mask

Primary DNS Server IP Address

Sample setup of DNS service

This sample setup of DNS service on your OSPanel server appliance assumes that you have already registered your domain with InterNIC or another registration service.

For more information on registering a Web site, visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org>.

In the following examples, we will configure a sample domain called "mydomain.com" for Web service and email service using a sample IP address 192.168.10.10.

The recommended minimum configuration for Web and email service requires the following records. These records allow anyone on the Internet to type either "mydomain.com" or "www.mydomain.com" to access your Web site.

- A Reverse Address (PTR) record for 192.168.10.10., which resolves to mydomain.com
- A Forward Address (A) record for mydomain.com, which resolves to 192.168.10.10 (You can generate this record automatically from the PTR record.)
- A Forward Address (A) record for www.mydomain.com, which resolves to 192.168.10.10
- A Mail Server (MX) record for mydomain.com, which resolves to www.mydomain.com

Important: Substitute your domain name and IP address where the sample domain name or sample IP address appears.

First, create a Reverse Address (PTR) record.

1. Select Server Management > Network Services > DNS. The DNS Settings table appears.
2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Reverse Address (PTR) Record from the Add Record... pull-down menu. The Add New Reverse Address (PTR) Record table appears; see Figure B-11.
 - ◆ In the IP Address field, enter 192.168.10.10.
 - ◆ Leave the subnet mask as 255.255.255.0.
 - ◆ In the Host Name field, enter www.
 - ◆ In the Domain Name field, enter mydomain.com.
4. Click the check box Generate Forward Address (A) Record to generate a Forward Address (A) record.
5. Click Save. The Primary Service List table reappears with the new Reverse Address (PTR) and

Forward Address (A) entries.

Figure B-11. Add New Reverse Address (PTR) Record table Sample setup of DNS service

Forward Address (A) record

Next, create a Forward Address (A) record.

1. Select Server Management > Network > DNS. The DNS Settings table appears.
2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Forward Address (A) Record from the Add Record... pull-down menu. The Add New Forward Address (A) Record table appears; see Figure B-12.
 - ◆ Leave the Host Name field blank
 - ◆ In the Domain Name field, enter mydomain.com
 - ◆ In the IP Address field, enter 192.168.10.10
4. Click Save. The Primary Service List table reappears with the new Forward Address (A) entry.

Figure B-12. Add New Forward Address (A) Record table

Finally, create a Mail Server (MX) record.

1. Select Server Management > Network > DNS. The DNS Settings table appears.
2. Click Edit Primary Services above the table. The Primary Service List table appears.
3. Select Mail Server (MX) Record from the Add Record... pull-down menu.

The Add New Mail Server (MX) Record table appears; see Figure B-13.

- ◆ Leave the Host Name field blank
 - ◆ In the Domain Name field, enter mydomain.com
 - ◆ In the Mail Server Name field, enter mail.mydomain.com
 - ◆ Under the Delivery Priority pull-down menu, leave the priority as Very High
4. Click Save. The Primary Service List table reappears with the new Mail Server (MX) entry.

Figure B-13. Add New Mail Server (MX) Record table



The screenshot shows a web form titled "DNS Add New Mail Server (MX) Record". It contains the following fields and controls:

- Host Name (optional)**: An empty text input field.
- Domain Name**: A text input field containing "domain.com".
- Mail Server Name**: An empty text input field.
- Delivery Priority**: A dropdown menu currently showing "Very High (20)".
- Buttons**: "Save" and "Cancel" buttons at the bottom.

You are now finished with creating your DNS records. To edit another domain, select another domain from the Select Domain or Network pull-down menu. You can select any domain that you have configured for the DNS server, Important: Click Apply Changes Now. This activates the changes you have made. If you exit this screen without saving your changes, they will not become active.

Brief history of the Domain Name System (DNS)

In the 1960s, the U.S. Department of Defense Advanced Research Projects Agency (ARPA, and later, DARPA) began funding an experimental wide area computer network called the ARPAnet. The ARPAnet used a centrally administered file called HOSTS.TXT that held all name-to-address mapping for each host computer connected to the ARPAnet. Since there were only a handful of host computers at the start, HOSTS.TXT worked well. When the ARPAnet moved to the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols and become known as the Internet, the network population exploded. HOSTS.TXT became plagued with problems, namely

- traffic and load
- name collisions
- consistency

A replacement for the HOSTS.TXT file was needed. The goal was to create a system that solved the problems inherent in a unified host table system. The new system should allow local administration of data and also make that data globally available.

In 1984, the architecture of a new system called Domain Name System (DNS) was designed and is the basis of the DNS service used today on the Internet.

DNS is a distributed database that allows local administration of the segments on the overall database. Data in each segment of the database are available across the entire network through a client-server scheme consisting of name servers and resolvers.

What is a DNS record? People are much more comfortable dealing with names rather than strings of numbers. A domain name such as "sun.com" is much easier to remember than the IP address, which consists of four octets of numbers such as 63.77.128.100. Domain names must be registered with Root Domain Registration Service; visit the Internet Corporation for Assigned Names and Numbers (ICANN) at <http://www.icann.org> for a list accredited domain-name registrars.

Computers, on the other hand, prefer numbers to names. Since computers have the final say when a user is looking for a company Web site, a mechanism is needed to convert the human-friendly domain name to the computer-friendly IP address.

DNS records on a DNS server perform this function. The records translate a domain name to an IP address; a record equates a domain name such as "sun.com" to an IP address such as 207.91.131.30. Once the domain name has been converted or "resolved" to an IP address, then (and only then) can the user connect to your Web site.

Without DNS and domain names, the user would be required to remember the IP address of every site they wanted to visit. With DNS servers and DNS records, customers and their software can easily remember how to get to your site.

Who manages your DNS records? Your DNS records can reside on any BlueQuart server appliance that has the DNS service enabled. You or your administrator can easily configure a OSPanel server appliance to act as a DNS server. To provide DNS service, InterNIC requires a site to maintain both a primary and a secondary server. Your OSPanel server appliance can act as the primary server and a DNS server from your Internet service provider (ISP) can act as the secondary server.

How does DNS work?

The basic method that allows a domain name to direct customers to your Web site is shown in Figure B-14. This diagram describes a request made by a Web browser as the customer attempts to log on to your Web site.

To determine which primary name server contains your domain name:

1. The local name server (the DNS resolver/browser machine) contacts the root domain name server maintained by the several Internet root server authorities.
2. The root domain name server returns the IP address of the primary name server responsible for the requested domain name.
3. The local name server contacts the primary name server.
4. The primary name server holds the IP address information for the domain name in a database and satisfies the request from the local name server.
5. If the primary name server is unavailable, the local name server contacts the secondary name server that satisfies the request from the local name server. The local name server returns to the Web browser with the IP address for the requested domain name.
6. Using the IP address, the Web browser contacts the company Web server.

7. The company Web server sends the Web page to the local name server.