Parallels® Pro Control Panel

Parallels Pro Control Panel 10.3.3 for Linux Site Administrator's Guide

REVISION 1.0

Legal and Copyright Notice

ISBN: N/A

Parallels

660 SW 39th Street

Suite 205

Renton, Washington 98057

USA

Phone: +1 (425) 282 6400

Fax: +1 (425) 282 6444

Contents

C H A P T E R 1

Preface

In this chapter:

Typographical Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the **System** tab.
	Titles of chapters, sections, and subsections.	Read the **Basic Administration** chapter.
Italics	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called *wildcard character* search.
`Monospace`	The names of commands, files, directories, and domain names.	The license file is located in the `http://docs/common/licenses` directory.

`Preformatted`	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	**`# ls -al /files`** `total 14470`
`Preformatted Bold`	What you type, contrasted with on-screen computer output.	**`# cd /root/rpms/php`**
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4

Feedback

If you have found a mistake in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback using the online form at http://www.parallels.com/en/support/usersdoc/. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

C H A P T E R 2

About Parallels Pro Control Panel for Linux

Parallels Pro Control Panel for Linux (formerly known as Ensim Pro for Linux) is packaged with core Web hosting services and features that allow you, as Site Administrator, to manage a range of services for your organization.

Note: For simplicity, we will refer to Parallels Pro Control Panel for Linux as “Parallels Pro Control Panel” throughout this guide.

Control Panels

Parallels Pro provides two separate Web-based user control panels for Site Administrators and User Administrators:

- The Site Administrator control panel (on page 14)
- The User Administrator control panel (on page 15)

Each control panel allows easy access to key features and streamlines common configuration and administration tasks.

Note: The Site and User Administrator control panels are designed to work with Internet Explorer 5.0 and higher and Netscape 6.2 and higher. Using other browsers might produce unpredictable results.

CHAPTER 3

Quick-start Guide for Site Administrators

This quick-start guide is composed of a number of interlinked Help-system topics that show you how to complete common tasks.

Click a link below to learn about the task. Then click the quick-start links at the top or bottom of the topic to proceed through the guide. You can keep this guide open while you complete each task in the control panel.

Quick-start topics:

CHAPTER 4

Using the Control Panels

In this chapter:

Site Administrator Control Panel

The Site Administrator control panel is a graphical user interface (GUI), or a control panel, designed to help the domain owner, manage the hosted domains and the services that are available to your users.

Note: The Site Administrator control panel is designed to work with Internet Explorer 5.0 and higher and Netscape 6.2 and higher. Accessing this control panel with other browsers might produce unpredictable results.

Using this control panel you can:

- Set up your site's security features (on page 78)
- Manage your site's user accounts (on page 26)
- Manage the Power Tools enabled for your site (on page 192)
- Set up password-protected directories (on page 219)
- Set up your organization's email services (on page 152)
- Manage your site's directories and files (on page 198)
- View your site's usage reports (on page 96)
- Export your site's data (on page 236)
- Import your site's data (on page 239)

How to Access the Site Administrator Control Panel

To access the Site Administrator control panel from any computer connected to the Internet, enter the following URL in a browser window:

`Error! Hyperlink reference not valid.`

where `<example.com>` is the domain name of your site and `/admin` directs you to the Site Administrator Welcome page.

Note: You can also access the Site Administrator control panel through a link on the default home page your service provider sets up for your domain on the Internet. However, after you replace the default home page with your own, this link is no longer available to you.

User Administrator Control Panel

The User Administrator control panel is a graphical user interface (GUI), or control panel, designed to help you and your site's other users manage contact information and email services.

Note: The User Administrator control panel is designed to work with Internet Explorer 5.0 and higher and Netscape 6.2 and higher. Accessing this control panel with other browsers might produce unpredictable results.

Using this control panel, you and your users can:

- View or change account contact information
- Set personal email preferences, such as vacation messages
- Send and receive email messages over the Internet
- Export and import files

As Site Administrator, you add users (on page 27) to your domain. This provides each user with a unique user name and password, used to log on to the User Administrator control panel.

In addition, you can add a user account for yourself (on page 33) so you can log in to the User Administrator control panel to manage your own email. You can access the Site Administrator email account using the link to SquirrelMail (on page 145) on the Configuration page of the Site Administrator control panel, but you cannot log on to the User Administrator control panel to manage your email account until you add yourself as a user.

How to Access User Administrator Control Panel

You can access the User Administrator control panel through a link on the default home page your service provider sets up for you when you register your domain name. However, after you replace the default home page with your own, this link is no longer available unless you place it on your home page.

To access the User Administrator control panel from any computer connected to the Internet, enter the following URL in a browser window:

`http://<example.com>/user`

where `<example.com>` is the domain name of your site.

Additional Login Information for Users

After you add a user to your site, you need to let them know the user name and password you assigned to their account as well as instructions for logging on to the User Administrator control panel and using the services, such as email, available to them. All of this information is provided in the Help topic that describes how to add users (on page 27).

Using the Dashboard

The **Dashboard** page allows you to view the configuration settings of your site, and also manage it using a single page.

To go to the **Dashboard** page:

- Log on to site administrator control panel.
- On the home page, click the **Dashboard** tab.

Dashboard options for site administrators

AnnounceIt!	Parallels Pro uses AnnounceIt! to notify you of critical business updates. You can click on the message to view the details.

My Web Site Category

Section	Description
Unique Page Hits	Displays the number of hits on your Web site on a weekly, monthly, or biannually basis.

Users and Mailboxes Category

Users (Mailboxes):	Displays the total mail boxes used by the users.
Disk Used by Mail :	Displays the total used disk space.
Mails In Queue:	Displays the number of mails in the queue.
Mail Queue Size:	Displays the mail queue size.
Aliases:	Displays the number of aliases.
Responders:	Displays the number of responders.
Mailing Lists:	Displays the number of mailing lists.
Details:	Displays the details of the mail box sizes.

Site Overview Category

Section	Description
General	Displays the general information about your site.

General (Service Status)	Displays the status of the services currently provisioned for your site. The status of a service is represented by for enabled, and for disabled.
Disk Space (MB)	Displays the total, used, and available hard disk space for your site.
Data Transfer (MB)	Displays the Web and FTP traffic on your site. You can view this information on a daily, weekly, monthly, or yearly basis.

C H A P T E R 5

Setup Tasks

In this chapter:

Applying a New Skin

You can change the appearance of your control panel by creating a skin or customizing available skins.

Note: The user accounts hosted on the site inherit the visual appearance of the control panel.

➢ ***To apply a new skin:***

1. In the shortcuts section of the Home page, click **Manage Skins** (Tools section).
2. In the Manage Skins area, select the option button next to the skin you want to apply.
3. Click **Preview** to preview the control panel with the selected skin.
4. Click **Apply** to apply the skin to the control panel. This process takes a few seconds.
5. Log out from the control panel by clicking **Log out** in the Login Info panel.
6. Log in again using your account information. The control panel displays the new skin.

Accessing and Using Services

This topic describes the available services. Your service provider determines which services are enabled for your site.

User Names and Passwords for Accessing Services

You use your Site Administrator user name and password to access services. If you change your Site Administrator password, you are also changing the password you use to access services such as FTP, Telnet, and SSH. These services all use the same password.

If you have Microsoft FrontPage Extensions enabled for your site, however, be aware that the Microsoft FrontPage Administrator password is on a separate system and does not change automatically. You can change the FrontPage Administrator user name or password using the FrontPage Extension Permission Management Interface (on page 139).

Service Description and Access Information

Note: Your site might not have all of the services listed. For more information about a service, contact your service provider.

Service name	Description
Apache Web server	Responds to requests from Web browsers. The Web server serves requests from browsers by retrieving a requested file or executing a CGI script.
Domain Name Server	Translates site names into IP addresses. DNS is a distributed database that performs name translations. To manage this information effectively, DNS has a distributed architecture, composed of many DNS servers in a hierarchical fashion. Each server is responsible for both name-to-IP-address and IP-address-to-name translations.
Mailing Lists (Majordomo)	Manages mailing lists. Mailing lists are commonly used to circulate topic discussions. A mailing list includes a set of list members. Whenever a list member posts an email message to the mailing list email address, that email message is distributed to all list members.

Microsoft FrontPage Server Extensions	Allows you to support users who want to use Microsoft FrontPage to manage their Web sites. In the control panel, you can access FrontPage administration Web pages from the Web Server Manager.
WebDAV Server	WebDAV (Web-based Distributed Authoring and Versioning) allows you to collaboratively edit and manage files on the remote Web servers.
Miva Merchant	Provides ecommerce support for sites. Miva Merchant enables you to create multiple online storefronts and support ecommerce on a site.
mod_perl for Apache	mod_perl enables you to create dynamic content by utilizing the full power of the Apache web server to create stateful sessions and customized user authentication systems. You can use Perl to manage Apache and respond to requests for Web pages.
MySQL Database	Allows you to work with your SQL databases. MySQL is a widely used relational database management system for SQL databases. A relational database stores data in separate tables rather than in one big table. A database management system allows you to add, access, and process data stored in a SQL database. In the control panel, you can use phpMyAdmin to set up, configure, and view your databases.
Open SSH Secure Shell	Provides secure remote access to another system over a network. In the case of the control panel, SSH allows you to log on to the server remotely and move files, run scripts, or search across multiple files in a secure environment. To use an SSH connection you need to be familiar with the UNIX operating system and commands.
Open SSL Secure Web	Provides secure Web pages. SSL is a protocol that transmits private documents through the Internet. It creates a secure connection between a client and a server over which any amount of data can be sent securely. SSL works by using a private key to encrypt data transferred over the SSL connection. In the control panel, you can secure your site through the Web Server Manager.
PHP Hypertext Preprocessor for Apache	Creates dynamic Web pages. PHP (PHP Hypertext Preprocessor) is a server-side, cross-platform, HTML embedded scripting language.
phpMyAdmin Web-based MySQL Administration	Allows you to manage your MySQL databases over the Internet. phpMyAdmin can handle administration of entire MySQL database servers or just a single database over the Internet by removing any platform-specific limitations.

Power Tools	Streamlines the installation and use of off-the-shelf Web applications. Power Tools provide ecommerce, content management, forums, chat, and other dynamic features of Web sites.
POP3 + IMAP Server	POP3 (Post Office Protocol, version 3) is a protocol used to retrieve email from a mail server. IMAP (Internet Messaging Access Protocol) is a protocol that retrieves messages from the mail server. Using IMAP, you can search through your email messages using keywords and selectively download messages. The IMAP server allows users to archive email messages in folders, share mailboxes with other users, access multiple mail servers at one time, and more efficiently access email attachments. Both POP and IMAP mail servers accept SMTP-formatted email messages.
FTP	Transfers files over the Internet. FTP (File Transfer Protocol) allows you to transfer files over the Internet. Anonymous FTP (if available) allows you to use an FTP site without creating a user account. To use FTP, you need to be familiar with FTP commands or use a program that manages those commands for you.
Anonymous FTP	An anonymous way to transfer files over the Internet. Anonymous FTP allows you to use an FTP site without creating a user account. To use anonymous FTP, you need to be familiar with FTP commands or use a program that executes those commands for you.
Email	Routes outgoing and incoming mail using SMTP. Sendmail is an SMTP (Simple Mail Transfer Protocol) mail server that routes SMTP email messages through the Internet to be stored on a mail server. SMTP is the most common email protocol on the Internet. Sendmail also allows you to manage your email features, such as email aliases, responders, and spam filters.
SquirrelMail Web-based Email	Provides Web-based access to email accounts. Squirrel Mail is an email client that uses IMAP to provide your email account users with Web-based access to their email messages.
Telnet	Provides remote access to another system over a network. Telnet is a common terminal emulation protocol that connects computers locally or across the Internet. It allows a user at a local computer to log onto a remote computer and run a program. To use a Telnet connection you need to be familiar with the UNIX operating system and commands.
Vacation message	Automatically responds to incoming email.

MailScanner	Email scanning service that scans incoming and outgoing emails for viruses.
Spam Filtering	Spam filtering service that scans email messages for spam and enables user level control and management of spam.
AWStats Web/FTP Log Analyzer	AWStats is a free powerful and featureful tool that generates advanced web and ftp server statistics, graphically.
Analog Web/FTP Log Analyzer	Measures the usage traffic on your Web and FTP servers. Analog Web/FTP Log Analyzer compiles statistics about which Web pages are most popular, which countries people are visiting from, which Web site visitors tried to follow broken links from, and other such information.
Webalizer Web/FTP Log Analyzer	A free log file analysis application. Webalizer generates highly detailed usage statistics for Web and FTP servers in easily comprehensible graphical and tabular formats. The logs generated are a statistical encapsulation of user traffic on your server.

Setting Up Your Web Site

In this section:

How to Publish Content to Your Web Site

Publishing content to your Web site means creating HTML and other Web pages and placing them on your site so that they can be viewed on the Internet.

Publication Tasks

➢ ***To publish content to your Web site you need to:***

1. Create the Web pages you want to publish (on page 67)
2. Copy your Web pages to your site (on page 68)
3. Check or preview your new Web pages (on page 70)

Setting Up Your Site's Email

In this section:

Setting up Your Site's Email Services

If your service provider enables email services for your site, you and your users can send and receive email over the Internet.

Set-up Tasks

To set up your organization's email service, complete these tasks:

- Add user accounts (on page 27) for yourself and other users. User accounts enable users to access email and other services from the User Administrator control panel. If you are using the quick-start guide (on page 12), these tasks are steps 3 (on page 33) and 4 (on page 27).
- Set up mailing lists (on page 157) (if available). Mailing lists are lists of email recipients that can receive email as a group. They are useful when you want to send messages, such as system updates, to a group of users.
- Add aliases (on page 162). An email alias is a method of mapping a nickname to an actual email address. They are useful when you want to map a nickname, such as "sales," to one or more email addresses.
- Add responders (on page 166). Responders are a method of automatically replying to incoming email messages. Responders can be set up only for aliases. Whenever anyone sends email to the alias, a prepared reply is automatically returned to the sender.
- Add spam filters (on page 170). Spam filters block unwanted email that originates from outside your site's mail server.

About Your Own Personal Email Accounts

As the Site Administrator, you can immediately send and receive email (on page 144) using your Site Administrator email account.

You can use message forwarding (on page 168) to forward email sent to your Site Administrator account to another email account. This prevents your Site Administrator email from taking up disk space on your site and makes it possible for you to access messages from another account.

However, to take advantage of other email management features and the User Administrator control panel, you need to create a user account for yourself (on page 27). You cannot manage your System Administrator email account through the User Administrator control panel.

After you have created your account, you can log in to the User Administrator control panel (on page 15) to set your personal preferences, such as aliases (on page 161) and responders (on page 165), you want to use for your User Administrator email account.

Setting up Other User Accounts

In this section:

About Adding User Accounts

You add user accounts when you want to create accounts that individuals can use to access services through your site.

These are the types of user accounts you can add:

- Mailbox and service accounts (on page 27)
- FrontPage user accounts (on page 31)
- htaccess user accounts for access to password-protected directories (on page 222)

Adding Mailbox and Service Users

You add mailbox and service user accounts when you want to provide someone with access to your site's services.

After you have added an account, the individual can log in to the User Administrator control panel to send and receive email, manage their contact information, and use services such as FTP, Telnet, and SSH.

Note: To enable a user to publish content to your Web site using Microsoft FrontPage Extensions, your service provider needs to enable FrontPage Extensions for your site. To determine whether FrontPage Extensions is enabled for your site, check the Configuration (on page 64) window. Also, you need to add a FrontPage Extensions user account (on page 31) for the user.

➢ ***To add a mailbox and service user account:***

1 **Optional**: If you are adding many users with similar settings, you can set the User Defaults template (on page 136) to preset the disk quota and services options on the Add User form.
2 Click the **Shortcuts** tab on the Home page.
3 In the shortcuts area, click **Add User** (Users section). The Add User form opens.
4 In the **User Name** field, enter a user name for the Site Administrator.

 Note: This username also becomes the first part of the individual's email address (`<username>@<example.com>`), but you do not need to type the @ symbol or site name in this field.

5 In the **Full Name** field, enter the complete name of the Site Administrator
6 In the **Password** field, enter a password for the Site Administrator.

 Passwords are case-sensitive.

7 Retype the password in the **Confirm Password** field.
8 In the **Disk Quota** field, enter the amount of disk space, in megabytes, you want to reserve for the user. To allow an unlimited amount of disk space, type `0` (zero). To determine how much disk space is available on your site, check the Configuration page (on page 64).

 Note: Be aware that disk quotas are not supported on NFS-mounted servers. If you know your site is on an NFS-mounted server, or if you receive an error in this field when adding an account, type **0** (zero) in this field.

 To determine whether your site is on an NFS-mounted server, contact your service provider.

9 **Optional:** Enable the user's access to any of the following services:

a **Telnet**. If Telnet is available to your site, you can select the **Telnet** check box to allow the user to connect remotely to your site's server using a Telnet connection. Through this connection, users who are comfortable using a UNIX shell environment can log on to your site and search, copy, run scripts, and perform other tasks. To prevent Telnet access, leave the check box blank.

b **CGI**. If CGI service is enabled for the site, you can select the **CGI** check box to enable the user to run CGI scripts.

Note: The CGI scripts for user subdomains will be located in the home directory of the user under the public_html folder.

`/home/<user_name>/public_html/cgi-bin`

To access the CGI scripts from the browser, type

`http://<domain_name>/~<user_name>/cgi-bin/<script_name>`
where:
`<domain_name>` is the domain name of the site on which the subdomain is hosted
`<user_name>` is the user name of the user who owns the subdomain
`<script_name>` is the name of the cgi script

c **SSH Secure Shell**. If SSH (Secure Shell) is available to your site, you can select the **SSH Secure Shell** check box to allow the user to connect remotely to the server using an SSH connection. SSH provides a secure connection through which users who are comfortable using a UNIX shell environment can log on to your site to search, copy, run scripts, and perform other tasks. To prevent SSH access, leave the check box blank.

d **FTP**. If FTP is available to your site, you can select the **FTP** check box to allow the user to use FTP, File Transfer Protocol, to transfer files between their computer and your site. This service is especially useful for individuals who need to upload content to your site and who are not using Microsoft FrontPage to publish content. To prevent FTP access, leave the check box blank.

10 **Optional**: If you want to create a user subdomain, select the **Create a User Subdomain** checkbox, otherwise leave it blank.

Note: A user subdomain is a subdomain that has the same name as the user being added. The subdomain will also, by default, be located in the home directory of the user under the public_html folder. The subdomain directory cannot be changed by the user.

For example, if you enable a user subdomain for the user, `myname`, then the user subdomain will be called `myname` and will be located at `/home/myname/public_html/`

The subdomain can be accessed as `http://myname.example.com`

Important: When you enable a user subdomain, ensure that you have enabled any one of the following services for the user: FTP, Telnet or SSH. If you do not enable any of these services the user will be unable to upload content to the subdomain.

11 Click **Add**. The user account is added.

Be sure to notify the user that the account is ready and briefly explain how to access the account. You might want to provide instructions for accessing services (on page 20) you enabled in addition to providing the login information.

Login information includes:

- The URL of the User Administrator control panel:
  `http://<example.com>/user`
- The user name and password you created for the account
- The user's email address: `<user_name>@<example.com>`
- SquirrelMail login information: `<user_name>@<example.com>`
- Telnet login information

  On a Name-based site:

  `<user_name>@<domain_name.com>`

  or

  `<user_name>#<domain_name.com>`

  On an IP-based site:

  `<user_name>`
- SSH access information

  On a name-based site type:

  `<user_name>@<domain_name.com>`
  or
  `<user_name>#<domain_name.com`
  where `<user_name>` is the User Administrator user name and `<domain_name.com>` is the site name of your site.

  On an IP-based site type:
  `<user_name>`
  where `<user_name>` is the User Administrator user name.
- FTP login information

  On a name-based site:

  `<user_name>@<domain_name.com>`

  or

  `<user_name>#<domain_name.com>`

  On an IP-based site:

  `<user_name>`
- Anonymous FTP login information

  On a name-based site

  `anonymous@<domain_name.com>`

  or

`anonymous#<domain_name.com>`

or

`ftp@<domain_name.com>`

or

`ftp#<domain_name.com>`

On an IP-based site

anonymous or **ftp**

where `<user_name>` is the user name you created for the user and `<example.com>` is the site name of your site.

Adding FrontPage User Accounts

Note: This topic applies to sites with Microsoft FrontPage Extensions enabled. To determine whether you have these services, click **Site Information** (Tools section) in the shortcuts area.

Users can publish content to your Web site directly from their computer using Microsoft FrontPage.

To use this service:

- You need to have FrontPage Extensions enabled for your site
- You need to add FrontPage user accounts for your users
- Users need to have FrontPage installed on their computers

For systems without FrontPage Extensions, users can upload content to the Web server using FTP, Telnet, or SSH (whichever is enabled for the site).

➢ ***To add a FrontPage user account:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (Web Server section). The Manage Users form opens.
3. On the Manage Users form, click **Microsoft FrontPage Extension Permission Management Interface**.
4. On the login form, type your Site Administrator user name and password.

   Note: Unless you change it in the FrontPage Extensions interface, this is the original password of your Site Administrator account. This password does not change when you change your Site Administrator password.

   The FrontPage Server Extensions Web page opens in a new window.
5. In the Users and Roles section, click **Manage Users.**
   The Manage Users form opens.
6. Click **Add a User.**
7. Complete the Add a User form, then click **Add User**.
8. Notify the user of the user name and password you assigned to the account. The user types this user name and password when they open the Web in FrontPage. For more information on opening Webs in FrontPage, see the FrontPage documentation.

Setting up Your Own Account

In this section:

Adding Yourself as a User

If you want to access the User Administrator control panel to manage your own user-level email account, you need to add yourself as a user to the site.

➢ ***To add yourself as a user:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Add User** (Users section). The Add User form opens.
3. In the **User Name** field, enter the name you want to type when you log on to the User Administrator control panel. User names can be up to 40 alphanumeric characters in length, and they cannot contain spaces.

Note: The user name entered here also becomes the first part of your email address, for example `<username>@<example.com>`, but you do not need to type the @ symbol and site name in this field.

1. In the **Full Name** field, enter your first and last names. Names in this field can be up to 40 alphanumeric characters in length, and they can contain spaces.
2. In the **Password** field, enter the password you want to use to log on. Passwords are case sensitive, cannot contain spaces, and have to be at least one character in length. Allowed characters include: a-zA-Z 0-9 , . - _ / + $ ~ : % @ !
3. In the **Confirm Password** field, retype the password.
4. In the **Disk Quota** field, enter the amount of disk space, in megabytes, you want to reserve for yourself. To allow an unlimited amount of disk space, type **0** (zero). To determine how much disk space is available on your site, check the Configuration page (on page 64).

Note: Be aware that disk quotas are not supported on NFS-mounted servers. If you know your site is on an NFS-mounted server, or if you receive an error in this field when adding an account, type **0** (zero) in this field.

To determine whether your site is on an NFS-mounted server, contact your service provider.

4. **Optional**: Enable access to any of the following services:

Note: Your Site Administrator account enables you to log on to all of the services available to your site. If you enable these services for your User Administrator account as well, you can use either account to log in to these services.

a. **FTP**. If FTP is available to your site, you can select the **FTP** check box so you can use FTP, File Transfer Protocol, to transfer files between your computer and your site. This service is especially useful for individuals who need to upload Web pages to your site and who are not using Microsoft FrontPage to publish content. To prevent FTP access, leave the check box blank.

b **SSH Secure Shell**. If SSH (Secure Shell) is available to your site, you can select the **SSH Secure Shell** check box so you can connect remotely to your site using an SSH connection. SSH provides a secure connection through which users who are comfortable using a UNIX shell environment can log on to your site to search, copy, run scripts, and perform other tasks. To prevent SSH access, leave the check box blank.

c **Telnet**. If Telnet is available to your site, you can select the **Telnet** check box so you can connect remotely to your site using a Telnet connection. If you are comfortable using a UNIX shell environment, you can log on to your site through Telnet to search, copy, run scripts, and perform other tasks. To prevent Telnet access, leave the check box blank.

5 **Optional**: If subdomains are enabled for your site, you can upload Web site content to a subdomain. To add yourself as a user of the subdomain, check the **Create a user subdomain** checkbox.

Note: A user subdomain is a subdomain with the same name as the user being added. For example, if you are adding a user, Bob, to your site, `mysite.com`, and if you select the **Create a User Subdomain** checkbox, then a subdomain 'bob' will be created. The subdomain can be accessed as `http://bob.mysite.com`.

For user subdomains, the web content directory defaults to the public_html directory of the user. Thus, the content for the subdomain, bob, will be placed in the directory `/home/bob/public_html/`.

If you want to upload your subdomain content to a directory other than the public_html directory, then you must first add yourself as a user without selecting the **Create a User Subdomain** checkbox, then add a new subdomain (on page 118), and assign ownership to yourself.

---

5 Click **Add**.

Your user account is added. Your account and service login information is listed below. Learn more about accessing services (on page 20).

- The URL of the User Administrator control panel: `http://<example.com>/user`
- The user name and password you created for the account
- The email address: `<user_name>@<example.com>`
- SquirrelMail login information: `<user_name>@<example.com>`
- Telnet login information

  On a Name-based site:

  `<user_name>@<domain_name.com>`

  or

  `<user_name>#<domain_name.com>`

  On an IP-based site:

  `<user_name>`
- SSH access information

On a name-based site type:

<user_name>@<domain_name.com>
or
<user_name>#<domain_name.com
where <user_name> is your User Administrator user name and <domain_name.com> is the site name of your site.

On an IP-based site type:
<user_name>
where <user_name> is your User Administrator user name.

- FTP login information

  On a name-based site:

  <user_name>@<domain_name.com>

  or

  <user_name>#<domain_name.com>

  On an IP-based site:

  <user_name>

- Anonymous FTP login information

  On a name-based site

  anonymous@<domain_name.com>

  or

  anonymous#<domain_name.com>

  or

  ftp@<domain_name.com>

  or

  ftp#<domain_name.com>

  On an IP-based site

  anonymous or **ftp**

  where <user_name> is your user name and <example.com> is the site name of your site.

Changing Your Site Administrator Information

You can change your Site Administrator password and email contact address (on page 36) at any time. You cannot change your Site Administrator user name, however.

For increased security, change your Site Administrator password after you first log on to the Site Administrator control panel and periodically thereafter.

Important: When you change your Site Administrator password, you are also changing the password you use to access email, FTP, Telnet, and SSH as Site Administrator. These services all use the same password and are updated automatically when you change it.

However, if your site uses Microsoft FrontPage Extensions, be aware that the Microsoft FrontPage Administrator password is independent of the Site Administrator password. It is the same initially, but it does not update automatically. You can change the FrontPage Administrator user name or password using the FrontPage Extension Permission Management Interface (on page 139).

➢ ***To change your Site Administrator information:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Change Password** (Tools section). The Edit Site Administrator form is displayed.
3. In the **New Password** field, enter a new password.
4. In the **Confirm New Password** field, retype the password.
5. In the **Administrator Email** field, enter the email address at which you want to receive email notifications.
6. Click **Update**.

CHAPTER 6

Managing DNS Zones

In this chapter:

Introduction to DNS and Name Servers

The Domain Name System (DNS) is the mechanism that translates Internet domain names preferred by users, such as `example.com`, into IP addresses used by computers, such as `10.0.0.1`. This translation is required because the network layer of the Internet uses IP addresses to identify domains; however, Internet users prefer to use names rather than IP addresses. The Internet has 13 special DNS name servers called “root name servers”. The root name servers know the name servers responsible for each top-level domain.

When your computer wants to resolve a name, it sends a request to one of the root name servers asking it to resolve the name. The root name server looks at the top-level domain name, and replies with the name server who is responsible for that top-level domain. Your computer then contacts that name server, which repeats the process, either returning a translation, or returning the identity of a name server who can service the request..

Domain Name Registration

When you want to host a domain with a service provider, you need to let your service provider know the name of your domain along with details of the services that you want to make available on your domain. Your service provider registers the domain name and the About DNS name servers

To perform domain name and IP address translations efficiently, DNS has a distributed architecture composed of many hierarchical DNS name servers. Each DNS name server is responsible for both name-to-IP-address translations (called A forward lookup uses a domain name to find the IP address.) and IP-address-to-name translations (called A reverse lookup uses the IP address to find the domain name.). Each DNS name server manages the lookups for domain name spaces. In DNS, these domain name spaces are referred to as **zones.** The term zone is used to denote information, such as host records, about a domain.

To make a domain or zone accessible to the Internet, the domain name must be registered with at least two **DNS name servers**: a The master name server is the primary server that serves requests for the domain. and a The slave name server provides backup service when the master name server is unavailable. It receives its data for a domain from the master name server. (or backup name server). for the domain with an ICANN-Accredited Registrar and creates the domain. When the domain is created, zones and related zone records required for the domain are automatically created.

Note: You can create zones and records for your site, if your service provider has enabled zone management capability for the site. If enabled, you will see the **DNS** option in the shortcuts section of the Home page.

Further, your ability to manage zones and their records depend on the policy settings configured by your service provider. For example, if your service provider has disabled the add A record setting in the policy file, you will be unable to add A records. Contact your service provider if you want the settings changed.

Managing DNS Zones for Your Domain

If your service provider has enabled you to perform DNS-related actions for your domain, you can:

- View (on page 40) and modify (on page 41) SOA settings for a zone
- View (on page 43) the list of zones
- Add (on page 45), refresh (on page 45), and remove (on page 46) zones
- Add (on page 52), update (on page 50), and remove (on page 51) zone records

View (on page 61) and remove (on page 61) DNS logs For complete information on DNS, the following books are recommended.

- *DNS and BIND*, by Paul Albitz and Cricket Liu, O'Reilly & Associates, 4th Edition, April 2001
- *TCP/IP Illustrated, Volume 1: The Protocols*, by W. Richard Stevens, Addison-Wesley, 1994

Working with SOA Records

In this section:

About SOA Records

Each DNS zone has an SOA record. When you add a zone to a domain, a Start of Authority (SOA) record is automatically created for the zone. This record designates the start of the zone and specifies where in the domain name space the name server has authority. The record also specifies timing information for a zone transfer, which is the process of transferring lookup data from the master name server to the slave server. You can modify the default SOA settings for a zone (on page 41).

Viewing SOA Settings for a Zone

➢ ***To view the SOA settings for a zone:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone whose SOA settings you want to view, and in the **Actions** column, click .
3. In the Start of Authority Configuration section, the SOA settings (on page 41) for the zone are displayed.

SOA Configuration Form

The SOA settings for a zone are as follows:

- **Name Server** (Listed only for zone-specific SOA). The name of the server on which the zone resides.
- **Administrator Email**. The email address of the administrator responsible for the master DNS name server.
- **Refresh interval**. The frequency (how often), in seconds, the slave name server checks with the master name server for updated lookup information.
- **Retry interval**. The frequency (how long), in seconds, a slave server must wait before retrying a failed zone transfer from the master name server. Normally, the retry interval is shorter than the refresh interval.
- **Expire interval**. The upper limit, in seconds, that a slave name server can use the lookup data it currently has before the data expires.
- **Minimum Time To Live**. The length of time, in seconds, the slave name server can cache data.

Modifying a Zone-specific SOA Record

You can modify the SOA record of a zone only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy does not enable you to update the SOA record for the zone. Contact your service provider if you want the settings changed.

➢ ***To modify a zone-specific SOA record:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone whose SOA record you want to modify, and in the **Actions** column, click . The configuration file for the zone is displayed.
3. On the SOA form, click **Edit SOA Configuration**. The Edit Start of Authority (SOA) Configuration form opens.
4. In the **Master Name Server** field, enter the name of your primary DNS name server.
5. Complete the SOA configuration (on page 41) form.
6. Click **Update SOA Configuration**.

Working with DNS Zones

In this section:

About DNS Zones

DNS zones specify the domain name boundaries in which a DNS server has authority to perform name translations. Each zone contains records (on page 48) that specify how to resolve the host names associated with the zone or domain.

Important: If you add records to an alias zone (that is, a zone added to an alias domain), before you remove the alias domain, make sure you manually migrate all the records to another zone.

You can add (on page 45) and remove (on page 46) zones through the Site Administrator control panel.

Viewing the List of Zones

➢ ***To view your existing zones:***

- In the shortcuts section of the Home page, click Zones (DNS section). The Zone List form opens displaying the list of zones in your current DNS configuration. The following information is displayed:
  - Zone Name. The name of the zone.
  - Zone Type. The type of zone. It can be one of the following types:
    - Master. A master zone contains the master copy of data in a zone.
    - Slave. A slave zone is a zone that obtains its data from the master zone.
    - Forward. A forward zone is a zone that transfers lookup requests to the master and slave servers for a domain.
  - Actions. The actions you can perform on any zone.
    - - View (on page 44) the SOA settings.
    - - View (on page 50) the list of records.
    - - Refresh (on page 45) the zone configuration.
    - - Remove (on page 46) zones.

Viewing Zone Information

You can view the zone configuration file and the SOA settings for a zone.

➢ ***To view zone information:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).

2 In the Zone List form, locate the zone for which you want to view details, and in the **Actions** column, click 

. The configuration file for the zone is displayed.

- **Zone configuration**. The configuration information for the zone.
  - **Type.** The type of zone - master, slave, or forward.
  - **File**. The name of the file where the zone information is saved for retrieval at any time.
  - **Allow-update**. Specifies the transaction signature (TSIG) key that is used by the name server to authenticate updates from external servers.
  - **Allow-transfer**. Specifies the host names of the servers that can receive zone transfers from the server.
- **SOA Configuration**. The SOA settings (on page 41) for the zone.

Adding Zones to a Name Server

You can add zones to a name server only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add zones to the name server. Contact your service provider if you want the settings changed.

➢ ***To add a zone to the name server:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).
2 Click **Add Zone**. The Add Zone form opens.
3 In the **Zone Name** field, enter the name of the new zone, for example, **myzone.myname.com**.
4 Click **Add**.

Parallels Pro adds the new zone to your DNS configuration and automatically creates the following DNS records.

- Name server (NS) record (on page 48) specifying the zone's name server. The default is the server on which the zone operates.
- Start of Authority (SOA) record (on page 40) specifying where within the domain name space the name server has authority.

The Zone List is updated with the new entry.

Refreshing Zones

When the data in the master zone file is updated, the copies of the zone file on the slave servers must be updated. To enable updates to happen automatically, the master zone must be configured to propagate changes to the slave zones. This is typically done by configuring the **allow- transfer** attribute in the master zone configuration file. The slave servers authorized to receive updates refresh their copy of zone information when the expiry interval specified in the SOA record for the zone is reached or when they receive an update notification from the master server. Alternatively, you can initiate a zone update when you need to synchronize the master and slave copies.

➢ ***To refresh a zone:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).
2 In the Zone List form, locate the zone you want to refresh and in the Actions column, click . The zone is updated.

Removing Zones from the Name Server

You can remove zones only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy does not enable you to remove zones from the name server. Contact your service provider if you want the settings changed.

➢ ***To remove a zone:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone you want to remove and in the Actions column, click .
3. In the confirmation window, click **OK** to remove the zone.

Parallels Pro removes the zone from your DNS configuration.

Working With DNS Zone Records

In this section:

About DNS Zone Records

DNS zone records specify zone information for the name-to-address translations performed by the domain name server. The Name Server (NS) record for the zone's name server, and Host (A) records for the FTP server and the domain (www) are automatically created for you, but you can add others. You can modify the record information at any time.

Note: If you added records to an alias zone (that is, a zone added to an alias domain), before you remove the alias domain, make sure you manually migrate all the records to another zone.

Another type of zone record, called an SOA record, serves a very specific purpose and is described in the topic About SOA records (on page 40).

The following table describes the supported DNS record types.

DNS Record Types

Use this record:	To specify:
Name Server (NS)	The host name of a DNS server that is authoritative for the domain. **Note**: A DNS zone requires one NS record. If you have only one NS record in a zone, you cannot remove that NS record.
Host (A)	A 32-bit IP address for forward host-name-to-IP-address mapping.
AAAA	A 128-bit IP address for forward host-name-to-IP-address mapping.
Pointer (PTR)	A host name for a reverse IP- address-to-host mapping.

Alias (CNAME)	A mapping between one host name and another. This record tells the DNS server that any requests made to the alias name are to be redirected to the host to which the alias points. The target host does not have to be within the local domain. **Tip:** *Create a Host (A) record before you create the alias.* **Caution!** Do not use a CNAME alias record for a name- based domain, or an NS or MX record.
TXT	Text you want to associate with a host name. You can include SPF-standard compliant text.
SRV	Services available for a domain.
Mail Exchanger (MX)	A mail server other than the SMTP server provided by your service provider. You can specify more than one external mail server. **Tip:** *Create a Host (A) record for the host running your mail server before you create the MX record.*

Viewing DNS Zone Records

When you create a new zone, a Name Server (NS) record is automatically created for the zone's name server and Host (A) records for the FTP server and the domain (www). You can view (on page 50) your zone records from the Host List.

Viewing Existing Records

➢ ***To view existing records:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).

2 In the Zone List form, locate the zone whose host list you want to view, and in the **Actions** column, click . The Host List form opens. It displays all existing records for the zone.

The columns in this form include:

- **Host -** The host name of the DNS zone in which the record resides.
- **Record Type -** The type (on page 48) of DNS record.
- **Data -** The domain name or IP address of the domain on which the zone resides, and additional information specific to a record.
- **Actions -** The column that allows you to update (on page 50) or remove (on page 51) a record.

Updating DNS Zone Records

You can update zone records only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to update zone records. Contact your service provider if you want the settings changed.

➢ ***To modify a DNS record:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).

2 In the Zone List form, locate the zone whose record you want to modify, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.

3 Locate the specific record you want to change and in the **Actions** column, click . The Update form for the specific record opens. For detailed information about specific record fields, see Adding records to a zone (on page 52).

4 Complete the fields and click **Update**.

Removing DNS Zone Records

You can remove zone records from a name server only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to remove zone records. Contact your service provider if you want the settings changed.

➤ ***To remove records from a zone:***

1 In the shortcuts section of the Home page, click **Zones** (**DNS** section).

2 In the Zone List form, locate the zone you want to remove a record from, and in the **Actions** column, click . The Record List form opens. It displays the existing records for the zone.

3 Locate the specific record you want to remove and in the **Actions** column, click .

The record is removed from your DNS configuration.

Adding Zone Records

In this section:

Adding DNS Zone Records

When you create a zone, a Name Server (NS) record for the zone's name server, and Host (A) records for the FTP server and the domain (www), are automatically created. You can add other zone records or modify existing records if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add or modify zone records. Contact your service provider if you want the settings changed.

Note: If you add records to an alias zone (that is, a zone added to an alias domain), before you remove the alias domain, make sure you manually migrate all the records to another zone.

You can add:

- Name Server (NS) records (on page 53)
- Host (A) records (on page 54)
- Reverse Address (PTR) records (on page 56)
- Alias (CNAME) records (on page 57)
- Mail Exchanger (MX) records (on page 58)
- AAAA records (on page 55)
- SRV records (on page 60)
- TXT records (on page 59)

Adding a Name Server (NS) Record

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

Important: Add a Host (A) record (on page 54) before you create the NS record.

➢ ***To add an NS record:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).
2 In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click ☰. The Record List form opens. It displays all existing records for the zone.
3 Click **Add NS Record**. The Update Name Server (NS) Record form opens.
4 **Optional**: If you are creating a subdomain, enter the name of the subdomain in the **Name Server Zone** field; for example, ShoppingMall.acme.east.com.

   Note: You must create the subdomain first, if you intend to use one.

5 In the **Name server** field, enter the host name of the DNS server responsible for the DNS resolution of this subdomain.
6 Click **Add**.

Adding a Host (A) Record

A Host (A) record specifies a 32-bit IP address for forward host-name-to-IP-address mapping.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

➢ ***To add an Host (A) record:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click ☰. The Record List form opens. It displays all existing records for the zone.
3. Click **Add A Record**. The Update Address (A) Record form opens.
4. In the **Host Name** field, enter the name of the host you want to map.
5. In the **IP Address** field, enter the IP address to which the host will map.
6. To automatically create a Reverse Address (PTR) record for the address to which the host maps, select the **Update Reverse Address Record** check box.

   If you do not want to create a Reverse Address record now, you can manually add a Reverse Address (PTR) record for reverse lookup later.

   Important: Before you add a Host Record with the PTR option, you must create the zone (on page 45) to which this record points; otherwise, the reverse pointer record will not take effect.

   ---
7. Click **Add**.

Adding an AAAA Record

An AAAA record specifies a 128-bit IP address for forward host-name-to-IP-address mapping.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

➢ ***To add an AAAA record:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays the existing records for the zone.
3. Click **Add AAAA Record**. The Update Address (AAAA) Record form opens.
4. In the **Host Name** field, enter the name of the host you want to map.
5. In the **IP Address** field, enter the IP address to which the host will map. The IP address must be in the IP version 6 format, for example 1:2f:3:4a:5:6:7:8.
6. Click **Add**.

Adding a Reverse Address (PTR) Record

A Reverse Address (PTR) record specifies a host name for a reverse IP-address-to-host mapping.

Site Administrators acting as Server Administrators for their own domains will need to contact their service provider to find out if in-addr.arpa zones have been delegated to their control. If they have not, they can create PTR records, but they will have no effect. They will need to submit any in-addr.arpa changes to their service provider for the changes to take effect.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

➢ ***To add a PTR record:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.
3. Click **Add PTR Record**. The Update Reverse Address (PTR) Record form opens.
4. In the **Hostname.domain** field, enter the name of the host to which the IP address should map.
5. In the **IP Address** field, enter the IP address you want to map to the host.
6. To automatically create a Host (A) record for the host to which the IP address maps, select the **Update Address Record** check box.

   Note: If you do not want to create a Host (A) record now, you can manually add a Host (A) record for the forward lookup later.

7. Click **Add**.

Adding an Alias (CNAME) Record

An Alias (CNAME) record maps one host to another. The target host does not have to be within the local domain.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

Note: Add a Host (A) record (on page 54) for the source (originating) host before you create the alias.

Caution: Do not use a CNAME alias record for a name-based domain, or an NS or MX record.

➢ ***To add a CNAME record:***

1. In the shortcuts section of the Home page, click **Zones** (DNS section).
2. In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.
3. Click **Add CNAME Record**. The Update Alias (CNAME) Record form opens.
4. In the **Alias.domain** field, enter the name of the source host you want to map to a second host.
5. In the **Target Host Name** field, enter the fully qualified name of the host to which the alias will point.

   Note: The host name must be the fully qualified domain name because the entry does not have to be a member of the local domain.

6. Click **Add**.

Adding a Mail Exchanger (MX) Record

A Mail Exchanger (MX) record specifies a mail server for the domain other than the mail server provided by your service provider. You can designate more than one external mail server for the domain.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

Note: Add a Host (A) record (on page 54) for the host running your mail server before you create the MX record pointing to it.

➢ ***To add an MX record:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).
2 In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.
3 Click **Add MX Record**. The Update Mail Exchanger (MX) Record form opens.
4 Optional: In the **Mail Domain** field, enter the name of the subdomain this mail server will serve; for example, Mall.acme.east.com.
5 In the **Mail Server** field, enter the name of the mail server that will serve your domain.
6 **Optional**: If you are designating more than one external mail server for the domain, use the **Precedence** field to set the delivery priority among the mail servers.

Note: The lower the number in this field, the higher the priority. For example, if you have two mail servers, you could assign a delivery priority of 3 to one server and 4 to the other. Mail would be delivered to the precedent 3 mail server first. If delivery fails there, it would be delivered to the precedent 4 mail server.

7 Click **Add**.

Adding a TXT Record

A TXT record specifies text information that you want to associate with a domain. The text can be a maximum of 255 characters in length.

➢ ***To add a TXT record:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).

2 In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.

3 Click **Add TXT Record**. The Update Text (TXT) Record form opens.

4 In the **Host Name** field, enter the name of the host with which you want to associate relevant text.

5 In the **Text** field, enter the information you want to associate with the host.

6 Click **Add**.

Adding an SRV Record

An SRV record specifies the services available for a domain.

You can add the record only if your service provider has enabled the capability in the DNS policy file. If not enabled, the control panel displays a message stating that the policy settings do not allow you to add the zone record. Contact your service provider if you want the settings changed.

➢ ***To add an SRV record:***

1 In the shortcuts section of the Home page, click **Zones** (DNS section).
2 In the Zone List form, locate the zone you want to add a record to, and in the **Actions** column, click . The Record List form opens. It displays all existing records for the zone.
3 Click **Add SRV Record**. The Update Address (SRV) Record form opens.
4 In the **Service** field, enter the name of the service you want to make available on the host, for example, **POP**.
5 In the **Protocol** field, enter the name of the protocol that the service will use, for example `TCP` or `UDP`.
6 In the **Priority** field, enter a number between 0 and 65535 to indicate the priority at which the target host can be contacted. Low values indicate high priority.

Note: Target hosts that contain the same priority are contacted in the order defined by the **Weight** field.

7 In the **Weight** field, enter a number between 0 and 65535 to indicate the order in which target hosts assigned the same priority can be contacted. The weight value is specified for target hosts that have the same priority and indicates a higher probability of the record being selected. Specify **0** if no record selection is required.

Note: Records with weight greater than 0 have a higher probability of being selected than records with weight 0.

8 In the **Port** field, enter the port number at which the service will communicate with the target host. The port number should be a value between 0 and 65535.
9 In the **Target Host Name** field, enter the domain name of the server on which the service is hosted, for example, `example1.com`.

Note: The name you specify must have one or more address records specified. The name should not be an alias for the host name.

10 Click **Add**.

Managing DNS Logs

In this section:

Viewing DNS Logs

You can view a detailed report of every DNS-related event or action performed on your site if your service provider has enabled the capability while creating the site. If not enabled, the control panel displays a message stating that logging is disabled for the site. Contact your service provider if you want the settings changed.

The following information is displayed:

- **Index**. The unique identifier generated for a log entry.
- **Date**. The date (in yyyy-mm-dd format) when the action was performed.
- **Time**. The time (in hh-mm-ss format) when the action was performed.
- **Action**. The type of action performed, for example *Add zone,* to describe the action of adding a zone.
- **Zone**. The name of the zone on which the action or event is reported.
- **Record Type**. The type of zone record, for example, CNAME.
- **Host Name**. The name of the record.
- **Data**. The domain name or IP address of the domain on which the zone resides, and additional information specific to a record.
- **Actions**. The actions you can perform on the log entry. You can remove the log entries (on page 61) at any time.

Removing DNS Logs

➢ ***To remove a log entry:***

1. In the shortcuts section of the Home page, click **DNS Log** (DNS section).
2. In the **Actions** column of the log entry you want to remove, click ✘.
3. In the confirmation window, click **OK** to confirm the deletion.

C H A P T E R 7

Managing Your Site

In this chapter:

Checking Site Information

In this section:

Checking Your Site's Settings

When you first access the Site Administrator control panel, and periodically thereafter, you might want to check your site's settings and resource allocation for accuracy. Only your service provider can change these settings. If you see an error, contact your service provider to have it corrected.

➢ ***To check your site settings:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Site Information** (Tools section).

The Configuration page (on page 64) is displayed. This page shows your site's current settings. Only your service provider can change these settings.

Configuration Page

The Configuration page shows your site's current settings. These settings are established and maintained by your service provider.

Note: Only your service provider can change your site settings.

➢ ***To get to the Configuration page:***

In the shortcuts section of the Home page, click **Site Information** (Tools section).

On this page you can perform several tasks (on page 64) and view the following information:

- **Site Name**. The site name of your site.
- **Email Contact.** The email address to which your service provider sends notifications about your site. These might include disk usage and bandwidth information.
- **Administrator User Name**. Your Site Administrator user name. You use this name to log on to the Site Administrator control panel and services on your site.
- **Name-based or IP Address**. One of the following:
  - If you have a name-based site, this field displays the IP address of the server on which your site is hosted.
  - If you have an IP-based site, this field displays the actual IP address of your site.
- **Disk Space Used/Allocated.** The amount of disk space (in megabytes) already in use on your site (Used) in comparison to the total amount of disk space available to your site (Allocated).
- **Maximum Number of Users.** The maximum number of users that you can create on your site.
- **Services & Options**. The services and features available to your site, as configured by your service provider. To change your service options, contact your service provider.

  For additional details about services, see accessing and using services (on page 20).

From the Configuration page you can:

Check your site's bandwidth usage (if available). This is displayed toward the top in the Services & Options section. **Used** indicates the amount of bandwidth your site has used during the monitoring period. **Threshold** indicates the upper limit of bandwidth available to your site.

Preview your Web page content. You can preview Web page content from the Configuration page using the **Domain Preview** link in the Services & Options section under Web Server. This link makes it possible to preview Web sites that are too new to be available on the Internet (less than 48 hours old).

Access email through SquirrelMail. You can open SquirrelMail to access your email using the **Email URL** link in the Services & Options section. The link appears toward the bottom of the Configuration page.

Adding Content to your Web Site

In this section:

Default Home Page

When setting up your Web-hosting services, your service provider creates a default home page for your domain. Until you change it, this is the page your visitors see when they go to your site `<example.com>` on the Internet. The file name of this default home page is `index.html`, and it is located on your site in the `var/www/html` directory. The text of the default home page is shown below.

Note: The default home page, index.html, is overwritten (replaced) when you publish content to your Web site (on page 23).

Welcome to <domainname.com>!

This is a place-holder for the DOMAINNAME home page.

If you are the domain owner:

Log on to the Site Administrator control panel to start managing this site (you might want to bookmark this link).

Through the Site Administrator control panel you can:

Set up your site's security and view your site's traffic reports

- Manage your site's user accounts and export/import your site's data
- Set up your site's email services (if enabled for your site)

After you log in, be sure to visit the online Help quick-start guide. It will help you get up and running in no time!

If you are a user account holder:

Log on to the User Administrator control panel to start managing your account (you might want to bookmark this link).

Through the User Administrator control panel you can:

How to Publish Content to Your Web Site

Publishing content to your Web site means creating HTML and other Web pages and placing them on your site so that they can be viewed on the Internet.

Publication Tasks

➢ ***To publish content to your Web site you need to:***

1. Create the Web pages you want to publish (on page 67)
2. Copy your Web pages to your site (on page 68)

3 Check or preview your new Web pages (on page 70)

Creating Content for Your Web Site

Quick-start guide: home (on page **12**) 1 (on page **63**) 2 (on page **36**) 3 (on page **33**) 4 (on page **27**) 5 (on page **25**) 6 (on page **143**) 7

This is the first step in publishing content to your Web site.

Web site content includes HTML pages and other files that can be displayed by browsers. There are many ways to create this content. The easiest way is to use a Web site authoring tool such as Netscape's Composer (which is free and contained in Netscape Communicator and Netscape Navigator browsers), or to purchase and use Microsoft FrontPage or Macromedia Dreamweaver. These tools write HTML code for you, and using them is similar to using a word processor such as Microsoft Word.

As an alternative, you can create Web pages by writing the HTML code yourself in a text editor program such as Notepad. You can find more information about creating Web pages on the Internet by accessing a search engine, such as Google (http://www.google.com) and searching for Web Monkey, CNET Web Builder, HTML Goodies, Yale Web Style Guide, or W3C HTML.

Creating a Home Page

One of the first content pages you need to create is a home page for your site. Your service provider created a default home page (on page 66) for you, and until you change it, this is the page your visitors see when they go to your site, `<example.com>`. The file name of this default page is `index.html`.

When you create your new home page, you should name it `index.html`. When you copy it to your site, it will replace the default index.html page as your home page.

Note: The default home page has links to the Site and User Administrator control panels. If you use the default page to access either of these control panels, be sure to bookmark or otherwise save these links. They will not be accessible after you replace the default home page.

Next step in publishing content:
copy content from your computer to the Web server **(on page 68)**

Copying Your Web Content to the Web Server

Quick-start guide: home (on page **12**) 1 (on page **63**) 2 (on page **36**) 3 (on page **33**) 4 (on page **27**) 5 (on page **25**) 6 (on page **143**) 7

After you have created your content files (on page 67), you can publish them by copying them from your computer to your site. You place your content files in the directory or folder named `html`, which is located on your site in the var/www directory. The path to the directory is `var/www/html`.

To copy files from your computer to your site, you can use any of the following methods. Click any of the following links to learn more about the method.

- The File Manager section of the Site Administrator control panel (on page 68)
- An FTP connection (on page 68)
- FrontPage, a program you can use to edit and publish HTML files (on page 68)

Note: Before you publish content, decide which method you want to use to copy your files to your site. You should avoid going back and forth between these methods because each method manages files, users, and directories differently.

The Site Administrator File Manager

This is the section of the control panel you use to manage the files and directories on your site. When you use this method, you drill down to the appropriate directory, `/var/www/html`, then browse to the files on your computer and copy them from your computer to that directory.

Important: If you are uploading files from a Microsoft Windows system, be aware that the File Manager performs binary transfers; that is, it does not convert Windows text format to UNIX text format. HTML files will not be affected; however, scripts might not work properly when transferred. To ensure that scripts work properly, use an FTP connection (on page 20) to upload script files, rather than the File Manager.

Learn more about using the File Manager (on page 20)

An FTP Connection

When you use this method, you use the FTP (File Transfer Protocol) service to connect to your site and copy the files to the `/var/www/html` directory.

Learn more about FTP connections (on page 20)

Microsoft FrontPage

Microsoft FrontPage is an HTML authoring tool you can use to create and publish Web site content to the `/var/www/html` directory. If your site is configured with Microsoft FrontPage Extensions, you can publish pages to your site directly from FrontPage. To find out whether Microsoft FrontPage Extensions is enabled for your site, check to see if it is listed as enabled on the Configuration page. To learn more about using FrontPage, see the FrontPage documentation.

Replace the Default Home Page

A default home page, named `index.html`, is created for your domain when your site is set up. It is located on your site in the `/var/www/html` directory. Until you replace it, this is the page your visitors see when they go to your site `<example.com>`. Show me the default home page (on page 66).

Note: The default home page has links to the Site and User Administrator control panels. If you use the default page to access either of these control panels, be sure to bookmark or otherwise save these links before replacing the page. They will not be accessible after you replace the page.

You can either continue to use the default home page or create a new one and copy it to your site as described above. Make sure your new home page is named `index.html` and placed in the /var/www/html directory.

Note: The Web server is set up to use the index.html page in the `/var/www/html` directory as the home page of your site.

If you have completed these steps successfully, you are ready to proceed to the next step and preview your new Web content.

Next step in publishing content: Previewing your Web content **(on page 70)**

Previewing Web Page Content

Quick-start guide: home (on page **12**) 1 (on page **63**) 2 (on page **36**) 3 (on page **33**) 4 (on page **27**) 5 (on page **25**) 6 (on page **143**) 7

After you have copied your Web page content to your site (on page 68), you can preview it in a browser.

➢ ***To preview your home page:***

In the address field of a browser program, type your site name. For example:

`http://<domain_name.com>/`

where `<domain_name.com>` is your site name.

➢ ***To preview other pages or files:***

- In the address field of a browser program, type your site name followed by / and the new file name. For example:

`http://<domain_name.com>/<filename>`

- where `<domain_name.com>` is your site name and `<filename>` is the name of the page you want to preview.

Note: If you have had your site name for more than 48 hours and cannot access it over the Internet, contact your site name registrar to make sure the DNS information for your site is correct. If your site is less than 48 hours old, you can preview it as described below.

Previewing the Content of New Domains

If your site is less than 48 hours old, the DNS information for the site might not have had time to propagate to all servers on the Internet, and your site might not be available for general viewing. However, you can still preview the content and CGI scripts (on page 73) used on your domain.

➢ ***To preview the content of a new domain:***

In the address field of your Internet browser, enter the following URL:

`http://<server_IP_address>/~admin<#>`

where:

- `<server_IP_address>` is the IP address of the control panel server on which your site is hosted, and
- `#` is the site preview number.

Note: The site preview number is assigned when your service provider sets up your site. The number appears in the Web server section of the Configuration page.

Quick-start guide: home (on page **12**) 1 (on page **63**) 2 (on page **36**) 3 (on page **33**) 4 (on page **27**) 5 (on page **25**) 6 (on page **143**) 7

Using CGI Scripts

In this section:

About CGI Scripts

CGI (Common Gateway Interface) scripts are small programs used on many Web sites.

These programs are written in a computer language such as Perl, Tcl, C or C++, and they function between HTML pages and other programs on the Web server. For example, a CGI script could allow search data entered on a Web page to be sent to a database for lookup. It could also format the results of that search as an HTML page and send it back to the requester.

CGI scripts reside on your site, and they obtain data using environment variables (on page 73) that the Web server makes available to them.

For additional information about CGI scripts, see:

- Uploading and running CGI scripts (on page 72)
- Environment variables (on page 73)

Uploading and Running CGI Scripts

You can upload and run CGI scripts to make your site interact with databases and other applications.

➤ ***To upload and run a CGI script:***

1 Write or obtain the CGI script.

Note: If you are writing a script that sends out email, make sure to include a valid email address in the **From** field header; otherwise, all replies are returned to the Web server and becomes unavailable to you.

2 Copy the script to the CGI directory on your site. If you are unsure of the name of your CGI directory, check the Configuration page. You can derive your CGI directory name from the Script Alias listed on the Configuration page. For example, if your script alias is `cgi-bin`, then your CGI directory name is `/var/www/cgi-bin`.

Important: If you are on a Microsoft Windows system, you need to upload CGI scripts to your site through an FTP connection instead of through the File Manager. Further, when you upload through FTP, upload files as ASCII, so that hidden characters inserted into the CGI script by Windows are translated correctly. If these characters are not translated correctly, the CGI scripts do not work.

If you are on a Linux system, you can upload CGI scripts to your site through the File Manager. Linux does not add hidden characters to files, so no translation is needed.

3 Change the CGI script file permissions (on page 211) to the following settings:

- **Owner:** Allow Read, Write, and Execute
- **Group:** Allow Read and Execute
- **Others:** Allow Read and Execute

4 Open your Internet browser and in the a**ddress** field, enter the following URL:

```
http:// <web_server_name>/<script alias>/<script name>
```

Your CGI script runs. The results appear in the browser window.

Environment Variables Used with CGI Scripts

Environment variables are used in CGI scripts (on page 71) to represent information that is updated by the Web server when the scripts run. Using environment variables, scripts can get and use up-to-date information without having to store that information themselves.

In addition to the standard environment variables, the following three environment variables are available to all scripts on your site:

- `SITE_ROOT`. The root path of your site
- `SITE_CGIROOT`. The top level CGI path of your site
- `SITE_HTMLROOT`. The top level HTML CGI path of your site

You can use these variables in your CGI scripts to avoid hard-coding directory path names. This ensures that path names are always correct, even if those path names change.

Previewing CGI Scripts

➢ ***To preview CGI scripts (on page 71) used on your site:***

In the address field of your Internet browser, enter the following URL:

```
http://<server_IP_address>/<domain_name>.com/
<ScriptAlias>
```

where:

- `<server_IP_address>` is the IP address of the server on which the control panel is hosted
- `<domain_name>` is the fully qualified name of the domain
- `<ScriptAlias>` is the CGI script directory for the domain.

Securing Your Site

In this section:

About Site Security

Your service provider configures the security environment for your site. Depending on the security level assigned to the site, certain services for the site run in protected mode within the restricted environment of the site's file system, technically referred to as a chrooted environment. This prevents you and the site users from accessing data or resources pertaining to other sites on the server.

Your site can be configured for one of the following security levels:

- High security
- Medium security
- Low security

To find out the security level assigned to your site, contact your service provider.

High Security

High security runs certain services, that are vulnerable to security breaches, inside the restrictive environment of the site's file system.

The services that are secured are:

- CGI scripts
- Telnet/Secure Shell
- mod_perl/mod_php

CGI Scripts

CGI scripts can present security loopholes in two ways:

- They can reveal information about the host system thus enabling hackers to break into the system
- When the scripts process remote user input, such as the contents of a form, they become vulnerable to remote exploits that subvert the scripts to run potentially destructive commands

High security places CGI scripts inside the restrictive part of the site's file system.

Important: High security poses problems if the CGI scripts used by the site source required libraries or configuration files from outside the site's file system, in which case, the necessary files must be copied across to the site's file system.

For example, if a CGI script uses Perl, then all the Perl libraries and configuration files must be copied into the CGI directory.

Telnet/Secure Shell

Remote login services like Telnet or SSH allow users to interact with remote computers on the Internet. They can expose your system to denial-of-service attacks and enable hackers to run subversive code.

High security locks remote user logins (administrator and users of the site) to the restrictive environment of their home directories. When you or any of the site users connect to the site, you are directly logged in to the home directory of your site, preventing view or access to any system-wide resources from the site's operating environment.

mod_perl/mod_php

mod_perl and mod_php are modules that allow users to run scripts on the Web server, thus exposing your Web server to potential exploits.

High security disables the mod_perl and mod_php services for a site. Scripts using mod_perl or mod_php cannot be run on the site.

Important: In high security sites, the `.pl` (Perl) files located at `/var/www/perl` and the `.php` files are run as CGI processes. However, in medium and low security sites, the `.php` files are managed by mod_php and the `.pl` files located at `/var/www/perl` are managed by mod_perl. To take advantage of the full capabilities of these services, you must opt for medium or low security. To have your security level reset, contact your service provider.

Medium Security

Medium security offers a loosely knit security environment wherein remote login services are secured, but CGI scripts run in a vulnerable environment.

The following services are secured.

- CGI scripts
- Telnet/Secure Shell
- mod_perl/mod_php

CGI Scripts

CGI scripts are not locked into the site's file system. This compromises security but eliminates file sharing constraints posed by secured CGI scripts.

Telnet / Secure Shell

Telnet and SSH services are secured as in high security. Remote user logins (administrator and users of the site) are restricted to the protective environment of the site's file system.

mod_perl / mod_php

mod_perl and mod_php services are enabled for the site. Your site can run scripts using mod_perl or mod_php.

Low Security

Low security provides an open operating environment. You can share or access files (depending on file access privileges) residing on the server. Users of your site are, however, restricted to the home directory of the site.

Your site is also enabled to run mod_perl and mod_php scripts.

None of the following services are secured for the site.

- CGI scripts
- Telnet/Secure Shell
- mod_perl/mod_php

CGI scripts

While CGI scripts reside within the site's file system, the administrator of the site can access or share system wide resources outside the cgi-bin directory.

Telnet / Secure Shell

With low security, administrators can use the Telnet or SSH remote login service to traverse the file hierarchy outside the site's home directory. Users, however, are restricted to the home directory of the site.

Note: For IP-based sites, remote access, using the Telnet service, is locked into the site's file system. When the Site Administrator or the site users connect to the site they are logged directly into their home directory. To override this limitation, Site Administrators need to connect to the control panel server on which the site is hosted. To connect to the server, contact your service provider for the IP address or host name of the server and then log in with the user name <user_name>@<site_name>.

---

mod_perl / mod_php

mod_perl and mod_php services are enabled for the site enabling site users to run scripts using these applications.

About SSL Certification

If you store sensitive data, such as customer profiles, on your site, you can secure your site by obtaining a Secure Sockets Layer (SSL) certificate.

Note: SSL certificates are available to IP-based domains only; you cannot obtain an SSL certificate for name-based domain.

SSL is a protocol that transmits private documents through the Internet. It creates a secure connection between a client and a server over which data can be sent securely. SSL works by using a private key to encrypt data transferred over the SSL connection.

SSL certificates are available from a Certificate Authority (CA), such as VeriSign®.

➢ ***To secure your domain:***

1. Generate an SSL certificate request (on page 79)
2. Request a certificate from a Certificate Authority (CA) (on page 80)
3. Load the SSL certificate onto your domain (on page 81)
4. Restart the Web server (on page 81)

Generating an SSL Certificate Request

This is the first step in securing your IP-based site.

Note: Name-based sites cannot use SSL certificates.

➢ ***To generate a certificate request:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Generate SSL Certificate** (Web Server section). The Generate SSL Certificate form opens.
3. In the **2-Letter Country Code** field, enter the international abbreviation for the country in which your business resides.
4. In the **State/Province** field, enter the complete name of the state or province in which your business resides. Do not abbreviate the state; spell it out.
5. In the **City** field, enter the complete name of the city in which your business resides.
6. In the **Company** field, enter the name of your business.
7. In the **Organization** field, enter the type of industry in which your company does business.
8. In the **Common Name** field, enter the site name of your business (without the www prefix).
9. In the **Email** field, enter the email address of the person who will receive the SSL certificate.

   Note: Once the certifying authority (for example, Verisign) approves the request for a SSL certificate, you will receive the SSL certificate at the specified email address from the certifying authority.

10. Click **Generate Certificate.**

    The SSL window displays a new certificate request in encrypted form.

Next step in securing your site:

Requesting a certificate from a Certificate Authority (on page **80**).

Requesting a Certificate from a Certificate Authority

This is the second step in securing your IP-based site. Before you perform this step, you need to have generated a certificate request (on page 79).

Note: Name-based sites cannot use SSL certificates.

➢ ***To request a certificate from a Certificate Authority:***

1. Generate an SSL certificate request (on page 79) if you have not done so already.
2. Copy the encrypted request onto your local system clipboard.
3. Open another Internet browser window, and go to the Web site of the Certificate Authority you want to use, for example, VeriSign.
4. On the Certificate Authority's Web site, follow the instructions for submitting the encrypted certificate request. Since you have copied it to your clipboard, you can paste the request directly into the appropriate window.
5. The Certificate Authority will send you an SSL certificate, usually through email.

Next step in securing your site:

Loading the certificate onto your site **(on page 81)**

Uploading the Certificate on Your Domain

This is the third step in securing your IP-based site. Before you complete this step, you need to have generated a certificate request (on page 79) and requested a certificate from a Certificate Authority (on page 80).

Note: Name-based sites cannot use SSL certificates.

➢ ***To load the certificate:***

1 Generate the certificate request (on page 79) and request a certificate from a Certificate Authority (on page 80) if you have not done so already.

2 Open the email from the Certificate Authority, and copy the contents onto your local system into a text editor program, such as Notepad.

3 Once you have copied the contents into a text editor program, leave the program open on your desktop.

4 Start a browser and log in to the Site Administrator control panel.

5 Click the **Shortcuts** tab on the Home page.

6 In the shortcuts area of the Home page, click **Import SSL Certificate** (Web Server section). The Save SSL Certificate window opens.

7 Copy the certificate information from the text editor program, then paste it into the **Server Certificate** text box.

8 Copy the intermediate certificate information from the text editor program, then paste it into the **Intermediate Certificate** text box. This is an optional field, and can be left blank if the utility does not provide you the certificate.

9 Click **Import**.

10 To enable security for your site, you must have your service provider restart your site's Web server (on page 81).

Your site is not secure until your service provider notifies that your site's Web server has been restarted.

Restarting Your Site's Web Server

Some tasks, such as loading a security certificate to secure a site, require that your site's Web server be restarted. Restarting the Web server means physically turning the server off, then turning it back on.

To restart your site's Web server, contact your service provider; the Web server cannot be restarted from the Site Administrator control panel.

Managing Your Web Server

In this section:

About the Web Server

The Web server is a computer running a Web server software application that enables it to respond to requests received from browsers. Every Web server has an IP address and a domain name. For example, if you enter the URL, `http://www.example.com/index.html` in your browser, this sends a request to the server whose domain name is *example.com*. The server then fetches the page named index.html and sends it to your browser.

Web server management tasks include:

- Viewing your Web server settings (on page 83)
- Viewing your Web server log reports (on page 84)
- Securing your domain using SSL Certification (on page 78)
- Setting up protected directories on the server (on page 219)
- Creating the groups for protected directories (on page 222)
- Managing the users in protected directory groups (on page 226)
- Accessing the Microsoft FrontPage administration interface (if enabled)
- Managing WebDAV user accounts (on page 140)

About Web Server Log Files

Web server log files can be helpful in forecasting possible marketing trends and monitoring your Web site for problems with visitor access.

The Web server provides two log files, CustomLog and ErrorLog.

CustomLog

This report contains information about visitors to your Web site. Every time a visitor accesses your Web site, a line of text containing details about the visitor and the nature of the request is written to this log file.

ErrorLog

This report contains information on errors encountered by visitors accessing your Web site. This information can be valuable for analyzing server problems or problems with specific Web pages.

How to access Web server log files (on page 84)

Viewing Web Server Settings

Web server settings include the name of the Web server, the name of the administrator who manages the Web server, and information about directories on the Web server. Only your service provider can change these settings.

➢ ***To view the Web server settings:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Configuration** (Web Server section).

   Information on this form includes:

   - **Server Name.** The full name of the Web server.
   - **Server Administrator.** The email address of the person who manages the Web server.
   - **DocumentRoot.** The directory in which your site's Web-related files are located.

Viewing Web Server Log Files

The Web server log files provide information about the Web server. You can view the files directly from the Site Administrator control panel, or download them to your local system for viewing.

➢ ***To view the log reports:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Log Files** (Reports section).
3 Choose the type of file you want to read. File types include CustomLog (on page 83) and ErrorLog (on page 83).
4 In the **Actions** column of the file you want, click **Download**.
5 To view the reports, do one of the following:
   a Click **Open** to view the reports directly from the control panel.
   The Open With window opens prompting you to select a program with which to view the log report.
      - Select **WordPad** from the Program list.
      - Click **OK**.
      The log report opens in WordPad.
   b Click **Save** to download the reports to your local system before viewing them. The log report is saved to the specified location.

Web Server Plugins

If your service provider enables it for your site, you can use the mod_perl plugin for the Apache Web server. The Apache/Perl integration project brings together the full power of the Perl programming language and the Apache HTTP server.

Advantages of mod_perl:

- Writes Apache modules entirely in Perl
- Save the overhead of starting an external interpreter, i.e. the penalty of Perl start-up time
- Allows you to easily do things that are more difficult or impossible in regular CGI programs,such as running sub requests
- Allows you to have full access to the inner workings of the Web server and can intervene at any stage of request-processing

Viewing Site Usage Reports

In this section:

Checking Bandwidth Usage

Bandwidth usage reports quantify the amount of network traffic experienced by your site. You can use the information from bandwidth reports for your billing and resource allocation needs.

Note: If your site is new, you may have to wait a few minutes before bandwidth statistics become available. Also, no statistics are available until there is traffic on your site. The information is updated every 2 hours.

➢ ***To view your site's bandwidth usage:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Site Traffic** (Reports section).

The Bandwidth Reports (on page 86) window opens.

Bandwidth Reports Page

The Bandwidth Reports page shows your site's bandwidth usage, by service, from the start of the monitoring period to the current day.

Note: If your site is new, you may have to wait a few minutes before bandwidth statistics become available. Also, no statistics are available until there is traffic on your site. The information is updated every 2 hours.

➢ ***To get to the Bandwidth Reports page:***

1 Click the **Shortcuts** tab on the Home page.

2 Click **Site Traffic** (**Reports** section) in the shortcuts area.

On this page you can perform several tasks and view the following information:

In the Bandwidth Usage Reports section:

- **View monthly Reports**. A list of the past reports available for your site.

In the Summary <*monitoring period start and end dates*> section:

- **Bandwidth (Entire Site).** A bar graph that shows the bandwidth used (darker shade) and the bandwidth available (lighter shade).
- Statistics Last Updated. The date (in yyyy/mm/dd format) on which the bandwidth usage report was last updated.
- **Total Used Bandwidth.** The bandwidth (in megabytes) your site used during the selected month.
- **Allowed Quota.** The maximum bandwidth (in megabytes) allocated to your site for the selected month.

Note: If your site exceeds the bandwidth quota threshold, which is determined by your service provider, an email notification is sent to the Site Administrator's email address (on page 36).

- **Available Quota.** The amount of bandwidth, in megabytes, that is unused and available to the site. This amount is the difference between the bandwidth allocated to the site and the bandwidth the site has used.

Usage Breakdown for Services for <*site name*> <*monitoring period*>

The columns in this section include:

- **Service.** The name of the service using bandwidth on your site. Bandwidth usage is reported for the following services.
  - **HTTP** - Quantifies bandwidth consumed by traffic on your HTTP server.
  - **HTTPS** - Quantifies bandwidth consumed by traffic on your HTTPS server.

Note: The Header information for both HTTP and HTTPS is reported separately so that the HTTP and HTTPS usage information corresponds to the statistical data provided by log analyzers.

- **FTP** - Quantifies bandwidth consumed by traffic on your FTP server.
- **IMAP** - Quantifies bandwidth consumed by traffic on your IMAP server.
- **POP3** - Quantifies bandwidth consumed by traffic on your POP3 server.
- **SMTP** - Quantifies bandwidth consumed by traffic on your SMTP server.
- **SSH** - Quantifies bandwidth consumed by traffic on your SSH server.
- **Telnet** - Quantifies bandwidth consumed by traffic on your Telnet server.
- **Other Services** - Quantifies bandwidth consumed by traffic on custom configured servers.

Note: If you have configured a service distinct from any of the above-mentioned services, it is qualified as “Other Services”. For example, if you have configured a service, RSH, bandwidth consumed by traffic on this server will be classified as other services.

- **All Services** - Cumulative bandwidth usage statistics for all of the above-mentioned services.

- **Usage.** A bar graph showing how much incoming and outgoing network traffic is on your site.
- **Incoming (MB).** The bandwidth, in megabytes, used by the service for incoming network traffic.
- **Outgoing (MB).** The bandwidth, in megabytes, used by the service for outgoing network traffic.
- **Total (MB).** The total bandwidth, in megabytes, used by the service.
- **% of All.** The total bandwidth, shown as a percentage, used by this service in comparison to other services.

On this page you can:

- View past bandwidth usage reports by clicking the arrow in the View Monthly Reports list, then selecting a time period.

  The time periods are based on the bandwidth monitoring cycle, which is established by your service provider.

Analyzing Server Logs

In this section:

About Log Analysis

Every server comprises a repository of actions and events that occur on the server. This repository is called the “Logs” directory and contains a raw log file called “Log”. This file contains raw information (information that is not formatted or analyzed; simply plain statistical data) that quantifies user traffic on your Web and FTP servers, and is updated on a nightly basis.

Intelligent analysis of this data provides a statistical baseline that can be used to determine server load, failed requests and other events that illustrate site usage patterns. This information can be distilled to provide valuable leads on marketing and site management.

A typical log report conveys the following:

- The number of requests received by your server
- The date and time when the request was made
- The pages or files requested
- The address of the requesting host
- The page from which a user visited your site
- The last page viewed by a user on the site

You can use any of the following log analysis tools to analyze your Web and FTP server logs.

- Webalizer (on page 89)
- Analog (on page 96)
- AWStats (on page 101)

Using Webalizer to Analyze Server Logs

In this section:

About Webalizer

Webalizer is a log file analysis tool. Webalizer generates highly detailed usage statistics for Web and FTP servers in easily comprehensible graphical and tabular formats. The logs generated are a statistical encapsulation of user traffic on your site.

The reports are generated in accordance with the configuration options set for Webalizer by your service provider.

Webalizer reports are generated at a scheduled time, the settings of which are configured by your service provider, but you can override these settings to generate a report at any time using the Generate Reports (on page 95) option.

Note: You can change the behavior of Webalizer reports for your site by configuring (on page 93) Webalizer from the command line interface. You can not reconfigure Webalizer from the Site Administrator control panel.

Features of Webalizer

1 Fast processing of log files

Log files, over a period of time, grow to very large sizes. A relatively small Web site that has several thousand visitors a month accumulates approximately 25 megabytes of log files per month. Most log file analysis tools are slow, processing the log files at speeds of only 2-3 megabytes per minute. Webalizer can be very fast; on a 200Mhz pentium machine, over 10,000 records can be processed in one second, with a 40 Megabyte file taking roughly 15 seconds (over 150,000 records).

2 Portable

Webalizer is compatible with a range of hardware configurations (Intel x86, Power PC, Sparc, Mips4) and operating systems (Linux, Solaris, OS/2) and can be easily ported from one system to another.

3 Configurable reports

Webalizer can be configured with custom options at any time by modifying the respective Webalizer configuration file (Web/FTP).

4 Incremental processing of logs

Incremental processing of logs enables large log files to be split up into multiple files for processing, without any loss of data.

Supported log formats

Server logs follow defined standards in the way information is stored in a log file.

Webalizer supports the following log formats.

1 Common Log File (CLF) format

The CLF format specifies data such as the machine name or IP address from which the user made the request, as well as the information on the resource requested. This is the most commonly used format.

2 Combined log format

An extension of the Common Log File format, with additional information on referrals, user agents and cookies.

3 Xferlog format

The xferlog format is generated by the wu-ftpd and contains information on inbound and outbound requests.

4 Squid proxy logs

Squid logs record access information, system configuration errors and resource consumption (eg, memory, disk space).

Report generation

Webalizer provides Web and FTP log reports in HTML format that can be viewed with any browser. It provides a highly detailed report of the activity on your server, manifest in a variety of reports (on page 91). Webalizer reports are generated in accordance with the schedule and report settings configured for your site by your service provider.

Note: To generate a report as and when needed, you must override the schedule settings (set by your service provider) using the Generate Reports (on page 95) option.

About Webalizer Reports

Webalizer provides Web and FTP log reports in HTML format that can be viewed using any browser.

Web Server log report

The Web server log report shows the usage pattern recorded on your Web server. The report provides detailed graphical and columnar representation of usage information.

FTP Server log report

The FTP server log report shows the usage pattern recorded on your FTP server. The report includes detailed graphical and columnar representation of usage information.

Note: You cannot perform a combined analysis of Web and FTP logs. They must be analyzed separately.

Types of Report

Webalizer produces several types of reports in HTML format.

The reports generated by Webalizer are:

- **Usage summary**

  This graph provides the following information:

  - Pages/Files/Hits: Indicates the requests the site has served
  - Visits/Sites: Indicates the requests the site has received
  - KBytes: Indicates in KBytes the amount of data sent by your server

- **Summary by Month**

  The Summary by Month report shows the daily average, monthly total and the grand total of user traffic on the site. The months listed in the report are linked to a comprehensive monthly report that provides detailed statistical information (for Web and FTP server) about user traffic for the month.

About Log Report Captions

The tabulated list below explains the various captions used in the Webalizer log reports.

Caption	Desription
Hits	The total number of requests received by the server during a given time period (month, day, hour). A hit is an incoming request. **Note:** Any request (request for html pages, cgi scripts, graphics, audio files) qualifies as a hit.
Files	The total number of hits (requests) that resulted in files being sent to the user. A file is an outgoing response. **Note**: Not all hits will send data: some hits may result in 404-Page not found errors, some hits may be served from the browser's cache. The difference between hits and files gives an estimate of repeat visitors. The greater the difference between the two, the more people are requesting pages they have cached (have viewed already).
Pages	A page request made to the Web or FTP server for the first time. If the same sites continues to make requests to your server within a given duration (time-out or active session), they will not be counted as separate visits. If the active session times out since the last request made by the site, then the subsequent request will be logged as a separate visit. **Note**: Only actual pages (.htm, .html, .cgi) will qualify as a visit, visits as a result of links to graphic, audio or any non-page URLs will not qualify as a visit.
Sites	The number of unique IP addresses or hostnames that made requests to your Web or FTP server. **Note:** This number may not be give an accurate representation of the visitors to your server, as many users may appear to come from a single site as in the case of name based sites.
Kbytes (KB)	The amount of data transferred from the Web or FTP server to the requesting host. One KB is equivalent to 1024 bytes.

Configuring Webalizer for Sites

Webalizer reports must be configured from the command line interface. You can not configure Webalizer using the Site Administrator control panel.

Webalizer reports are generated in accordance with the options set in the Webalizer configuration file. The configuration file is called `webalizer.conf` and placed in the respective Webalizer directories (Web/FTP) inside the file system of the site.

You can modify the configuration options to change the default behaviour of Webalizer reports.

➢ ***To change the configuration information:***

1 Connect to your site using the Telnet or SSH remote login service.

Important: To use Telnet or SSH, your service provider must enable Telnet or SSH remote login services for your site. SSH is recommended as a secure remote login service.

- If you are using the SSH service, type the following at the command line prompt.

  `ssh` ***<username@sitename>***

  For example, if you have the user name, myname, for the site, mysite.com, then type, `ssh myname@mysite.com`

- If you are using Telnet, type the following:

  `telnet mysite.com`

2 Enter your user name and password, when prompted.

3 Browse to the `/etc/webalizer` directory, and locate the Webalizer configuration file, `webalizer.conf`.

- To locate the configuration file for the Web server, type the following:

  ```
  cd /etc/webalizer/Web
  ls
  ```

- To locate the configuration file for the FTP server, type the following:

  ```
  cd /etc/webalizer/ftp
  ls
  ```

  You will find the webalizer.conf listed.

4 Open the configuration file by using a text editor of choice.

  ```
  vi webalizer.conf
  ```

The configuration file opens. Each option is preceded by a detailed description of the option.

Note: When you modify the configuration file, do not change the default output directory, `outputdir` (where the Webalizer reports will be located), otherwise the reports will not be visible from the Site Administrator control panel.

5 Change the configuration options as needed.

6 To save the changes and exit the configuration file, type the following command.

```
:wq
```

To view the report, Generate a report (on page 95).

Viewing Web Server Log Report

➢ ***To view the Webalizer report for your Web server:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Webalizer Reports** (Reports section).

3 On the Webalizer Reports page, if not already selected, click **Web Server** to view the Webalizer report for your Web server.

Note: If server logs have not yet been generated, no report is generated; you will find the following message, `Could not get requested site report because Web Server logs have not yet been generated`.

You can generate a report, by forcing generation of server logs. See Generating reports (on page 95) to generate a report.

In the Usage Statistics area, the following reports are displayed:

a Usage Summary for the site (on page 91)

This report is a graphical depiction of site usage summary obtained from the server logs of the past 12 months.

b Summary by Month (on page 91)

This report is a columnar statistical synopsis of the Web server usage for the past 12 months. The months are linked to more detailed reports on the Web server logs.

Viewing FTP Server Log Report

➢ ***To view the Webalizer report for your FTP server:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Webalizer Reports** (Reports section).
3 On the Webalizer Reports page, click **FTP Server** to view the Webalizer report for your FTP server logs.

Note: If server logs have not been generated, no report is generated; you will find the following message, `Could not get requested site report because FTP Server logs have not yet been generated`.

You can generate a report, by forcing generation of server logs. See Generating reports (on page 95) to generate a report.

In the Usage Statistics area, you will find the following reports.

a Usage Summary for the site (on page 91)

This report is a graphical depiction of site usage summary obtained from the server logs of the past 12 months.

b Summary by Month (on page 91)

This report is a columnar statistical synopsis of the FTP server usage for the past 12 months. The months are linked to more detailed reports on the FTP server logs.

Generating Reports

By default, Webalizer reports are generated only when Webalizer runs at the scheduled time, the settings of which are configured by your service provider. The Generate Reports option enables you to generate reports as and when required.

➢ ***To generate reports:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Log Manager** (Web server section).
3 Review the rotation configuration and click **Rotate**.

Note: When you click Rotate, a request is submitted to the control panel. The control panel processes these requests every 10 minutes and updates your report.

4 Click the **Shortcuts** tab on the Home page.
5 In the shortcuts area of the Home page, click **Webalizer Reports** (Reports section).
6 Choose the type of report you want to view:
   - Click **Web Server** to view the Web Server Webalizer report (on page 94).
   - Click **FTP Server** to view the FTP Server Webalizer report (on page 95).

Using Analog to Analyze Server Logs

In this section:

About Site Usage Reports

From time to time, it is useful to check the performance of your Web and FTP servers to be sure Web site visitors are not encountering access problems and also to gauge the success of your Web site. Statistical activity reports are available for both the Web server (on page 99) and the FTP server (on page 100).

You can view reports from the Sites Report Manager. Reports are run once per day. For new sites, the first report becomes available after 24 hours.

Site usage reports provide the following information:

- General Summary (on page 97)
- Monthly Summary (on page 97)
- Daily Summary (on page 97)
- Hourly Summary (on page 97)
- Domain Report (on page 97)
- Organization Report (on page 97)
- Host Report (on page 97)
- Directory Report (on page 97)
- File Type Report (on page 97)
- Browser Report (on page 97)
- Failures Report (on page 97)

Site Usage Report Types

The following types of site usage reports are available:

- General Summary
- Monthly Summary
- Daily Summary
- Hourly Summary
- Domain Report
- Organization Report
- Host Report
- Directory Report
- File Type Report
- Browser Report
- Failures Report

General Summary

The General Summary shows overall statistics about the traffic on your Web site during the period you specified.

Statistics include:

- **Total Requests.** The total number of files downloaded, including graphics.
- **Total Page Requests.** The number of pages downloaded.
- **Total Bytes Served.** The total amount of data transferred, in bytes.

Failed Requests. The number of failed requests.

- **Distinct Hosts Served.** The number of unique computers from which requests have come.
- **Distinct Files Served.** The number of unique files requested.

Monthly Summary

The Monthly Summary shows the number of requests and the number of pages requested for each month over the time period specified. The summary also shows the months that your Web site had the most traffic. The number of requests and the number of pages requested are expressed as a percentage of the entire amount shown for all months.

Daily Summary

The Daily Summary shows the number of requests and the number of pages requested for each day of the time period specified. The summary also shows the days on which your Web site had the most traffic. The number of requests and the number of pages requested are expressed as a percentage of the entire amount shown for all days.

Hourly Summary

The Hourly Summary shows the number of requests and the number of pages requested for each hour of the day over the time period specified. The summary also shows the hours during which your Web site had the most traffic. The number of requests and the number of pages requested are expressed as a percentage of the entire amount shown for all days.

Domain Report

The Domain Report shows the countries of the host systems that visited your Web site. It lists the host IP addresses and notes when the address was not resolved. The report also shows the countries from which you received the most traffic on your Web site. The statistics include the number of requests and the number of pages requested, expressed as a percentage of the entire amount shown for all countries.

Organization Report

The Organization Report shows the organizations (such companies, institutions, service providers) under which the host machines that visited your Web site were registered. It lists the organization IP addresses and notes when the address was not resolved. The report also shows the organizations from which you received the most traffic on your Web site. The statistics include the number of requests and the number of pages requested, expressed as a percentage of the entire amount shown for all organizations.

Host Report

The Host Report shows the host machines that visited your Web site. It lists the host IP addresses and notes when the address was not resolved. The report also shows the hosts from which you received the most traffic on your Web site. The statistics include the number of requests and the number of pages requested, expressed as a percentage of the entire amount shown for all hosts.

Directory Report

The Directory Report shows the directories the requested files came from. The report also shows the directories serving the most file requests. The statistics include the number of requests and the number of bytes retrieved from the files, expressed as a percentage of the entire amount shown for all directories.

File Type Report

The File Type Report shows the file types, by extension (such as .gif), of those files that were requested on your Web site. The statistics include the number of requests and the number of bytes retrieved from the files, expressed as a percentage of the entire amount shown for all files.

Browser Report

The Browser Report shows the name and version of each browser from which requests originated. The statistics include the number of requests from each browser and the percentage of requests, expressed as a percentage of all requests from all browsers.

Failures Report

The Failures Report shows the file name from which the requests originated. The statistics include the number of requests from each browser and the percentage of requests, expressed as a percentage of all requests from all browsers.

Viewing Page-request Statistics

The Web server gathers statistics about the pages requested by visitors to your Web site, and you can view these statistics at any time.

➢ ***To view page-request statistics:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Analog Reports** (Reports section).
3. Choose the time frame for which you want to view statistics by clicking the options along the top of the form. The default timeshare is **Running Total**. The other timeshare options are:
   - **This Week:** Includes all statistics recorded for the current week.
   - **Last Week:** Includes all statistics recorded beginning last week to today.
   - **Two Weeks Ago:** Includes all statistics recorded beginning two weeks ago to today.
   - **Three Weeks Ago:** Includes all statistics recorded beginning three weeks ago to today.

   The report showing a breakdown of Web site statistics for the selected time frame. Each report includes the following information.

   - General Summary (on page 97)
   - Monthly Summary (on page 97)
   - Daily Summary (on page 97)
   - Hourly Summary (on page 97)
   - Domain Report (on page 97)
   - Organization Report (on page 97)
   - Host Report (on page 97)
   - Directory Report (on page 97)
   - File Type Report (on page 97)
   - Browser Report (on page 97)
   - Failures Report (on page 97)

Viewing FTP Page-request Statistics

FTP usage statistics show the connections that have been made to your site's Web server through the FTP (File Transfer Protocol) service. You can view reports about your FTP site at any time.

➢ ***To view FTP usage reports:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Analog Reports** (Reports section).
3. Click **FTP Server**.
4. On the FTP Server form, select the time frame in which you want to view the statistics by clicking the options along the top of the form. The default time frame is **Running Total**. The other time frame options are:
   - **This Week.** Includes all statistics recorded for the current week.
   - **Last Week.** Includes all statistics recorded beginning last week to today.
   - **Two Weeks Ago.** Includes all statistics recorded beginning two weeks ago to today.
   - **Three Weeks Ago.** Includes all statistics recorded beginning three weeks ago to today.

   The report is displayed. It shows the FTP statistics for the selected time frame. Each report includes the following information:

   - General Summary (on page 97)
   - Monthly Summary (on page 97)
   - Daily Summary (on page 97)
   - Hourly Summary (on page 97)
   - Domain Report (on page 97)
   - Organization Report (on page 97)
   - Host Report (on page 97)
   - Directory Report (on page 97)
   - File Type Report (on page 97)
   - Browser Report (on page 97)
   - Failures Report (on page 97)

Changing the Language Used in the Site Reports

Site reports can be generated in several languages.

➢ ***To change the language used in site reports:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Analog Reports** (Reports section).
3 On the Site Reports page, click **Report Language**.
4 On the Language preference for Site Reports form, select the language you want to use, then click **Update**.

Using AWStats to Analyze Server Logs

Parallels Pro Control Panel 10.3.3 introduces support of AWStats log analyzer for generating Web and FTP servers' statistics. If this feature was enabled by your hosting provider, you can view statistics generated by AWStats for your site.

In this section:

About AWStats

AWStats is short for Advanced Web Statistics. AWStats is a powerful log analyzer which creates advanced Web, ftp, mail and streaming server statistics reports based on the rich data contained in server logs. Data is graphically presented in easy to read web pages. AWStats is a free software distributed under the GNU General Public License.

Designed with flexibility in mind, AWStats can be run through a Web browser CGI (common gateway interface) or directly from the operating system command line. Through the use of intermediary data base files, AWStats is able to quickly process large log files, as often desired. With support for both standard and custom log format definitions, AWStats can analyze log files from Apache (NCSA combined/XLF/ELF or common/CLF log format), Microsoft's IIS (W3C log format), WebStar and most web, proxy, wap and streaming media servers as well as ftp and mail server logs. As AWStats works from the command line as well as a CGI, it is compatible with web hosting providers which allow CGI and log access.

Features

- Wide range of log formats. AWStats can analyze: Apache NCSA combined (XLF/ELF) or common (CLF) log files, Microsoft IIS log files (W3C), WebStar native log files and other web, proxy, wap, streaming media, ftp and mail server log files. See AWStats F.A.Q. for examples.
- Reports can be run from the operating system command line and from a web browser as a CGI (common gateway interface). In CGI mode, dynamic filter capabilities are available for many charts.
- Statistics update can be run from a web browser as well as scheduled for automatic processing.
- Unlimited log file size.
- Load balancing system split log files.
- Support 'nearly sorted' log files, even for entry and exit pages.
- Reverse DNS lookup before or during analysis; supports DNS cache files.
- Country detection from IP location (geoip) or domain name.
- Plugins for US/Canadian Regions, Cities and major countries regions, ISP and/or Organizations reports (require non free third product geoipregion, geoipcity, geoipisp and/or geoiporg database).
- WhoIS lookup links.
- Vast array of configurable options/filters and plugins supported.
- Modular design supports inclusion of addition features via plugins.
- Multi-named web sites supported (virtual servers, great for web-hosting providers).
- Cross Site Scripting Attacks protection.
- Reports available in many international languages. See AWStats F.A.Q. for full list. Users can provide files for additional languages not yet available.
- No need for esoteric perl libraries. AWStats works with all basic perl interpreters.
- Dynamic reports through a CGI interface.
- Static reports in one or framed HTML or XHTML pages; experimental PDF export through 3rd party "htmldoc" software.

- Customize look and color scheme to match your site design; with or without CSS (cascading style sheets).
- Help and HTML tooltips available in reports.
- Easy to use - all configuration directives are confined to one file for each site.
- Analysis database can be stored in XML format for easier use by external applications, like XSLT processing (one xslt transform example provided).
- A Webmin module is supplied.
- Absolutely free (even for web hosting providers); source code is included (GNU General Public License).
- Works on all platforms with Perl support.
- AWStats has an XML Portable Application Description.

About AWStats Reports

AWStats' reports include a wide range of information on your web site usage:

- Number of Visits, and number of Unique visitors.
- Visit duration and latest visits.
- Authenticated Users, and latest authenticated visits.
- Usage by Months, Days of week and Hours of the day (pages, hits, KB).
- Domains/countries (and regions, cities and ISP with Maxmind proprietary geo databases) of visitor's hosts (pages, hits, KB, 269 domains/countries detected).
- Hosts list, latest visits and unresolved IP addresses list.
- Most viewed, Entry and Exit pages.
- Most commonly requested File types.
- Web Compression statistics (for Apache servers using mod_gzip or mod_deflate modules).
- Visitor's Browsers (pages, hits, KB for each browser, each version, 123 browsers detected: Web, Wap, Streaming Media browsers..., around 482 with the "phone browsers" database).
- Visitor's Operating Systems (pages, hits, KB for each OS, 45 OS detected).
- Robots visits, including search engine crawlers (381 robots detected).
- Search engines, Keywords and Phrases used to find your site (The 122 most famous search engines are detected like Yahoo, Google, Altavista, etc...)
- HTTP Errors (Page Not Found with latest referrer, ...).
- User defined reports based on url, url parameters, referrer (referer) fields extend AWStats' capabilities to provide even greater technical and marketing information.
- Number of times your site is added to Bookmarks / Favorites.
- Screen size (to capture this, some HTML tags must be added to a site's home page).
- Ratio of integrated Browser Support for: Java, Flash, Real G2 player, Quicktime reader, PDF reader, WMA reader (as above, requires insertion of HTML tags in site's home page).
- Cluster distribution for load balanced servers.

Configuring AWStats for Sites

AWStats reports are configured from the command line interface. You can not configure AWStats using the Site Administrator control panel.

AWStats reports are generated in accordance with the options set in the AWStats configuration file. You can modify the configuration options to change the default behaviour of AWStats reports.

➢ ***To change the configuration information:***

1 Connect to your site using the Telnet or SSH remote login service.

Important: To use Telnet or SSH, your service provider must enable Telnet or SSH remote login services for your site. SSH is recommended as a secure remote login service.

- If you are using the SSH service, type the following at the command line prompt.

  `ssh` ***<username@sitename>***
  For example, if you have the user name, myname, for the site, mysite.com, then type, `ssh myname@mysite.com`

- If you are using Telnet, type the following:

  `telnet mysite.com`

2 Enter your user name and password, when prompted.

3 At the command prompt, type the following command to modify the configuration file:

- To modify the configuration file of Web server

```
vi /etc/awstats/awstats.<siteN>.conf
```

- To modify the configuration file of FTP server

```
vi /etc/awstats/awstats.ftp.<siteN>.conf
```

4 The configuration file opens. Each option is preceded by a detailed description of the option. Use the definitions in the configuration file to help you modify the file.

Note: When you modify the configuration file, do not change the default output directory, `outputdir` (where the AWStats reports will be located), otherwise the reports will not be visible from the Site Administrator control panel.

5 Change the configuration options as needed.

6 To save the changes and exit the configuration file, type the following command:

```
:wq
```

To view the report, Generate a report (on page 106).

Viewing Log Reports

➢ ***To view statistics for Web/FTP server:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **AWStats Reports** (**Reports** section).

3 On the **AWStats Reports** page, if not already selected, click **Web Server** or **FTP Server** to view the AWStats report for your Web or FTR server.

Note: If server logs have not yet been generated, no report is generated; you will find the following message, `Could not get requested site report because Web Server logs have not yet been generated`.

You can generate a report, by forcing generation of server logs. See Generating reports (on page 95) to generate a report.

Please refer to AWStats Web site (http://awstats.sourceforge.net/) for a detailed description of reports provided by this tool.

Generating Reports

AWStats runs at the scheduled time, the settings of which are configured by your service provider. The Generate Reports option enables you to generate reports as and when required.

➢ ***To generate reports:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Log Manager** (Web server section).

3 Review the rotation configuration and click **Rotate**.

Note: When you click Rotate, a request is submitted to the control panel. The control panel processes these requests every 10 minutes and updates your report.

4 Click the **Shortcuts** tab on the Home page.

5 In the shortcuts area of the Home page, click **AWStats Reports** (Reports section).

6 Choose the type of report you want to view:

- Click **Web Server** to view the Web Server report.
- Click **FTP Server** to view the FTP Server report.

Viewing Disk Usage Reports

In this section:

Overview of Disk Usage Reports

The disk usage report provides a statistical summary of the amount of disk space consumed by the site and its users. The report is useful in tracking the usage status and identifying users that are approaching or exceeding the allocated limit. You can use this information to prevent issues caused due to insufficient disk space.

The report displays the following usage information for the site:

- Used Quota (MB). The amount of disk space (in megabytes) consumed by the site, displayed as a percent value.
- Total Usage (MB). The amount of disk space (in megabytes) consumed by the site, displayed as an absolute value.
- **Allocated Quota** (MB). The amount of disk space (in megabytes) allocated to the site.

When the site reaches or exceeds its usage limits (on page 107), you receive an email notification informing you about the usage status.

Types of Usage Limits

The usage limits operational on the site are as follows:

- **Threshold**. The threshold is a percentage value of the allocated quota for the site and is set by your service provider. The current threshold is displayed at the top left corner of the reports page. When the site reaches or exceeds its threshold, an email notification is sent to the Site Administrator.
- **Critical Limit**. The critical limit is the usage limit reached when the site is 3 MB short of reaching the allocated quota. You cannot change the critical limit. When the site reaches or exceeds its critical limit, you receive an email notification.
- **Hard limit**. The hard limit is the amount of disk space allocated to the site and is set when your service provider creates the site.

Important: It is important that measures be taken to avoid disk space consumption in excess of the site's allocated quota. Exceeding the allocated quota can result in corruption of the site's database.

Viewing the Disk Usage Reports

➢ ***To view the disk usage report:***

In the shortcuts section on the Home page, click **Disk Usage Reports** (Reports section).

The following information is displayed:

- **Status - The current usage status for site users. The status is indicated by the following buttons:**
  -  - Indicates that the usage level is below the allocated threshold.
  -  - Indicates that the usage level exceeds the site's threshold.
  -  - Indicates that the usage level exceeds the quota allocated to the user.
- **User** - The name of the user.
- **Usage** - A bar graph showing how much disk space is used in comparison to how much is assigned to the user.
- **% Used Quota -** The amount of disk space (in megabytes) consumed by the user, displayed as a percent value.
- **Total Usage (MB) -** The amount of disk space (in megabytes) consumed by the user, displayed as an absolute value.
- **Allocated Quota (MB) -** The maximum amount of disk space (in megabytes) allocated to the user.

Downloading Disk Usage Reports

You can download disk usage reports to your local system and view them with a spreadsheet program such as Microsoft Excel or a text editor such as Notepad. When opened in a spreadsheet program, the usage report information is displayed in columns. When opened in a text editor, the information is displayed in a list with each value separated by a comma (Comma Separated Value (CSV) format).

Important: Downloading usage reports does not collect real-time data. It simply enables you to download the most recent report, which is updated according to an established schedule.

➢ ***To download the report:***

1 In the shortcuts section on the Home page, click **Disk Usage Reports (**Reports section).

2 Click **Export Report**. You can choose to save the report or open the report in an appropriate program.

Emailing Disk Usage Reports

The disk usage report is emailed as a CSV file (Comma Separated Value) that can be viewed in a spreadsheet program such as Microsoft Excel or a text editor such as Notepad. The report is sent to your email address.

➢ ***To email the report:***

1 In the shortcuts section on the Home page, click **Disk Usage Reports** (Reports section).

2 Click **Email Report**.

Managing Server Logs

In this section:

About Logrotate

The Log Manager uses the Logrotate utility to manage the server log files. Depending on the frequency and size of the log files, Logrotate archives the log data. The system then populates the empty log file with fresh log data. This is called log rotation.

Why Logs Need to be Rotated

Log files, on a busy server, grow very quickly. A server that receives 100,000 requests a day could generate an access-log file of 10 to 20 MB in size. Over time, such log files consume a great deal of disk space if they are not compressed and rotated on a regular basis.

How Logrotate Works

Logrotate compresses and rotates logs based on the thresholds configured for size and frequency. You set these thresholds when you configure Logrotate (on page 112). Thresholds are saved in the configuration file, logrotate.conf, located inside the file system of the site.

When the log file reaches the set thresholds, Logrotate archives it in the same directory. The system then writes new log data to the empty log file.

Note: Before Logrotate is scheduled to run, the system generates Webalizer and Analog log reports.

By default, logs are compressed and placed in an archive file.

For example, if the `access-log` file for the server has reached the rotate threshold, then it is compressed as an `access-log.gz` file and fresh logs are written to the `access-log` file, which is now your current log file.

You can set Logrotate to archive uncompressed files, however.

For example, if the `access-log` file for the server has reached the rotate threshold, then a new file, `access-log.1` is created into which the existing log data is archived, and fresh log data written to the `access-log` file, which is now your current log file.

Factors to Consider When Configuring Log Rotation

When you configure log rotation, you may want to consider the following factors.

- **Amount of available disk space**

  The disk space allocated to your site is important in determining the threshold that you set for your log files. If your site has limited disk space, you need to set a lower threshold.

  If your server runs out of disk space, system performance drops, and you lose fresh log data.

  Important: If your server runs out of disk space and a log rotate is scheduled to run, you will lose important log data.

- **Log size and traffic level**

  On high-traffic sites, log files grow quickly. Review your site's traffic level and the expected log file size when setting your log threshold.

- **Frequency of rotation**

  Logs can be rotated four times daily, once a day or weekly, depending on the rate at which log files expand. In general, high-traffic sites require more frequent rotation than low-traffic sites.

Configuring Logrotate

Logrotate is a utility that rotates the following log files based on the settings you configure.

- Web server logs
- FTP server logs
- Majordomo logs

You can set your log files to rotate four times a day, once a day, or once a week. You can also change (on page 113) the Logrotate settings at any time.

➢ ***To configure Logrotate:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Log Manager** (Web Server section). The Logrotate window opens and the Automated Log Rotation Parameters form is displayed.

3 In the **Frequency** field, choose the rate at which you want to rotate the log. Frequency options include:

   - **4 times daily**. The log file is rotated every 6 hours.
   - **Daily**. The log file is rotated once a day.
   - **Weekly**. The log file is rotated once a week.

   Note: This schedule is kept only if the log file has not reached the size specified in the **Log File Size** field.

4 In the **Log File Size** field, enter the maximum size of the log file (in bytes, kilobytes, or megabytes).

   Note: When log files reach the specified size, the logs are rotated before the scheduled rotation.

5 In the **Number of Archives** field, enter the maximum number of archives you want to retain on the server. You can retain up to 5 archives.

   Important: When the number of log archives exceed the set value, the archive is deleted.

6 Click **Rotate**. The log is purged into an archive file, enabling the empty file to receive fresh logs. This process can take up to 10 minutes to complete.

Changing Configuration Information

➢ ***To change the Logrotate configuration information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Log Manager** (Web Server section). The Logrotate window opens and the Automated Log Rotation Parameters form is displayed.

3 Change the log rotation parameters (on page 112) as required.

4 Click **Update.**

The configuration changes take effect when Logrotate runs the next time.

Managing Subdomains

In this section:

About Subdomains

Subdomains are lower-level domains hosted on a registered root domain.

For example, if you own the root domain name *example.com*, you can host a subdomain, *sales*, on your root domain. Users can access the subdomain, by typing the subdomain URL, *sales.example.com,* in a browser just as they do *example.com*. You do not have to register the subdomain, since it is based on your registered root domain name.

http://	subdomain	.	example	.	com
	3rd level domain		2nd level domain		Top-level domain or 1st level domain

Subdomains enable you to organize and position Web data and services into distinct online channels. Supporting business units, separate product lines and diverse geographies of enterprises can be effectively web-managed as subdomains.

Note: To create subdomains, your service provider must enable subdomains for your site. You can add subdomains to name-based as well as IP-based sites. The number of subdomains you can create is also set by your service provider at the time of creating your site.

Advantages of Subdomains

Subdomains offer the following advantages:

1 Reinforce branding and Web presence

Subdomains enable you to create distinct online service channels for affiliated business data and services while preserving brand association. This reinforces brand value and extends your Web presence through alternative channels of service.

2 Simplify management of large domains

Large domains can be split up into separate logical entities in alignment with your organizational setup and web-managed separately. Thus, your enterprise can have a separate yet affiliated Web presence for sales, support, human resources, and other business divisions apart from your primary Web site.

3 Independent private online repository of content

Each subdomain has its own private repository of online content resources. The subdomain folder contains all the content resources necessary for the subdomain to be accessible from a Web browser. This segregation averts content or resource violation and ensures secure management of subdomain content.

The Subdomain Environment

Subdomains, at the file system level, are simply subfolders that contain the requisite Web content for the subdomain.

You can create two types of subdomains:

- Regular subdomains

  Regular subdomains can be created using the Add subdomain (on page 118) option. Regular subdomains can be located anywhere in the site's file system within the subdomain The base directory indicates the location in the site's file system where all the regular subdomains for the site are located..

  All the regular subdomains for the site are, by default, placed in the `/var/www` directory, also called the base directory. Your service provider sets the base directory.

  For example, if `/var/www` is the base directory set by your service provider and you create a subdomain, `mysubdomain,` then your subdomain is located at `/var/www/mysubdomain`

- User subdomains

- User subdomains can be created using the Add User (on page 27) option. A user subdomain is a subdomain that has the same name as its owner. The subdomain is, by default, located in the home directory of the user under the `public_html` folder. The subdomain directory cannot be changed by the user.
- For example, if you enable a user subdomain for the user, `myname`, then the user subdomain is called `myname` and is located at `/home/myname/public_html/`

Subdomains inherit the security level (on page 75) and aliases (on page 114) defined for the root domain. The security level inherited by the subdomain determines the operating environment of the subdomain. You can enable CGI Support (on page 114) for subdomains to enable users to run CGI scripts.

Aliases

Aliases are nicknames or alternative web addresses that map to an existing subdomain. Subdomains inherit the aliases configured for the root domain. To determine if aliases are available for the subdomain, see the **URL** field in the Subdomains Details (on page 120) form. You will find the subdomain URL along with the list of aliases (if the root domain has aliases).

Note: You can access subdomains using aliases only if the root domain is configured with aliases.

If your root domain, ***example.com***, is configured to be accessible using the alias, ***example.net***, then the subdomain, ***sales***, hosted on the root domain can also be accessed using the alias, ***sales.example.net***.

CGI Support

CGI scripts enable you to capture and process information dynamically. They can be used to retrieve information from a database, collect Web statistics and perform searches.

CGI scripts are placed in the cgi-bin directory under the subdomain folder. Thus, if the subdomain, *sales*, is located within the `/var/www/sales/` directory, then the CGI scripts for the subdomain will be placed in the `/var/www/sales/cgi- bin/` directory in the root domain's file system.

To run a subdomain CGI script, in the Address field of your Web browser, type the following:
`http://`<subdomain_name>`.`<domain_name>`/cgi-bin/`<script_name>
where:
<subdomain_name> is the name of your subdomain
<domain_name> is the domain name of the site on which your subdomain is hosted
<script_name> is the name of the cgi script

As a Site Administrator, you can:

- Create (on page 118) subdomains for a registered domain
- View (on page 120) current subdomain details
- Change (on page 121) subdomain settings
- Set (on page 122) default subdomain settings
- Delete (on page 122) subdomains

Before Creating a Subdomain

Before creating a subdomain, have the following information ready.

- **Name of the subdomain** - Choose a name for your subdomain.
- **Full directory path of the subdomain** - The name of the directory where all the required content resources for the subdomain will be located.

Adding Subdomains

To add subdomains, your site must be set up to host subdomains. Only your service provider can change this setting. If subdomains are enabled for your account, the **Subdomains** option is listed in the shortcuts area.

The number of subdomains you can add is set by your service provider. You can choose to be the owner of a subdomain or delegate ownership to a user of the site.

Important: Before you assign the subdomain to a user, ensure that you have created a user (on page 27) for the site.

➢ ***To add a subdomain:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Subdomains** (Web Server section).

3 In the Subdomain submenu, click **Add Subdomain**. The Add Subdomain form opens.

4 Enter the name of the subdomain in the **Name** field.

Note: To create a subdomain *sales* for the site, www.example.com, enter only ***sales*** in the **Name** field and not ***sales.example.com***. Note that the domain name of your site is already suffixed in the **Name** field.

5 In the **Owner** field, click the arrow to select an owner for the subdomain.

Note: Any existing user of the site can be authorised to be the owner of the subdomain. You can also choose to be the owner of the subdomain.

6 In the **Full Directory Path** field, enter the name of the subdomain directory. You will upload your subdomain content to this directory.

Note: The **Full Directory Path** is prefixed by the path, `/<base_directory>/`
`Where:`
`<base_directory>` is the directory path set by your service provider while creating the site. The default base directory is `/var/www`.

For example, if you specify ***mysubdomain*** in the **Full Directory Path** field and `/var/www` is the base directory configured by your service provider, then your subdomain is located at `/var/www/mysubdomain`.

Important: The subdomain directory, once defined, cannot be changed.

7 In the **CGI Support** field, select the checkbox if you want users to run CGI scripts on the subdomain, otherwise leave it blank.

Note: The CGI scripts for the subdomain will be placed in the cgi-bin directory under the subdomain folder.

For example, if your subdomain is located at `/var/www/`***<subdomain_name>***, then your CGI scripts will be placed in the following location:
`/var/www/`***<subdomain_name>***`/cgi-bin/`
where ***<subdomain_name>*** is the name of your subdomain.

Your subdomain can run any script placed in the cgi-bin directory. To run a subdomain CGI script, in the Address field of your Web browser, type
`http://`<subdomain_name>`.`<domain_name>`/cgi- bin/`***<script_name>***
where:
<subdomain_name> is the name of your subdomain
<domain_name> is the domain name of the site on which your subdomain is hosted
<script_name> is the name of the cgi script

8 Click **Add Subdomain**.

Viewing the List of Subdomains

Note: To view subdomains, your site must be set up to host subdomains. Only your service provider can change this setting. If subdomains are enabled for your account, the **Subdomains** option is listed in the shortcuts area.

➢ ***To view the list of subdomains:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Subdomains** (Web Server section). The Subdomain window opens, displaying the list of subdomains.

The following information is displayed:

- **Name -** The name of the subdomain.
- **Owner -** The name of the user who owns the subdomain. The owner of the subdomain can upload content to the subdomain.
- **CGI -** Indicates whether the subdomain is configured to run CGI scripts. If marked for CGI-compliance, a check mark appears against the corresponding subdomain. A cross appears against subdomains that do not have CGI capability.
- **Actions -** Allows you to:
  - change subdomain settings (on page 121)
  - delete subdomains (on page 122)

Viewing Subdomain Details

Note: To view subdomains, your site must be set up to host subdomains. Only your service provider can change this setting.

➢ ***To view subdomain details:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Subdomains** (Web Server section).

3 In the **Name** column, click the name of the subdomain whose details you want to view. The Subdomain Details form opens.

The following is a tabulation of the form fields that appear in the Subdomain Details form.

This field:	Shows:
Name	Name of the subdomain.
URL	The Web address of the subdomain, along with the list of aliases inherited from the root domain (only if the root domain has aliases configured for it) For example, the subdomain, ***sales***, hosted on the root domain, ***example.com***, will be listed as, http://sales.example.com Note: If your domain, www.example.com, has an alias, www.example.net, then the subdomain ***sales.example.com***, can also be accessed using the inherited alias, ***sales.example.net***.
Owner	The name of the user who owns the subdomain.
Full Directory Path	The location where the content resources for the subdomain are uploaded. The **Full Directory Path** is the location from where the Web server will serve content to the browser.
CGI Support	A Boolean value [Yes,No] that indicates whether CGI support is enabled for the subdomain.
CGI script directory	The directory path where the CGI scripts for the subdomain are located.

Changing Subdomain Settings

➢ ***To change the subdomain settings:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Subdomains** (Web Server section). The Subdomain window opens, displaying the list of subdomains.
3. In the Subdomain list, click in the **Actions** column next to the subdomain whose settings you want to change. The Edit Subdomain form opens.
4. Modify your subdomain settings as required.
5. Click **Update**.

Viewing Default Subdomain Settings

Subdomains are configured with the settings and capabilities defined in the Subdomain Default (on page 121) form. All subdomains assume the values specified in this form, unless you choose to change the subdomain settings (on page 121).

➢ ***To view the default settings for a subdomain:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Subdomains** (Web Server section). The Subdomain window opens, displaying the list of subdomains.
3. In the Subdomain submenu, click **Defaults**. The Subdomain Defaults form opens.

   The following information is displayed.

Field name	**Description**
Base Directory	The base directory indicates the location in the site's file system where all the regular subdomains for the site are located.
Owner	The name of the user who owns the subdomain.
CGI Support	A Boolean value [Yes, No] that indicates whether CGI support is enabled for the subdomain.

Changing Default Subdomain Settings

You can change the default settings for a subdomain at any time. Subdomains assume the default values specified in the Subdomain Defaults (on page 121) form.

➢ ***To change the default settings for a subdomain:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Subdomains** (Web Server section). The Subdomain window opens.

3 In the Subdomain submenu, click **Defaults**. The Subdomain Defaults form opens.

4 Click **Edit Defaults** at the bottom of the form. The Edit Subdomain Defaults form opens.

5 Modify the subdomain settings as required.

6 Click **Update Defaults**.

Deleting Subdomains

You can delete a subdomain that ceases to be viable or useful. When you delete a subdomain, the directory containing the subdomain resources is deleted; the subdomain can no longer be accessed.

Important: The delete action is irreversible. Use this option with caution.

➢ ***To delete a subdomain:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Subdomains** (Web Server section). The Subdomain window opens.

3 In the Subdomain list, click  in the **Actions** column next to the subdomain you want to delete. The Confirm Delete window opens.

4 Click **OK** to delete the subdomain.

CHAPTER 8

Working with Internationalized Domain Names (IDN)

In this chapter:

Overview of Internationalized Domain Names (IDN)

An internationalized domain name (IDN) is a domain name that contains non-ASCII characters - characters that are native to a region or language and do not belong to the ASCII standard, for example: `http://www.fargbolaget.nu`.

A typical domain name uses characters from the ASCII character set, for example, `http://www.example.com`. The network protocols, especially DNS, recognize only ASCII characters in a domain name. Non-ASCII characters therefore cannot be used in domain names without a mechanism to map these non-ASCII characters to their ASCII-encoded representations.

How Does IDN Work?

Typically, when you use the browser to connect to a domain (comprising ASCII characters), the browser sends a request to the authoritative domain name server for the IP address corresponding to the requested domain. The DNS protocol requires the domain names to be represented using the ASCII character set.

In the case of IDNs, if a browser needs to resolve an internationalized domain name, it must first convert the domain name from its native character set to an alternative representation in the ASCII character set. This conversion is defined by a well-defined standard known as ASCII-compatible encoding (ACE) described in RFC 3490. When your browser automatically performs the translation for a domain name from its IDN representation to its equivalent ACE representation, it is said to be **IDN- compliant.**

Some of the IDN-compliant browsers are:

- Netscape Navigator 7.1 (or higher)
- Mozilla 1.4 (or higher)
- Microsoft Internet Explorer

Important: Microsoft Internet Explorer requires the i-Nav plug-in (http://www.idnnow.com/) from Verisign® to work correctly with IDN.

Translation of IDNs to ASCII-compatible Encoding (ACE) or Punycode

When an IDN-compliant browser receives a request for an IDN, it translates the domain name into a sequence of ASCII characters prefixed by `xn--`. The translated domain name is called ASCII-compatible encoding (ACE) or Punycode and complies with the network protocol standard.

For example, when you type `http://www.fargbolaget.nu` into a browser, the browser sends the following ASCII-encoded string to the DNS: `http://www.xn--frgbolaget-q5a.nu`

Domain Name Representation in the Control Panel

The control panel displays the IDN representation of the domain name. To view its ASCII-encoded equivalent, click the link **show text name** next to the IDN. A pop-up window opens displaying the ASCII-encoded representation. The visual mapping enables you to easily co-relate an IDN with its ASCII-encoded representation.

Caveats

IDN is based on evolving standards. As of now, not all browsers have in-built support for internationalized domain names. Therefore, you need IDN-compliant applications to take advantage of IDN.

Please review the following related topics for more information:

- IDN compatibility requirements for applications (on page 126)
- Using IDNs with email addresses (on page 129)
- Using remote access services to connect to IDN domains (on page 130)

IDN Compatibility Requirements for Applications

Applications must be IDN-compliant in order to work with internationalized domain names. The following sections lists some of the applications that are IDN-compliant along with their requirements.

Important: If your application is not IDN-compliant, you must use the ASCII-encoded representation (on page 124) of the domain name to access the domain. To view the ASCII-encoded representation, refer to your account details provided in the email sent by your administrator.

If you are using the Microsoft Windows platform, you need to install (on page 131) native fonts on your system to ensure that the non-ASCII characters are rendered correctly.

Web Browsers

The following section lists the browser requirements.

- Microsoft Internet Explorer

  Platform: Windows

  Applications Supported: Internet Explorer 5.0 and higher

  Plug-ins: i-Nav
- Netscape Navigator

  Platform: Windows, Mac OS X, Linux

  Version: 7.1 and higher
- Mozilla

  Platform: Windows, Mac OS X, Linux

  Version: 1.4 and higher

Email Clients

The following section lists the requirements for email clients.

Microsoft Outlook

```
Platform: Windows
Version: Microsoft Outlook 2000, 2002 (XP), 2003; Outlook
Express 5.0 and higher
Plug-ins: i-Nav
```

FTP Clients

The following section lists the requirements for FTP clients.

Secure FTP

Platform: Windows

Version: 4.0.2004 and higher

Core FTP

Platform: Windows

Version: Pro 1.3 and higher

Telnet / SSH clients

The following section lists the requirements for Telnet/SSH clients.

Absolute Telnet

Platform: Windows

Version: 3.13 and higher

For a comprehensive list of IDN-compliant applications, please visit VeriSign (http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/page_002201.html).

Connecting to an IDN Domain

You can connect to a domain using its IDN or ASCII-encoded representation.

Important: If your application is not IDN-compliant, you must use the ASCII-encoded representation (on page 124) of the domain name to access the domain. To view the ASCII-encoded representation, refer to your account details provided in the email sent by your administrator.

Connecting to an IDN Domain Using IDN Representation

Your Web browser must be IDN-compatible (on page 126) to connect to a domain using its IDN representation, otherwise you will be unable to connect to the domain.

In the **Address** field of the Web browser, type the domain name.

For example:

http://<idn_domain_name.com>/

where <idn_domain_name.com> is the IDN representation of the domain name

Example

To connect to the domain `fargbolaget.nu`, type:

`http://fargbolaget.nu/`

Connecting to an IDN Domain Using ASCII-Encoded Representation

If your Web browser is not IDN-compatible, you can connect to a domain using its ASCII-encoded representation.

In the **Address** field of the Web browser, type the ASCII-encoded representation of the domain name.

For example:

http://<ascii_encoded_domain>/

where ***<ascii_encoded_domain>*** is the ASCII-encoded representation of the domain name

Example

To connect to the domain `fargbolaget.nu` using its ASCII-encoded representation `xn—frgbolaget-q5a.nu`, type:

`http://xn--frgbolaget-q5a.nu/`

Using IDNs in Email Addresses

When you create email aliases (on page 162), mailing lists (on page 157), or forward email messages (on page 169) to an account hosted on an IDN domain, you can qualify the email address with the IDN representation of the domain on which the account is hosted.

Important: If your application is not IDN-compliant, you must use the ASCII-encoded representation (on page 124) of the domain name. To view the ASCII-encoded representation, refer to your account details provided in the email sent by your administrator.

If you are creating an email alias for an account on the domain ***<idn_domain>***`.com`, you may enter the email address `user@<idn_domain>.com` in the **Alias** field.

Example

To create an email alias for an account `user1` on the domain `fargbolaget.nu`, type the email address as follows:

`user1@fargbolaget.nu`

However, if your browser is not IDN-compatible, you must use the ASCII-encoded representation of the domain in the email address as follows:
`user@<ascii_encoded_domain>.com.`

Example

To create an email alias for an account `user1` on the domain `fargbolaget.nu` using its ASCII-encoded representation `xn—frgbolaget- q5a.nu`, type the email address as follows:

user1@xn--frgbolaget-q5a.nu

Working with Email Clients

If your email client is IDN-compatible (on page 126), you can use the IDN representation of domain names when you configure an email account or send messages using an email client. If the email client does not provide IDN support, you must use the ASCII-encoded representation of the domain name in the email address.

Note: Email clients running on the Linux operating system do not support IDN. You must qualify the email address with the ASCII-encoded representation of the domain on which the account is hosted.

Using Remote Access Services to Connect to IDN Domains

If your application is IDN-compliant (on page 126), you can use the IDN representation of a domain name to access domains when you use remote access services such as FTP, Telnet, or SSH. Additionally, you must configure the services to use the character set **UTF-8** to enable correct interpretation of IDNs.

Important: If your application is not IDN-compliant, you must use the ASCII-encoded representation (on page 124) of the domain name to access the domain.

Connecting to IP-based Domains

➢ ***To connect to an IP-based domain using a non-IDN compliant client (such as Telnet/SSH/FTP on Linux):***

1 Connect to the domain using the domain name or IP address.

`#ssh` ***<ascii_encoded_domain>***

For example, to connect to the domain `fargbolaget.nu` using its ASCII encoded representation `xn—frgbolaget-q5a.nu`, type:

#ssh xn—frgbolaget-q5a.nu

2 Enter the user name and password.

Connecting to Name-based Domains

➢ ***To connect to a name-based domain using a non-IDN compliant client (such as Telnet/SSH/FTP on Linux):***

1 Connect to the domain using the domain name or IP address.

`#ssh` ***<ascii_encoded_domain>***

For example, to connect to the domain `fargbolaget.nu` using its ASCII encoded representation `xn—frgbolaget-q5a.nu`, type:

`#ssh xn—frgbolaget-q5a.nu`

1 Enter the user name (in the format ***<user@ascii_encoded_domain>***) and password.

Installing Native Fonts on a Microsoft Windows Desktop

If you use the Microsoft Windows platform, you must install related native fonts to ensure that non-ASCII characters are displayed appropriately.

➢ ***To install native fonts:***

1 Select **Start > Settings > Control Panel**.

2 In the Control Panel window, locate and double-click **Regional Options** from the list of displayed options. The **Regional Options** window opens.

3 In **Your locale (location)** area, select the country that represents your locale.

4 In **Language settings for the system** area, select the checkbox corresponding to the language whose fonts you want to install.

5 Click **Ok**. You will be prompted to insert the CD-ROM that contains the installation files. Insert the Windows Setup CD-ROM into your disk drive and click **OK**. If the required files reside on a network server, browse to the location on the network server.

6 Restart your desktop.

CHAPTER 9

Managing Users

In this chapter:

About Adding User Accounts

You add user accounts when you want to create accounts that individuals can use to access services through your site.

These are the types of user accounts you can add:

- Mailbox and service accounts (on page 27)
- FrontPage user accounts (on page 31)
- htaccess user accounts for access to password-protected directories (on page 222)

Logging on to the User Administrator Control Panel

Parallels Pro Control Panel Automatic login also called auto-login does not require you to know the User Administrator's user name and password. You are automatically logged in using the User Administrator's account information. you into the User Administrator control panel when you click on a user account. Auto-login is especially useful if the User Administrator has forgotten the password, and requires you to access the User Administrator control panel and reset the current password.

As a User Administrator you can also perform other administrative tasks, for example, access emails, manage email account settings, or export and import user data. While you work as a User Administrator, your Site Administrator session remains active for a duration of 60 minutes. If no activity is noted during this period, the session expires. As you perform multiple roles, stacked login ensures that your multiple sessions remain easily accessible and functional.

To log on to the User Administrator control panel:

1. On the Menu, click **Mailboxes/Users**. The **Manage Users** list is displayed.
2. In the **User Name** column, click the name of the user. A dialog box opens and confirms that you want to log on at the User Administrator level.
3. Click **OK.** The User Administrator shortcuts page opens, which lists the tasks you can perform as the User Administrator.

Managing Mailbox Users

In this section:

About Users and Mailboxes

A user is a person with an account on your domain. You must set up user accounts on your domain before users can access services, such as email, or make an FTP connection to the Web server.

Note: You must create a user account for yourself if you want to access the User Administrator control panel. As Site Administrator, you have a default email account, but you do not have a User Administrator account.

About Mailboxes

When you add a user, an email address and a mailbox is automatically created for that user.

About the User Defaults Template

If you are adding many users with similar settings, you can set the User Defaults template (on page 136) to preset the disk quota and services options on the Add User form.

This template is not required to add a user to a domain; however, it can make adding multiple users easier and faster by establishing default user values.

When you add a new user to a domain, the control panel pre-fills the add user form with the defaults you set. You can change them before you add the user, however.

Mailboxes/Users Page

The Mailboxes/Users page provides information about the mailbox user accounts on your site. As Site Administrator, you can add (on page 27), remove (on page 137), or change (on page 137) user accounts from this page.

➢ ***To get to the Mailboxes/Users page:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (**Users** section).

On this page you can perform several tasks and view the following information:

- . A check box you can click to select users. When you click the box in a user's row, a checkmark appears in the box and the user is selected. If you click **Remove Users** at the bottom of the form, the selected user accounts are removed.
- **User Name**. The name the user types to log in to the User Administrator control panel.
- **Full Name**. The full name of the user.
- **Options**. The services available to the user.
- **Actions**. Links to tasks you can perform.

From this page you can:

- View all of the user accounts on your site (on page 138)
- Search for a specific user (on page 138)
- Add new users (on page 27)
- Change user information (on page 137)
- Remove users (on page 137)
- Set up a User Defaults template (on page 136)

Adding Mailbox and Service Users

Please, refer to this document (on page 27).

Creating a User Defaults Template

Before you add mailbox and service users, you might want to change the User Defaults template so that the disk usage and service options available to users are pre- filled according to your preferences. This template is not required, but it can make adding multiple users easier and faster.

The default settings appear on the add user form, although you can change them as needed before you add the user.

➢ ***To create a User Defaults template:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Add User** (Users section).
3 On the Mailboxes/Users submenu, click **Set User Defaults**. The Set User Defaults form opens.
4 In the **Disk Quota** field, enter the amount of disk space, in megabytes, that will be allotted to each user. To allow an unlimited amount of disk space, type `0` (zero).

Note: The control panel does not support quotas on NFS-mounted servers. For NFS-mounted servers, type `0` (zero).

5 In the **Telnet** field, if you want to allow users to connect remotely to the server using a Telnet connection, select the check box; otherwise, leave it blank.
6 If CGI service is enabled for the site, you can select the **CGI** checkbox to enable the user to run CGI scripts.
7 In the **SSH Secure Shell** field, if you want to allow users to connect remotely to the server using an SSH connection, select the check box; otherwise, leave it blank.
8 In the **FTP** field, if you want to allow users to transfer files using FTP, select the check box; otherwise, leave it blank.
9 Click **Update**. The defaults appear on the add user form whenever you add a user.

Changing User Information

On occasion, it may be necessary to change a user's account information, for example, to change a password or to enable access to services.

➢ ***To update user information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Users section).

3 **On the Manage Users list, l**ocate the user whose information you want to change, then the **Actions** column, click . The Edit User form opens.

4 Change the user's information, then click **Update**.

Removing Users

When users are no longer working on your domain, you can remove their mailbox and service accounts to conserve resources and maintain security.

Note: A special alias called site_blackhole is automatically created when the domain is created. It is not shown in the list of aliases and its only purpose is to act as a repository for all garbage email.

When a user with an alias is removed, the alias can still remain (as it may be referenced by other aliases), but the target user name is replaced by site_blackhole. When an email message is sent to this alias, it will go to site_blackhole. Therefore, when you delete a user, you will see the alias set to site_blackhole.

➢ ***To remove a user from a domain:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Users section).

3 On the Manage Users list, locate the user you want to remove, then in the **Actions** column, click . The confirmation window is displayed.

4 Verify that you want to remove the user, and then click **OK**.

Searching for a Specific User

You can search by keywords to quickly locate a user from the User List.

➢ ***To search for a user:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Users section). The Manage Users list is displayed. Search fields appear above the list.

3 In the first search field, click the arrow and choose whether you want to search by user name or full name.

4 In the second search field, enter the keywords on which you want to search.

5 Click **Search**.

The system searches for users that match your criteria and lists them in the form.

Viewing Your Existing Users

You can view all of your existing users from the User List. You can also search (on page 138) for a specific user.

➢ ***To view existing users:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Users section).

The Manage Users form opens displaying information about all of your existing users. This information includes:

- **User Name.** The name with which the user logs on to the domain.
- **Full Name.** The user's first and last names.
- **Options.** The services available to the user.
- **Actions. Links to tasks such as** modifying (on page 137) and removing (on page 137) users.

Managing FrontPage Users

In this section:

Adding FrontPage User Accounts

Please, refer to this document (on page 31).

Managing FrontPage User Accounts

➢ ***To change or remove a FrontPage user account:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Manage Users** (Web Server section). The Manage Users form opens.
3 On the Manage Users page, click the link at the bottom of the form, **Microsoft FrontPage Extension Permission Management Interface**.
4 On the login form, type your Site Administrator user name and password. Unless you change it in the FrontPage Extensions interface, this is the original password of your Site Administrator account. This password does not change when you change your Site Administrator password.
5 On the FrontPage Server Extensions Site Administration page, click **Manage Users**.
6 To change a user's information, click the user name.
7 Make any changes on the user information page, then click **Submit**. The user information is changed. Be sure to notify the user of the change.

Managing WebDAV Users

In this section:

Managing WebDAV

WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to the HTTP protocol, which allows users to collaboratively edit and manage files on the remote Web servers.

Note: This topic applies to sites with WebDAV enabled. To determine whether you have this service enabled, click **Site Information** (Tools section) in the shortcuts area.

Using WebDAV, you can:

- Add a WebDAV user (on page 140)
- Remove a WebDAV user (on page 141)
- Change a WebDAV user (on page 141)

Adding a WebDAV User

➢ ***To add a WebDAV user account:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (Web Server section). The WebDAV User List form opens.
3. On the WebDAV User List page, click **Add User**. The Add WebDAV User form opens.
4. In the **User Name** field, enter the name for the WebDAV user.
5. In the **Password** field, enter the password for the WebDAV user.
6. Retype this password in the **Confirm Password** field.
7. Click **Add User**.

   The control panel creates a WebDAV user using the data you provided on this form. The name of this user will appear in the WebDAV User List form.

Removing a WebDAV User

➢ ***To remove a WebDAV user information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Web Server section). The WebDAV User List form opens.

3 On the WebDAV User List page, locate the WebDAV user you want to remove, then click ✗ in the **Actions** column.

4 In the confirmation window, click **OK**.

The user account is removed from the list.

Changing WebDAV User Accounts

➢ ***To edit a WebDAV user information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Web Server section). The WebDAV User List form opens.

3 On the WebDAV User List page, locate the WebDAV user whose information you want to change, then click in the **Actions** column. The Edit WebDAV User form opens.

4 In the **Username** field, change the name for the WebDAV user.

5 In the **Password** field, change the password for the WebDAV user.

6 Retype this password in the **Confirm Password** field.

7 Click **Update User**.

8 Click **Reset** to undo the changes and restore the default values.

CHAPTER 10

Managing Email

In this chapter:

Sending and Receiving Email

In this section:

How to Send and Receive Email

If your service provider has enabled email for your site, you and the users you add can send and receive email over the Internet using the email services available through your site.

Options for Accessing Email

As Site Administrator, you have three options for sending and receiving email:

1. When you are logged in to the Site Administrator control panel, Open the SquirrelMail service (on page 145) using a link on the Configuration page. Then, log on to your SquirrelMail account (on page 146) using your Site Administrator user name and password.
2. Create a user account (on page 33) for yourself, then log in to the User Administrator control panel to access your email services.
3. Obtain an email program (on page 144) such as Microsoft Outlook or Eudora to access your email services. If you use one of these email programs, you need to configure the program to get your email from the mail server for your site.

Option 2 enables you to use the User Administrator control panel. You cannot log in to the User Administrator control panel using your Site Administrator user name and password.

About Using Email Programs

To send and receive email, you can use email programs, such as SquirrelMail, Microsoft Outlook, and Eudora, which are also known as email clients. These programs enable your personal computer to send and receive email through the control panel, the computer that hosts your Web site on the Internet.

Using SquirrelMail

SquirrelMail is a Web-based program; it is one of the services that comes with your Web site. You can access SquirrelMail directly from the Site Administrator or User Administrator control panels, or from any Web browser. SquirrelMail is automatically configured to send and receive email through your site's mail server. How to access SquirrelMail (on page 145)

Using Other Email Programs

You can purchase, install, and use other programs such as Microsoft Outlook and Eudora to access your email services. When you use these programs, however, you need to configure them to access your email through your site's mail server. For more information about using other email programs, see each program's documentation.

Note: When you set up your email program, remember to select the SMTP Auth tag in the setup screen.

About SquirrelMail

SquirrelMail is an email client that uses IMAP (Internet Message Access Protocol) to provide you access to your email messages directly on the Internet.

Note: You can use SquirrelMail only if your service provider has enabled the 'SquirrelMail Web-based Email' and 'Email' services for your site.

SquirrelMail can be used to read, reply to, forward, compose, and store your email messages. You can access SquirrelMail and your Web-based email account from any computer with Internet access and a browser.

Note: File attachments are limited to 2 MB by default; however, your site may have a custom size limit. Contact your service provider for the exact size limit. SquirrelMail does not warn you if your file attachment is over the size limit.

Once you open SquirrelMail (on page 145), you can:

- Log on and manage your email messages (on page 146)
- Get Help using SquirrelMail (on page 147)
- Return to Site Administrator (on page 147)

Opening SquirrelMail

You can open SquirrelMail in three ways:

- From the Site Administrator control panel
- From the User Administrator control panel
- From a computer with Internet access

From the Site Administrator Control Panel

➢ ***To open SquirrelMail:***

1 In the shortcuts area of the Home page, click **Site Information** (Tools section). The Site Information window opens displaying the site configuration.

2 In the Services & Options area of the Configuration form, locate **Email URL**. You might need to scroll down to the bottom of the page to see this link.

3 Click the **Email URL** Web address. A separate window opens displaying the SquirrelMail login form.

Note: If a separate window does not open, you can open another Internet browser window, and in the **Address** field of the browser, enter the following URL:

`http://<your-domain.com>/squirrelmail/src/login.php`

You are now ready to log on to SquirrelMail (on page 146).

From the User Administrator Control Panel

Note: Before you or your users can use the User Administrator control panel to access SquirrelMail, you need to add a user account (on page 27).

➢ ***To open SquirrelMail:***

1 Log in to the User Administrator control panel by entering the following URL in a browser:

`http://<yoursite.com>/user`

where ***<yoursite.com>*** is the domain name of your site.

2 In the shortcuts menu on the Home page, click Email Access (Email section). The SquirrelMail login page is displayed.

3 Log on to SquirrelMail (on page 146) using your User Administrator login.

From a Computer with Internet Access

➢ ***To open SquirrelMail:***

1 Connect to the Internet.

2 Start a Web browser program.

3 In the address field of the Web browser, type the following URL:

http://<your_domain.com>/squirrelmail/src/login.php

where ***<yoursite.com>*** is the domain name of your site.

The SquirrelMail login page is displayed and you can log on to SquirrelMail (on page 146) using your Site or User Administrator login.

Logging on to SquirrelMail

You log on to SquirrelMail when you want to view or manage your email messages.

You can log on to SquirrelMail using your Site Administrator user name and password, or the user name and password of your User Administrator account if you created one.

➢ ***To log on to SquirrelMail:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Site Information** (Tools section). The Site Information window opens displaying the Configuration form.

3 In the Services & Options area of the Configuration form, locate **Email URL**. You might need to scroll down to the bottom of the page to see this link.

4 Click the Web address next to the **Email URL** field. A separate window opens displaying the SquirrelMail login form.

5 In the **Email** field, enter the user name portion of your Site Administrator or User Administrator email address. The site name portion of your email address displays automatically.

Note: If the displayed site name is not correct, overwrite the displayed name and enter your entire email address.

6 In the **Password** field, enter your Site Administrator or User Administrator password.

7 Click **Login**.

The SquirrelMail Inbox window opens displaying all of your existing email messages.

Note: File attachments are limited to 2 MBs by default; however, your domain may have a custom size limit. Contact your service provider for the exact size limit. SquirrelMail does not warn you if your file attachment is over the size limit.

Getting Help Using SquirrelMail

If you want more information about using SquirrelMail features, refer to the SquirrelMail online Help system.

➢ ***To open the SquirrelMail Help system:***

1 Open SquirrelMail (on page 145) and log on (on page 146).
2 In the SquirrelMail Inbox window, click **Help**. The Help window opens.
3 To see a list of Help topics, click **Table of Contents**.

Returning to the Site Administrator Control Panel

Because SquirrelMail opens in a separate window, you can use SquirrelMail and without logging out of the Site Administrator control panel. To return to the Site Administrator control panel, click anywhere in the Site Administrator window to make it the active window on your desktop. The SquirrelMail window remains open.

Using Microsoft Outlook Express to Send and Receive Email

You need to configure the Microsoft Outlook Express email client in order to read your email messages using Microsoft Outlook Express.

When you configure the email client, you must specify the SMTP and POP/IMAP server configuration to authenticate the connection.

This section provides instructions on accessing and manually setting up your mailbox using Microsoft Outlook Express and the SMTP server configuration required to authenticate the connection.

Accessing and Setting up Your Mailbox

➢ ***To access and set up your mailbox using Microsoft Outlook Express:***

1 Start Outlook Express by clicking on the **Microsoft Outlook Express** icon on your desktop.

> **Note**: If you are opening Microsoft Outlook Express for the first time, the Internet Connection Wizard displays automatically.
>
> If you have configured Microsoft Outlook Express before, and you want to add a new email account, you must manually launch the Internet Connect Wizard.
>
> To launch the wizard:
>
> 1. Start Microsoft Outlook Express by clicking on the **Microsoft Outlook Express** icon on your desktop.
>
> 2. From the menu bar, choose **Tools > Accounts**.
>
> 3. In the dialog box, click **Add.**
>
> 4. Select and click **Mail.**
>
> The Internet Connection Wizard opens.

2 In the **Display name** field, enter your name as you want it to appear in the outgoing messages.

3 Click **Next**.

4 In the **E-mail address** field enter your email address. This is the address other people use to send email messages to you.

5 Click **Next**.

6 In the **Incoming mail (POP3, IMAP) server** field, enter the domain name or the IP address of your domain.

7 In the **Outgoing mail (SMTP) server** field, enter the domain name or the IP address of your domain.

8 Click **Next**.

9 In the **Account name** field, enter **<**username@domain.com**>** for both IP-based and name-based sites.

10 In the **Password** field, enter your mailbox password.

11 Click **Next**.

12 In the last setup window, click **Finish.**

This adds the new account. You can now specify your email settings.

Specifying Email Settings

➢ ***To specify your email settings:***

1 Start Microsoft Outlook Express by clicking the **Microsoft Outlook Express** icon on your desktop.

2 Choose **Tools > Accounts**.

3 In the Internet Accounts dialog box, click the **Mail** tab.

4 Select the new account and click **Properties.**

5 In the Properties window, click the **Servers** tab.

6 In the Outgoing Mail Server area, select the **My server needs authentication** check box.

7 Click **Settings.**

8 Select the **Use same settings as my incoming mail server** option.

Note: If you are setting this for the first time, this option will already be selected.

9 Click **OK.**

10 Click **OK** again.

Your account is ready to use.

Using Microsoft Outlook to Send and Receive Email

You need to configure the Microsoft Outlook email client in order to read your email messages using Microsoft Outlook.

When you configure the email client, you must specify the SMTP and POP/IMAP server configuration to authenticate the connection.

This section provides instructions on accessing and manually setting up your mailbox using Microsoft Outlook and the SMTP server configuration required to authenticate the connection.

Important: This section assumes that you have Microsoft Outlook installed on your computer and that your network properties are configured correctly.

To read your email messages using Microsoft Outlook, you will need to configure several Microsoft Outlook email service options.

➢ ***To set Microsoft Outlook options:***

1. Start Microsoft Outlook by right-clicking on the **Microsoft Outlook** icon on your desktop.
2. Select **Properties** from the menu.
3. Click the **Add** tab.
4. In the Use the following information services area, select the **Internet Email** checkbox and click **Next**.
5. Click **Set up Mail Account**. The Mail Account Properties window opens.
6. In the **Mail Account** field, enter the name by which you would like to refer to your mail server, for example, Parallels Pro Mail Server.
7. In the User Information area, fill in the following information.
   - **Name**. Enter your first and last name.
   - **Organization**. Enter the name of your organization.
   - **E-mail Address**. Enter your email address, for example, mymail@domain.com.
8. Click the **Servers** tab.
9. In the Server Information area, enter the following information.
   - **Incoming mail (POP3)**. Enter the domain name or IP address of the mail server designated as the POP3 server.
   - **Outgoing mail (SMTP)**. Enter the domain name or IP address of the mail server designated as the SMTP server.
10. In the Incoming Mail Server area, enter the following information.
    - **Account Name**. Enter the user account name at which you will receive your emails.

    Note: Enter **<username@domain.com>** as the account name for both IP-based and name-based sites.

- **Password**. Enter your mailbox password.

11 In the Outgoing Mail Server area, select the **My server requires authentication** check box.

12 Click **Settings**. The Outgoing Mail Server window opens.

13 In the Logon Information area, if not already selected, select the **Use same settings as my incoming mail server** option and click **OK**.

14 Click **OK** again to return to the Microsoft Outlook Setup Wizard and click **Next**.

15 Click **Next** again, then click **Finish**.

Your mailbox displays.

Understanding Email Servers

In this section:

About Your Email Servers

If your service provider has enabled email for your site, you have two servers, Sendmail (on page 152) and Majordomo (on page 152) (if available), to help you manage your site's email requirements.

About Sendmail

The Sendmail SMTP (Simple Mail Transfer Protocol) server processes outgoing and incoming email.

Sendmail is an SMTP mail server that routes SMTP email messages through the Internet to be stored on a mail server, such as POP3 or IMAP. SMTP is the most common email protocol on the Internet.

To access Sendmail features, click **Aliases**, **Responders**,or **Spam Filters** in the shortcuts section of the Home page (Email section).

For more information see:

- About email aliases (on page 161)
- About email responders (on page 165)
- About spam (on page 170)
- About message forwarding (on page 168)

About Majordomo

Majordomo is a service used to automatically manage email mailing lists.

Mailing lists are lists of email recipients that can receive email as group. When you create a mailing list, messages sent to the mailing list email address are automatically sent to every email address on the list. Mailing lists are commonly used to circulate topic discussions. A mailing list includes a set of list members. Whenever a list member posts an email message to the mailing list email address, that email message is distributed to all list members.

To manage mailing lists through Majordomo, click **Mailing Lists** in the shortcuts area of the Home page (Email section). For more information, see About email mailing lists (on page 153).

About Majordomo

If your service provider enables email for your site, you can perform the following Majordomo tasks through the Site Administrator control panel:

- View your existing mailing lists (on page 158)
- Create new mailing lists (on page 157)
- Remove mailing lists (on page 160)
- Add members to a mailing list (on page 157)
- Remove members from a mailing list (on page 160)

About Email Services

If your service provider enables email for your site, you can manage the following email services through the Site Administrator control panel:

- Email aliases (on page 161)
- Email responders (on page 165)
- Mailing Lists (on page 157)
- Sendmail Reject List (on page 171)
- Message forwarding (on page 169)

About Email Services for Roaming Authentication

In this section:

About Roaming Authentication Email Services

A roaming authentication service enables your site users to access their domain's mail server from anywhere outside the network.

You need to have a roaming authentication service if:

- You have roaming customers and want your mail server to be accessible to them while on the move
- You want to restrict access to authentic users so that your mail server is not vulnerable to spamming from unauthenticated sources

You can opt for any of the following roaming authentication services:

- Poprelay (on page 155)
- SMTP-AUTH (on page 155)

If you are using Poprelay, users only need to check their mails once in order to use their domain mail server to relay messages. If you are using SMTP_AUTH, you need to configure your email client to send your user name and password for authentication each time you need to connect to your domain mail server. SMTP_AUTH is a more secure authentication service than Poprelay.

Note: You can select the appropriate authentication service when you configure your mail client. By default, Poprelay is enabled by the control panel. To use SMTP_AUTH, you must select the SMTP_AUTH tag (this depends on the mail client you are using) and provide the authentication user name and password.

For information on how to configure your mail client, see the program's documentation.

Using Poprelay Authentication Service

Poprelay is a roaming authentication service that enables domain users to log onto their domain mail server and send messages from outside the network. Users must check the email messages in their account (pop) before they can send messages (relay) from their domain account, that is, pop before relay. Poprelay does not require additional configuration of the mail client.

Important: Users must first unlock the mail server by checking mails from their account before sending messages, failing which any attempt to send messages will result in a ‘Relaying Denied’ error.

Users can directly log into their mail server from anywhere in the world and relay messages using their domain mail account for two consecutive days (3000 minutes). On expiration of this authentication period users will have to again unlock their mail server in order to send email messages.

When a user logs onto the mail server from outside the network, the IP address of the computer, from which the user initiates a connection to his mail server, is recorded in the mail log file.

This IP address is verified with the list of permissible relay addresses (addresses that are authenticated to send messages via the domainвЂ™s mail server). If the IP Address is permitted to relay, then the user can send messages from wherever he is for two consecutive days.

Using SMTP_AUTH Authentication Service

SMTP_AUTH is an authentication service that enables itinerant users to send mails from anywhere using their domain mail server. SMTP is short for Simple Mail Transfer Protocol, while AUTH is short for Authentication.

Note: You must configure your mail client to enable SMTP_AUTH authentication. For more information about configuring your email client, see the program’s documentation.

To use SMTP_AUTH, you must configure your mail client to send the authentication user name and password to the domain mail server. You must select the SMTP_AUTH tag (this will depend on the email client you are using) and provide the required user name and password whenever you need to send mail.

Working With Mailing Lists

In this section:

Creating Mailing Lists

Mailing lists are lists of email recipients that can receive email as group. When you create a mailing list, messages sent to the mailing list email address are automatically sent to every email address on the list. If you sometimes send messages to all of the email users on your site, you can create a mailing list to streamline the process. You manage mailing lists through the Majordomo service.

➢ ***To create a mailing list:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Mailing Lists** (Email section). The Mailing Lists window opens.
3. Click **Create a Mailing List.** The Add a Mailing List form opens.
4. In the **List name** field, enter a name for the new mailing list. The name must be in lowercase letters. The name you enter is combined with `@<example.com>` as the email address of the mailing list.
5. In the **List Administrator Email Address** field, enter the email address of the person who will manage this mailing list.
6. In the **List Administrator Password** field, enter the password for the mailing list administrator.
7. In the **Confirm List Administrator Password** field, enter the password again.
8. Optional: In the **Description** field, enter a one-line description of the mailing list, such as for what the list will be used.
9. Optional: In the **Welcome Message** text box, enter a welcome message that will be sent to all new members on this mailing list, introducing the mailing list and describing how it is to be used.
10. Optional: In the **Email Footer** text box, enter useful information related to the mailing list, such as the name of the mailing list, the email address of the mailing list, or the Web site address.
11. Click **Create.**

Go to quick-start guide:
Set up your site's email services **(on page 25)**

Adding Members to Mailing Lists

As Site Administrator, you can use the Site Administrator control panel to manually add members to mailing lists on your domain. In addition, email users can subscribe to mailing lists by sending commands to the Majordomo server (on page 159) through email messages.

➢ ***To add members to a mailing list:***

1. Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Mailing Lists** (Email section). The Mailing Lists form opens, showing the current mailing lists on the domain.

3 Locate the mailing list to which you want to add members and in the **Actions** column, click .

4 Click **Add Member**.

5 In the text box, enter the email addresses of the users you want to add to the list, separating each address with commas.

6 Click **Subscribe**.

Majordomo sends an introductory message to each new member on the list, and also sends an email message to the List Maintainer informing the administrator that a new member is added to the list.

Viewing Your Mailing Lists

You can view all of your organization's mailing lists through the Site Administrator control panel.

➢ ***To view your organization's mailing lists:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Mailing Lists** (Email section).

The Mailing Lists form opens displaying all your existing mailing lists.

Sending Majordomo Commands

One of the benefits of using Majordomo to manage mailing lists is the ability to send commands to the Majordomo server. These commands make it possible to automate tasks such as adding or removing members to the list and getting information about the list.

You send majordomo commands to the following address:

`majordomo@`***<site name.com>***

where ***<site_name.com>*** is the name of your domain.

In the body of the email message, you can include one or more of the commands listed in the Majordomo email commands table.

Note: The email message must include *only* commands in the body of the email message; it can contain no other text.

Majordomo Email Commands

Command	**Description**
help	Receive an email message with detailed help about Majordomo
info *<mailing list name>*	Receive an email message stating when the mailing list was created or modified
lists	Receive an email message showing all the mailing lists on the domain
which *<email address>*	Receive an email message indicating the mailing lists to which the user at the email address you specify has subscribed
who *<mailing list name>*	Receive an email message listing the users who have subscribed to this mailing list
subscribe *<mailing list name> <email address>*	Add the user at the email address you specify to the mailing list you specify
Unsubscribe *<mailing list name>*	Remove yourself from the mailing list you specify
signoff *<mailing list name>*	Remove yourself from the mailing list you specify

Removing Members from Mailing Lists

Members can unsubscribe to mailing lists by sending commands to the Majordomo server (on page 159). As Site Administrator, however, you can use the Site Administrator control panel to manually remove members from lists.

➢ ***To remove a member from a mailing list:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Mailing Lists** (Email section). The Mailing Lists form opens, showing the current mailing lists on the domain.
3 Locate the mailing list from which you want to remove members and in the **Actions** column, click . The Member Management form opens.
4 Locate the email address of the member you want to remove and in the **Actions** column, click .
5 In the confirmation window, click **OK**.

The member is removed from the mailing list.

Removing Mailing Lists

➢ ***To remove a mailing list:***

1 Click the **Shortcuts** tab on the Home page.
2 **In the shortcuts area, click Mailing Lists (Email section). T**he Mailing Lists form opens, showing the current mailing lists on the domain.
3 Locate the mailing list you want to remove and in the **Actions** column, click .
4 In the confirmation window, verify the mailing list you are removing, then click **OK**.

Working with Aliases

In this section:

About Email Aliases

An email alias is a method of mapping a nickname to an actual email address. You can map aliases to:

- Mailboxes on your site's mail server
- Email addresses
- Other aliases

Whenever someone sends email to an alias at your site, the message is sent to all of the actual email addresses mapped to the alias.

For example, you could create an alias for your Sales department called `sales`. When anyone sends email to `sales@`<example.com>, the message is delivered to all of the addresses mapped to `sales`.

How Aliases and Mailing Lists Differ

Aliases are similar to mailing lists in that you can map an alias to more than one email address. In effect, this creates a list with multiple users who can receive email through the alias. Aliases differ from mailing lists, however, in that they lack scalability. Mailing lists use Majordomo (on page 157), a service that uses commands to add, remove, and manage the email addresses associated with the list and automates many tasks. Aliases are mapped individually either by Site or User Administrator; they lack the automated features of Majordomo.

Also, you can use responders to automatically reply to messages sent to aliases. You cannot use responders with mailing lists.

How Aliases Work with Responders

Aliases can be set up to use responders. Responders are prepared replies that are returned automatically to incoming email. For example, if you have an alias called `sales`, you might want to add a responder that automatically returns information about your sales department to the sender.

To set up an alias to use a responder, you first create an alias (on page 162), then add a responder to it (on page 166).

How to Manage Email Aliases

You can manage all of the email aliases on your site through the Email Manager in the Site Administrator control panel.

Note: You and your users can manage the aliases you own through the User Administrator control panel. For instructions, see the User Administrator Online Help.

From the Email Manager in the Site Administrator control panel, you can:

- View all the email aliases used on your site (on page 163)

- Add additional email aliases (on page 162)
- Update existing email aliases (on page 163)
- Remove email aliases (on page 164)

Adding Email Aliases

As Site Administrator, you can add email aliases for your site. In addition, you and your users can add aliases for yourselves through the User Administrator control panel. You can manage all of the email aliases on your site through the Site Administrator control panel.

➢ ***To add an email alias through the Site Administrator control panel:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Aliases** (Email section). The Aliases form opens, showing the current aliases on the site.
3. Click **Add an Alias.** The Add Alias form opens.
4. In the **Alias** field, enter a name for the new alias.
5. In the **Forward To** field, specify users on this site who will be included in the alias by clicking the arrow and choosing the users from the list.

   The list includes both users and other aliases. The full name of the user is shown in parentheses.

   Note: By default, the **Forward To** list above this field retains a selected name. If you are forwarding the email only to users outside the site, deselect the user in the **Forward To** list by pressing and holding the **Ctrl** key while clicking on the name.
6. In the **Forward To (outside of domain)** field, specify users outside the site who will be included in the alias. Enter the email addresses, separated by commas.
7. Click **Add Alias.**

Go to quick-start guide:
Set up your site's email services **(on page 25)**

Viewing Your Email Aliases

As Site Administrator, you can view a list of all the aliases on your site. This includes aliases you create as Site Administrator and aliases your users create through the User Administrator control panel.

To view all of the email aliases used on your site:

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Aliases** (Email section). The Aliases form opens, showing the current aliases on the site.

   The columns in this form are:

   - **Alias -** The name of the alias.
   - **User/Email Address -** The email address or user name to which the alias maps.
   - **Actions -** From this column you can update (on page 163) or remove (on page 164) an alias.

Updating Email Aliases

As a Site Administrator, you can update any of the email aliases used on your site.

➢ ***To update an email alias:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Aliases** (Email section). The Aliases form opens, showing the current aliases on the domain.
3. Locate the alias you want to update and in the **Actions** column, click  .The Edit Alias form opens.
4. In the **Forward To** field, specify users on this domain who will be included in the alias by clicking the arrow and selecting or deselecting the users from the list.
   The list includes both users and other aliases. The full name of the user is shown in parentheses.

Note: By default, the **Forward To** list above this field retains a selected name. If you are forwarding the email only to users outside the domain, de-select the user in the **Forward To** list by pressing and holding the CTRL key while clicking on the name.

1. In the **Forward To (outside of domain)** field, specify or clear users outside the domain who will be included in the alias. Enter the email addresses, separated by commas.
2. Click **Update Alias**.

Removing Email Aliases

As a Site Administrator, you can remove any of the email aliases used on your site.

➢ ***To remove an email alias:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Aliases** (Email section). The Aliases form opens, showing the current aliases on the domain.

3 In the Alias form, locate the alias you want to remove and in the **Actions** column, click .

4 In the confirmation window, click **OK.**
The alias is removed from the list of aliases.

Working with Responders

In this section:

About Responders

A responder is a method of automatically replying to incoming email.

Responders can be set up for aliases only. They cannot be set up for individual email addresses or mailing lists. Whenever anyone sends email to the alias, a prepared reply is automatically returned to the sender.

For example, you might want all email sent to your customer service department to receive an automatic reply about your hours and contact information. To do so, you can create an alias called `customerservice` then create a responder for that alias. Whenever email is sent to `customerservice@`<example.com>, the prepared reply is sent automatically.

How Responders Differ from Vacation Messages

Both responders and vacation messages automatically reply to incoming email. However, they have these key differences:

- Responders can be set up only for aliases; vacation messages are set up for email addresses.
- Vacation messages are sent only once. If users send multiple messages to an email address that has a vacation message enabled, they receive only one automatic reply. Messages sent to aliases using responders receive replies each time the message is sent.
- As Site Administrator, you can manage all of the responders used on your site through the Site Administrator control panel. Vacation messages can be managed only by individual users through the User Administrator control panel.

How to Manage Responders

You can manage all of the responders for your site from the Email Manager in the Site Administrator control panel.

From the Email Manager, you can:

- View existing autoresponders (on page 167)
- Add additional autoresponders (on page 166)
- Update existing autoresponders (on page 167)
- Remove autoresponders (on page 168)

Adding Responders

As Site Administrator, you can add responders for aliases used on your site. In addition, you and your users can add responders through the User Administrator control panel. Whenever anyone sends email to the alias, a prepared reply is automatically returned to the sender.

Responders can be set up for aliases only. They cannot be set up for individual email addresses or mailing lists.

Note: Before you add a responder, you need to add an alias.

➢ ***To add a responder:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Responders** (Email section). The Responders form opens, showing all the existing responders on the domain.
3. Click **Add a Responder**. The Add Auto Responder form opens.
4. In the **Alias** field, click the arrow and from the list, choose the name of the user or alias for which the responder is being created.
5. In the **Subject** field, enter the subject that will qualify the auto-responder message. For example, enter `Thanks for your request.`
6. In the **Message** field, enter the message you want to send in reply to the incoming email.

   For example, to customers who email you to request a catalog of your services, you might send the following reply: "`Thank you for your interest. We are sending you the information you requested.`"
7. Click **Add Responder**.

   The control panel adds the response to the directory `/usr/share/opcenter/responders`.

Go to quick-start guide:
Set up your site's email services **(on page 25)**

Viewing Responders

As Site Administrator, you can view a list of all the responders on your site. This includes responders you create as Site Administrator and responders your users create through the User Administrator control panel.

➢ ***To view all of the responders used on your site:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Responders** (Email section). The Responders form opens, showing all the existing responders on the domain.

The columns in this window are:

- **Alias.** The name of the alias for which the responder is created.
- **File.** The file in which the response is stored.
- **Actions.** From this column, you can update (on page 167) or remove (on page 168) an responder.

Updating Responders

As Site Administrator, you can update any of the responders used on your site.

➢ ***To update an responder:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Responders** (Email section). The Responders form opens, showing all the existing responders on the domain.

3 Locate the alias whose responder you want to update and in the **Actions** column, click . The Edit Auto Responder form opens.

4 In the **Subject** field, enter the subject that will qualify the responder message. For example, enter *Thanks for your request*.

5 In the **Message** field, enter the message you want to send in reply to the incoming email.

6 Click **Update Responder**.

Removing Responders

As Site Administrator, you can remove any of the responders used on your site.

➢ ***To remove a responder:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Responders** (Email section). The Responders form opens, showing all the existing responders on the domain.

3 In the Responders form, locate the alias whose responder you want to remove and in the **Actions** column, click ❌.

4 In the confirmation window, click **OK**.

Working with Message Forwarding

In this section:

About Message Forwarding

Message forwarding is a service that redirects, or forwards, email sent to your Site Administrator email address. Once you set up message forwarding, messages are automatically forwarded to the address you specify. Forwarded messages are accessible only through the account to which they are forwarded. No copies are kept in the System Administrator email account.

Message forwarding is useful when you want access all of your email through one account, or when you want to prevent Site Administrator email from taking up too much disk space on your site.

Important: Email messages sent to your Site Administrator email address can quickly accumulate and devour disk space. To save disk space, you can use message forwarding. If you do not use message forwarding, it is recommended that you periodically forward Site Administrator email to an off-site address, then delete it from your account.

You can set up (on page 169), view (on page 169), and stop (on page 169) message forwarding.

Setting up Message Forwarding

➢ ***To set up message forwarding:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Forward Administrator Email** (Email section). The Forward form opens.

3 On the Forward form, click . The Editing Forward form opens.

4 In the **Forward Administrator's Email To** field, enter the email address to which you want to forward your email messages.

5 Click **Update**.

Note: If your email account contains email messages prior to setting up message Nforwarding, they are not forwarded. Only those email messages that you receive after you set up message forwarding are forwarded.

Viewing Your Message Forwarding

➢ ***To view your existing message forwarding information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Forward Administrator Email** (Email section).

The Forward form opens displaying the forwarding address for the Site Administrator's email. If no address appears on the Forward form, messages are not being forwarded.

Removing Message Forwarding

➢ ***To stop message forwarding:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Forward Administrator Email** (Email section). The current message forwarding address is displayed.

3 On the Forward form, click . The Editing Forward form opens.

4 In the **Forward Administrator's Email To** field, clear the existing email address and leave the field blank.

5 Click **Update**.

Managing Spam

In this section:

Overview of Spam Filtering

Spam is an unsolicited email message. You can control spam by creating a Sendmail Reject List (on page 171) or by using the **Spam Filtering** service to enable user-level spam control.

To provide spam filtering capability to users, your service provider must enable the service for your site.

Note: If the service is enabled for your site, the service is displayed in the View Services page along with the list of services available for your site. You do not have to perform any special configuration tasks in the control panel to enable spam filtering capability for your site users.

When the service is enabled for your site, the User Administrator is automatically invested with the ability to create email filter lists, set the spam threshold, and configure spam management options. If you want to configure spam settings for your email account, you must log in with your account user name and password to the User Administrator control panel and configure the spam settings.

You can also use the Sendmail Reject List (on page 171) to reject spam. The Sendmail Reject List and spam filter lists vary in their approach and flexibility (on page 172) in managing spam.

Using the Sendmail Reject List to Manage Spam

The Sendmail Reject List is a list of email sources that you identify as sources of unsolicited email. It disallows delivery of email messages from the sources identified in the list to any site user. For example, if you include the IP address `1.2.3.4` in the Reject List, all email messages that originate from the address will be blocked from being relayed to all users of the site.

The address source can be any of the following:

- An email address - The email address is blocked.
- A site - All email messages that originate from the site are blocked.
- An IP address - All email messages that originate from the specified IP address are blocked.

  If you enter a partial IP address, all email messages that originate from any IP address in the subnet are blocked. For example, specifying `1.2.3` will block all IP addresses in the subnet, `1.2.3.0` through `1.2.3.255`.

You can also use the Spam Filter service (on page 170) to control and manage spam. The Sendmail Reject List and spam filter lists vary in their approach and flexibility (on page 172) in managing spam.

Using the Sendmail Reject List and Spam Filtering Service

The control panel offers two spam filter options - the Sendmail Reject List (on page 172) and Spam Filtering (on page 172) service - that vary in their approach and flexibility in managing spam.

Note: You do not have to perform any special configuration tasks in the control panel to enable spam filtering capability for your site users. The service is automatically available to your users when enabled for the site by your service provider.

While the Sendmail Reject List enables effortless global control on relay of spam email messages to site users, the Spam Filtering service allows for discretionary management of spam by the users themselves.

Sendmail Reject List

Email sources that you identify as illegitimate can be blocked from being delivered to any user of the site.

Advantages

- The Sendmail Reject List allows global control on the relay of email messages to site users. The email sources included in the Reject List are blocked from being delivered to any site user.
- Rejecting spam at the site level correspondingly reduces the scale of spam filtering at the user level. This releases system resources that would otherwise be utilized for scanning.
- Rejecting spam at the site level reduces the risk of email viruses infiltrating the network.

Spam Filtering service

While the Sendmail Reject List allows rejection of spam email messages, the Spam Filtering service allows discretionary management of spam.

Advantages

The Spam Filtering service allows flexibility in controlling and managing spam. The User Administrator can review the email messages and choose to delete spam messages, have them delivered as an attachment, or quarantine them in a spam folder.

Disadvantages

- Filtering at the user level introduces security risks posed by email viruses.

CHAPTER 11

Managing Other Services

In this chapter:

Overview of Services

In this section:

Viewing the List of Services

The Services list shows the services available to your site.

➢ ***To get to the Services page:***

On the System Menu at left, click Services.

On this page you can perform several tasks and view the following information:

- **Name**. The name of the service. See service descriptions (on page 20) for details about each service.
- **Version**. The version of the service running on the server.
- **Status**. The current status of the service. States include:
  - . The service is running.
  - . The service is not running. If a service is not running, contact your service provider.
  - **Blank (no icon)**. The service exists but there is no running state. Services without running states include Majordomo, SquirrelMail, Microsoft FrontPage 2002 Server Extensions, and Vacation Responder/Email Forward.
- **Actions**. Links to tasks you can perform.

On the Services List You Can

- Access a service's settings and properties by clicking  in the **Actions** column.

Accessing and Using Services

This topic describes the available services. Your service provider determines which services are enabled for your site.

User Names and Passwords for Accessing Services

You use your Site Administrator user name and password to access services. If you change your Site Administrator password, you are also changing the password you use to access services such as FTP, Telnet, and SSH. These services all use the same password.

If you have Microsoft FrontPage Extensions enabled for your site, however, be aware that the Microsoft FrontPage Administrator password is on a separate system and does not change automatically. You can change the FrontPage Administrator user name or password using the FrontPage Extension Permission Management Interface (on page 139).

Service Description and Access Information

Note: Your site might not have all of the services listed. For more information about a service, contact your service provider.

Service name	Description
Apache Web server	Responds to requests from Web browsers. The Web server serves requests from browsers by retrieving a requested file or executing a CGI script.
Domain Name Server	Translates site names into IP addresses. DNS is a distributed database that performs name translations. To manage this information effectively, DNS has a distributed architecture, composed of many DNS servers in a hierarchical fashion. Each server is responsible for both name-to-IP-address and IP-address-to-name translations.
Mailing Lists (Majordomo)	Manages mailing lists. Mailing lists are commonly used to circulate topic discussions. A mailing list includes a set of list members. Whenever a list member posts an email message to the mailing list email address, that email message is distributed to all list members.

Microsoft FrontPage Server Extensions	Allows you to support users who want to use Microsoft FrontPage to manage their Web sites. In the control panel, you can access FrontPage administration Web pages from the Web Server Manager.
WebDAV Server	WebDAV (Web-based Distributed Authoring and Versioning) allows you to collaboratively edit and manage files on the remote Web servers.
Miva Merchant	Provides ecommerce support for sites. Miva Merchant enables you to create multiple online storefronts and support ecommerce on a site.
mod_perl for Apache	mod_perl enables you to create dynamic content by utilizing the full power of the Apache web server to create stateful sessions and customized user authentication systems. You can use Perl to manage Apache and respond to requests for Web pages.
MySQL Database	Allows you to work with your SQL databases. MySQL is a widely used relational database management system for SQL databases. A relational database stores data in separate tables rather than in one big table. A database management system allows you to add, access, and process data stored in a SQL database. In the control panel, you can use phpMyAdmin to set up, configure, and view your databases.
Open SSH Secure Shell	Provides secure remote access to another system over a network. In the case of the control panel, SSH allows you to log on to the server remotely and move files, run scripts, or search across multiple files in a secure environment. To use an SSH connection you need to be familiar with the UNIX operating system and commands.
Open SSL Secure Web	Provides secure Web pages. SSL is a protocol that transmits private documents through the Internet. It creates a secure connection between a client and a server over which any amount of data can be sent securely. SSL works by using a private key to encrypt data transferred over the SSL connection. In the control panel, you can secure your site through the Web Server Manager.
PHP Hypertext Preprocessor for Apache	Creates dynamic Web pages. PHP (PHP Hypertext Preprocessor) is a server-side, cross-platform, HTML embedded scripting language.
phpMyAdmin Web-based MySQL Administration	Allows you to manage your MySQL databases over the Internet. phpMyAdmin can handle administration of entire MySQL database servers or just a single database over the Internet by removing any platform-specific limitations.

Power Tools	Streamlines the installation and use of off-the-shelf Web applications. Power Tools provide ecommerce, content management, forums, chat, and other dynamic features of Web sites.
POP3 + IMAP Server	POP3 (Post Office Protocol, version 3) is a protocol used to retrieve email from a mail server. IMAP (Internet Messaging Access Protocol) is a protocol that retrieves messages from the mail server. Using IMAP, you can search through your email messages using keywords and selectively download messages. The IMAP server allows users to archive email messages in folders, share mailboxes with other users, access multiple mail servers at one time, and more efficiently access email attachments. Both POP and IMAP mail servers accept SMTP-formatted email messages.
FTP	Transfers files over the Internet. FTP (File Transfer Protocol) allows you to transfer files over the Internet. Anonymous FTP (if available) allows you to use an FTP site without creating a user account. To use FTP, you need to be familiar with FTP commands or use a program that manages those commands for you.
Anonymous FTP	An anonymous way to transfer files over the Internet. Anonymous FTP allows you to use an FTP site without creating a user account. To use anonymous FTP, you need to be familiar with FTP commands or use a program that executes those commands for you.
Email	Routes outgoing and incoming mail using SMTP. Sendmail is an SMTP (Simple Mail Transfer Protocol) mail server that routes SMTP email messages through the Internet to be stored on a mail server. SMTP is the most common email protocol on the Internet. Sendmail also allows you to manage your email features, such as email aliases, responders, and spam filters.
SquirrelMail Web-based Email	Provides Web-based access to email accounts. Squirrel Mail is an email client that uses IMAP to provide your email account users with Web-based access to their email messages.
Telnet	Provides remote access to another system over a network. Telnet is a common terminal emulation protocol that connects computers locally or across the Internet. It allows a user at a local computer to log onto a remote computer and run a program. To use a Telnet connection you need to be familiar with the UNIX operating system and commands.
Vacation message	Automatically responds to incoming email.

MailScanner	Email scanning service that scans incoming and outgoing emails for viruses.
Spam Filtering	Spam filtering service that scans email messages for spam and enables user level control and management of spam.
AWStats Web/FTP Log Analyzer	AWStats is a free powerful and featureful tool that generates advanced web and ftp server statistics, graphically.
Analog Web/FTP Log Analyzer	Measures the usage traffic on your Web and FTP servers. Analog Web/FTP Log Analyzer compiles statistics about which Web pages are most popular, which countries people are visiting from, which Web site visitors tried to follow broken links from, and other such information.
Webalizer Web/FTP Log Analyzer	A free log file analysis application. Webalizer generates highly detailed usage statistics for Web and FTP servers in easily comprehensible graphical and tabular formats. The logs generated are a statistical encapsulation of user traffic on your server.

Viewing Enabled Services

You can view all of the services available to your site. Your service provider determines which services are enabled for your site.

➢ ***To view all enabled services:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click View Services (Tools section). The Service list (on page 174) is displayed. It shows all the services available to your site.

For details about each service, see the service descriptions (on page 20).

Changing Service Settings

If a service is configurable, you can change its settings to suit your business needs.

The following services are configurable:

- Email (on page 153) (email aliases, responders, spam filters, message forwarding)
- Majordomo (on page 153) (mailing lists) (if available)
- Miva Merchant (on page 196) (e-commerce)
- MySQL (on page 181) (database management)
- Web Server (on page 82) (Open SSL Secure Web and links to Microsoft FrontPage 2002 Server Extensions)

Changing Service Settings

➢ ***To change service settings:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **View Services** (Tools section). The Service List, which shows the services available to your site, is displayed.

3 Locate the service whose settings you want to change, then in the **Actions** column of that service, click .

Checking whether a Service Is Running

The status of a service can be determined from the Service List.

➢ ***To check whether a service is running:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **View Services** (Tools section). The Service List form opens displaying a list of services.

3 On the Service List form, locate the **Status** column. Icons in this column indicate the state of the service.

Status icons include:

- . The service is running
- . The service is not available

Note: Some services, such as Majordomo (if available) and Miva Merchant, have no running state. The **Status** column for these services is blank.

Managing MySQL Database Server

In this section:

MySQL Databases Overview

In this section:

Introduction to MySQL Databases

MySQL is a widely used relational database management system for SQL databases. A database management system allows you to add, access, and retrieve data stored in a SQL database.

A relational database stores data in separate tables rather than in one table. This adds speed and flexibility in accessing and retrieving data. The tables are linked by defined relations making it possible to combine data from several tables on request.

About the MySQL Database Server

The MySQL Database Server is very fast, reliable, and easy to use. Its architecture makes it extremely fast and easy to customize. The MySQL Server is designed to handle large databases and has been successfully used in highly demanding production environments. Its connectivity, speed, and security make MySQL Server highly suited for accessing databases on the Internet.

Some of the key features of the MySQL database server are:

1 **Portability**
   - Works on a range of platforms enabling you to port your databases across different operating environments
   - Provides APIs for C, C++, Eiffel, Java, Perl, PHP, Python, Ruby, and Tcl allowing you to write programs using any of these applications
   - Possesses parallel processing capability; multiple CPUs can be used to process data faster and more efficiently

2 **Security**
   - A secure password system that is very flexible, and allows host-based verification. Passwords are secure because all password traffic is encrypted when you connect to a server.

3 **Scalability**
   - Efficient in handling large databases. You can create databases with more than 50,000 tables.

If your service provider has enabled MySQL for your site, you can:

- Connect to the PHPMyAdmin MySQL interface to manage your SQL databases (on page 183)
- Change your MySQL password (on page 186)
- View the list of databases for a site (on page 187)
- Create databases (on page 188)

Important: The control panel creates a random MySQL password when it creates a site with MySQL support. You must reset the MySQL password when you log onto the Site Administrator control panel for the first time. This is important so that your MySQL password is not invalidated when you install the script packages enabled for the site.

For more information about using the PHPMyAdmin MySQL Administration Tool, see PHPWizard (www.PHPWizard.net).

For more information about working with MySQL databases, see MySQL (www.mysql.com).

About Multiple MySQL Databases

Your hosting services make it possible to use multiple MySQL databases with your site.

Note: To use multiple MySQL databases, your service provider must enable the MySQL service while creating the site and specify the number of databases that you can create.

Creating Multiple Databases

Your service provider determines the number of databases that can be created for your site. As of now, the control panel supports only one user per database.

Note: The control panel does not implicitly create databases when a site is created, even if the site is enabled to support the MySQL database service.

- The disk space consumed by a database counts toward a site's total disk quota. If a database consumes disk space in excess of the site's disk quota, you will receive an error stating that the disk is full.
- The databases are backed up when you back up the site.

Administering Databases

MySQL databases are administered by the database administrator designated by your service provider. Database administrators cannot create or delete databases. You cannot change the name of the database administrator though you can change the password.

Note: To perform operations on a database as the Site Administrator, you must be assigned the role of the Database Administrator by your service provider, and log in using this information. You **cannot** perform operations on a database using your site user name or password.

As a Site Administrator, you can:

- Create (on page 188) MySQL databases
- Delete (on page 189) MySQL databases

Managing Site Databases

In this section:

Connecting to the PhpMyAdmin MySQL Interface

If MySQL is available to you, you can connect to the phpMyAdmin MySQL interface to work with your SQL databases.

Note: You must connect to the phpMyAdmin interface as a Database Administrator to access your MySQL databases. Your database administrator user name is assigned to you by your service provider while creating the site. To find out your database administrator user name, in the shortcuts section of the Home page, click **Site Information** (Tools section). On the Configuration page, scroll down to the **MySQL** section to find the required information.

➢ ***To connect to the phpMyAdmin MySQL interface (if enabled for your site):***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **MySQL Administration Tool** (MySQL section). The Configuration window opens and displays information about, and links to the PhpMyAdmin **MySQL Administration Tool.**
3. Click **MySQL Administration Tool.**

   A new window opens, and you are prompted for your MySQL user name and password.

For more information about using the phpMyAdmin MySQL Administration Tool, see www.PHPWizard.net.

Connecting to MySQL Databases in a Secure Environment

The security level (on page 75) configured for a site defines the access and operational limits for applications and files hosted on the site. When you want to connect to the MySQL databases of your site, ensure that the security settings of the site do not conflict with the MySQL connection settings, otherwise you will be unable to connect to the databases.

Note: To ascertain the security level assigned to your site, contact your service provider.

The information in this topic is pertinent only to MySQL connections established using the command line or Web scripts. You may skip this topic if you are using the phpMyAdmin interface to manage your databases.

The following sections discuss the MySQL connection settings you need to configure (if you are using the command line) for different security levels.

- Connecting to a MySQL database on a high security site
- Connecting to a MySQL database on a medium security site
- Connecting to a MySQL database on a low security site

Connecting to a MySQL Database on a High Security Site

On a high-security site, the CGI scripts, remote login services (telnet, SSH), mod_perl, and mod_php services are restricted to the site's file system. The Site Administrator and users of the site are logged into the home directory of the site and therefore cannot access system-wide files.

When you attempt to connect to a MySQL database in your Web scripts or using the command line, the high security settings cause the connection to fail with an error. This is because the MySQL socket file, `mysql.sock`, required for connecting to the MySQL server, resides at the system level (`/var/lib/mysql/mysql.sock`) and is unavailable to the site's file system.

To connect to the MySQL database, you need to specify the IP address of the host on which the MySQL server is located and the port number.

You need to use the following command to connect to the databases.

```
mysql -h 127.0.0.1 -P 3306 -u <username> - p<password>
```

Where:
-h 127.0.0.1 is the IP address of the local host
-P 3306 is the port number
-u <username> is the user name of the Site Administrator account
-p<password> is the password of the Site Administrator account

Important: Ensure that you specify `127.0.0.1` for the `– h` option. If you specify "localhost" or "localhost.localdomain" then the MySQL client library attempts to connect to the local socket, `/var/lib/mysql/mysql.sock`. This will result in an error.

Further, ensure that you do not leave a space between the `-p` option and the password. Leaving a space implies that the password is the database name.

Connecting to a MySQL Database on a Medium Security Site

On a medium security site, the remote login services (telnet, SSH) are restricted to the site's file system. The Site Administrator and users of the site are logged into the home directory of the site and therefore cannot access system-wide files.

When you attempt to connect to a MySQL database using the command line or in your Web scripts, the medium security settings cause the connection to fail with an error. This is because you are not authorized to access the MySQL socket file, `mysql.sock` (required for connecting to the MySQL server) that resides at the system level (`/var/lib/mysql/mysql.sock`).

To connect to the MySQL database, you need to specify the IP address of the host on which your MySQL server is located and the port number.

You need to use the following command to connect to the databases.

```
mysql -h 127.0.0.1 -P 3306 -u <username> - p<password>
```

Where:
`-h 127.0.0.1` is the IP address of the local host
`-P 3306` is the port number
`-u <username>` is the user name of the Site Administrator account
`-p<password>` is the password of the Site Administrator account

Important: Ensure that you specify `127.0.0.1` for the `– h` option. If you specify "localhosNt" or "localhost.localdomain" then the MySQL client library overrides this and attempts to connect to the local socket, /`var/lib/mysql/mysql.sock`. This will result in an error.

Further, ensure that you do not leave a space between the `-p` option and the password. Leaving a space implies that the password is the database name.

Connecting to a MySQL Database on a Low Security Site

A low security site provides unrestricted access (except for access restricted by file or directory permissions) to files on the control panel server. Since the security settings do not impose access or operational limits, you can connect to the MySQL databases using the MySQL socket file, `/var/lib/mysql/mysql.sock`. Since this is the default mode of connection, you do not have to set the port number and the IP address of the host name on which the databases are located.

You need to use the following command to connect to the databases.

```
mysql -u <username> - p<password>
```

Where:
`-u <username>` is the user name of the Site Administrator account
`-p<password>` is the password of the Site Administrator account

Changing Your MySQL Password

If MySQL is enabled for your site, you can change your MySQL password at any time. We suggest you change your password after the first time you log on the MySQL interface.

Important: The control panel creates a random MySQL password when it creates a site with MySQL support. You must reset the MySQL password when you log onto the Site Administrator control panel for the first time. This is important so that your MySQL password is not invalidated when you install the script packages enabled for the site.

➢ ***To change your MySQL password:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Change Password** (MySQL section).

The Change Database Administrator Password form opens.

Note: Only your service provider can change the Database Administrator name, which appears in the Database Administrator field.

---

3 In the **New Password** field, enter a new password.

4 In the **Retype New Password** field, type the password again to confirm it.

5 Click **Update**.

Viewing a Site's Databases

You can view a complete list of your site's databases along with information specific to each database.

➢ ***To view your site's databases:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **MySQL Administration Tool** (MySQL section).

3 In the MySQL submenu, click **List Databases**. The MySQL Databases page opens.

The List MySQL Databases page displays information about all of your current databases of the site.

You can view the following information.

- **Database Name.** The name of the MySQL database.
- Space Consumed. The disk space consumed by the database (in Kilobytes).
- **Actions.** This column allows you to:
  - change the database name (on page 189)
  - delete a database (on page 189)

Creating Databases

Databases are not automatically created when your service provider enables MySQL for your site; you need to create them. Your service provider determines the number of databases you can create.

Note: Disk space resource for a database is limited to the disk quota available for the site. If the database exceeds the available disk resources for the site, an error stating that the disk is full will be evidenced.

➢ ***To create a database:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **MySQL Administration Tool** (MySQL section).

3 **In the MySQL submenu,** click **Create Database.** The Create Database form opens.

4 Enter a name for the database in the **Database Name** field. For uniqueness, the name of the database is prefixed with the corresponding Site ID. You may choose to retain it or overwrite.

Important: Database names should not exceed the maximum limit of 64 characters, inclusive of the prefix. For example, if your database prefix is 30 characters long, you must restrict the name of your database to a maximum of 30 characters, to conform to the limit (64). Four characters are reserved for internal use.

Note: The Database Administrator is assigned by your service provider at the time of creating the site. This information is pre-filled in the **Database Administrator** field and cannot be changed, except by your service provider.

5 Click **Save**.

If the database has been successfully created, it will be added to the list of current databases for the site. An appropriate message is displayed above the list of databases.

If the process fails, or succeeds with attendant warnings, click the **Details** link to view related information.

Changing Database Names

You can change the name of a database at any time.

➢ ***To change a database's name:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **MySQL Administration Tool** (MySQL section).

3 In the MySQL submenu, click **List Databases**. The MySQL Databases form opens.

4 Click in the **Actions** column next to the database whose name you want to change. The Rename MySQL Database form opens.

5 Rename the database.

Note: The prefix of the database cannot be changed.

Important: Database names should not exceed the maximum limit of `64` characters, inclusive of the prefix. For example, if your database prefix is `30` characters long, you must restrict the name of your database to a maximum of `30` characters, to conform to the limit (64). Four characters are reserved for internal use.

6 Click **Save**.

On successful renaming, an appropriate message appears in the Status panel.

Deleting Databases

You can delete a database at anytime. A Database Administrator, though, is not allowed to delete databases.

Important: A database once deleted cannot be recovered. Use this option with caution.

➢ ***To delete a database:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **MySQL Administration Tool** (MySQL section).

3 In the MySQL submenu, click **List Databases**. The MySQL Databases form opens.

4 Click in the **Actions** column next to the database you want to delete.

5 Click **OK** to confirm the deletion.

Managing Power Tools

In this section:

About Power Tools

Power Tools are off-the-shelf Web applications that provide e-commerce, content management, forums, chat, and other dynamic features of Web sites. If your service provider enables Power Tools for your site, the Power Tools shortcut appears on the Home page of the Site Administrator control panel.

To install and use Power Tools on your site, you need to have sufficient disk space and database resources.

For tools that require databases:

- You need MySQL available on your site
- You must have changed the default MySQL password (on page 186) before installing the tool

You can install (on page 192) and manage (on page 193) the tools enabled by your service provider. For a complete list of the available tools, click **Power Tools** (Tools section) in the shortcuts section of the home page.

Power Tools Page

➢ ***To get to the Power Tools page:***

If your service provider has enabled Power Tools for your site, click Power Tools in the Tools shortcut on the Home page.

This page shows the Power Tools available to your site. On this page you can perform several tasks and view the following information:

- **Power Tool Home Page**. The icon representing the tool. Click this to go to the tool's Internet home page.
- **Description**. A brief overview of the tool.
- **Installations**. The number of times the tool has been installed on your site. If **0** appears in this column, the tool has yet to be installed on your site.
- **Actions**. Links to tasks you can perform.

On this page you can:

- Access the Internet home page of the tool by clicking the tool's icon.
- Click **Action** column links. These include:

1. , install the tool (on page 192). This takes you to a page where you can install the tool on your site.
2. , list installations (on page 193). This takes you to a page listing all the installations of the tool. There, you can reconfigure (on page 193) or uninstall (on page 195) tools if necessary. This is available only if you have already installed the tool.

Installing Tools

If Power Tools is enabled for your site, you can install and use Power Tools on your site.

Power Tools do not use any of your site's allocated disk space or other resources until you install them. To install tools, however, you need to have enough disk space and database availability for the tools. If you do not have enough of these resources, contact your service provider to increase your settings.

If you are installing a tool that requires a database, you need MySQL available on your site and you need to have changed the default MySQL database password (on page 186) before you install the tool.

➢ ***To install a tool:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Power Tools** (Tools section). If you do not see this link, your service provider has not enabled Power Tools for your site.

3 On the Power Tools page, click in the **Actions** column of the tool you want to install.

4 Provide the information required on the installation form. This information includes:

- Where to install the tool on your site.
- The user who will own the tool. This user owns all of the files associated with the tool.
- A user name for tool administration. If the tool has a control panel, this is the user name required for access.
- A password for tool administration. If the tool has a control panel, this is the password required for access.
- Database information. Many tools require their own databases. For these tools, you need to have databases enabled and available.

1 When you have completed the form, click **Install**.

The tool is installed. If additional steps are required to use the tool, they are listed on the confirmation page.

Installations Page

The installations page lists each of the installations of a tool on your site. You can see this page only if you have installed a tool on your site.

To get to the installations page:

1 On the shortcuts page, click **Power Tools**.

2 On the Power Tools page, click the **List Installations** icon in the Actions column.

Information on this page includes:

- **Power Tool URL**. The Internet address of the installation. Click this address to access the tool.
- **Installation Path**. The location on your site where the tool's software is installed.
- **Actions**. Tasks you can perform. These include:
  - , change information about the tool or recover missing files
  - , remove the installation

Changing Installed Tools

You can change the parameters of Power Tools you have installed.

➢ ***To change an installed tool:***

1 Go to the On the Home page, click the **Power Tools** shortcut in the Tools section. If you do not see this link, your service provider has not enabled Power Tools for your site.. The tools available to your site are displayed.

2 On the Power Tools page, click in the **Actions** column of the tool you want to change. If you do not see the icon, you have not yet installed the tool (on page 192). The installations page is displayed.

3 In the **Actions** column of the installation you want to change, click . The current settings are displayed.

4 Change the settings of the tool. Click the Help icons next to the field names for more information about the settings.

5 Click **Reconfigure**.

Upgrading User Instances of a Tool

You must individually upgrade each user instance to upgrade the existing user instances of a tool to its latest version. When you upgrade, you can choose to back up the data and files specific to a tool.

➢ ***To upgrade:***

1. Go to the On the Home page, click the **Power Tools** shortcut in the Tools section. If you do not see this link, your service provider has not enabled Power Tools for your site.. The tools available to your site are displayed.
2. In the **Actions** column of the tool that you want to upgrade, click .
3. In the **Actions** column of the user instance that you want to upgrade, click . The current settings are displayed. Change the settings of the tool, if required. Click the Help icons next to the field names for more information about the settings.
4. Click **Reconfigure**.
5. In the **Available updates** section, select the version you want to upgrade to and click **Upgrade To**.
6. Optional: If you want to back up data and files specific to the tool, enter the backup information.
7. Click **Upgrade**.

   The user instance of the tool is upgraded.

Changing the Owner of an Installed Tool

You can change the owner of Power Tools you have installed.

➢ ***To change a tool's owner:***

1. Go to the On the Home page, click the **Power Tools** shortcut in the Tools section. If you do not see this link, your service provider has not enabled Power Tools for your site..

   The tools available to your site are displayed.
2. On the Power Tools page, click in the **Actions** column of the installation you want to change. If you do not see the icon, you have not yet installed the tool (on page 192).

   The installations page is displayed.
3. In the **Actions** column of the installation you want to change, click . The current settings are displayed.
4. In the power tool owner drop-down menu, choose the user you want to own the tool, then click **Reconfigure**.

Removing Installations of Tools

You can remove an installation of a tool if you want to permanently delete that installation from your site. When you remove an installation, the tool itself remains available to your site, but the installation, or instance, is removed.

➢ ***To remove an installation of a tool:***

1 Go to the On the Home page, click the **Power Tools** shortcut in the Tools section. If you do not see this link, your service provider has not enabled Power Tools for your site..

The tools available to your site are displayed.

2 On the Power Tools page, click in the **Actions** column of the installation you want to remove. If you do not see the icon, you have not yet installed the tool (on page 192).

A page showing all installations of the tool is displayed.

3 In the **Actions** column of the installation you want to remove, click .

4 In the dialog box, click **OK**.

Managing Miva Merchant

In this section:

Connecting to Miva Merchant

Miva Merchant allows you to create multiple online storefronts on your domain. If Miva Merchant is enabled for your site, you can connect to the Miva Merchant interface and set up a new storefront, manage your existing storefronts, and access the actual storefront itself.

➢ ***To connect to Miva Merchant:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **View Services** (Tools section). The Service List form opens, showing the services enabled for your site.

3 On the Service List form, locate **Miva Merchant** and in the **Actions** column, click . The Miva Merchant Configuration form opens and displays links to various Miva interfaces.

4 Click the link to access the feature you want.

The links in this form are:

- **Miva Merchant Setup.** Allows you to enter first time setup information in Miva Merchant following the installation.
- **Miva Merchant Administration.** Allows you to create your ecommerce storefront.
- **Miva Merchant.** Connects to your actual storefront.
- **Miva Merchant Upgrade.** Provides information about Miva Merchant and hosting services upgrades.

C H A P T E R 1 2

Managing Directories and Files

In this chapter:

File Manager Overview

The File Manager enables you to manage files and directories that are stored on your site.

These files include scripts and other files used on your Web site, email data, and other files you place on your site. The File Manager displays information, provides access to file-related tasks, and helps you navigate through directories (on page 201).

➢ ***To get to the File Manager:***

In the shortcuts area of the Home page, click **Manage Files** (File Manager section).

Tasks in the File Manager section

Working with files:

- Opening files on your site (on page 209)
- Viewing file properties (on page 210)
- Changing file permissions (on page 211)
- Modifying files on your site (on page 212)
- Copying and moving files between directories (on page 215)
- Copying files from your site to your workstation (on page 216)
- Copying files from your workstation to your site (on page 217)
- Removing files from your site (on page 218)

Working with directories:

- Opening directories (on page 202)
- Viewing properties of directories (on page 204)
- Changing directory permissions (on page 205)
- Renaming directories (on page 205)
- Copying and moving directories (on page 207)
- Removing directories (on page 208)

Information displayed on File Manager pages

- File and directory information (on page 198)
- Clipboard commands (on page 198)
- Clipboard contents (on page 198)
- Upload information (on page 198)

File and Directory Information

- **Path:/**<name of current directory>. The path name of the directory you are currently viewing. Each directory and subdirectory is separated by /.
- **Check box**. A box you click to select the item. When you click the check box, appears in the box. Any commands you execute in the Commands section, such as **Add File(s) to Clipboard** or **Delete File(s)**, are applied to the checked items. The Commands section appears below the file and directory information.
- **Name**. The icon and name of the directory or file. In the **Name** column you can:
  - Click , , or to access an item's properties. Grayed out icons are symbolic links (see "About Actual and Symbolic Links" on page 203).
  - Access directories by clicking directory names.
  - Download files by clicking file names.
  - Click ..to go up to the parent (next higher) directory.
- **Size**. The size of the directory or file.
  - B indicates bytes
  - KB indicates kilobytes
  - MB indicates megabytes
- **Owner**. The user to whom the file or directory belongs. This owner can change or remove item; items that belong to Root cannot be changed or removed.
- **Actions**. Commands you can perform on the file or directory. Commands include:
  - . Edit the file in a text editor. This option is only available if the file is editable in a text editor and if you have write permission for the file.
  - . Remove the file. This option is only available if you have write permission for the file.

Note: To view permissions, click the icon associated with the file .

Command Information

- **Add File(s) to Clipboard**. Place a file on the clipboard so that it can be copied to another location on the site. When you click **Add File(s) to Clipboard**, all files that are selected (files or directories that have in the check box next to their icon) are added to the clipboard.
- **Delete File(s)**. Remove files or directories from the site. When you click **Delete File(s)**, all files that are selected (files that have in the check box next to their icon) are removed from the site. To delete a directory check the force box before you click Delete File(s).
- **Make directory**. Create a new directory. Type the name of the directory you want to create, then click **Make directory**. The new directory is added to the current directory. The current directory is shown toward the top of the page in the **Path** bar.

Clipboard Contents

Note: This section appears only if you have added a file to the clipboard.

- **Check box <*path and file name*>**. The check box you click to select the file and the path name to the file on the clipboard.
- Clipboard commands:
  - **Copy**. Click to copy the selected clipboard contents to the current directory.
  - **Move**. Click to move the selected clipboard contents from its present directory to the current directory.
  - **Clear**. Click to remove the selected clipboard contents from the clipboard.

Upload Information

- **Upload file**. The file you want to upload, or copy from your computer to your site. To locate a file on your computer, click **Browse**, select the file, then click **Open**.
- **And save as**. The name you to give the file. This can be the same as the file's original name or any name you choose, with or without an extension. To upload the file, type a name for the file in the **And save as** field, then click **Upload**.

Working with Directories

In this section:

Navigating Through Directories

Using the File Manager to navigate through directories on your site is similar to navigating through the directories on your own computer. The File Manager section represents directories and files using folder and file icons.

➢ ***To get to the File Manager:***

In the shortcuts area of the Home page, click **Manage Files** (File Manager section).

Things to keep in mind when you move through directories:

- The **Path** bar toward the top of the page shows which directory you are currently in. Directories are separated by /.
- **Path:/** is the top level directory.
- Click **icons** to access properties.
- Click **directory names** (text) to move to directories.
- Click **file names** to download files.
- Click ..to move up to the next higher directory (not available if you are in the top-level directory, which is shown in the Path bar as /).
- The File Manager uses both actual and symbolic links (see “About Actual and Symbolic Links” on page 203).

Opening Directories

Using the File Manager, you can open and manage directories on your site.

You can open a directory to see the sub-directories and files contained within it. Once you open a directory, you can then open a subdirectories within it, and in this manner, *drill down* in the contents of each directory.

To check where you are in the directory structure, look at the top of the Path form. The directory path is displayed there. You can always return to a previous directory level.

To open a directory:

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 On the directory list, locate the directory you want to open, then click the underlined name of that directory, for example, click **var**.

   The directory window opens, displaying the sub-directories and files contained within it.

4 To open a subdirectory, locate the subdirectory you want to open, and click the underlined name of that subdirectory.

After you open a directory, you can:

- Create additional directories (on page 206)
- Rename existing directories (on page 205)
- View directory properties (on page 204)
- Change directory permissions (on page 205)
- Copy and move directories (on page 207)
- Remove directories (on page 208)

Returning to the Previous Directory Level

To return to a previous directory level after browsing to a directory, in the **Name** area of the Path form, click at the top of the directory list. The previous directory level is displayed.

About Actual and Symbolic Links

In the File Manager section of the Site Administrator control panel, directories and files are shown as either **actual** or **symbolic links:**

- Actual links are links to files or directories that are located in the directory shown. Actual links are represented by color icons:  and .
- Symbolic links are shortcuts that are usually placed in top-level directories to provide quick access to directories and files that lie deeper in the directory structure. Symbolic links are represented by the grayed-out icon: .

In the File Manager section, you can work with existing symbolic links the same way you work with actual links; you can open, rename, or move them.

However, you can add symbolic link directories and files only when you are logged on to your site through Telnet or SSH service.

Considerations for Working with Symbolic Links

Because symbolic link directories and files are shortcuts to existing actual directories or files, the following considerations apply:

- When you move or delete a directory or file to which a symbolic link directory or file refers, you will break the link. Broken link directories and files are represented with  and .
- When you delete a symbolic link directory or file, you only remove the shortcut link. The data in the actual file to which the symbolic link directory or file refers remain intact. To remove the data, you must delete the actual directory or file.

Viewing Directory Properties

You can view information about a directory and check its properties, such as read, write, and execute permissions.

➢ ***To view directory information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 On the directory list, locate the directory you want to open, then click or next to it.

The Properties form opens displaying information about the directory.

The information includes:

- **The type of directory**. The type name is located at the top of the form
- **Path.** (Symbolic Link directory only). Where in File Manager the link resides
- **Link to.** (Symbolic Link directory only). The item to which actual directory the link refers
- **Owner.** The owner of directory
- **Group.** The group to which the owner belongs
- **Size.** The size of the directory in bytes
- **Last modified.** The date and time of the last change to the directory
- **Permissions section**. This section shows the read, write, and execute permissions of the directory.

Changing Directory Permissions

You can change the read, write, or execute permissions of directories you own on your site. However, you cannot change permissions of the `/home` or `/` (root) directories.

➢ ***To change directory permissions:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 On the directory list, locate the directory you want to open, and click or next to it.

The directory window opens displaying the current permissions.

4 In the Permissions area of the directory window, select the check box to grant permission or clear the check box to deny permission.

Note: Some changes, such as removing Read permission from the owner of a directory, cannot be made.

5 Click **Update Permissions**.

Renaming Directories

You can rename directories you own on your site. You cannot rename any directory in the directory `/` (root).

➢ ***To rename a directory:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 Browse (on page 202) to the directory you want to rename.

4 In the **Name** area of the Path form, locate the directory you want to rename, and click or next to it. The directory window opens.

5 In the **Commands** area of the directory window, in the **Rename to** field, enter the new name for the directory.

6 Click **Rename**.

Creating Additional Directories

You can create additional directories on your site at any time; however, you cannot create directories under the directory level / (root).

Note: Symbolic links to directories can be created only through a Telnet or SSH connection.

➢ ***To create a directory:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.
3. Browse (on page 202) to the directory under which you want to create a subdirectory.
4. In the **Commands** area of the Path form, in the **Make directory** field, enter the name of the new directory.
5. Click **Make directory.**

   The directory appears on the directory list.

Copying and Moving Directories

You can copy and move directories on your site from one directory to another by using the **Clipboard Contents** section of the File Manager. You can remove clipboard contents at any time.

Note: You must own the directory you are copying or moving. Further, you must have write permission for the directory into which you are copying or moving the directories.

➢ ***To copy or move a directory:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 Browse (on page 202) to the directory you want to copy or move.

4 In the **Name** area of the Path form, locate the directory you want to copy or move, and select the check box next to it.

5 In the **Commands** area of the Path form, click **Add File(s) to Clipboard.**

The File Manager displays the directory name in the Clipboard Contents area of the Path form.

6 Browse (on page 202) to the directory into which you want to copy or move the directory.

The directory window of the destination directory opens.

7 In the **Clipboard Contents** area of the Path form, locate the name of the directory you want to move or copy and select the check box next to it.

8 Do one of the following:

- To copy the directory to this destination directory, click **Copy**.
- To move the directory to this destination directory, click **Move**.

Note: If the Move operation fails, File Manager compensates by making a copy of the directory in the destination directory; however, you must manually remove the directory from its original directory.

Removing Contents from the Clipboard

➢ ***To remove directories from the Clipboard:***

1 In the Clipboard Contents area of the Path form, select the check boxes of the directories you want to remove.

2 Click **Clear**.

Removing Directories

You can remove from your site any of the directories you own.

➢ ***To remove a directory:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.
3 Browse (on page 202) to the directory you want to remove.
4 In the **Name** area of the Path form, locate the directory you want to remove, and select the check box next to it.
5 In the **Commands** area of the Path form, select the **force** check box.

Important: If you do not select the **force** option, you cannot remove the directory.

6 Click **Delete File(s)**.

Working with Files

In this section:

Opening Files

You can open files to see their contents. You may have to drill down (on page 202) to the directory that contains the file you want to open. For more information about opening directories, see the topic Opening Directories (on page 202).

➢ ***To open a file:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.
3. If necessary, browse (on page 202) to the directory that contains the file you want to open.
4. In the Path form, locate the file you want to open, then click the underlined name of that file.

After you open a file, you can:

- View file properties (on page 210)
- Change file permissions (on page 211)
- Rename files (on page 211)
- Modify the contents of some file types (on page 212)
- Copy and move files (on page 215)
- Move files from your site to your local system (on page 216)
- Move files from your local system to your site (on page 217)
- Remove files from your site (on page 218)

Viewing File Properties

You can use the File Manager section of the Site Administrator control panel to view information about files on your site and check their read, write, and execute permissions.

➢ ***To view file information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to view.

4 In the Path form, locate the file you want to view, and click next to it. The Properties form opens displaying information about the file.

The information includes:

- **The type of file**. The name is located at the top of the form
- **Path** (Symbolic Link file only). Where in File Manager the file resides
- **Link to** (Symbolic Link file only). The file to which a symbolic link refers
- **Owner.** The owner of the file
- **Group.** The group to which the file's owner belongs
- **Size.** The size of the file in bytes
- **Last modified.** The date and time of the last change to the file
- **Permissions**. The read, write, and execute permissions of the file

Changing File Permissions

You can change the read, write, or execute permissions of files you own on your site. However, you cannot change permissions of files in the `/home` or `/` (root) directories.

➢ ***To change a file's permissions:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to change.

4 In the Path form, locate the file you want to change, and click next to it.

The file window opens displaying the current permissions.

5 In the Permissions area of the file window, select the check box to grant permission or clear the check box to deny permission.

Note: Some changes, such as removing Read permission from the owner of a file, cannot be made.

1 Click **Update Permissions**.

Renaming Files

As Site Administrator, you can rename any files that you own. However, you cannot rename files in the root directory (/).

➢ ***To rename a file:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to change.

4 In the **Name** area of the Path form, locate the file you want to rename, and click next to it. The file window opens.

5 In the **Commands** area of the file window, in the **Rename to** field, enter the new name for the file.

6 Click **Rename**.

Modifying Files

You can modify files in certain formats directly through the File Manager section of the Site Administrator control panel. Files that can be modified include HTML and text files; files that cannot be modified include graphical images and other binary files.

You must have write permission to be able to modify files. To determine permissions, you can view file properties (on page 210).

➢ ***To modify a file:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to change.

4 In the **Name** area of the Path form, locate the file you want to modify, and click next to it. The file window opens displaying the file text in a text box.

Note: If you do not see a next to the file, you cannot modify that file directly through the Site Administrator control panel.

5 Make your changes in the text box.

6 To save your changes, in the **Commands** area, click **Save**.

Editing the index.html File

The home page of your Web site is a file named `index.html`. This is the Web page visitors see when they access your site from the Internet.

The file is originally created by your service provider and stored on your site. You can edit the file through the File Manager, or you can replace it by copying your own index.html file to the Web server (on page 68).

Instructions

➢ ***To edit the index.html file:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 In the File Manager, browse to the `var/www/html` directory. If you are in the Root directory, and the **Path to current directory** bar shows `/`, drill down by clicking **var**, then **www**, then **html**.

Be sure to click the name of the directory; if you click the folder icon, you access the directory's properties.

When you are in the directory, the **Path to current directory bar** at the top of the page shows `var/www/html`.

4 In the **Name** area of the Path form, locate the file named index.html, then click  in the **Actions** column of that file. A window opens displaying the contents of the file.

5 Delete the text in the file by highlighting all of the text, then pressing Delete.

6 Copy the text between the horizontal lines below, then paste it into the file. To copy, highlight the text by dragging your mouse across it while pressing the left mouse button, then hold down the CTRL while pressing C. To paste, place the cursor in the file then hold down CTRL while pressing V.

```
<html>
<head>
<title>My new home page</title>
<meta http-equiv=”Content-Type” content=”text/html;
charset=iso-8859-1”>
</head>
<body bgcolor=”#FFFFFF” text=”#000000”>
<p align=”center”> </p>
<p align=”center”><font face=”Verdana, Arial, Helvetica, sans-
serif” size=”3”><b><font color=”#009900” size=”6” face=”Times
New Roman, Times, serif”>
Hello World!</font></b></font></p>
<p align=”center”><b><font face=”Verdana, Arial, Helvetica,
sans-serif” size=”3”>
```

```
Welcome to my <i><font color="#009900">new</font></i> home
page.</font></b></p>
</body>
</html>
```

7 Scroll to the bottom of the page, then click **Save**.

8 Open a browser and go to your home page. If the page has already been open in a browser window, be sure to refresh or reload the page. The page shows your new text.

As an alternative to editing the file in the File Manager, you can create your own index.html file (on page 67) and upload it to your site.

Copying and Moving Files

You can copy and move files on your site from one directory to another by using the Clipboard Contents section of the File Manager. You can remove the Clipboard contents (on page 207) at any time.

Note: You must own the file you are copying or moving. You also must have write permissions to the directory into which you are copying or moving the files. To determine permissions, you can view directory properties (on page 204).

➢ ***To copy or move a file:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to copy or move.

4 In the **Name** area of the Path form, locate the file you want to copy or move, and select the check box next to it.

5 In the **Commands** area of the Path form, click **Add File(s) to Clipboard.**

File Manager displays the file name in the Clipboard Contents area of the Path form.

6 Browse (on page 202) to the directory into which you want to copy or move the file.

The directory window of the destination directory opens.

7 In the **Clipboard Contents** area of the Path form, locate the name of the file you want to move or copy and select the check box next to it.

8 Do one of the following:

- To copy the file to this destination directory, click **Copy**.
- To move the file to this destination directory, click **Move**.

Note: If the Move operation fails, File Manager compensates by making a copy of the file in the destination directory; however, you must manually remove the file from its original directory.

Removing Contents from the Clipboard

➢ ***To remove file from the Clipboard:***

1 In the Clipboard Contents area of the Path form, select the check boxes of the file you want to remove.

2 Click **Clear**.

Moving Files from Your Site to Your Local System Using the File Manager

Moving files from your site to your local system (your laptop or desktop computer) is called *downloading*. You can download files from your site to your local system using the File Manger section of the Site Administrator control panel.

➢ ***To download a file to your local system:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to download.

4 In the **Name** area of the Path form, locate the file you want to download, and click the file's underlined name.

5 Save the file to a directory on your local system.

Moving Files from Your Local System to the Server Using the File Manager

Moving files from your local system (your laptop or desktop computer) to your site is called *uploading*. You can upload files from your local system to your site using the File Manager section of the Site Administrator control panel.

Note: If you are uploading files from a Microsoft Windows system, be aware that the File Manager performs binary transfers; it does not translate Windows text format to UNIX text format. HTML files are not affected; however, scripts might not work properly when uploaded through the File Manager. To ensure that scripts work properly, use an FTP connection (on page 20), rather than the File Manager, to upload script files.

➢ ***To upload a file to the server using the File Manger:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory in which you want to upload the file. If you are uploading HTML content for your Web site, upload them to the directory **/var/www/html**. If this directory does not already exist, create it though File Manager. See the topic Creating additional directories (on page 206) for instructions.

4 In the **Upload File to** area of the Path form, in the **Upload File** field, enter the complete path name of the file, or click **Browse** to locate the file in your local system.

5 In the **Save As** field, enter the name of the file you want to upload to the server.

Note: Do not include the directory path in the file name; include only the file name.

---

1 Click **Upload**.

Removing Files

You can remove files from your site using the File Manager section of the Site Administrator control panel. However, you must own a file to remove it.

➢ ***To remove a file:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Files** (File Manager section). The directory list is displayed.

3 If necessary, browse (on page 202) to the directory that contains the file you want to remove.

4 In the **Name** area of the Path form, locate the file you want to remove, and select the check box next to it.

5 In the **Commands** area of the Path form, click **Delete File(s)**.

Protecting Directories

In this section:

About Protecting Directories

You can limit access to files stored on your site by requiring users to type a password to gain access. This is known as “protecting directories.”

When users attempt to access a file in a protected directory, the Web server displays a login window. Users with access privileges enter their user names and passwords to access the file. Users without access privileges cannot access the file.

How to Protect Directories

You protect directories in one of two ways:

- Through the Site Administrator control panel (on page 221) if Microsoft FrontPage Extensions **are not enabled for your site**.
- Through the FrontPage Extensions interface if FrontPage Extensions **are enabled** for your site.

Note: To determine whether FrontPage extensions are enabled for your site, click **Site Information** (Tools section) in the shortcuts area, then check whether FrontPage is shown as available in the Services and Options section of the Configuration window.

About htaccess Files

When you protect a directory on your site, you limit access to it by requiring that users enter passwords to access files in the directory. When you do this in the Site Administrator control panel (on page 221), an htaccess file (HT is derived from hypertext) containing permission information is created.

The htaccess file contains information about the authorization name for the directory, and the names of the groups who are allowed to access files contained within this directory.

Another file, which contains individual user names and passwords (HT user accounts) of users who belong to the group, is also created. When a user attempts to access a protected directory, the Web server first verifies that the user is included in a group listed in the htaccess file, then prompts for a user name and password before verifying and granting the user access to the directory.

Note: If you have FrontPage Extensions enabled on your site, you use the FrontPage Extensions interface to protect directories.

Protecting Directories Through the FrontPage Interface

Note: This topic is for systems with Microsoft® FrontPage® Extensions enabled. If you do not have FrontPage extensions enabled, use the Site Administrator control panel to protect directories (on page 220).

You can protect directories on your site to limit access to files located in those directories. If you have FrontPage enabled for your site, you do this through the FrontPage interface. You can link to this interface from the Site Administrator control panel.

Important: You can protect directories only; you cannot protect individual files. If you want to protect a single file, either place that file in an existing protected directory, or create a directory specifically for that file, then protect the directory.

➢ ***To access the Microsoft FrontPage interface:***

1 Click the **Shortcuts** tab on the Home page.
2 In the shortcuts, click **Configuration** (Web Server section).
3 Click **Protect Directories**.
4 In the Protect Directories form, click **Microsoft FrontPage Server Extensions Permission Management** Interface.

Note: Your Microsoft FrontPage login information is the original Site Administrator user name and password assigned to you when your site was created. If you have changed your Site Administrator user name or password since then, the change is not reflected in FrontPage login. You can change the FrontPage login using the FrontPage Extension Permission Management Interface. For more information, see the FrontPage user documentation.

Protecting Directories Through the Site Administrator

In this section:

Protecting Directories Through the Site Administrator Control Panel

Note: This topic is for systems **without** Microsoft® FrontPage® Extensions. If you have FrontPage enabled, you need to use the FrontPage interface to protect directories.

You can password-protect directories on your site to limit access to files located in those directories. If your site does not have FrontPage enabled, you do this through the Site Administrator control panel.

Important: You can protect directories only; you cannot protect individual files. If you want to protect a single file, either place that file in an existing protected directory, or create a directory specifically for that file, then protect the directory.

➢ ***To protect a directory:***

1 If you have not done so already, create an HTAccess group (on page 222), then specify the user or users who belong to the group (on page 222). You need to create a at least one group and add at least one user to that group before you can protect a directory.

2 Click the **Shortcuts** tab on the Home page.

3 In the shortcuts, click **Configuration** (Web Server section).

4 Click **Protect Directories**. A list of the directories on your site, identified as either unprotected or protected, is displayed.

5 From the directory list, locate the directory you want to protect, then in the **Actions** column, click . The **Protect Directory** form opens.

6 In the **AuthName** field, enter a descriptive name for the directory you want to protect. When users attempt to access files, this name is displayed in the login window as the **Realm**.

   For example, to protect a directory of employee salary information, you might type `Compensation`.

7 In the **Add to Group(s)** field, specify the groups that are allowed to access this directory.

   Note: You can select or clear multiple directories by pressing and holding down the CTRL key while clicking the directory names.

8 Click **Protect**. The directory is now protected. Users are required to enter user names and passwords before accessing information in the directory.

Creating Groups for Protected Directories

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

The Web server manages access to password-protected directories on your site based on groups. Before you can protect a directory, you need to create at least one group, then add at least one user to that group.

➢ ***To create a group:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Groups** (Web Server section). A list of existing groups currently in the group file is displayed.
3. Click **Add Group**.
4. In the **Enter Group name** field, enter a name for the group you are creating.
5. Click **Add Group**.

   You are now ready to add users (on page 222)to this group.

Creating User Accounts for Protected Directories

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

To give users access to password-protected directories on your site, you add HT Access (HT is derived from hypertext) user accounts for them. When you create this user account, you add it to a group, and the user is given the group's access privileges.

Important: Before you create a HT Access user account, you need to have created a group (on page 222).

➢ ***To add an HTAccess user account:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (Web Server section). A list of user names is displayed.
3. Click **Add User**.
4. In the **User Name** field, enter a user name for the new user.
5. In the **Password** field, enter a password for the user.
6. In the **Confirm Password** field, retype the password.
7. In the **Belongs to group(s)** field, select the group or groups to which you want to add the user. You can add the user to multiple groups by pressing and holding down the **Ctrl** key while clicking the group names.

8 Click **Add/Edit**. The new user name displays in the lower section of the form.

9 Notify the user the account has been created and provide the user name and password you assigned so they can access protected directories.

Changing User Passwords for Protected Directories

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

You can change the passwords users enter when they access protected directories on your site. These are HTAccess passwords only; they differ from the passwords users enter to access services and the User Administrator control panel.

➢ ***To change a user's HTAccess password:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click **Manage Users** (Web Server section). A list of user names is displayed.

3 Click **Add User**.

4 In the **User Name** field, enter the user name of the user whose information you want to change.

5 In the **Password** field, type a new password for the user.

6 In the **Confirm Password** field, enter the new password again.

7 In the **Belongs to group(s)** field, select the group or groups to which the user belongs.

8 Click **Add/Edit**.

9 Notify the user that the password has been changed.

Changing User Access Privileges

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

You can change users' access to password-protected directories on your site by removing them from the group or groups with access privileges. Users must belong to at least one group, however. To revoke all access privileges, you need to remove the user's htaccess account (on page 225).

➢ ***To change users' access privileges:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (Web Server section). A list of user names is displayed.
3. Click **Add User**.
4. In the **User Name** field, enter the user name of the user whose privileges you want to change.
5. In the **Password** and **Confirm Password** fields, type the password for the user. If this password differs from the one originally assigned, notify the user that the password has been changed.
6. In the **Belongs to group(s)** field, click the arrow and from the list, select only the group or groups to which you want the user to belong. To remove a user from a specific group make sure the group is not selected.

   Users must belong to at least one group.

   Note: You can select multiple groups by pressing and holding down the CTRL key while clicking the group names.
7. Click **Add/Edit**.

Removing User Access Privileges

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

When users no longer need access to password-protected directories on your site, you can remove their HTAccess accounts from the system.

➢ ***To remove an HTAccess account:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts area, click **Manage Users** (Web Server section). A list of user names is displayed.
3. In the **User Name** list, locate the user whose privileges you want to remove.
4. Click  in the **Actions** column.

Removing Groups from Protected Directories

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

If you want to remove one group's access to a password-protected directory on your site, you can remove the directory's protection (on page 226), then protect it again (on page 221) for the group or groups with continuing access privileges.

As an alternative, you can remove the group (on page 226) to prevent its members from accessing the protected directory.

Removing Protection from a Directory

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

When you remove password-protection from a directory on your site, all access limitations are removed from the directory. This makes it possible for users to access files in the directory without entering user names and passwords.

➢ ***To remove protection from a directory:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts, click **Configuration** (Web Server section). A list of the directories on your site, identified as either unprotected or protected, is displayed.
3. From the directory list, locate the directory from which you want to remove protection, and in the **Actions** column, click .

   The HTAccess file is removed from the directory.

Removing Protected Directory Groups

Note: This topic is for systems **without** Microsoft FrontPage Extensions. If you have FrontPage Extensions enabled, you need to use the FrontPage interface to manage protected directories.

Remove groups that have access to password-protected directories on your site only when you want to delete the groups from the system permanently. Users assigned to the group are not removed, but they can no longer use the access privileges of the group.

➢ ***To remove a group:***

1. Click the **Shortcuts** tab on the Home page.
2. In the shortcuts, click **Configuration** (Web Server section).

3 In the shortcuts area, click Manage Groups (Web Server section). A list of the directories on your site, identified as either unprotected or protected, is displayed.

4 From the directory list, locate the directory from which you want to remove protection, then in the **Actions** column, click .

C H A P T E R 1 3

Exporting and Importing Data

In this chapter:

Export and Import Overview

An export operation backs up the selected data to a specified export server while an import operation restores the selected data to the specified import server. You can export and import the following data.

- Site data (on page 232)
- User data (on page 235)

Note: You must have FTP access (on page 231) to export and import files.

Known Issues in Export and Import

- The MySQL password is exported as metadata; however, the password is not imported if a site is migrated between servers.
- Site statistics is not exported.

Preparing for Export and Import

Before you export or import data, review the preparatory information and the recommended tips to ensure successful export and import operations.

Before You Begin

Before you begin, verify that you meet the specified requirements and have the requisite information to export and import data.

- At least one of the FTP servers (on page 231) recommended by Parallels Pro
- The host name or IP address of the FTP server you want to use for export and import
- Your FTP login user name and password
- **Optional**: The complete directory path on the FTP server
- **Optional**: Maximum size of the file being exported or imported

Note: Various file systems and FTP server utilities have limits on the file size they can handle. If the size of your file exceeds the file management capacity of the file system or the FTP server utility on your server, the file is split into multiple files before continuing with the export or import operation.

- Sufficient disk space on the target server to accommodate the data, otherwise the operation will fail.

Tips for Successful Export and Import

Review the tips provided in this section to avoid export and import issues.

1 Schedule export operations during a period of low activity.

Importing Web sites that reference non-variable Site IDs (hard-coded) to a different control panel server renders the site inaccessible. Do not use non- variable Site IDs in Web content. Use Using environment variables, scripts can get and use up-to-date information without having to store that information themselves.

In addition to the standard environment variables, the following three environment variables are available to all scripts on your site:

- **SITE_ROOT**. The root path of your site
- **SITE_CGIROOT**. The top level CGI path of your site
- **SITE_HTMLROOT**. The top level HTML CGI path of your site

1 It is recommended that content developers use these variables to avoid hard-coding Site IDs. This ensures that path names are always correct, even if those path names change. provided by the application.

2 The export and import operation fails on certain FTP servers. Parallels Pro recommends the use of certain FTP servers **(on page 231)** for successful export and import operations.

3. Files exported from versions 3.0 or 3.1 are incompatible with later versions. Export these files using the latest version of the control panel after you upgrade from the older versions.
4. Exporting data using FTP does not change the access permissions of exported archives. If you want these archives to be secure, you must modify the default FTP permissions as needed.

Recommended FTP Servers for Export and Import

You must have access to an FTP server to transfer data using the FTP option. Parallels Pro recommends use of the following FTP servers for successful export and import operations.

FTP Servers Running on Linux or Unix Platforms

Use one of the following FTP servers to export or import files.

- WU-FTPD
- ProFTPD
- vsftpd

FTP Servers Running on Microsoft Windows Platforms

- FTP server installed on IIS

  FTP servers installed on IIS are configured to support the “MS-DOS” directory listing style while the control panel follows the “Unix” directory listing style. As a result, if you export files using the IIS FTP server with the “MS-DOS” directory listing style, the files do not display in the control panel when you try to import these files.

  To resolve this, reset the directory listing style on the IIS FTP server to “Unix” as described below.

➢ ***To reset the directory listing style:***

1. Click **Start > Settings > Control Panel**. The Control Panel window opens.
2. Locate the option, **Administrative Tools** and double-click the icon.
3. In the Administrative Tools window, locate the option, **Internet Services Manager**, and double-click the icon. The Internet Information Services window opens.
4. Click next to the name of your desktop computer to expand the access tree. The list of sites and servers installed are displayed.

   Note: By default, the FTP server is stopped.

5. Select **Default FTP Site** and click to start the FTP server.
6. Select **Action > Properties**. The **Default FTP site Properties** window opens.
7. Select the **Home Directory** tab.
8. In the **Directory Listing Style** area, select **Unix**.
9. Click **Apply > OK**.

   The exported files now display in the control panel when you import the files.

About Site Export

A Site export backs up the following data.

- The site user accounts and service configuration information and related files are exported.

  The export includes the following information.

  User configuration information
- Files in the site owned by the user

Since the site configuration information is also exported, you have the functional independence to migrate your site between the control panel servers and successfully import it whenever needed.

Note: To restore an export onto a new server, you must contact your service provider and provide him with the necessary site export details to restore the site.

Your service provider can also export your site but cannot export the site and user data separately.

When you export a site, the following archives are created.

- A compressed file (.gz) of the site
- A compressed file (.gz) for each user of the site

The naming convention of an exported file is as follows:

<server_hostname>_<site_name>_<export_type>_<YYYY>_<Month>_<date>_<Hours>_Minutes> **.** `tar.gz`

Where:
<server_hostname> is the name of the control panel server on which your site is hosted
<site_name> is the name of the site being exported
<export_type> indicates the type of export (site)
<YYYY>_<Month>_<date>_<Hours>_Minutes> is the time-stamp when the data is exported.

For example, exporting a site ***mysite.com*** on the server ***example.com*** on Jan 06, 2003 at 11.30 creates the following file:

```
example.com_mysite.com_site_2003_January_06_11_30.tar.gz
```

What Is Exported

The following information is exported as metadata in the form of an XML file. The metadata comprises information about the exported data.

- DNS information comprises the DNS settings configured for the zone along with zone information for the site.

- Service configuration information includes the service settings configured for a site when you create or modify a site.
- File ownership and their permissions
- Site information comprises the site name, IP address, site ownership information, services information, site databases and tables.

Site user account information includes the following.

- User configuration information
- Files in the site owned by the user

What Is Not Exported

The following files and directories are not exported.

Note: All the path names are relative to the site's base directory, `/home/virtual/`***<site-id>***`/fst/`

- **Analog configuration information**
  - `/var/usage/web/analog.cfg`
  - `/var/usage/ftp/analog.cfg`
- **Anonymous FTP account information**
  - `/var/ftp/etc/group`
  - `/var/ftp/etc/ld.so.cache`
  - `/var/ftp/etc/passwd`
- **Skins and related customizations**
  - `/usr/lib/opcenter/skins/`
- **IMAP authentication information**
  - `/etc/imap.pamlist`
- **Security certificate information**
  - `/etc/httpd/conf/ssl.crt/*.*`
  - `/etc/httpd/conf/ssl.key/*.*`
  - `/etc/httpd/conf/ssl.csr/*.*`
- **proFTPd authentication information**
  - `/etc/proftpd.pamlist`
- **Email account information**
  - `/etc/aliases.db`
  - `/etc/mail/mailertable.db`
  - `/etc/smtp_relay.pamlist`
  - `/etc/mail/mailertable.local_domains`
- **Site information**
  - `/etc/domainname`

  - /etc/group
  - /etc/hosts
  - /etc/ld.so.cache
  - /etc/nsswitch.conf
  - /etc/passwd
  - /etc/pwdb.conf
  - /etc/shells
  - /etc/HOSTNAME
  - /etc/mail/domain-info.m4
- **SquirrelMail configuration file generated by Parallels Pro**
  - $HTML_ROOT/squirrelmail/config/ensim_config.php
- **SSH authentication information**
  - /etc/ssh.pamlist
- **Telnet authentication information**
  - /etc/telnet.pamlist
- **Bandwidth statistics**
- **Scheduled export settings**
  - /etc/cron/*.*
- Files not owned by group **adminxyz** (for example, admin123) or **root**

About User Export

A User export backs up the user configuration information and files owned by the user.

When you export a user, a compressed .gz file is created for each user.

The naming convention of an exported file is as follows:

<server_hostname>_<user_name@site_name>_<export_type>_<YYYY>_<Month>_<date>_<Hours>_Minutes>`.tar.gz`

Where:
<server_hostname> is the name of the control panel server on which your site is hosted
<user_name@site_name> is the name of the user being exported
<export_type> indicates the type of export
<YYYY>_<Month>_<date>_<Hours>_Minutes> is the time-stamp when the data is exported.

For example, exporting a user `user1` on the site `mysite.com` on Jan 06, 2003 at 11.30 creates the following file:

`example.com_user1@mysite.com_user_2003_January_06_11_30.tar.gz`

Exporting Data

Tip: Export site and user files in different directories for easy identification of the files when you import.

Example. Export Site files to a `site_export` directory and User files to a `user_export` directory.

To export data, click the **Shortcuts** tab on the Home page, then click **Export/Import** (Tools section) in the shortcuts area, and follow the instructions below.

You need to choose the type of export, select the appropriate mode of transfer and provide the required miscellaneous information.

- wizard Step1: Choose the type of export

1 In the **Type of Export** area, select one of the following option buttons.

   a Site (on page 232)

   b Users (on page 235)

   Click the arrow in the **Users** list, and choose one of the following.

   - **All** - To export all user accounts
   - ***<name of the User>*** - To export a particular user. Press `CTRL + the left mouse button` to select multiple users.
   - wizard Step2: Select the mode of transfer

2 Choose the mode of data transfer to the export server.

   You can choose to download or use the FTP protocol to export the data to the server. Large files may take a long time to transfer depending on the quality of your Internet connection. Use the FTP (on page 231) option for a faster and more reliable transfer.

   a **Download** - Recommended for exporting small files to a desktop.

   - In the Download area, select the **Download** option button to download to a desktop or local server.
   - Go to Step3 of the wizard.
   - Click **Download.**
     The Download File window opens.
   - Click **Download file.**
     The File Download window opens. You can open the file or save the file to your computer.
   - Click **Save**.
   - In the Save As dialog, enter or retain the default name of the export file.

   b **FTP** - Recommended for exporting large files to a remote FTP server.

Important: You should have the FTP (on page 231) server utility installed on the export server to use this transfer mode.

- Select the **FTP** option button to transfer the files using FTP to a remote FTP server.
- In the **FTP Server** field, enter the host name or IP address of the FTP server you want to use as the export server.
- In the **FTP Login** field, enter the user name of your account on the FTP server.
- In the **FTP Password** field, enter the password of your account on the FTP server.
- In the **FTP Location** field, enter the path of the export directory on the FTP server. If you leave the field blank, the files are saved to the home directory of the user specified in step 3.

Important: If the specified directory does not exist, the export fails and an email message containing the error is sent to you.

- **Optional**: In the **Maximum Export File Size** field, enter the maximum size of the export file.

Important: Various file systems and FTP server utilities have limits on the file size they can handle. If the size of your export file exceeds the file management capacity of the file system or the FTP server utility on your export server, the file is split into multiple files before continuing with the export.
The split files follow the naming convention given below:
<exportfilename.tar.gz>
<exportfilename.1.tar.gz>
<exportfilename.2.tar.gz>
where `exportfilename` *i*s the name of your export file.

- Go to Step3 of the wizard.
- Click **Export**.

- wizard Step3: Enter miscellaneous information

3 In the **Email** field, enter the email address at which you want to receive export status notifications by email. The status of the export is conveyed to the specified address.

Troubleshooting Export and Import Issues

If you encounter problems that you cannot troubleshoot or resolve using the information in the following table, contact your administrator.

Problem	Solution
Importing Web sites that contain hard-coded Site IDs onto a different server renders the site inaccessible.	Use environment variables in the Web site content.
The import operation fails if an IP-based site is imported to a server hosted on a network that shares the IP address of the exported site.	Contact your administrator to resolve the issue.
The export and import operation fails on certain FTP servers.	Parallels Pro recommends the use of select FTP servers (on page 231) for successful export and import operations.
Files exported from versions 3.0 or 3.1 are incompatible with later versions of the control panel.	Export these files using the latest version of the control panel after you upgrade from the older version.

Importing Archived Data

In this section:

About Importing Data

You can selectively import files from an export archive using the Download (on page 240) option or the FTP (on page 240) option.

Review the following important notes before you import files.

- If a file by the same name, as the one being imported, exists on your server, the existing file is not replaced or overwritten, in other words, the file is not restored from the backup.
- The import operation automatically uncompresses the archive and updates your working directories with the archived content.

  Do **NOT** manually uncompress the file to make changes to the archived files and upload them again as a compressed .gz file. If the files in the archive are manually modified, you cannot import files from the archive again. This is a security measure to ensure that the archived files are not corrupted by malicious scripts.
- When you import a site, if the server on which the site is being imported uses a MySQL database having the same name as the one being imported, then the prefix of the database name is changed. This can make your databases inaccessible. It is advised that you import the site onto a different server that does not use a database with the same name.

  Also, if the Database Administrator name already exists on the server where the database is being imported, the name is automatically changed to ensure uniqueness. You must subsequently change any references to the old administrator name, otherwise you will be unable to connect to the database.
- Restoring files may take a long time to complete, depending on the size of the archived files and the speed of your network connection. FTP is recommended as a faster and more reliable option when transferring files.

Using FTP to Import Data

The FTP option is recommended for large files.

Note: You should have the FTP (on page 231) service running on the export server.

➢ ***To import data using FTP:***

1 In the Shortcuts section of the Home page, click **Export/Import** (Administration section).

2 Click **Import Using FTP**.

3 In the **FTP Server** field, enter the name of the FTP server where you have archived the exported data.

4 In the **FTP Login** field, enter the user name of your account on the FTP server.

5 In the **FTP Password** field, enter the password of your account on the FTP server.

6 In the **FTP Location** field, enter the full path to the export directory on the FTP server. If you leave the field blank, the location defaults to your home directory.

   Note: You do not have to specify the path if the exported data is stored in the **home** directory of your account.

7 In the **Email** field, enter the email address at which you want to receive import status notifications.

8 Click **Connect**.

9 Select the check boxes next to the files you want to import.

   Note: Files split into multiple files during an export can be imported as a single file. Select the main export file (***<exportfilename>***.tar.gz), then select the **Enable Recurse** check box (displayed at the end of the file listing). Do not select the individual files (***<exportfilename>.<x>***.tar.gz> where ***<x>*** indicates each individual file) that constitute the main export file.

10 Click **Import**.

   The status of the import is conveyed through email notifications to the specified address.

Using Download to Import Data

The Download option is recommended for small files.

➢ ***To import data using the Download option:***

1 In the Shortcuts section of the Home page, click **Export/Import** (Administration section).

2 Click **Import Using Download**.

3. In the **Select Export File** text box, enter the name of the export file. Alternatively, click **Browse** to locate the file.
4. In the **Email** field, enter the email address at which you want to receive import status notifications by email. If you do not want to receive email notifications, leave the field blank.
5. Click **Import**. A confirmation dialog opens.
6. Click **OK** to proceed with the import.

Scheduling Exports

In this section:

Scheduling Exports

When you schedule an export, you automate the export to occur at a pre-set date, time, and location.

To schedule an export, click the **Shortcuts** tab on the Home page. In the shortcuts area, click **Export/Import**, then click **Schedule Export**. The Scheduled Export window opens. Click **Schedule**.

Follow the wizard to schedule an export.

You need to choose the type of export (Site (on page 232) or User (on page 235)), enter schedule information, provide necessary FTP account details and other miscellaneous information.

- wizard Step1: Choose the type of export

1 Choose the type of export, by selecting one of the following option buttons in the **Type of Export** area.

   a Site - Exports your site.

   b Users - Exports data pertaining to site users.

   Click the arrow in the **Users** list, and choose one of the following.

   - **All** - To export all user accounts
   - ***<name of the User>*** - To export a particular user. Press CTRL + the left mouse button to select multiple users.

- wizard Step2: Enter the export Schedule information

2 Select the frequency at which you want to export data.

   Select any one of the following options in the **Frequency** field.

   - **Daily** - Exports files daily at the scheduled time
   - **Weekly** - Exports files weekly at the scheduled day and time
   - **Monthly** - Exports files monthly at the scheduled date and time

1 Click the arrow in the **Minutes** list, and select a number between 0 and 59.

2 Click the arrow in the **Hours** list, and select a number between 0 and 23.

3 Click the arrow in the **Day of Week** list, and select a day between Sunday and Saturday.

4 Click the arrow in the **Day of Month** list, and select a number between 1 and 31.

> **Important**: If you select a value in the **Day of Month** field that is not common to all the months, the export fails to run as scheduled on certain months.
> For example, if you select `31`, no export will be initiated on months that contain `30` or `28` days.

- wizard Step3: Enter FTP information

5 In the **FTP Server** field, enter the name of the FTP server you want to use as the export server.

6 In the **FTP Login** field, enter the user name of your account on the FTP server.

7 In the **FTP Password** field, enter the password of your account on the FTP server.

8 In the **FTP Location** field, enter the absolute path to the export directory on the FTP server.

> **Important**: If you leave the field blank or the specified directory does not exist, the export fails and an email message containing the error is sent to you.

- wizard Step4: Enter miscellaneous information

3 Optional: In the **Maximum Export File Size** field, enter the maximum size of the export file.

> **Important**: Various file systems and FTP server utilities have limits on the file size they can handle. If the size of your export file exceeds the file management threshold of the file system or the FTP server utility on your export server, the file is split into multiple files before continuing with the export operation.
> The split files follow the naming convention as given below:
> ***<exportfilename.tar.gz>***
> ***<exportfilename.1.tar.gz>***
> ***<exportfilename.2.tar.gz>***
> where `exportfilename` is the name of your export file.

4 Click the arrow in the **Unit** list, and select the appropriate quantifying unit (Megabytes or Gigabytes).

5 In the **Email** field, enter the email address at which you want to receive export status notifications. If you do not want to receive email notifications, leave the field blank.

6 Click **Schedule**.

The list of scheduled exports is updated.

Viewing the List of Scheduled Exports

➢ ***To view the list of scheduled exports:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click Export/Import (Tools section).

3 Click **Schedule Export**. The list of scheduled exports is displayed with the following information.

- **Type** - The type of export scheduled
- **Frequency** - The number of times an export is scheduled to run. The frequency can be daily, weekly or monthly.
- **FTP Properties** - The name of the export FTP server
- **Email** - The email address to which export notifications are sent
- **Actions** - The actions you can perform on the page. You can change (on page 244) the export schedule, or delete (on page 244) the export schedule.

Changing the Export Schedule Information

➢ ***To change the export schedule information:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click Export/Import (Tools section).

3 Click **Schedule Export**.

4 Click in the **Actions** column next to the export whose schedule information you want to change.

5 Modify the information as required.

6 Click **Update**.

Deleting a Scheduled Export

➢ ***To delete a scheduled export:***

1 Click the **Shortcuts** tab on the Home page.

2 In the shortcuts area, click Export/Import (Tools section).

3 Click **Schedule Export.**

4 Click in the **Actions** column next to the schedule you want to delete.
A Confirm Delete dialog opens, requesting confirmation for the delete.

5 Click **OK** to confirm the deletion.

The export schedule is removed from the list of scheduled exports.