Parallels® Pro Control Panel

Parallels Pro Control Panel 10.3.3 for Linux Server 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 (formerly known as Ensim Pro) is designed to simplify Web hosting (on page 12) by controlling and automating common hosting tasks.

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

Parallels Pro Control Panel is a robust control panel solution for small and large professional hosting providers. Parallels Pro Control Panel includes all the tools and features that you, as a hosting provider, need to build compelling, commercial-quality plans for shared and reseller hosting.

Benefits of Parallels Pro Control Panel

Parallels Pro Control Panel allows you to:

- Configure hosting applications such as Apache Web server and FTP server.
- Create new sites (IP-based or name-based).
- Manage site settings and configuration options.
- Manage site content - including databases and subdomains.
- Define mail aliases and options.
- Analyze site Web traffic reports.
- Export and import site content.

Advanced features:

- Define targeted, compelling Service Plans for shared site and reseller hosting. By defining a Service Plan once, you can establish new customers very quickly, while controlling application settings and resource quotas.
- Review detailed reports of bandwidth usage per site and allow accurate and complete billing of all traffic used by sites.
- Protect shared sites with a virtual private file system and provide additional site security and prevent theft of customer’s data.
- Delegate administration to your customers, including your resellers, site owners and site users, while simultaneously reducing your support calls and improving customer satisfaction.

Delegating control

The control panels allow many different users to easily manage their specific Web hosting administrative tasks.

The user levels include:

- SERVER OWNER - managed by the Server Administrator
- RESELLER - managed by the Reseller Administrator
- SITE OWNER - managed by the Site Administrator
- USER ACCOUNT HOLDER - managed by the User Administrator

About the Server Administrator

The server level of administration is designed for the hosting provider or reseller who either owns server hardware or has remote access to physical servers.

As the owner of servers, you are called the Server Administrator, and can:

- Set up your server with Web hosting capabilities
- Configure the server applications for your customers
- Create new sites
- Manage existing sites
- Export and import data and configuration scripts
- Automate many frequently performed administrative tasks

To begin managing your server level tasks, log on to the control panel as the Server Administrator.

About the Reseller Administrator

The reseller level of administration is designed for individuals or businesses who want to resell or manage sites without actually owning or maintaining hardware. As a reseller, you buy sites from an ISP or hosting provider and resell them to individual customers. If you are already a Web site creator, designer, or consultant, becoming a reseller is a perfect way of diversifying and expanding your business.

As the reseller, you are called the Reseller Administrator, and can:

- Create new sites
- Manage existing sites
- Customize the control panel

To begin managing your reseller level tasks, log on to the control panel as the Reseller Administrator.

Note: You cannot perform operating system level tasks like starting and stopping services.

About the Site Administrator

The site level of administration is designed for businesses that want to manage their hosted sites and the services installed on the sites.

As the owner of sites, you are called the Site Administrator, and can:

- Set up security features for an entire site or just an individual Web site
- Manage the user accounts on an entire site or just an individual Web site
- Set up protected directories on the Web server
- Set up your site email and FTP features
- Work with the directories and files on your site
- View traffic reports about your site
- Export and import site and user data

To begin managing your site level tasks, log on to the control panel as the Site Administrator.

Note: The Server Administrator automatically has access to the Site Administrator control panel.

About the User Administrator

The user account level of administration is designed for someone who subscribes to a site and is assigned a user account.

As the subscriber, or user account holder, you are called the User Administrator, and can:

- Maintain your account contact information
- Set up your email services
- Access your email messages over the Internet
- Publish your Web site content
- Export and import files from your Web site

To begin managing your user level tasks, log on to the control panel as the User Administrator.

C H A P T E R 3

Web Hosting Concepts

Web hosting involves an understanding of the following concepts.

- URLs and domain names
- Domain Name Registrars
- Host names and IP addresses
- IP-based and name-based Web sites

URLs and domain names

To get to a Web site, you have to click on, or type in, its name in a Web browser. The name of the Web site is technically referred to as a URL (Uniform Resource Locator) and looks something like this:

`http://example.com.`

A URL consists of two parts, the "`http://`" which tells the browser to use the HTTP protocol to get to your site, and your site's name, "`example.com`" which is technically called the site's domain name. A domain name is a human-understandable and unique name for your site.

Notice that a domain name consists of a series of strings separated by dots. Each string within a domain serves to make the overall domain name unique. For instance, suppose there are two companies both called "MyCo Corporation" in, say, the US and India. Then, they could be assigned the domain names `myco.us` and `myco.in`. Thus, both of them have the string "`myco`" in the domain name, but the suffix "`us`" or "`in`" makes them unique.

Domain Name Registrars

To keep things manageable, the Internet authorities have created a set of "top level domains" like "`com`", "`net`", "`org`", "`edu`" and so on. A Domain Name Registrar is given control over one or more of these top-level domains.

Anyone who wants a domain within a top level domain (that is, a domain name ending in the top-level domain's name) contacts a Domain Name Registrar and asks the registrar to register their name. The registrar ensures that the name is unique, and, for a small fee, registers the name. For instance, if MyCo Corporation would want to own the domain name `myco.com`, it can contact the Domain Name Registrar for the "`.com`" domain and ask the registrar to register the domain name `myco.com`. Once this is done, anyone can type `myco.com` and get to the `myco.com` site. There are many Domain Name Registrars, and some of them, like register`.com` are very popular.

Host names and IP addresses

When you type in a URL into a browser, your computer has to contact the computer on the Internet (also called a host) that contains the Web site with that name. For example, if you type `http://myco.com` in your browser, your computer has to contact the computer that hosts the `myco.com` Web site. It does so by sending a packet (a small amount of data) to the `myco.com` computer saying "show me the main page of the `myco.com` Web site". The `myco.com` Web site replies with the main page. To make this work, the Internet has to somehow transmit packets from your computer to the computer that hosts the `myco.com` Web site. While the `myco.com` computer is easily identified by its unique domain name, it is really much easier to transmit the packet if the destination is identified by a number rather than a name. The number that corresponds to a domain name is called a computer's IP address, for example `129.31.212.144.`

Every computer on the Internet and every Web site must correspond to an IP address. Your Web site hosting company will provide you with a set of IP addresses that you can allocate to the Web sites that you create.

IP-based and name-based Web sites

There are two ways to host domains. The first is to create the domain with its own IP address. This is called IP-based hosting. You must create IP-based domains if the domain needs anonymous FTP and its own secure-site (SSL) support.

The second way to host domains is to create a domain that shares the primary IP address of the server. This is called name-based hosting. Name-based domains receive most of the benefits of an IP-based domain without occupying an IP address.

All of the standard sets of server applications are available to IP-based and name-based sites, except SSL encryption. SSL is not supported for name-based sites.

IP addresses happen to be scarce resources. To conserve IP addresses, you can arrange to have many sites share the same IP address.

CHAPTER 4

Quick-Start Guide for Server Administrators

This quick-start guide is composed 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 each topic to proceed through the guide.

CHAPTER 5

Managing the Server

In this chapter:

Overview of Licensing

The Parallels Pro Control Panel license determines the number of sites you can host and manage on your server for a stipulated time period. You receive the license key in the order confirmation email sent by Parallels Pro Control Panel after you purchase Parallels Pro Control Panel from Parallels Online Store at http://www.parallels.com/en/buyonline/pro/. The license key is a 25-character alphanumeric key.

You can choose to install the license during installation or when you log in to Parallels Pro Control Panel after the installation. If you choose to apply the license after installation, you are prompted to register (on page 17) the license before you log into Parallels Pro Control Panel.

How licensing works

During installation, Parallels Pro Control Panel creates a scheduled task (also called a cron job) on the Parallels Pro Control Panel server. This scheduled task periodically checks whether Parallels Pro Control Panel has contacted the Parallels Pro Control Panel License Server (PCPLS, formerly known as ELS - Ensim Online Server) to authenticate and register the license. If not, it forces Parallels Pro Control Panel to contact the licensing server when you log in to Parallels Pro Control Panel. If the license is not registered, you are prevented from logging into Parallels Pro Control Panel.

During registration, Parallels Pro Control Panel calls the License Server and sends the following details for authenticating the license and subsequent registration.

- The Parallels Pro Control Panel version installed on the server
- The number of domains hosted on the Parallels Pro Control Panel server
- The Parallels Pro Control Panel server's operating system name and version
- The Fully Qualified Domain Name (FQDN) of the Parallels Pro Control Panel server
- The IP address of the Parallels Pro Control Panel server
- The MAC address of the Parallels Pro Control Panel server's network card

After registration, you can view (on page 18) or upgrade (on page 18) your license information at any time.

Renewing licenses

Parallels Pro Control Panel periodically connects to the License Server to determine the status of the license and automatically renews it on expiration. You do not have to manually renew your licenses. The license expires only if the call to the License Server fails after repeated attempts. To resolve the issue, contact Parallels Pro Control Panel support.

Registering the License

You are prompted to register Parallels Pro Control Panel with the License Server when you log in to Parallels Pro Control Panel after the installation.

During registration, Parallels Pro Control Panel connects to the License Server to retrieve license information pertinent to the version of Parallels Pro Control Panel you install on the server. If Parallels Pro Control Panel fails to connect to the License Server during the first registration attempt, you are offered a grace period of 7 days. During this period, Parallels Pro Control Panel continues its attempts to contact the License Server. The grace period does not reset each time a call is made to the License Server. During the grace period, you can continue to perform management operations using the control panel. After expiration of the grace period, you are prevented from logging in to Parallels Pro Control Panel if you have not registered the server with the License Server successfully.

If registration fails on multiple attempts, resolve the issues before you proceed. No grace period is available for failed registrations after the first attempt.

➢ ***To register the license:***

1. Obtain a new license key from Parallels Online Store.
2. Type the Parallels Pro Control Panel Web address in a browser window and log in with your account information.
3. Type the license key. Ensure that you type the alphabetic characters in uppercase.
4. Click **Register**.
5. After registration, the home page of Parallels Pro Control Panel is displayed.
6. If the license registration is not successful the first time, you can click **Continue** to proceed to perform management operations using Parallels Pro Control Panel for a grace period of 7 days.

Troubleshooting registration failures

The following table lists the possible reasons why the registration process can fail.

Error	Solution
Unable to contact the licensing server to validate the license.	▪ Ensure that you are connected to the network. ▪ Ensure that your firewall configuration is not blocking access to the License Server.
The Parallels Pro Control Panel licensing server is down.	Repeat the registration process at a later time.

Viewing License Information

To view your current license information, in the shortcuts section of the Home page, click **License** (**Configuration** section). The following information is displayed.

- **State.** The current state of the license, whether active or expired.
- **Issue Date:** The date and time when the license was activated or issued.
- **Upgradeable:** Whether or not the license can be upgraded to a higher capacity license.
- **Product:** The name of the product using the license.
- **Product Type.** The type of product (Parallels Pro Control Panel).
- **Domain Limit:** The number of domains that can be hosted and managed on Parallels Pro Control Panel using the license.

From this page, you can:

- Update your license (on page 18)
- Renew your license (on page 19)

Updating Your License

You need to update your license if you want to increase your current license capacity.

➢ ***To update your license:***

1. Obtain a new license key from Parallels Online Store at http://www.parallels.com/en/buyonline/pro/.
2. In the shortcuts section of the Home page, click **License** (**Configuration** section). The current license information is displayed.
3. Click **Update License**. The current license key is displayed.
4. Update the license key.
5. Click **Register**.

Renewing Your License

Typically, Parallels Pro Control Panel is configured to periodically contact the License Server. If Parallels Pro Control Panel has been unable to contact the License Server due to network or firewall issues and you want Parallels Pro Control Panel to establish communication with the license server after you resolve the issue, you need to renew your license. When you renew your license, Parallels Pro Control Panel contacts the License Server and obtains the most recent license information (if the license information has changed since the last communication).

➢ ***To renew your license:***

1 In the shortcuts section of the Home page, click **License** (**Configuration** section). The current license information is displayed.

2 Click **Renew License**.

Using the Configuration Page

You can view and manage your server configuration and resource settings using links on the Configuration page.

From the **Configuration** page, you can:

- View your network settings (on page 20)
- View your disk resource usage (on page 20)
- Change the system time zone (on page 22)
- Apply a new skin (on page 23)
- Apply a custom logo (on page 24)
- Change your user name, password and email address (on page 21)
- Restart the control panel (on page 25)
- Reboot the host server (on page 25)
- Update your license (on page 18)
- Renew your license (on page 19)
- Use AnnounceIt! (on page 104)

Viewing Server Settings

In this section:

Viewing Your Network Settings

The basic network settings are configured during the installation. You can only view the information displayed on the screen.

➢ ***To view your network settings:***

In the shortcuts section of the Home page, click **Network Settings** (**Configuration** section). The **Network Settings** page is displayed.

The fields in this form include:

- **Host Name:** The name of the server
- **Domain Name:** The domain name of the server
- **Default Gateway:** The gateway or router address assigned to the server
- **Master Server:** The IP address of the main DNS server
- **Slave Server:** The IP address of the backup DNS server
- **IP Address:** The IP address reserved for the server
- **Netmask:** The subnet mask address assigned to the server

Viewing Your Disk Resource Usage

You can view your disk resource usage information at any time. The disk usage information illustrates the amount of disk space used by your disk as against the allocated space, and the residual disk space.

Note: The usage information is not displayed for disks using the LVM (Logical Volume Management) partitioning scheme.

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

In the shortcuts section of the Home page, click **Disk Usage** (**Configuration** section).

The **Disk Info** page is displayed. The columns in this form include:

- **Partition:** The partitions on the server
- **Mount Point:** The location on the server where the partition is mounted
- **Total:** The total amount of disk space allocated to the server
- **Used:** The amount of disk space already used
- **Available:** The amount of disk space still available for use
- **Used %:** Displays a bar graph of the percentage of used disk space

---

Note: If the partition disk space reaches 90% of allocated capacity, a warning appears on the Site List page.

Configuring the Server

In this section:

Changing Your User Information

You can change your Server Administrator user name, password, and contact email address at any time.

➢ ***To change your user information:***

1. In the **shortcuts** section of the Home page, click **Change Administrator** (**Configuration** section). The **Change Administrator** page is displayed.
2. To change your user name, in the **Administrator User Name** field, enter a new name.
3. To change your password, in the **Password** field, enter a new password.
4. In the **Confirm Password** field, type your new password again.
5. To change the email address where notifications will be sent, in the **Administrator Email** field, enter the new email address.
6. Click **Update**.
7. Your changes take effect immediately.

Changing the System Time Zone

You can change the system time zone at any time.

➢ ***To change the system time zone:***

1. In the **shortcuts** section of the Home page, click **Time Zone** (**Configuration** section).
2. On the **System Time** page, click **Edit Settings**.
3. In the **Edit Time Zone** field, scroll through the list and select your local time zone.
4. Click **Update.**
5. The change takes effect immediately.

Changing Interface Language

In standard distribution of Parallels Pro Control Panel there is no possibility to choose a system language other than English. More languages can be added by means of installing language packs. We provide Spanish and German language packs that can be downloaded from Parallels Pro Control Panel download page.

After you install a language pack, you can choose your interface language on the login page.

Parallels Pro Control Panel 10.3.3 and up prevents interface pages where a different language is enabled from resetting to English. For this purpose, it includes a file `/etc/appliance/language` in which *en_US* is set as default language. This file is added after Parallels Pro Control Panel 10.3.3 installation or update.

To prevent your pages from resetting to English, manually set your language in `/etc/appliance/language`, for example *de_DE,* instead of default. Make sure this file contains no other records.

Note: If you want your system to behave the way it did before 10.3.3 version, manually remove the file `/etc/appliance/language`.

Applying a New Skin

You can change or customize the appearance of your control panel with A skin is a collection of images that enable you to alter the visual style and presentation of a user interface. Skin customizations allow you to extend your corporate look and feel to affiliated web sites and thus convey brand association and unity. of your choice.

Note: The sites hosted on the server assume the visual style of the control panel.

➢ ***To apply a new skin:***

1 In the **shortcuts** section of the Home page, click **Manage Skins** (**Configuration** section).

2 In the **Skins** area, select the 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.

Note: You must log out by clicking **Log Out** in the **Login Info** panel, and log in again using your account information, for the new skin to get applied.

Using a Custom Logo

The Parallels Pro Control Panel logo is the default logo displayed on all of the control panels. You can replace this default logo with your own by saving the logo you want to use as a file named `logo.gif`, then uploading it through the Server Administrator control panel or copying it to the customization directory on the server as described in the instructions below.

The default Parallels Pro Control Panel logo is used for all of the control panels, unless you specify a customized logo.

Resellers can display a logo for their Site and User Administrator Control Panel. This can be done by uploading the logo to the server, through the Reseller Administrator Control Panel.

Using the control panel to change the logo

➢ ***To upload your logo to the server:***

1. In the **shortcuts** area of the Home page, Click **Upload Logo** (**Configuration** section).
2. In the **Upload new logo** field, enter the name of your custom logo file including the full path or click **Browse** to locate and select the file on your computer.

Note: Your logo size should not exceed 73 x 46 pixels.

---

3. Click **Upload Logo**.

➢ ***To reset the logo to a default logo:***

1. In the **shortcuts** section of the Home page, click **Upload Logo** (**Configuration** section).
2. Click **Change to Default Logo.**

Using the command line to change the logo

When you use the command line interface to change the logo, ensure that your custom logo is named `logo.gif`, then copy it to the customization directory on the server as described in the instructions below.

➢ ***To replace the Parallels Pro Control Panel logo:***

1. Size your logo to 73 x 46 pixels and save it as a GIF file with the following file name:

   `logo.gif`.
2. If you have not done so already, create an FTP user account so you can make an FTP connection to the server. To create an FTP user account:
3. Make an SSH connection to the server, then type:

```
useradd <ftp_username>
```

where ***<ftp_username>*** is the name you want to assign to your FTP account.

4 Set your password by typing:

```
password <ftp_username>
```

where ***<ftp_username>*** is the name you assigned to your FTP account, then follow the prompts to set your password.

5 Connect to the server through FTP, then copy your logo.gif file to the server.

6 Using SSH, log on to the server as the root user.

7 Use either the move (mv) or copy (cp) command to move your logo.gif file to the customization directory `/etc/appliance/customization/`. For example:

```
mv /home/<ftp_username>/logo.gif \
/etc/appliance/customization/logo.gif
```

where `<ftp_username>` is the user name of your FTP user account on the server.

Restarting the Control Panel

Restarting the control panel does not stop any service currently running on the server but makes it unavailable for use for a few minutes.

➢ ***To restart the control panel:***

1 In the **shortcuts** section of the Home page, click **Restart/Reboot** (**Configuration** section).

2 Click **Restart Control Panel**.

The system safely shuts down the control panel, then starts it again.

Restarting the Host Server

Restarting the server restarts any service currently running on the server and makes the server unavailable for a few minutes.

➢ ***To restart the host server:***

1 In the **shortcuts** section of the Home page, click **Restart/Reboot** (**Configuration** section).

2 In the **Reboot Serve**r area, Click **Reboot**.

The system safely shuts down the server, then starts it again.

C H A P T E R 6

Managing Services

In this chapter:

Service Descriptions

Services are software applications, scripts, or packages that are enabled when you add or modify a site. The services are optional and may not be installed on the server.

Web Server

- *Apache Web Server*. Responds to Web browser requests.
- *Mod_perl for Apache*. Enables you to write Apache modules entirely in Perl. It embeds a Perl (Practical Extraction and Report Language) interpreter into the Apache server, so that the dynamic content produced by Perl scripts can be served in response to incoming requests, without the significant overhead of re-launching the Perl interpreter for each request.
- *WebDAV server*. 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.
- *PHP Hypertext Preprocessor for Apache*. Creates dynamic Web pages. PHP (PHP Hypertext Preprocessor) is a server- side, cross-platform, HTML embedded scripting language.

Python

- *Python*. Enables you to write system utility programs and scripts. Python is a popular, object-oriented, interpretive scripting language used for writing system utilities and Internet scripts.

FTP

- *FTP*. Transfers files over the Internet. FTP (File Transfer Protocol) allows you to transfer files across the Internet.
- *Anonymous FTP*. Allows you to use an FTP site without a password and without creating a user account.

DNS

- *DNS* (if available). Translates domain names into IP addresses. DNS is a 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.

MySQL

- *MySQL*. Allows you to work with your SQL databases. MySQL is a widely used relational database management system for SQL databases. A database management system allows you to add, access, and process data stored in a SQL database.
- *phpMyAdmin Web Based MySQL Administration*. Allows you to manage your SQL databases over the Internet. phpMyAdmin can handle administering entire MySQL database servers or just a single database over the Internet by removing any platform-specific limitations. In the control panel, you can use phpMyAdmin to set up, configure, and view your databases.

Email

- *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 enables management of email features, such as email aliases, responders, and spam filters.
- *POP3 + IMAP Server*. Processes incoming mail. POP3 (Post Office Protocol, version 3) and IMAP (Internet Messaging Access Protocol) mail servers store incoming email messages until users download them to their computers. In addition to storing incoming email 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.
- *SquirrelMail Web-based Email*. Provides Web-based access to email accounts. SquirrelMail is an email client that uses IMAP to provide your email account users with access to their email messages directly on the Internet.
- *Mailing Lists (Majordomo)* (if available). 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.
- *MailScanner*. Email scanning service that scans incoming and outgoing emails for viruses.
- *Virus Scanning (Clam AntiVirus)*. Interfaces with the MailScanner to integrate with the mail server for scanning incoming and outgoing emails for viruses.
- *Spam Filtering*. A spam filtering service that scans email messages for spam and enables user level control and management of spam.
- *Vacation Auto-responder*. Automatically responds to incoming email messages with a predetermined response. Vacation Autoresponder creates automated email responses that replies to incoming email messages during times when the user is not available to check and reply to email messages. This feature is most commonly used when a user intends to be unavailable for an extended period of time.

Network Connection

- *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. The protocol runs on your computer and connects your local computer to a server on the network. It also allows a user at a local computer to log on to a remote computer.
- *OpenSSH Secure Shell*. Provides secure remote access to another system over a network. Secure Shell (SSH) is a facility for logging into a remote machine and remotely executing commands on a remote machine. It is intended to provide secure encrypted communications between two untrusted hosts over an insecure network.
- *OpenSSL 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. You can secure a domain through the Web Server Manager (of the control panel).

FrontPage

- *Microsoft FrontPage Server Extensions*. Allows you to support customers who want to use Microsoft FrontPage to manage their Web sites. You can access FrontPage administration Web pages, as the Site Administrator, from the Web Server Manager (of the control panel).

Dynamic Web Content

- *Power Tools*. Enables customers to install and use off-the- shelf Web applications through the Site Administrator control panel. Power Tools are used to provide e-commerce, content management, forums, chat, and other dynamic features of Web sites.
- *Miva Merchant*. Provides e-commerce support for domains. Miva Merchant enables you to create multiple online storefronts and support e-commerce on a domain.

Statistics

- *Webalizer Log Analyzer*. Webalizer (on page 151) is a free web server log file analysis tool. Webalizer generates usage statistics for Web and FTP servers in easily comprehensible graphical or tabular formats. The logs generated are a statistical encapsulation of user traffic on your server and can be viewed in HTML format.
- *AWStats 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. The Analog Web/FTP Log Analyzer is an automated log analysis program that compiles Web site traffic statistics into an easy to read and understand form.

Using the Power Tools Add-on

In this section:

Overview of 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.

Web applications have become popular since they are widely available from the open-source community, and they enable a Web designer to provide dynamic content without writing a program. However, installing the applications correctly and configuring them for a Web site often requires system administration expertise, which many Web designers do not have.

When you install the Parallels Pro Control Panel Power Tools add-on, it is automatically available to your resellers. In addition, you can offer it as a service to sites. Site Administrators can use Power Tools to install and configure Web applications on their sites through the Site Administrator control panel. They can do this without special system administration knowledge or expertise, and more important, without needing to call you for support.

Note: As new versions of Power Tools are made available, you must notify Site Administrators to upgrade the user instances to the latest version of the tool (if they want to deploy the user instances on the latest version of the tool).

If you have the Power Tools add-on installed, Power Tools appears on the installed services list (on page 36).

For a complete list of the available tools, please refer to the **Power Tools** section, in the **Server Administrator** control panel.

Managing Power Tools

Using the Power Tools add-on, you can:

- View the Power Tools available on your system.
- View information about a tool (on page 34).
- Enable/disable tools for a site (on page 33).
- View the number of installations of a tool (on page 34).
- View sites that have installed a tool (on page 35).
- Prevent further installations of a tool (on page 35).

For this release of Power Tools, you cannot:

- Upgrade tools.
- Remove tools from the system.
- Add new tools.
- Remove a tool installation from a site. This can only be done at the Site Administrator level.

Installations Page

The Installations page lists the sites that have installed a tool. On this page you can perform several tasks and view the following information:

- **Site**. The names of sites that have installed the tool.
- **Installations**. The number of installations on each site. Sites can have several installations of each tool.

On this page you can:

- Click the tool icon to go to the Internet home page of the tool.
- If the tool is enabled: Click **Disable Tool** to prevent site administrators from installing the tool even if it is enabled for their site. However, if a site already has an existing installation of the tool, the existing installation is not affected.
- If the tool is disabled: click **Enable Tool** to make it available to sites. After the tool is enabled, site administrators can install it provided it is enabled for their site (on page 33).

When the Power Tools add-on is installed, you can access this page by clicking **Power Tools** in the Tools shortcut on the Home page, then clicking the List Installations icon in the **Actions** column of the tool.

Available Power Tools Page

The Available Power Tools page shows the tools available through the Power Tools add-on. On this page you can perform several tasks and view the following information:

- **Enabled**. The current state of the tool. States include:

  ↑. The tool is enabled at the system level. Site administrators can install the tool provided that it is enabled for their site (on page 33).

  ↓. The tool is disabled at the system level. This prevents site administrators from installing the tool even if it is enabled for their site. However, if a site already has an existing installation of the tool, the existing installation is not affected.
- **Power Tool Home Page**. The icon representing the tool. Click this icon to go to the home page of the site.
- **Description**. A brief overview of the tool.
- **Installations**. The number of times the tool has been installed on sites in your system. Sites can have multiple installations of each tool.
- **Actions**. Links to tasks you can perform. These change, depending on which tasks are available.

On this page you can:

- Perform tasks by clicking icons in the **Actions** column. Icons and tasks include:

  , enable a tool that is disabled.

  , disable a tool that is enabled. This prevents site administrators from installing the tool, but does not affect existing installations.

, view all installations of a tool. This shows the sites in your system that have installed the tool, and the total number of installations on sites in your system.

When the Power Tools add-on is installed, you can access this page by clicking **Power Tools** on the left navigation bar. You can also click **Power Tools** in the Tools shortcuts on the Home page.

Enabling Power Tools for Resellers

If you have the Power Tools add-on installed, the resellers can automatically enable Power Tools for their sites.

If you disable individual Power Tools (on page 35), the tools continue to be available to resellers. Sites created by resellers, however, cannot install tools you have disabled.

Enabling Power Tools for a Site

You can enable Power Tools for a site when adding the site or later. After you enable Power Tools for a site, the site administrator can install the individual Power Tools.

➢ ***To enable Power Tools for a site when adding a site:***

1. In the shortcuts section of the Home page, click **Add Name-based Site** (**Sites** section) or **Add IP-based Site**, depending on the type of site you want to create.
2. On the **Add Site** form, complete the Site Information section, then click **Advanced**.
3. In the Power Tools section at the bottom of the form, select the check box next to Enable Power Tools, then choose the tools you want to enable for the site.

Note: If you clear the Power Tools check box, Power Tools is disabled for the site. The individual tools selected are still disabled, but they are activated if you enable Power Tools for the site later.

---

1. Click **Add Site**.

   Power Tools is enabled for the site.

➢ ***To enable Power Tools for a site after you have added the site:***

1. In the shortcuts section of the Home page, click **List Sites** (**Sites** section).
2. Locate the site you want to change and in the **Actions** column, click . The **Edit Site** form opens.
3. In the **Power Tools** section at the bottom of the form, select the check box next to Power Tools, then choose the tools you want to enable for the site.
4. Click **Update Site**.

   Power Tools is enabled for the site. Additional information about installing and using tools is provided in the Site Administrator online Help.

Changing the Tools Enabled for a Site

You can change the tools available to a site by editing the site's Power Tools options.

➢ ***To edit a site's options:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to change and in the **Actions** column, click . The **Edit Site** form opens.

3 In the Parallels Pro Control Panel **Power Tools** section at the bottom of the **Edit Site** form, select the check box next to **Power Tools**, then choose the tools you want to enable for the site.

Note: If you want to disable Power Tools for a site, clear the Power Tools check box in the Power Tools section. This prevents the Site Administrator from installing or managing Power Tools.

4 Click **Update Site**.

The selected tools are enabled for the site.

Viewing the Number of Installations of a Tool

The number of installations of a tool is the number of instances in which the tool is being used on sites in your system.

Sites might have multiple installations of a tool. For example, a site might use an e-commerce tool at several different URLs. Each URL uses a separate installation of the tool.

➢ ***To view the number of installations of a tool:***

In the shortcuts section of the Home page, click **Power Tools** (**Tools** section). On the Available Power Tools page (on page 31), the **Installations** column indicates the number of installations of each tool.

Viewing Information About a Tool

You can view information about tool, such as the sites using it and the number of installations on each site.

In addition, Internet links to the tool’s distributor are provided for each tool.

➢ ***To view information about a tool:***

1 In the shortcuts section of the Home page, click **Power Tools** (**Tools** section). The Available Power Tools page (on page 31) is displayed.

2 On the **Available Power Tools** page, click the number of installations (Installation column) for the Power Tool whose information you want to view. The Installations page (on page 31) is displayed.

Viewing Sites that Use a Tool

You can view a list of the sites that have installed Power Tools and the number of installations of each Power Tool on each site.

➢ ***To view sites that use a tool:***

1. In the shortcuts section of the Home page, click **Power Tools** (**Tools** section). The **Available Power Tools** page is displayed.
2. On the **Available Power Tools** page, click the number of installations (**Installation** column) for the Power Tool whose information you want to view. The Installations page (on page 31) is displayed.

   The sites that use the tool are displayed in the **Sites** column. The number of installations on each site is shown in the **Installations** column.

Preventing Further Deployment of a Tool

You can disable a tool if you want to prevent sites from installing it. There are two ways to disable a tool:

- Disable the tool at the site level (on page 35)
- Disable the tool at the system level (on page 35)

When you disable a tool at the site level, you prevent the site from installing it. When you disable a tool at the system level, you prevent all sites from installing it.

When you disable a tool, existing installations are not affected. You cannot remove site installations from the Server Administrator control panel; existing installations can be removed only from the Site Administrator control panel.

➢ ***To disable a tool at the site level:***

1. In the shortcuts section of the Home page, click **List Sites** (**Sites** section).
2. Locate the site for which you want to disable the tool, and in the **Actions** column, click . The **Edit Site** form opens.
3. In the **Power Tools** section at the bottom of the form, clear the check box next the tool you want to disable for the site. To disable all tools, clear the check box next to **Enable Power Tools**.
4. Click **Update Site**.

   The tool is no longer available to the site through the Site Administrator control panel. However, the existing installations are not affected.

➢ ***To disable the tool at the system level:***

1. In the shortcuts section of the Home page, click **Power Tools** (**Tools** section).
2. Click , in the **Actions** column of the tool you want to disable.

   The tool is no longer available to any site through the Site Administrator control panel. However, the existing installations of the tool are not affected.

Disabling Power Tools for a Site

You can disable Power Tools to prevent a site from installing or managing Power Tools.

➢ ***To disable Power Tools:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).
2 Locate the site you want to change and in the **Actions** column, click . The **Edit Site** form opens.
3 In the **Power Tools** section at the bottom of the Edit Site form, clear the **Enable Power Tools** check box in the **Power Tools** section. You do not need to clear the individual tools in the **Power Tools** section; they are all disabled if the **Power Tools** check box is cleared. However, the individual tools are activated if you enable Power Tools for the site later.
4 Click **Update Site**.

Site Administrators can no longer install or manage Power Tools.

Viewing Installed Services

In this section:

Viewing the List of Installed Services

➢ ***To view all installed services:***

1 On the left navigation bar, click **Services**.
2 The **View Subscribed Services** form opens displaying a list of all the services currently installed on the server.

On this page, you can:

- View all installed services (on page 36)

Note: If you want to read a brief description about each application, refer to Service descriptions (on page 27).

- Open a service (on page 38) to modify the existing configuration settings

Note: Not all services can be modified through the Server Administrator.

- Start (on page 102), stop (on page 102), and restart (on page 102) some services
- Check whether a service is running (on page 37)

Viewing the Status of a Service

You can quickly check whether a service is running or not by checking the **Subscribed Services** form.

➢ ***To check whether a service is running:***

1 On the left navigation bar, click **Services**. The **Subscribed Services** form opens displaying a list of service.

2 On the **Subscribed Services** form, locate the **Status** column.

The icons in this form indicate whether the service is available or unavailable.

 The service is running

 The service is stopped and is unavailable

Note: Some services, such as Majordomo (if available) and Miva Merchant, have no running state. The **Status** column of these services is blank.

Configuring Services

In this section:

Accessing Configurable Services

If a service is configurable, you can open the service (on page 38) to change the default configuration settings to suit the needs of your business and customers. If you want to read a brief description about each service, refer to service descriptions (on page 27).

Whenever you open a service, you open up an Application Manager that allows you to manage the features of that specific service.

You can open only the following services to change their default settings.

- DNS (if available)
- Email (on page 89)
- FTP (on page 83)
- MySQL (on page 96)
- Web server (on page 38)

➢ ***To open a service:***

1 On the left navigation bar, click **Services**. The **Subscribed Services** form opens displaying a list of services.

2 Locate the service you want to modify, then in the **Actions** column of that service, click .

The configuration page for the service opens in the main window.

Configuring the Web Server

In this section:

Working with the Web Server

The Web server responds to requests from browsers, retrieves requested files or executes CGI scripts, and returns document or script results.

From the Web Server page you can:

- Update your Web server configuration (on page 39)
- View your Web server log reports (on page 41)
- Secure a domain using SSL certification (on page 142)

Changing the Web Server Configuration

You can configure the Web server to serve Web requests on any port, apart from the default port 80.

Important: To access sites running on a port other than the default (HTTP: 80; SSL: 443), you must specify the port number in the site URL, as follows: `http://`<site_name>`:`<port_number> where ***<site_name>*** is the host name of the site and ***<port_number>*** is the port that interfaces with the Web server.

Example: To access a site running on Apache 2.0 that interfaces with port `8000`, you must type the following: `http://example.com:8000`

If you configure the Web server to run on a port other than the default port, you must notify the Site Administrator about the change in the site URL.

➢ ***To change the Web server configuration:***

1 In the shortcuts section of the Home page, click **Web Server** (**Services** section).

2 In the **Web Server Configuration** form, click **Edit Configuration**.

3 In the **Web Server Name** field, enter the fully qualified domain name of the Web server.

4 In the **Web Server Administrator** field, enter the email address of the person responsible for managing the server.

5 In the **Number of Servers** field, enter the number of servers that start up when the Web server starts.

Note: Increasing this number leads to consumption of server resources, but also improves server responsiveness.

6 In the **Port** field, type the port number of the Web server.

Note: You may type 80 or a valid port number greater than 1024.

7 In the **SSL Port** field, type the port number of the SSL service.

Note: You may type 443 or a valid port number greater than 1024.

8 In the **Host Name Lookup**s field, select the check box if you want host names to be resolved; otherwise, leave the check box blank. Host name lookups determine the host names of every Web connection and note them in the log files.

Note: This process can slow down the Web server.

9 In the **Maximum Clients** field, enter the maximum number of simultaneous Web server connections.

Note: Each connection generates a process, consequently, too many connections can slow or stop the server; however, if you specify too few simultaneous connections, it can slow down the responsiveness of the Web server.

10 Click **Update**.

11 To make these changes effective, restart the Web server (on page 102).

Note: Services hosted on the Web server will be inaccessible for the length of time required to restart the Web server.

Viewing Your Web Server Log Reports

You can view your Web server reports directly from Parallels Pro Control Panel or download them to your local system for viewing.

About Web server log reports

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

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

CustomLog

This report contains information about visitors to your Web site. Every time a visitor visits 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.

Viewing the log reports

➢ ***To view the log reports:***

1. In the shortcuts section of the Home page , click **Log Files** (**Web Server/Databases** section).
2. Locate the report you want to read and in the **Actions** column, click **Download**.
3. To view the reports, do one of the following:
   - Click **Open**. 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**.
   - Click **Save** to download the reports to your local system before viewing them. The log report is saved to the specified location.

Configuring the DNS Server

In this section:

Getting the Most Out of Your Parallels Pro Control Panel DNS Server

In this section:

Overview of DNS Management in Parallels Pro Control Panel

Recognizing the business need for flexible and distributed name server configurations, Parallels Pro Control Panel has enhanced and extended its DNS (on page 44) capabilities, now providing for complex hosting requirements. Parallels Pro Control Panel enables distinctive name server configurations for different sites, facilitates communication with external name servers, updates zone records on external name servers, and allows for delegated zone management. It also maintains a detailed log of all DNS-related actions and events (on page 74) that you can use to identify and resolve issues.

DNS management in Parallels Pro Control Panel

To make a domain 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). You specify the master name server and the slave name server (on page 45) for the domain when you create a domain in Parallels Pro Control Panel.

Important: Before you create a domain, make sure you have registered the domain (on page 45).

Parallels Pro Control Panel implements the BIND DNS protocol enabling it to act as a name server. The name server settings determine the name resolution and zone management capabilities of your Parallels Pro Control Panel DNS server. You can configure your Parallels Pro Control Panel server to function as any of the following name servers:

- Master name server (on page 47)
- Slave name server (on page 47)
- Forward name server (on page 49)

Managing DNS zones

You can perform the following DNS-related actions.

- View (on page 55) and modify (on page 56) SOA settings for a zone
- View (on page 57) the list of zones
- Add (on page 59), refresh (on page 60), and remove (on page 61) zones
- Add (on page 66), update (on page 64), and remove (on page 65) zone records
- View (on page 74) and remove (on page 75) DNS logs

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..

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 and IP address need to be registered with at least two ***DNS name servers***: a The Primary DNS server is the authoritative master server that serves requests for the domain. and a The Secondary DNS server provides backup service when the Primary DNS server is unavailable. It receives its data for a domain from the Primary DNS server. (or backup name server). You can use the Parallels Pro Control Panel server or any external server as a master or slave name server. Using Parallels Pro Control Panel as a master or slave name server reduces administrative overheads as Parallels Pro Control Panel automatically creates zones for any site that is created on Parallels Pro Control Panel.

For complete information on DNS, we recommend the following books.

- *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

Managing DNS Settings

If you are using Parallels Pro Control Panel as a name server, you can perform the following DNS related tasks through the Server Administrator interface:

View your DNS server information (on page 55)

View (on page 58), add (on page 59), manage, and remove (on page 61) DNS zones

View (on page 63), add (on page 66), update (on page 64), and remove (on page 65) zone records

About Domain Name Registration

Before you create a domain, you must register the domain with ICANN or an ICANN-Accredited Registrar. ICANN is an international organization responsible for managing the assignment of domain names and IP addresses. An ICANN-accredited registrar typically provides domain registration services for one or more top level domains, for example, Go Daddy is an ICANN-accredited registrar for the `.biz`, `.com`, `.net`, `.org`, `.info`, and other top level domains.

To register a domain, you need to inform your domain name registrar about the domain name and the name servers responsible for handling queries related to that domain and all names that belong to that domain. A name server is a host that translates the text name of a domain into the numeric IP address of the domain.

Typically, more than one name server is assigned to the domain to provide fault tolerance and load-balancing. When you assign multiple name servers to a domain, you need to configure one of the servers as the master name server and the rest as slave name servers. The queries for the domain are handled by the master and all of the slaves in a round-robin fashion. You specify the name servers for a domain (on page 45) when you create the domain.

Specifying the Name Servers for a Domain

A name server is a host that translates the text name of a domain into the numeric IP address of that domain. Parallels Pro Control Panel is bundled with the BIND service, which enables an Parallels Pro Control Panel server to act as a name server. By default, your Parallels Pro Control Panel server is set as the master name server. You can update this setting when you create a domain.

➢ ***To configure or update the name server settings:***

1. In the shortcuts section of the Home page, click **Add IP-based Site** or **Add Name- based Site** (**Sites** section).
2. On the **Add Site** form, click **Advanced**.
3. In the **Master** field (**DNS** section), enter the name of the master server.

4 In the **Slave** field (**DNS** section), enter the name of the slave server. If you want to specify multiple slave name servers, enter each name on a new line.

You can configure Parallels Pro Control Panel as one of the following name servers for a domain.

- Master name server (on page 47)
- Slave name server (on page 47)
- Forward name server (on page 49)

Using the Parallels Pro Control Panel DNS Server as a Master Name Server

When you create a domain configuring Parallels Pro Control Panel as the master name server, Parallels Pro Control Panel automatically creates the master zone and related zone records for the domain on the master name server.

Assuming that you want to configure the Parallels Pro Control Panel server `s1.isp.net` as the master name server for a domain named `myfirstcustomer.com`, perform the following steps:

1. In the **shortcuts** section of the Home page, click **Add IP-based Site** or **Add Name- based Site** (**Sites** section).
2. On the **Add Site** form, click **Advanced**.
3. In the **Master** field (**DNS** section), enter the host name of the Parallels Pro Control Panel server `s1.isp.net`.
4. In the **Slave** field (**DNS** section), enter the host name of the server you want to assign as a slave server. This can be another server running Parallels Pro Control Panel or any external server running a DNS service. If you want to specify multiple slave servers, specify each name on a new line. If you do not want to specify a slave server for the domain, leave the field blank.
5. Provide the other details in the form and click **Add Site**.
6. Parallels Pro Control Panel automatically creates the master zone `myfirstcustomer.com` and zone records for the domain. To verify, click **Zones** (**DNS**) in the shortcuts section of the Home page.

Note: If you have specified one or more slave servers during domain creation, Parallels Pro Control Panel allows the slave zones to obtain updates from the master server. However, Parallels Pro Control Panel cannot verify that slave zones for the domain are created on the slave servers. You must manually create a slave zone for the domain on the slave servers. You can do this before or after you create the domain.

Using the Parallels Pro Control Panel DNS Server as a Slave Name Server

If you are hosting Web sites on a server farm comprising many Parallels Pro Control Panel servers and other business servers, it may be more efficient from an organizational point of view, to have all the zones created on one single central server in the farm, regardless of which Parallels Pro Control Panel server hosts the domain. In this scenario, you may want to nominate one server, for example `nameserver.isp.net` as the master name server and set any Parallels Pro Control Panel server, for example `s1.isp.net` on which you are creating a domain, as the slave server that obtains updates from the master server.

Parallels Pro Control Panel creates a slave zone on the Parallels Pro Control Panel server `s1.isp.net`, and configures it to obtain updates from the master server, `nameserver.isp.net`.

Important: Before you create the site, you must create the zone on the master server `nameserver.isp.net`, otherwise, Parallels Pro Control Panel will not be able to add the required records inside the master zone. Further, the master server must be configured to allow the slave `s1.isp.net` to obtain updates from the master. If you want Parallels Pro Control Panel to add records to this zone, you must also allow `s1.isp.net` to update the zone that resides on `nameserver.isp.net`.

Assuming that you want to configure an external server `nameserver.isp.net` as the master name server and the Parallels Pro Control Panel server `s1.isp.net` as the slave name server for a domain named `myfirstcustomer.com`, perform the following steps:

1 In the shortcuts section of the Home page, click **Add IP-based Site** or **Add Name- based Site** (**Sites** section).
2 On the **Add Site** form, click **Advanced**.
3 In the **Master** field (**DNS** section), enter the host name of the external server `nameserver.isp.net`.

   Note: The external server can be any server running an implementation of the DNS protocol.

4 In the **Slave** field (**DNS** section), enter the host name of the Parallels Pro Control Panel server `s1.isp.net`.
5 Provide the other details in the form and click **Add Site**.

   Parallels Pro Control Panel automatically creates the slave zone `myfirstcustomer.com` and zone records for the domain. To verify, click **Zones** (**DNS**) in the shortcuts section of the Home page.

Using the Parallels Pro DNS Server as a Forward Name Server

If the name servers for your domains are hosted by an external ICANN-Accredited Registrar, such as Go Daddy, you need to specify the name servers of your service provider as the master and slave server respectively, for example `ns1.godaddy.net` and `ns2.godaddy.net`. In this scenario, the Parallels Pro Control Panel server acts as a forward server.

The zones for the domains on the Parallels Pro Control Panel server reside on the Registrar's servers. You need not create a DNS zone for the domains on the Parallels Pro Control Panel server. Parallels Pro Control Panel merely creates a forward zone for the hosted domain `customerdomain.com`. Any look up requests for the domain are forwarded in a round-robin pattern to the master server and slave servers.

Important: Before you create the site, make sure that the zone for the domain `customerdomain.com` is hosted on the external server `ns1.godaddy.com`. If the zone does not exist at the time of site creation, Parallels Pro Control Panel will not be able to add the required records inside the zone. Also note that Parallels Pro Control Panel will not attempt to contact the external servers `ns1.godaddy.com` and `ns2.godaddy.net` for *creating any records* unless the servers are added as external DNS servers (on page 52).

Assuming that the zone for the domain `myfirstcustomer.com` resides on the external master and slave servers `ns1.godaddy.net` and `ns2.godaddy.net` respectively, perform the following steps:

1. In the shortcuts section of the Home page, click **Add IP-based Site** or **Add Name- based Site** (**Sites** section).
2. On the **Add Site** form, click **Advanced**.
3. In the **Master** field (**DNS** section), enter the host name of the external server `ns1.godaddy.net`.

   Note: The external server can be any server running an implementation of the DNS protocol.

   ---
4. In the **Slave** field (**DNS** section), enter the host name of the slave name server `ns2.godaddy.net`.
5. Complete the **Add Site** form and click **Add Site**.

   Parallels Pro Control Panel automatically creates the forward zone `myfirstcustomer.com` for the domain. To verify, click **Zones** (DNS) in the shortcuts section of the Home page.

Note: Parallels Pro Control Panel will not be the authoritative name server for this zone, rather it will forward all lookup requests to `ns1.godaddy.com` and `ns2.godaddy.com`. The master server `ns1.godaddy.com` must be pre-configured to allow updates from the Parallels Pro Control Panel server `s1.isp.net`. Also, note that if `ns1.godaddy.com` is listed as an external server in the External Server List at the time of creating the domain, Parallels Pro Control Panel attempts to contact `ns1.godaddy.com` and add records to the `myfirstcustomer.com` zone on the server.

Specifying a Virtual Name Server as a Slave Server

If you are using Parallels Pro Control Panel as a DNS server, you can create a virtual name server to act as a slave DNS name server. This satisfies the requirement that you must have two DNS name servers to create a domain.

Be aware that creating a virtual name server does not actually provide redundancy because you are requesting Parallels Pro Control Panel to add a second IP address to the specified master name server. Since the IP address of the virtual slave server maps to the master server, if the master server stops operating, the slave server will as well.

➢ ***To specify a virtual slave name server:***

1. Stop the Domain Name Server. (on page 102)
2. In the shortcuts section of the Home page, click **Name Servers** (**DNS** section).
3. Locate **Virtual DNS Server** in the server list and in the **Actions** column, click ✎. The **Virtual DNS Setting** form opens.
4. In the **Virtual DNS Server Name** field, enter the fully qualified name of the DNS server you want to use as the virtual slave name server.
5. In the **Virtual DNS Server IP Address** field, enter the IP address of the virtual slave DNS server.
6. Click **Update**.
7. Restart the Domain Name Server. (on page 102)

Note: After making changes to the domain name server, you must restart the name server for your changes to take effect. It may take up to 48 hours for your DNS changes to be visible on the Internet.

Managing External DNS Servers

In this section:

About External DNS Servers

An external DNS server is any server running an implementation of the DNS protocol. The implementation can be BIND, Microsoft DNS, or any other implementation of the DNS protocol.

You can configure external DNS servers to act as the master or slave name servers for domains hosted on Parallels Pro Control Panel. When you configure external DNS servers as the master or slave name servers, Parallels Pro Control Panel cannot modify its local copy of the DNS zone because the DNS standard only allows the master's copy of a zone to be updated. Therefore, the Parallels Pro Control Panel server attempts to contact the external master name server to add the required DNS records within a zone. Make sure you have added the external server (on page 52) to Parallels Pro Control Panel, otherwise the Parallels Pro Control Panel server will be unable to contact the external server.

Viewing the List of External DNS Servers

To view the list of external DNS servers, in the shortcuts section of the Home page, click **External Servers** (**DNS** section). The **External Server List** form opens displaying the list of external servers.

From the **External Server List**, you can:

- Add external servers (on page 52)
- Update external server settings (on page 53)
- Remove external servers (on page 53)

Adding External DNS Servers

When you add an external server, Parallels Pro Control Panel updates the configuration file `/etc/virtualhosting/masterconf` on the Parallels Pro Control Panel server with information about the external server. The information in this file is used by Parallels Pro Control Panel to communicate with the external server.

➢ ***To add an external DNS server:***

1 In the shortcuts section of the Home page, click **External Servers** (**DNS** section). The **External Server List** form opens displaying the list of external servers.

2 Click **Add External Server**.

3 In the **Host Name** field, enter the name of the server. For example, `ns1.isp.net`.

4 In the **IP Address** field, enter the IP address of the server. For example, `65.65.65.65`.

5 In the **Key Name** field, enter the key name of the transaction signature that authenticates zone transfers for the external server. For example, `wp_default_key.` (note that the dot is part of the key name).

6 In the **Secret** field, enter the secret value of the transaction signature that authenticates zone transfers for the external server. For example, `IC6GU6asxPceF72LjQTfUQ==`.

Note: Usually, BIND name servers are configured to secure the zone updates using a transaction signature (TSIG) that uses a key/secret value pair. If your external server is running BIND, and is configured to protect zone updates using a key/secret value pair, enter the name of external server's key/secret value pair here. If your external server is also running Parallels Pro Control Panel, the key name you need to enter is **wp_default_key.** (the dot is part of the key name). The secret corresponding to that key can be obtained from the SOA Settings (on page 55) page on the control panel.

However, if your external name server is running another implementation of DNS, such as Microsoft DNS, chances are that it does not support the TSIG method of protecting zone updates. In this case, the external server must be configured to allow zone updates from your Parallels Pro Control Panel server, otherwise, the Parallels Pro Control Panel server will not be able to add records to any zone existing on the external name server.

---

7 Click **Add**.

Updating External DNS Server Settings

➢ ***To update the settings of an external DNS server:***

1 In the shortcuts section of the Home page, click **External Servers** (**DNS** section). The **External Server List** form opens displaying the list of external servers.

2 In the **Actions** column of the server, click .

3 Update the settings as required.

4 Click **Update**.

Removing External DNS Servers

When you remove an external server, the information for that server is removed from the configuration file `/etc/virtualhosting/masterconf` on the Parallels Pro Control Panel server. Once you remove the server, Parallels Pro Control Panel cannot create or update records on that external server. The existing zones and records on the server are left unchanged.

➢ ***To remove an external DNS server:***

1 In the shortcuts section of the Home page, click **External Servers** (**DNS** section). The **External Server List** form opens displaying the list of external servers.

2 In the **Actions** column of the server, click to remove the server.

3 In the confirmation window, click **OK** to remove the server.

Working with SOA Records

In this section:

About SOA Records

When you add a zone to a domain, Parallels Pro Control Panel automatically creates a Start of Authority (SOA) record. Each DNS zone has an SOA record. 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.

Parallels Pro Control Panel provides default information for the SOA records that are created for all the zones on the name server. This default information will apply to every SOA record created, unless you manually change the specific SOA record.

You can modify the SOA information default settings (on page 55) if you want to make a change that will affect every SOA record on the name server.

If you want to make a change that applies only to a specific SOA record, you can modify just the zone-specific SOA record (on page 56).

SOA Configuration Form

The SOA settings are as follows:

- **Master 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.

Viewing SOA Settings

You can view the transaction signature (on page 55) of the Parallels Pro Control Panel server and your existing DNS settings (on page 55) through the Server Administrator interface.

➢ ***Viewing the transaction signature of the Parallels Pro Control Panel DNS server***

A transaction signature is a key-secret pair that authenticates zone updates or transfers on a DNS server. To view the transaction signature of the Parallels Pro Control Panel DNS server, in the shortcuts section of the Home page, click **SOA** (**DNS** section). The **Configuration** window opens displaying the following transaction signature for the server.

- **Key**. The key value of the transaction signature.
- **Type**. The type of the key.
- **Secret**. The secret value of the transaction signature.

➢ ***Viewing the SOA settings***

To view the SOA settings, in the shortcuts section of the Home page, click **SOA** (**DNS** section). The **Configuration** window opens displaying your existing SOA settings (on page 54).

Modifying the Default SOA Record

The default information you set will apply to every SOA record created, unless you manually change the specific SOA record.

➢ ***To change the SOA default information:***

1. In the shortcuts section of the Home page, click **SOA** (**DNS** section).
2. On the **Start of Authority (SOA) Settings** form, click **Edit SOA Configuration**. The **Edit Default Start of Authority (SOA)** form opens.
3. Complete the SOA configuration (on page 54) form.
4. Click **Update SOA Configuration**.

Modifying a Zone-specific SOA Record

Parallels Pro Control Panel provides default information about the SOA records that are created for all the zones on the name server. The default information will apply to every SOA record created, unless you manually change the specific SOA record.

You can modify the SOA information default settings (on page 55) if you want to make a change that will affect every SOA record on the name server.

If you want to make a change that applies only to a specific SOA record, you can modify just the zone-specific SOA record.

➢ ***To modify a zone-specific 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 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 Complete the SOA configuration (on page 54) form.
5 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 62) 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 59) and remove (on page 61) zones through the Server 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 55) the SOA settings.

- view (on page 63) the list of records.

- refresh (on page 60) the zone.

- remove (on page 61) the zone.

Viewing DNS 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 54) for the zone.

Updating Zone Information

➢ ***To update your existing zones:***

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

2 Locate the zone you want to update and in the **Actions** column, click ☰. The **Host List** window for that zone opens displaying the current host settings.

For more information see About SOA records (on page 54), and About DNS Records (on page 62).

Adding Zones to a Name Server

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.

➢ ***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.com`.

4 In the **Master** field, enter the host name of the server that you want to designate as the master DNS server for the zone.

5 In the **Slaves** field, enter the host name(s) of the server(s) that you want to designate as the slave server(s) for the zone. Enter each host name on a new line.

6 Click **Add**.

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

7 Name server (NS) record (on page 62) specifying the zone’s name server. The default is the Parallels Pro Control Panel Control Panel server on which the zone operates.

8 Start of Authority (SOA) record (on page 54)specifying where within the domain name space the name server has authority.

9 The **Zone List** is updated with the new entry.

Enabling DNS for Sites

You may want to update the Parallels Pro Control Panel DNS server with the records and SOA settings of existing zones, if you have:

- Upgraded your control panel from Ensim Basic to Parallels Pro Control Panel
- Migrated from an external DNS server to the Parallels Pro Control Panel DNS server
- Changed the existing settings for a DNS zone and committed the update to the Parallels Pro Control Panel DNS server

➢ ***To update the Parallels Pro Control Panel DNS server:***

1. In the shortcuts section of the Home page, click **Enable DNS on Sites** (**DNS** section). The **Enable DNS on Sites** form opens listing all the sites for which you can update zone information.
2. Select all sites by selecting the **Select/Deselect all zones** check box, or select individual sites by selecting the check box corresponding to the site.
3. Click **Update DNS**.

   The Parallels Pro Control Panel DNS server is updated with the zone information of the selected sites.

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 information is updated.

Removing Zones from the Name Server

You can remove a zone 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; otherwise, the added records will be lost.

➢ ***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 . A confirmation dialog opens.
3. Click **OK** to remove the zone.

   Parallels Pro Control Panel 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.

Parallels Pro Control Panel automatically creates a Name Server (NS) record for the zone's name server, and Host (A) records for the FTP server and the domain name (www), 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 54).

The following table describes the different DNS record types that Parallels Pro supports.

Use this record:	To specify:
Name Server (NS)	The host name of a DNS server that is authoritative for the domain. If you add additional remote DNS servers, create a Host (A) record before you create the NS record for the server. **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 Parallels Pro. 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, Parallels Pro Control Panel automatically creates a Name Server (NS) record for the zone's name server and Host (A) records for the FTP server and the domain name (www). You can view your zone records from the Host List.

➢ ***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 **List of records** 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 62) 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 64) or remove (on page 65) a record.

Updating DNS Zone Records

Parallels Pro Control Panel automatically creates a Name Server (NS) record for the zone's name server, and Host (A) records for the FTP server and the domain name (www), but you can modify the information at any time. You can also modify any records you added.

➢ ***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 **List of records** 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 66).
4 Complete the fields and click **Update**.

Removing DNS Zone Records

You can remove records at any time.

Note: A DNS zone requires one Name Server (NS) record. If you have only one NS record in a zone, you cannot remove that NS record from the zone.

➢ ***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 List of records form opens. It displays all existing records for the zone.
3. Locate the specific record you want to remove and in the **Actions** column, click .

Parallels Pro Control Panel removes the record from your DNS configuration.

Adding Zone Records

In this section:

Adding DNS Zone Records

When you create a zone, Parallels Pro Control Panel automatically creates a Name Server (NS) record for the zone's name server, and Host (A) records for the FTP server and the domain name (www), but you can add others. You can also modify the record information at any time.

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 67)
- Host (A) records (on page 68)
- Reverse Address (PTR) records (on page 69)
- Alias (CNAME) records (on page 70)
- Mail Exchanger (MX) records (on page 71)
- AAAA records (on page 68)
- SRV records (on page 73)
- TXT records (on page 72)

Adding a Name Server (NS) Record

When you create a new zone, Parallels Pro Control Panel automatically creates an NS record for the zone's name server, but if you intend to use a DNS server other than the Parallels Pro Control Panel name server, you must change the NS record (on page 64) to reflect the name of that server. Also, if you intend to add additional remote DNS servers, you must create an NS record for each additional server.

Important: Add a Host (A) record (on page 68) 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.

➢ ***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 **List of records** 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 59) to which this record points; otherwise, the reverse pointer record will not take affect.

---

1 Click **Add**.

Adding an AAAA Record

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

➢ ***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 all 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.

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.

➢ ***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.

1 In the **Hostname.domain** field, enter the name of the host to which the IP address should map.

2 In the **IP Address** field, enter the IP address you want to map to the host.

3 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.

---

4 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.

Note: Add a Host (A) record (on page 68) 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 SMTP server provided by Parallels Pro. You can designate more than one external mail server for the domain.

Note: Add a Host (A) record (on page 68) 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 information.
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 host.

➢ ***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 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:

About DNS Logs

Parallels Pro Control Panel maintains a record of every DNS-related action performed on any of the sites hosted on your server. You can view the list of sites for which logs are maintained and further view detailed log information for each site. You can use the log entries to identify issues and resolve them.

When a site is deleted, by default, the DNS log entries for that site are removed. However, you can choose to retain the log entries for that site by setting the **orphanDNSLogEntries** attribute to **True** in the configuration file `/etc/ensim/epl.conf`.

➢ ***To change the setting:***

1. Log in as the root user to the Parallels Pro Control Panel server.
2. Using an editor of choice, open the configuration file `/etc/ensim/epl.conf`.
3. Locate the attribute **orphanDNSLogEntries** and set its value to **True**.
4. You will now be able to view the log (on page 75) entries of deleted sites in the control panel.

Viewing the List of DNS logs

You can view the logs for each site hosted on your server.

To view the list of logs, in the shortcuts section of the Home page, click **DNS Log** (**DNS** section). The following information is displayed.

- **Site**. The name of the site for which log information is displayed.
- **No. of Logs**. The number of logs entries for the site.
- **Actions**. The action you can perform on the logs of the site. You can remove all the log entries (on page 75) for the site.

Viewing the Log Details for a Site

You can view detailed log information for each site hosted on your server.

➢ ***To view the DNS log details for a particular site:***

1 In the shortcuts section of the Home page, click **DNS Log** (**DNS** section).
2 Click the name of the site for which you want to view the log details.
3 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.
   - **Type of 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 action or event is reported.
   - **Record Type**. The type of zone record, for example, CNAME.
   - **Record 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 a particular log entry (on page 75) at any time.

Removing DNS Log Entries for a Site

You can remove individual log entries or all the DNS logs for a site.

➢ ***To remove individual log entries:***

1 In the shortcuts section of the Home page, click **DNS Log** (**DNS** section).
2 Click the site name whose log entries you want to remove.
3 In the **Actions** column of the log entry you want to remove, click ✖. A confirmation dialog opens.
4 Click **OK** to confirm the deletion.

➢ ***To remove all the log entries for a site:***

1 In the shortcuts section of the Home page, click **DNS Log** (**DNS** section).
2 In the **Actions** column of the site whose logs you want to remove, click ✖. A confirmation dialog opens.
3 Click **OK** to confirm the deletion. All the log entries for the site are removed.

Setting DNS Policies

In this section:

Overview of the DNS Policy Framework

Parallels Pro Control Panel enables you to delegate zone management tasks to resellers and Site Administrators. Enabling resellers to manage the zones and records of their sites allows them the flexibility to leverage existing partnerships and easily manage administrative tasks involved in enhancing or extending existing business capabilities. However, while certain tasks such as adding or updating zone records may be delegated without concern, tasks such as SOA updates may affect the functioning of the name servers. To prevent changes or updates that may adversely affect the existing DNS configuration, Parallels Pro Control Panel creates policy files that you can use to restrict the zone management capabilities of resellers and Site Administrators.

Policy file

The policy file (on page 77) maps each DNS-related action to a corresponding identifier that can be assigned a **True (Yes)** or **False (No)** value. The assigned value determines whether or not a user can perform the action.

You can view the list of policy files (on page 78) at `/etc/virtualhosting/policies/`.

Structure of a Policy File

The policy file is an INI file that is easy to read and modify. The policy file contains sub-policies identified by a name. The default sub-policy is **bind**. The various options under a sub-policy identify the policy-related actions. You cannot add sub-policies; however, you may modify the existing ones.

The contents of a policy file are as follows:

```
[bind]
add_a = yes
add_aaaa = yes
add_cname = yes
add_mx = yes
add_ns = yes
add_ptr = yes
add_srv = yes
add_txt = yes
add_zone = yes
delete_a = yes
delete_aaaa = yes
delete_cname = yes
delete_mx = yes
delete_ns = yes
delete_ptr = yes
delete_srv = yes
delete_txt = yes
delete_zone = yes
edit_soa = yes
```

To revoke permission on an action, set the attribute to **no**; to grant permission, set the attribute to **yes**.

List of Policy Files

The list of available policy files are located at `/etc/virtualhosting/policies/`.

The following policy files are created by Parallels Pro Control Panel:

- `/etc/virtualhosting/policies/isp`. Policy file that provides the default settings for the Server Administrator.
- `/etc/virtualhosting/policies/isp.sitedefault`. Policy file that provides the default settings for any site created by the Server Administrator.
- `/etc/virtualhosting/policies/isp.resellerdefault`. Policy file that provides the default settings for any reseller created by the Server Administrator.
- `/etc/virtualhosting/policies/reseller`***<R>***. Policy file that provides the default settings for the reseller identified by the ID ***<R>***.
- `/etc/virtualhosting/policies/reseller`***<R>***`.sitedefault`. Policy file that provides the default settings for any site created by the reseller identified by the ID ***<R>***.
- `/etc/virtualhosting/policies/site`***<N>***. Policy file that provides the default settings for the Site Administrator of the site identified by the ID ***<N>***.

Modifying Policy Settings

To modify the policy settings, open the file in an editor, update the settings as required, and save the changes.

Action	Steps
Modifying the policy settings for the Server Administrator	The settings you configure in the file `/etc/virtualhosting/policies/isp` apply to the DNS-related actions performed by you. **1** Using an editor, open the file `/etc/virtualhosting/policies/isp`. **2** Change the settings as required and save the changes.
Modifying the policy settings for sites created by the Server Administrator	The settings you configure in the file `/etc/virtualhosting/policies/isp.sitedefault` apply to all the sites created by you. **1** Using an editor, open the file `/etc/virtualhosting/policies/isp.sitedefault`. **2** Change the settings as required and save the changes.
Modifying the policy settings for resellers created by the Server Administrator	The settings you configure in the file `/etc/virtualhosting/policies/isp.resellerdefault` apply to all the resellers created by you. **1** Using an editor, open the file `/etc/virtualhosting/policies/isp.resellerdefault`. **2** Change the settings as required and save the changes.
Modifying the policy settings for a particular reseller	**1** The settings you configure in the file `/etc/virtualhosting/policies/reseller`***<R>*** apply to the specified reseller. **2** Using an editor, open the file `/etc/virtualhosting/policies/reseller`***<R>***, where ***<R>*** is the reseller ID of the reseller. **3** Change the settings as required and save the changes.

Modifying the policy settings for sites created by a particular reseller	The settings you configure in the file /etc/virtualhosting/policies/reseller***<R>***.sitedefault apply all sites created to the specified reseller. **1** Using an editor, open the file /etc/virtualhosting/policies/reseller***<R>***.sitedefault, where ***<R>*** is the reseller ID of the reseller.. **2** Change the settings as required and save the changes.
Modifying the policy settings for a particular site	The settings you configure in the file /etc/virtualhosting/policies/site***<N>*** apply to the specified site. **1** Using an editor, open the file /etc/virtualhosting/policies/site***<N>***, where ***<N>*** is the site ID. **2** Change the settings as required and save the changes.

Working with Local Name Server

In this section:

About Local Name Servers

Local name servers are name servers, which the user adds to the Parallels Pro Control Panel server, in addition to the host name of the local server (such as ns1.domain.com, ns2.domain.com).

On this page you can:

- Add a local name server (on page 80)
- Update a local name server (on page 82)
- Remove a local name server (on page 82)

Viewing the List of Local Name Servers

➢ ***To view your existing local name servers:***

1. In the shortcuts section of the Home page, click **Local Name Servers** (**DNS** section).
2. The **Local Name Server List** form opens displaying the list of local name servers in your current DNS configuration. The following information is displayed:
   - **Name Server**. The name of the local name server.
   - **IP Address**. The IP address of the local name server.
   - **Actions**. The actions you can perform on any of the local name servers.

     - edit (on page 82) the local name server.

     - remove (on page 82) the local name server.

Adding a Local Name Server

➢ ***To add a local name server:***

1. In the shortcuts section of the Home page, click **Local Name Servers** (DNS section). The **Local Name Server List** form opens.
2. Click **Add Local Name Server**. The **Update Local Name Server** form opens.
3. In the **Name Server** field, enter the name of the new local name server, for example, `mylocalnameserver.com`.
4. In the **IP Address** field, enter the IP address for the name server.
5. Click **Add**. Parallels Pro Control Panel adds the new local name server to your DNS configuration.
6. You can click **Reset** to revert the changes.

Update a Local Name Server

➢ ***To update an existing local name server:***

1 In the shortcuts section of the Home page, click **Local Name Servers** (**DNS** section). The **Local Name Server List** form opens.

2 In the **Actions** column of the local name server you want to update, click . The **Update Local Name Server** form opens.

3 In the **Name Server** field, edit the name of the local name server.

4 In the **IP Address** field, edit the IP address of the local name server.

5 Click **Update.** Parallels Pro Control Panel updates the new local name server to your DNS configuration.

6 You can click **Reset** to revert the changes.

You cannot edit the localhost entry from the list of the local name servers.

Removing a Local Name Server

➢ ***To delete an existing local name server:***

1 In the shortcuts section of the Home page, click **Local Name Servers** (**DNS** section). The **Local Name Server List** form opens.

2 In the **Actions** column of the local name server you want to remove, click .

3 In the confirmation window, click **OK**. The local name server is removed from the list.

You cannot remove the localhost entry from the list of the local name servers.

Configuring the FTP Server

In this section:

Viewing Your FTP Server Settings

FTP (File Transfer Protocol) allows you to transfer files across the Internet. Anonymous FTP allows you to use an FTP site without a password and without creating a user account.

Note: Anonymous FTP is supported only in Parallels Pro.

The control panel provides default configuration settings for the FTP server. You can change these settings to suit the needs of your site.

➢ ***To view your FTP configuration:***

In the shortcuts section of the Home page , click **Configuration** (**FTP** section).

The Configuration form opens displaying your FTP settings. The fields are described in the FTP Server Configuration Information (on page 84).

Changing Your FTP Server Settings

The control panel provides default configuration settings for the FTP server. You can change these settings to suit the needs of your site.

➢ ***To change FTP configuration:***

1. In the shortcuts section of the Home page, click **Configuration** (**FTP** section).
2. In the **Configuration** form, click **Edit**. The Edit Configuration form opens, showing the current FTP server configuration.
3. Refer to FTP Server Configuration Information (on page 84) to help you change the FTP settings.
4. Click **Update**.

FTP Server Settings Description

The following table briefly describes each FTP server configuration field.

This field:	Displays:
ServerIdent	The message displayed on connect.
Anonymous	Whether or not a user can transfer files to the server anonymously. Enabled means the server supports anonymous transfers; disabled means it does not. **Note:** The default directory for all anonymous transfers is `/var/ftp`.
TimeoutIdle	The maximum number of seconds the FTP server allows a client to stay connected without receiving data on either the control or data connection. If data is received on either connection, the idle timer is reset. The default **TimeoutIdle** is **600** seconds. You can disable the timer by specifying **0**. Clients can stay connected indefinitely without sending data. **Note:** Disabling the timer is not recommended because a hanging TCP connection prevents a child server from existing. The child server then must be manually removed.
TimeoutNoTransfer	The maximum number of seconds a client can stay connected after authentication, without issuing a command. The command may be sending or receiving a file or receiving a directory listing that results in an active or passive data connection. The default **TimeoutNoTransfer** is **600** seconds.

TimeoutLogin	The maximum number of seconds a client can spend verifying a login ID and password. The login timer is not reset when a client transmits data and is only removed once a client has transmitted an acceptable USER/PASS command combination. The default **TimeoutLogin** is **300** seconds.
MaxInstances	The maximum number of simultaneous connections allowed.

Configuring the Mail Server

In this section:

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. The mail server rejects email messages from these sources thus prohibiting further relay to any site hosted on the server. For example, if you include the IP address `1.2.3.4` in the Reject List, all email messages that originate from this address will be blocked from being relayed to any site hosted on the server.

The email source can be:

- **An email address** - The email address is blocked.
- **A site** - All email addresses that originate from the site are blocked.
- **An IP address** - All email addresses that originate from the specified IP address are blocked.

  If you enter a partial IP address, 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 87) to enable user-level control and management of spam. The Sendmail Reject List and spam filter service vary in their approach and flexibility (on page 88) in managing spam.

Note: The **Spam Filter** service offered in the earlier versions of Ensim Pro/Basic is renamed to **Sendmail Reject List**. Parallels Pro Control Panel introduces a new Spam Filter service that uses the SpamAssassin™ tool to enable spam scanning.

Overview of Mail Scanning

Mail Scanning is an email scanning service that enables scanning of incoming and outgoing email messages for viruses. You can offer Mail Scanning as a service to your customers when you create a site or Service Plan. You can limit email scanning to incoming or outgoing email messages or enable scanning for both.

Note: When you enable or disable Mail Scanning, you automatically enable or disable virus scanning (on page 90) capability.

Interfacing with the Virus Scanning service

The Mail Scanning service serves as a scanning interface between the mail server and the Virus Scanning service. Its ability to act thus as a connecting interface enables the Virus Scanning service to extend its scanning services to incoming and outgoing email messages. When the control panel server receives an email message, a scan request is sent to the Mail Scanning service. Further, it routes the request to Clam AntiVirus (on page 90) to effect a virus scan.

The control panel uses the email scanning application **MailScanner** to provide email scanning capability. For detailed information on MailScanner, please visit http://www.sng.ecs.soton.ac.uk/mailscanner/.

Overview of Spam Filtering

Spam Filter is an email scanning service that Each email is evaluated against message rules that associate a textual pattern or characteristic with spam. Each rule is assigned a value called a score. When the text in an email matches a rule, a score is assigned to the email. If the sum of all such scores exceeds the set threshold, the message is categorized as spam. and enables user-level control and management of spam. You can offer spam filtering as a service to your customers when you create a site or Service Plan.

Note: When you enable spam filtering for a site, you automatically empower the User Administrator with The administrator can set the spam threshold that categorizes an email message as spam. Once identified as spam, he can choose to delete the spam email, have it delivered as an attachment or as a regular email to his inbox, or quarantine the email in his spam folder..

You can also use the Sendmail Reject List (on page 86) to reject spam. The spam filter lists and the Sendmail Reject List vary in their approach and flexibility (on page 88) in managing spam.

The control panel leverages the spam filtering tool **SpamAssassin™** to enable spam scanning. For detailed information on SpamAssassin, please visit http://useast.spamassassin.org/index.html.

Using the Sendmail Reject List and Spam Filtering Service

The control panel offers two options - the Sendmail Reject List (on page 86) and Spam Filtering (on page 87) service - that vary in their approach and flexibility in managing spam.

While the Sendmail Reject List enables effortless global control on spam, the Spam Filtering service allows for discretionary management of spam by the users themselves.

Sendmail Reject List

Email sources that you include in the Reject List are rejected by your mail server.

Advantages

- The Sendmail Reject List enables you to exercise global control over email messages that are relayed to the sites hosted on your server.
- Rejecting spam at the server 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 server level reduces the risk of email viruses infiltrating the network.

Disadvantages

- As the administrator of the control panel server, only you can exercise the right to control and manage spam using the Reject List. Users do not have the flexibility to access or review email messages that originate from a blacklisted source.

Spam Filtering service

While the Sendmail Reject List only allows rejection of spam email messages, the Spam Filtering service allows discretionary When you enable spam filtering, you delegate control and management of spam filtering to the User Administrator. Emails that originate from the Blocked Senders List (created by the User Administrator) are identified as spam. The spam email is accepted by the mail server and relayed to the site. Depending on the spam management options set by the User Administrator, the spam may be deleted, delivered as an attachment, or quarantined in a spam folder..

Advantages

- Spam management using the **Spam Filtering** service allows delegated management and flexibility in controlling spam. The User Administrator can review the email messages and choose to delete spam email 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.

Viewing Your Mail Server Settings

The control panel provides default configuration settings for your mail server.

➢ ***To view your email settings:***

1 In the shortcuts section of the Home page, click **Configuration** (**Email** section).

2 The **Configuration** form opens displaying the current settings. The fields in this form include:

- **Maximum Message Size -** the maximum number of bytes an email message can contain
- **Relay Domains -** the names or IP addresses of the domains that can use this server as their email server
- **Relay Status** - indicates whether the control panel server will authenticate the email source before enabling further relay

Changing Your Mail Server Settings

The control panel provides default configuration settings for the email server. You can change these settings to suit the needs of outgoing and incoming mail on your domain.

➢ ***To change your email settings:***

1 In the shortcuts section of the Home page , click **Configuration** (**Email** section).

2 In the **Configuration** form, click **Edit**. The **Edit Configuration** form opens showing the current SMTP email settings.

3 In the **Maximum Message Size** field, enter the maximum number of bytes an email message can contain.

Note: If you do not want to impose a limit on the message size, leave this field blank.

4 In the **Relay Domains** field, enter the names or IP addresses of the domains that can use this server as their SMTP mail server.

5 Depending on whether or not you want the control panel server to authenticate the email source before enabling further relay, select the appropriate **Relay Status** check box.

6 Click **Update**.

Sending Email Notifications to Reseller Administrators and Site Administrators

You can send email notifications to Reseller Administrators and Site Administrators when you perform any task or activity that affect reseller or site administration. For example, you can send an email notification when you perform backup or restore operations on a site or when a site is inaccessible.

➢ ***To send email notifications:***

1 In the shortcuts section of the Home page, click **Email Reseller/Site Administrators** (**Email** section).

2 In the **To** list, select from the following list of options. Use the CTRL key and the left mouse button to make multiple selections.

- **All Direct Customers**. Sends email notifications to Reseller Administrators and the Site Administrators of the sites created by you
- **All Resellers**. Sends email notifications to the Reseller Administrators
- **My Sites**. Sends email notifications to the Site Administrators of the sites created by you
- ***<reseller_name>***. Sends email notifications to the Reseller Administrator
- ***<site_name>***. Sends email notifications to the Site Administrator of the site

3 In the **Subject** field, enter the subject of the message.

4 In the **Message** field, type the email message.

5 Click **Send Email**.

Overview of Virus Scanning

Virus scanning is an email scanning service that scans incoming and outgoing email messages for viruses. The service plays a critical role in pre-emptying the proliferation of viruses and securing your network from related violations.

Important: You must enable the Mail Scanning service to avail of virus scanning capability.

The Virus Scanning service interfaces with the Mail Scanning service to integrate with the mail server and extend its virus scanning capabilities to incoming and outgoing email messages. When an email scan request is received by the control panel server, preliminary scanning is performed by the Mail Scanning service which then passes the scan request to the Virus Scanning service. The service scans email messages and attachments for patterns or characteristics (finger-prints) indicative of a virus before the email message is delivered to the mail server. If the email message is infected, it can be deleted, quarantined, or cleaned and delivered to the mail server.

The control panel leverages the services of the virus scanning application **Clam AntiVirus** to scan email messages for viruses. For detailed information on Clam AntiVirus, please visit http://clamav.elektrapro.com/.

Configuring Email Clients

In this section:

Configuring Microsoft Outlook Express

Note: The instructions for setting up and accessing a Microsoft Outlook or Microsoft Outlook Express mailbox are provided as separate Help topics in the Site Administrator and User Administrator online Help. However, if your customers request for related help, you may use the instructions provided here to help them set up their mailboxes using these clients.

When you configure the Microsoft Outlook Express 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 a mailbox using Microsoft Outlook Express and the SMTP server configuration required to authenticate the connection.

➢ ***To set up a mailbox using Microsoft Outlook Express:***

1 Start Outlook Express by clicking on the **Microsoft Outlook Express** icon on the desktop.

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:

a Start Microsoft Outlook Express by clicking on the **Microsoft Outlook Express** icon on your desktop.

b From the menu bar, choose **Tools > Accounts**.

c In the dialog box, click **Add**.

d 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.

➢ ***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.

Configuring Microsoft Outlook

Note: The instructions for setting up and accessing a Microsoft Outlook or Microsoft Outlook Express mailbox are provided as separate Help topics in the Site Administrator and User Administrator online Help. However, if your customers request for related help, you may use the instructions provided here to help them set up their mailboxes using these clients.

When you configure the Microsoft Outlook 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 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.

5 Click **Next**.

6 Click **Set up Mail Account**. The **Mail Account Properties** window opens.

7 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.

8 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. This is the address other people use to send email messages to you.

9 Click the **Servers** tab.

10 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.

11 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.

12 In the **Outgoing Mail Server** area, select the **My server requires authentication** check box.

13 Click **Settings**. The **Outgoing Mail Server** window opens.

14 In the **Logon Information** area, if not already selected, select the **Use same settings as my incoming mail server** option.

15 Click **OK,** then Click **OK** again to return to the Microsoft Outlook Setup Wizard.

16 Click **Next**.

17 Click **Next** again.

18 Click **Finish**.

Your account is ready to use.

Configuring the MySQL Server

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.

Note: The MySQL service is available only if you have installed MySQL as an add-on when you installed the control panel.

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:

- 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
- 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.
- Scalability
- Efficient in handling large databases. You can create databases with more than 50,000 tables.

If MySQL is available to you, you can:

- Connect to the phpMyAdmin MySQL interface to manage your SQL databases (on page 100)
- Change your MySQL password (on page 101)

For more information about using the MySQL Administration Tool, see www.PHPWizard.net.

For more information about working with MySQL databases, see www.MySQL.com.

Enabling Multiple MySQL Databases

The control panel enables support for multiple MySQL databases per site. Multiple databases enable you to organize your site's data effectively and efficiently.

Enabling MySQL Databases for a site

You can enable MySQL database support for a site at the time of creating the site.

How to enable MySQL for a site

Note: The MySQL databases are backed up when you back up the site.

When you enable MySQL, you must provide the following information:

- **Database Administrator.** Name of the Database Administrator for the site. The Database Administrator has complete administrative access and control privileges on the site's databases.

  Note: The Administrator of the site cannot change the Database Administrator assigned to the site.

- **Number of Databases.** Number of databases the Administrator of the site can create for the site

  Important: The control panel does not implicitly spawn a database when a site is created. Setting the limit to '**0**', enables the administrator to create unlimited databases for the site.
  Also, the disk space used by a site's MySQL databases consume available disk quota.

- **Database Prefix.** The prefix name for the site's databases. The prefix ensures that the database names are unique and do not conflict with any existing database. By default, the name of the site is used as the database prefix.

  Important: Changing the prefix changes the database name across all the databases of the site, causing your site databases to be inaccessible. Once you set the prefix for a database, it is strongly recommended that you do not change the prefix.
  If you change the prefix, you must replace the obsolete name references with the new name of the database.

Connecting to MySQL Databases in a Secure Environment

The security level (on page 114) 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 a 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.

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 (on page 98)
- Connecting to a MySQL database on a medium security site (on page 98)
- Connecting to a MySQL database on a low security site (on page 98)

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 using the command line or in your Web scripts, 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 in 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 "localhost" 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

Connecting to the phpMyAdmin MySQL Interface

If MySQL is available to you, you can connect to the phpMyAdmin MySQL tool to work with your SQL databases.

Your MySQL user name is **root**. You cannot change this user name.

Note: You must specify a MySQL password (on page 101) before you can successfully connect to the phpMyAdmin MySQL Administration Tool interface.

➢ ***To connect to the phpMyAdmin MySQL interface (if available):***

1. Specify a MySQL password. (on page 101)
2. In the shortcuts section of the Home page, click **MySQL** (**Web Server/Databases** section). The MySQL window opens and displays information about, and links to, the **MySQL Administration Tool**.
3. Click **MySQL Administration Tool.** A new window opens, and you are prompted for your MySQL user name and password.

Changing your MySQL Password

If MySQL is available to you, you can change your MySQL password at any time.

Note: You must specify a MySQL password before you can successfully connect to the MySQL Administration Tool (on page 100) interface.

➢ ***To change your MySQL password:***

1. In the shortcuts section of the Home page , click **MySQL** (**Web Server/Databases** section).
2. Click **Change Password**. The **Change MySQL Password** form opens.
3. In the **New Password** field, enter the new password.
4. In the **Retype New Password** field, type the password again to confirm it.
5. **Optional:** Select the **Force Password Change** check box only if you are unable to connect to MySQL and receive an "**Access Denied**" error while attempting to:
   - change the MySQL password
   - create/modify/enable/disable a site

   Note: When you select Force Password change the control panel automatically restarts MySQL.

1 Click **Save**.

Starting and Stopping Services

In this section:

Starting Services

Not all services are startable. If you do not see a next to the service you want to start, you cannot start this service through the control panel.

➢ ***To start a service:***

1 On the left navigation bar, click **Services**. The **Subscribed Services** form opens displaying a list of services.

2 In the **Subscribed Services** form, locate the service you want to start, and in the **Actions** column, click .

Stopping Services

Not all services are stoppable. If you do not see a next to the service you want to stop, you cannot stop this service through the control panel.

➢ ***To stop a service:***

1 On the left navigation bar, click **Services**. The **Subscribed Services** form opens displaying a list of services.

2 In the **Subscribed Services** form, locate the service you want to stop, and in the **Actions** column, click .

Restarting Services

Not all server applications are restartable. If you do not see a next to the server application you want to restart, you cannot restart this application through the control panel.

➢ ***To restart a server application:***

1 On the left navigation bar, click **Services**. The **Subscribed Services** form opens displaying a list of server applications.

2 In the **Subscribed Services** form, locate the server application you want to restart, and in the **Actions** column, click .

CHAPTER 7

Using AnnounceIt!

In this chapter:

Overview of AnnounceIt!

AnnounceIt! is a control panel message board that you and your resellers can use to publish messages to your customers. You can use AnnounceIt! to promote or announce new offerings to your customers and notify them of upgrades or maintenance activities that may affect their business operations.

You can publish messages to the reseller accounts and sites that you create. However, you cannot send messages or notifications to sites created by any of your resellers.

By default, AnnounceIt! displays notifications from Parallels Pro (on page 104). These notifications are not sent to your resellers. You can choose to receive or block these messages.

Parallels Pro Control Panel notifications

Parallels Pro uses AnnounceIt! to notify you of critical business updates. You can choose to receive or block these messages by updating (on page 107) the default settings.

- License messages
- The following license messages are displayed:
  - **Grace period**. The following message is displayed: `Parallels Pro has been unable to contact the License Server and is currently in grace period. Ensure that you are connected to the network and that your firewall configuration is not blocking access to the License Server.`
  - **Unable to contact License Server during the last attempt**. The following message is displayed: `Parallels Pro was unable to contact the License Server during the last attempt. Ensure that you are connected to the network and that your firewall configuration is not blocking access to the License Server.`
- Miscellaneous news/updates/announcements
- Messages regarding release of hotfixes, service updates, and other product announcements pertinent to you and your customers are displayed.

Using AnnounceIt!, you can:

- View the list of messages (on page 105)
- Add messages (on page 106)
- Update messages (on page 107)
- Update AnnounceIt! settings (on page 107)
- Delete messages (on page 107)

Viewing the List of AnnounceIt! Messages

You can view the list of messages on the **AnnounceIt!** message board on the home page of the control panel or by clicking **AnnounceIt!** (**Configuration** section) in the shortcuts section of the Home page. The list of messages are displayed.

AnnounceIt! displays the title of the messages. To view the message, click the message title.

➢ ***To view messages:***

1. In the shortcuts section of the Home page, click **AnnounceIt!** (**Configuration** section).
2. The **Message List** section displays the list of messages.

Note: AnnounceIt! displays a maximum of **5** messages on the message board.

Using AnnounceIt!, you can:

- Add messages (on page 106)
- Update messages (on page 107)
- Update AnnounceIt! settings (on page 107)
- Delete messages (on page 107)

Adding AnnounceIt! Messages

The messages you add are published immediately to the control panel message board of your customer. The messages are displayed whenever your resellers or Site Administrators log into the control panel.

Note: AnnounceIt! displays a maximum of **5** messages on the message board. If you have reached the message limit, you will be unable to add messages. To add a message, update or remove an existing message.

➢ ***To add messages:***

1 In the shortcuts section of the Home page, click **AnnounceIt!** (**Configuration** section).

2 In the **Message List** section, click **Add Message**.

3 In the **Message Title** field, enter the message title. Ensure that the message title does not exceed **256** characters.

4 In the **Intended Audience** field, click the arrow and select the audience you want to send the message to. Select one of the following:

- **Reseller Administrators.** The message is sent to all the Reseller Administrators.
- **Site Administrators.** The message is sent to the Site Administrators of the sites you created.

5 In the **Message Format** field, click the arrow and select one of the following options:

- **XHTML**. Select XHTML if you want to format the message using custom colors and custom character/paragraph formats. You must use appropriate XHTML tags to display text in the this format.
- **Text.** Select Text if you want to display the message in plain text without any formatting.

6 In the **Message** field, enter the message you want to publish. Ensure that the message size does not exceed **15** KB (kilobytes).

- **Text.** If you have chosen **Text** in the **Message Format** field, type the message in plain text.
- **XHTML**. If you have chosen **XHTML** in the **Message Format** field, type the message using XHTML tags. For example, if you want to display the message **This is a sample message** in bold, type the following:

```
<html>
<body>
This is a <b>Sample Message</b>.
</body>
</html>
```

Note: If you type the XHTML message in plain text, you will receive an error.

7 Click **Publish**.

Setting AnnounceIt! Preferences

By default, AnnounceIt! is configured to display announcements from Parallels Pro. You can choose to receive or block these messages by setting your own preferences.

➢ ***To set your preferences:***

1 In the shortcuts section of the Home page , click **AnnounceIt!** (**Configuration** section).

2 In the **Parallels Pro Announcement Settings** section, update the settings as required.

3 To receive messages from Parallels Pro, clear the check box **Ignore announcements from Parallels Pro**.

4 To block messages from Parallels Pro, select the check box **Ignore announcements from Parallels Pro**.

5 Click **Update**.

Updating AnnounceIt! Messages

➢ ***To update messages:***

1 In the shortcuts section of the Home page, click **AnnounceIt!** (**Configuration** section).

2 In the **Actions** column of the message you want to update, click .

3 Update the message as required.

4 Click **Update**.

Deleting AnnounceIt! Messages

➢ ***To delete messages:***

1 In the shortcuts section of the Home page, click **AnnounceIt!** (**Configuration** section).

2 In the **Actions** column of the message you want to delete, click .

3 In the confirmation window, click **OK**. The message is removed from the list of messages.

C H A P T E R 8

Using Crob Job Manager

In this chapter:

Overview of Cron Job Manager

Cron Job Manager is an application that allows you to create Cron Jobs, which is an automated process that operates at specified time intervals. It allows you to create commands on your server that completes the scheduled tasks automatically at intervals set by the Cron Job.

For example, you could set a Cron Job to periodically take a backup of your postgres database.

Using the Cron Job Manager, you can:

- View the list of Cron Jobs (on page 109)
- Add a Cron Job (on page 110)
- Enable a Cron Job (on page 109)
- Disable a Cron Job (on page 110)
- Update Cron Job settings (on page 111)
- Delete a Cron Job (on page 111)
- Emailing Cron Job reports (on page 112)

View the List of Cron Jobs

You can view the list of Cron Jobs on the home page of the control panel or by clicking **Cron Job Manager** (**Tools** section) in the shortcuts section of the Home page. The list of Cron Jobs is displayed.

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

- **Command**: The command used to define the Cron Job.
- **Frequency**: The frequency at which the Cron Job will run.
- **Status**:The status of the Cron Job. Whether the Cron Job is enabled or disabled.
- **Actions**: Links to tasks you can perform. These change, depending on which tasks are available.

Using the Cron Job Manager, you can:

- Add a Cron Job (on page 110)
- Enable a Cron Job (on page 109)
- Disable a Cron Job (on page 110)
- Update Cron Job settings (on page 111)
- Delete a Cron Job (on page 111)
- Emailing Cron Job reports (on page 112)

Enabling Cron Job

You can enable a Cron Job that is currently in the disabled status.

➢ ***To enable a Cron Job:***

1. In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section), the **Cron Job List** page is displayed.
2. On this page, select the icon to enable a Cron Job that is in disabled status. This enables the Cron Job and will run as per the schedule, which was defined previously.

Adding Cron Jobs

➢ ***To add a Cron Job:***

1. In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section). The **Cron Job List** form opens.
2. Click **Add Cron Job**.
3. On the **Add Cron Job** page, provide the following information:
   - In the **Command** field, enter a command.
     For example, the command `rm -f /tmp/xyz`, this command deletes the `xyz` file from the `/tmp` directory.
   - In the **Description** field, enter a brief description.
   - In the **Schedule** field, select the frequency at which you want to run the Cron Job. You can select the **Simple** or **Advanced** schedule for the Cron Job.
     - **Simple**: If you select this option, you can schedule to run the Cron Job hourly, daily, weekly, monthly, yearly, or at the time of reboot.
     - **Advanced**: If you select this option, you can select from the advanced options displayed in the panel.
     - In the **Minutes** list select a number between 0 and 59.
     - In the **Hours** list select a number between 0 and 23.
     - In the **Days** list select a day between 0 and 31.
     - In the **Months** list select the month.
     - In the **Weekdays** list select a day between Sunday and Saturday.
4. Click **Add Cron Job**, to create the Cron Job.
5. Click **Reset** to undo the changes and restore the default values.

Disabling Cron Job

You can disable a Cron Job to prevent it from running.

➢ ***To disable a Cron Job:***

1. In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section), the **Cron Job List** page is displayed.
2. On this page, select the icon to disable the Cron Job that is in enabled status. Selecting this option disables the Cron Job.

Updating Cron Job settings

➢ ***To update an existing Cron Job:***

1 In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section), the **Cron Job List** page is displayed.

2 On this page, select the icon to edit an existing Cron Job.

a The Cron Job details form opens. On this page provide the following information:

- In the **Command** field, edit the command.
- In the **Description** field, edit the description.
- In the **Schedule** field, select the frequency at which you want to run the Cron Job. You can select the **Simple** or **Advanced** schedule for the Cron Job.
  - **Simple**: If you select this option, you can schedule to run the Cron Job hourly, daily, weekly, monthly, yearly, or at the time of reboot.
  - **Advanced**: If you select this option, you can select from the advanced options displayed in the panel.
  - In the **Minutes** list select a number between 0 and 59.
  - In the **Hours** list select a number between 0 and 23.
  - In the **Days** list select a date between 0 and 31.
  - In the **Months** list select the month.
  - In the **Weekdays** list select a day between Sunday and Saturday.

3 Click **Update Cron Job**, to save the changes.

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

Deleting Cron Job

➢ ***To delete a Cron Job:***

1 In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section), the **Cron Job List** page is displayed.

2 On this page, select the icon to delete an existing Cron Job.

3 In the confirmation window, click **OK**. The Cron Job is removed from the list.

Emailing Cron Job Reports

The success or failure report of the Cron Job is sent to the email address you specify in the **MAILTO** field.

➢ ***To email the report:***

1. In the shortcuts section on the Home page, click **Cron Job Manager** (**Tools** section), the **Cron Job list** page is displayed. Click **Set MAILTO**.
2. The **Set MAILTO** form opens.
3. In the **MAILTO field**, specify the email address to which the report must be sent. You can add multiple recipients by providing a **comma** separated list of email address in this field.

CHAPTER 9

Managing Sites

In this chapter:

Using the Site Manager

You use the Site Manager to view and manage your sites and Service Plans.

From the Site Manager, you can:

- View and manage your existing sites (on page 138)
- Add additional IP-based (on page 135) or name-based (on page 134) sites
- Remove sites (on page 140)
- View existing Service Plans (on page 131)
- Create additional Service Plans (on page 132)
- Update an existing Service Plan (on page 132)
- Remove Service Plans (on page 133)

Overview of Site Security Levels

When multiple sites are hosted on a single server, sharing system resources, there is a high possibility of sabotage or inadvertent activity that may compromise the integrity of data. You can check misuse or malevolent activity by setting appropriate security features for each site when you create the site.

Depending on the security level chosen, 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 prohibits the resources of the secured site from unauthorized access; also, the administrator and users of the secured site cannot access data or resources pertaining to other sites on the server.

The control panel offers three security levels:

- High security
- Medium security
- Low security

High security

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

This security level is recommended if you provide a shared hosting environment and want to ensure a secure environment for sites that enable CGI scripting capability and remote access services.

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 uses the chroot mechanism to place CGI scripts inside the restrictive part of the site's file system.

Important: High security poses problems if the CGI scripts for a 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 site's file system.

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 jails remote user logins (administrator and users of the site) to the restrictive environment of their home directories. Administrators and users of the site are logged into their respective home directories, 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, so that users cannot run scripts using these modules 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 security 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 security or low security.

Medium security

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

Note: This security level preserves the settings of existing sites and allows CGI scripts to run without any modification.

- CGI scripts (on page 114)
- Telnet/Secure Shell (on page 114)
- mod_perl/mod_php (on page 114)

CGI scripts

CGI scripts are not jailed 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, allowing users to run these scripts on the site.

Low security

Low security enables all files residing on the server to be shared or accessed (depending on file access privileges) by the administrator of the site. Users, however, are always restricted to the home directory of the site.

This security level is recommended only for trusted user environments, as it allows remote access services and CGI scripts access to the whole server, including other user's data on the server. This security level is not recommended for shared hosting environments.

Important: Since low security provides an open operating environment, the administrator name must be unique across all the sites hosted on the server.

The 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 server on which the site is hosted and then log in with the user name ***<user_name>***`@`***<site_name>*** to the server.

---

mod_perl / mod_php

mod_perl and mod_php services are enabled for the site and can be used to run mod_perl and mod_php scripts on the site.

Service Plan Options

This topic explains options for service plans. You choose these options when you add or modify a service plan (on page 128) or site (on page 113).

Service plan options include:

Site information section

Option	Description and settings
Security Level	The security level assigned to a site establishes the operating environment of the site. Depending on the security requirements of the site, select one of the following options: ▪ High ▪ Medium ▪ Low
IP-Based Hosting (Service Plan field only)	Click this option if you are creating a Service Plan template for IP-based sites.
Name- Based Hosting (Service Plan field only)	Click this option if you are creating a Service Plan template for name-based sites.

DNS section

Option	Description and settings
Add to DNS	If you want to add an entry to the DNS server provided by the control panel, select the check box; otherwise, leave it blank.
Enable Zone Management	If you want to enable zone management capability for the reseller (if you assign the site to a reseller) or the Site Administrator, select the check box; otherwise, leave it blank.

Enable DNS Logging	If you want Parallels Pro to maintain a record of all the DNS-related events, select the check box; otherwise, leave it blank.
Master	Enter the fully qualified domain name of the server you want to designate as the primary (Master) DNS server.
Slaves (one per line)	Enter the fully qualified domain name of the server you want to designate as the secondary (Slave) DNS server. You can specify multiple slave servers, one entry per line.

Aliases section

Option	Description and settings
Domain Aliasing	If you want to allow other domain suffixes to map to this domain, select the check box; otherwise, leave it blank. In the text box, enter the specific domain suffixes you want to map to the domain, for example, `.net` or `.org`. Enter only one suffix per line. **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.
Aliases (one per line)	In the text box, enter the specific domain suffixes you want to map to the domain, for example, `.net` or `.org`. Enter only one suffix per line. **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.

Monitoring section

Option	Description and settings
Threshold (MB)	Enter the upper limit of network traffic (greater than 0), in Megabytes, that the site is allowed to have per month. **Note:** You will get a daily email message summarizing the sites that are over their bandwidth limit. If no sites are over the limit that day, you will not receive an email message.

Cycle Start	Specify the day of the month the bandwidth threshold monitor resets and begins a new monitoring session. Click the arrow and from the list, choose a number between **1** and **28**. For example, if you want the monitoring to start on the 10^{th} of each month, choose 10.
Analog Web/FTP Log Analyzer	If you want to provide your customers with analysis reports of Web and FTP server use, select the check box; otherwise, leave it blank. **Note:** If you enable this option, you must also enable the **Generate Web Logs** option.
Webalizer Log Analyzer	If you want to provide your customers with graphical log analysis reports of Web and FTP servers usage, select the check box; otherwise, leave it blank. **Note:** If you enable this option, you must also enable the **Generate Web Logs** option.
AWStats Log Analyzer	If you want to provide your customers with graphical log analysis reports of Web and FTP servers usage, select the check box; otherwise, leave it blank. **Note:** If you enable this option, you must also enable the **Generate Web Logs** option.

System Limits section

Option	**Description and settings**
Disk Quota	If you want to set a specific amount of disk space that can be assigned to a site, select the check box; otherwise, leave it blank. **Note:** You cannot set the disk quota for NFS servers. Leave this check box blank for sites on NFS servers.
Allocated Disk Quota (MB)	Enter the numerical amount (in MB) you want to assign.

User Quota	User quota defines the number of users that can be created for the site. ▪ To allow unlimited number of users: Do not select the **User Quota** checkbox; Leave the **Max Users** field empty. ▪ To allow limited number of users: Select the **User Quota** checkbox; Enter the maximum number of users in the **Max Users** field.
Maximum Number of Users	Enter the maximum number of users, for example, **25**, that you want to create for the site.

Web Server section

Option	Description and settings
Apache Web Server	If you want to provide Web server support to your customers, select the check box; otherwise, leave it blank.
Web Server Name	Enter the domain name prefix, for example "`www.`". If you do not specify a prefix, a DNS record will not be created for that domain name.
CGI	If you want to allow your customers to run CGI scripts on their Web servers, select the check box; otherwise, leave it blank. **Note:** Be aware that CGI scripts generate processes that can use extensive server resources.
Script Alias	Specify the directory in which you will store CGI scripts created for the site. The default directory is **cgi-bin**. If you are unsure of what to enter in this field, retain the default.
Secure Web (SSL) (for IP- based sites only)	If you want to provide your customers with secure Web pages, select the check box; otherwise, leave it blank. **Note:** **1.** Secure Web (SSL) is only available to IP-based sites. **2.** SSL encryption will slow down page browsing on the Web site. **3.** The customer must obtain a SSL certificate from a certifying authority. He is also provided with a self signed certificate, which is valid as any other certificate, however this may result in warning messages being displayed on the server.
Server Side Includes	If you want to allow your customers to create .shtml Web pages, select the check box; otherwise, leave it blank.

Mod_perl for Apache	If you want to allow your customers to use Mod_perl for Apache, select the check box; otherwise, leave it blank.
FrontPage Server Extensions	If you want to support customers who want to use Microsoft FrontPage to manage their Web site, select the check box; otherwise, leave it blank. **Note:** Microsoft FrontPage has its own protected directory feature. If you select the FrontPage option, your users cannot use the directory protection provided by the control panel. Your users can protect their directories through FrontPage instead. For information on this FrontPage feature, see the Microsoft FrontPage user guides. You can either enable FrontPage Server Extensions or WebDAV server for the users. If you enable FrontPage Server Extensions, the WebDAV server will be automatically unavailable to the users.
WebDAV Server	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. You can either enable WebDAV server or FrontPage Server Extensions for the users. If you enable the WebDAV server, FrontPage Server Extensions will be automatically unavailable to the users.
Alias	The default directory alias is `/perl/`.
Generate Web Logs	If you want to provide statistics about Web site traffic for the CustomLog (on page 41) report, and provide error information for the ErrorLog (on page 41) report, select the check box; otherwise, leave it blank. If you have enabled the **Analog Web/FTP Log Analyzer** option, you must also enable this option. The Generate Web Logs application provides the statistics used for the Analog Web/FTP Log Analyzer reports.
Tomcat 4	If you want to provide Tomcat 4 support to the site, select the check box; otherwise, leave it blank. **Note:** Tomcat 4 provides capabilities for running Java servlets/Java Server Pages (JSP) on the Web server.

Subdomains section

Option	Description and settings
Subdomain Interface	Select the check box to enable Site Administrators with access to the subdomain interface for creating and managing subdomains.
Maximum Subdomains	Enter the maximum number of subdomains that can be created for the site.
Base Directory	The base directory indicates the location in the site's file system where all the regular subdomains for the site can be located. Enter the complete path to the base directory. By default, they will be located under */var/www*.

E-Commerce section

Miva Merchant	If you want to allow your customers to create e-commerce storefronts using Miva Merchant, select the check box; otherwise, leave it blank.

File Management section

Option	Description and settings
File Manager	If you want to allow your customers to access, create, and remove files and directories on the site, select the check box; otherwise, leave it blank.
Export/Import	If you want to allow your customers to backup and restore data or configuration files, select the check box; otherwise, leave it blank.

Mail Access Protocol section

Option	Description and settings
POP3+IMAP Server	If you want to provide your email users access to their email from remote mail clients, select the check box; otherwise, leave it blank.

Mail section

Option	Description and settings

Email	If you want to allow your customers to send and receive email messages from the mail server on the site, select the check box; otherwise, leave it blank.
Mail Server Name	Enter the prefix you want to use, for example, "`mail.`".
Mailing List (Majordomo)	If you want to allow your email users to create mailing lists, select the check box; otherwise, leave it blank.
Vacation Auto-Responder	If you want to allow your email users to create vacation messages to automatically respond to incoming email messages, select the check box; otherwise, leave it blank. **Note:** If you select this option, and later temporarily remove it from the site then add it back to the site, you must notify your users to reactivate this feature. When you remove this feature from the site, Vacation Auto-Responder automatically resets the option to **Off** for any user account currently using the feature. Users will not be able to use this feature until they manually set it to **On** again.
Spam Filtering	If you want to allow your email users to manage spam, select the check box; otherwise, leave it blank.

Web-based Email Access section

Option	Description and settings
SquirrelMail Web-based Email	If you want to provide your customers access to their email messages over the Web, select the check box; otherwise, leave it blank.

Mail Scanner

MailScanner/Virus Scanner	If you want to enable email scanning for the site, select the check box; otherwise, leave it blank. **Note:** When you enable MailScanner, you automatically enable virus scanning for email messages delivered to the site.
Scan Incoming mail	If you want to allow only incoming email messages to be scanned, select the check box, otherwise leave it blank.
Scan Outgoing mail	If you want to allow only outgoing email messages to be scanned, select the check box, otherwise leave it blank.

Remote Login and Tools section

Option	Description and settings
Development Tools	If you want the virtual domain shell of your customers to have access to development tools like GCC or G++ compilers, select the check box; otherwise, leave it blank.
OpenSSH Secure Shell	If you want to allow your customers to log on and access the site using an SSH connection, select the check box; otherwise, leave it blank.
Telnet	If you want to allow your customers to log on and access the site using a Telnet connection, select the check box; otherwise, leave it blank. The maximum number of Telnet domains supported on one server is **250**.

File Transfer section

Option	Description and settings
FTP	If you want to allow your customers to transfer files to and from the site using an FTP connection, select the check box; otherwise, leave it blank. **Note**: Name-based sites support FTP file transfers at the Site Administrator level only. Other users can upload files to the site using the File Manager upload feature.
FTP Server Name	Enter the prefix you want to use, for example, "`ftp.`".
Anonymous FTP	If you want to allow anonymous users to access the FTP server without a password, select the check box; otherwise, leave it blank.

Database Server section

Option	Description and settings

MySQL	If you want to allow your customers to manage their SQL databases through MySQL, select the check box; otherwise, leave it blank. Do not configure the rest of the options in the **Database Server** section if you do not enable MySQL. **Note**: Enabling MySQL will also enable the MySQL set of command line tools for database management.
Database Administrator	The Database Administrator exercises administrative control over all the databases of the site. Enter the user name of the Database Administrator. *Note: By default, the site name is used as the database in this field*. The name should not exceed **16** characters. **Note**: If you leave this field blank, the default user name is the same name as you entered in the Administrator User Name field.
Number of Databases	Enter the maximum number of databases permissible for the site. **Important**: The value **0** enables the Site Administrator to create unlimited number of databases for the site.
Database Prefix	Enter a prefix for the database. The prefix is necessary to ensure that the database is unique to the site and can have a maximum of 30 characters. By default, the site name is used as the database prefix. If the name of the site exceeds **30** characters then the database prefix is truncated to 30 characters. **Prefix caveat** The prefix name, once set, must not be changed, as this will change the name of all the databases across the site. As a result of this, your site databases will be inaccessible. ➢ ***To restore connection to the database, do one of the following:*** **1** Revert to the original prefix. **2** Change the code references in your site pages so that they refer to the new prefix.

Reseller section

Option	Description and settings
Reseller	Select the reseller for whom you want to create sites using the service plan template. You must select the **Reseller Interface** check box before you select the reseller. **Note**: When you create a site using this Service Plan, the site will, by default, be owned by the reseller. The Service Plan template you create for resellers does not limit them in any way from defining their own Service Plan configurations.

Power Tools section

Option	Description and settings
Enable Power Tools	To enable Power Tools for a site, select the check box next to Power Tools. To allow Site Administrators to install individual tools, select the check boxes that appear next the tools. To prevent Site Administrators from installing individual tools, disable tools by clearing their check boxes. To disable Power Tools for a site, clear the check box next to Power Tools. If this check box is cleared, Power Tools is disabled even if individual tools are selected.

Working with Service Plans

In this section:

Using Service Plans to Create Sites

The control panel provides the tools to quickly and easily define and deploy Service Plans. Service Plans represent a bundle of services and resources, such as disk space, that you can sell to resellers and site owners. Based on the specific service plan configurations you choose, the control panel will deploy the necessary services and enforce the limits you have chosen for the site when you create it.

If you intend to create multiple sites, before creating the sites, you might want to first create Service Plan templates (on page 132). Each template can include different configurations that satisfy different business requirements. You can create as many Service Plan templates as you want. You can also set one of the Service Plan templates as the default plan used for new sites.

Note: These templates are not required to create a site; however, they can make creating multiple sites easier and faster.

Even if you create a site with a Service Plan, you can later modify the Service Plan for that specific site to customize it for your customer's requirements.

Before you define a Service Plan, it would be helpful to understand your customers' requirements and see what competitors are offering. You will want to put together an offer that is compelling to your target customers. There are a number of features that your customers will consider required, such as disk space and bandwidth. You also have the opportunity to differentiate your Service Plans by adding additional services.

If you are using the server primarily to host internal sites, defining Service Plans can ensure you allocate resources appropriately, as well as delegate appropriate control to your internal customers.

You can create Service Plans using the Sites Manager (on page 113).

Examples of Service Plans

Service Plans can be simple or complex, depending on the category they fall under: consumer, business, or reseller. Reseller Service Plans enable many Web sites to be hosted under one account, so you can set up Web site accounts and sell them to clients at any price you want. You then use your control panel to create, manage, and remove these hosting accounts.

Business Service Plans

Listed below (in order of complexity) are some examples of business Service Plans.

- GOLD
    - Account features
        - 125 MB of Web space
        - 25 email accounts
        - Unmetered bandwidth, meaning site owners will not be billed for usage

        - Dedicated IP address
    - Target customer
        - Anyone who is just starting out on the Internet
        - Anyone who does not need database or multimedia features
        - Any small business looking to launch its first Web site
        - Any family or individual wanting to display their Web site
- PLATINUM
    - Account features
        - 300 MB of Web space
        - 100 email accounts
        - Unmeasured bandwidth, meaning site owners will not be billed for usage
        - Dedicated IP address&emdash;one MySQL database
        - Database access
        - Multiple scripting language support (PHP4, SSI, Python, Perl, JSP&emdash;pre-built CGI script support
    - Target customer
        - Anyone who has a large personal or business Web site requiring a lot of Web space
        - Anyone who needs a site with MySQL, media streaming, and/or SSL support
        - Anyone who needs the reassurance that they will not quickly outgrow their hosting solution
- TITANIUM
    - Account features
        - 500 MB space
        - 200 email accounts
        - 10GB measured bandwidth
        - Manage multiple Web sites under one account&emdash;host 5 domains
        - PHP4, SSI, Python, Perl, JSP
        - MySQL database
    - Target customer
        - Anyone who has multiple Web sites they wish to host under one account
        - Anyone who needs a way to centrally manage multiple Web sites
        - Anyone who wants to consolidate existing Web hosting accounts into one low-cost option
- DIAMOND
    - Account features
        - 2 GB space
        - Unlimited email accounts

    - 20 GB measured bandwidth
    - Unlimited domains
    - PHP4, SSI, Python, Perl, JSP
    - ASP, Tomcat JSP
    - MySQL database
  - Target customer
    - Anyone who wants all the benefits of a dedicated server, but on a budget
    - Anyone with a large Web site that needs a maximum amount of storage
    - Anyone who runs resource demanding scripts

Reseller Service Plans

Listed below (in order of complexity) are some examples of reseller Service Plans.

- ECONOMY
  - 30 MB Disk Space
  - 750 MB Data/month
  - 2 Domains (e.g. www.name.com)
  - 10 POP3 Email Accounts
- PREMIUM
  - 250 MB disk space
  - 4500 MB data/month
  - 2 domains
  - 10 POP3 email accounts
- ECONOMY BULK
  - Unlimited domains
  - Unlimited POP3 email addresses
  - 500 MB disk space
  - 15000 MB monthly transfer
- PREMIUM BULK
  - Unlimited Web sites
  - Unlimited POP3 email addresses
  - 1500 MB disk space
  - 45000 MB monthly transfer

Viewing Existing Service Plans

You can view all of your existing Service Plan templates from the Sites Manager.

The Sites Manager displays the Service Plans in the Plan List.

➢ ***To view your existing Service Plans:***

1 In the shortcuts section of the Home page , click **List Plans** (**Sites** section). The Plan List window opens displaying the Service Plans.

The columns in this form include:

- **Plan Name -** The name of the **Service Plan** template.
- **Actions -** The column that allows you to add a site (on page 135) using the Service Plan, update (on page 132) an existing Service Plan, or remove (on page 133) the Service Plan.

Creating Service Plans

Before creating sites, you might want to create Service Plan (on page 128) templates. These templates are not required to create a site; however, they can make creating multiple sites easier and faster by establishing the services and utilities you want to assign to specific sites when you create them.

➢ ***To create a Service Plan template:***

1 In the shortcuts section of the Home page, click **Add Service Plan** (**Sites** section).

2 Use the Service Plan Options Information to help you complete the form.

3 In the **Save Plan** area, save the plan as a new template or overwrite an existing template. Do one of the following:

- To save the plan as a new plan, select the **Save as a new plan** option. In the adjacent text box, enter the name of the new plan.
- To update or overwrite an existing plan, select the **Save as an existing plan** option. From the list, click the arrow and choose a name.
- To save this plan as the default plan, click the arrow and choose **default**.

4 Click **Save**.

The control panel creates a Service Plan template using the data you supplied on this form. The name of this Service Plan template will appear in the Plan List form.

Updating Service Plans

➢ ***To update a Service Plan template:***

1 In the shortcuts section of the Home page , click **List Plans** (**Sites** section).

2 Locate the Service Plan you want to update and in the **Actions** column, click . The **Edit Service Plan** form opens.

Note: Use Reset if you want to enter new values for all the configurable options in the Service Plan.

1 Use the Service Plan Options Information to help you make changes to the form.

2 Click **Update Plan**.

Removing Service Plans

As your Service Plan needs change over time, you might prefer to retire some plans. Or, your customers might upgrade to more robust plans. For these and other reasons, you will want to remove a Service Plan.

➢ ***To remove a Service Plan:***

1 In the shortcuts section of the Home page, click **List Plans** (**Sites** section).

2 In the **Plan List** form, locate the plan you want to remove and in the Actions column, click .

Note: You cannot remove the Default Service Plan.

Creating New Sites

In this section:

Creating a Name-based Site

A site can be IP-based or name-based. IP-based sites have a unique IP address; name-based sites have a unique host name but share an IP address with the control panel server.

Name-based sites have certain limitations.

- Users do not have access to SSL secure domain certification
- A CNAME alias record cannot be entered into the DNS configuration.

Before you start, make sure you have all the required information to create a site.

➢ ***To create a name-based site:***

1 In the shortcuts section of the Home page, click **Add Name-based Site** (**Sites** section).

2 In the **Site Name** field, enter the name of the site you are creating.

Important: The site name must be the fully qualified name, containing both the host name and the domain name; do not include the www prefix. The total length of the database name (inclusive of the database prefix) should be less than 255 characters.

3 In the **Administrator User Name** field, enter a user name for the Site Administrator, the person who will manage this new site.

Important: You must not enter a user name starting with a number (such as ***123abc***). If you do, you will receive an error message and the site will fail to add.

4 In the **Administrator Password** field, enter the password for the Site Administrator.

5 Retype this password in the **Confirm Administrator Password** field.

6 In the **Email Contact** field, enter the email address of the Site Administrator.

7 Select an appropriate option in the **Security Level** field to set the security level (on page 114) for the site. (if available)

8 In the **Select a Service Plan** field (if available), do one of the following:

- If you want to use an existing Service Plan template (on page 128), click the arrow and from the list, choose the name of the template you want to use.
- If you do not want to use a Service Plan template, or if you want to manually assign the services available to this site, click **Advanced.**
- The **Add Name-based Site** form expands to display the **Service Plan** form that allows you to choose the service options you want to enable for the site.
- Use the Service Plan Options Information to help you complete the form.

9 Click **Add Site**.

The control panel creates the new name-based site and assigns a temporary, default home page for it. To view this temporary home page, go to: `http://`<your_site_name>.

Creating an IP-based Site

Before you start, make sure you have all the required information to create a site.

➢ ***To create an IP-based site:***

1 In the shortcuts section of the Home page, click **Add IP-based Site** (**Sites** section).

2 In the **Site Name** field, enter the name of the site.

Important: The site name must be the fully qualified name, containing both the host name and the domain name; do not include the www prefix. The total length of the database name (inclusive of the database prefix) should be less than 255 characters.

3 In the **Administrator User Name** field, enter a user name for the Site Administrator, the person who will manage this new site.

Important: You must not enter a user name starting with a number (such as ***123abc***). If you do, you will receive an error message and the site will fail to add.

4 In the **Administrator Password** field, enter a password for the Site Administrator.

5 Retype this password in the **Confirm Administrator Password** field.

6 In the **Email Contact** field, enter the email address of the Site Administrator.

7 Select an appropriate option button in the **Security Level** field to set the security level (on page 114) for the site. (if available)

8 In the **IP Address** field, enter the IP address you are assigning to the site.

9 In the **Select a Service Plan** field (if available), do one of the following:

- If you want to use an existing Service Plan template (on page 128), click the arrow and from the list, choose the name of the template you want to use.
- If you do not want to use a Service Plan template, or if you want to manually assign the services available to this site, click **Advanced.**
- The **Add IP-based Site** form expands to display the **Service Plan** form that allows you to choose the service options you want to enable for the site.
- Use the Service Plan Options Information to help you complete the form.

10 Click **Add Site**.

The control panel creates the new IP-based site and assigns a temporary, default home page for it. To view this temporary home page, go to: `http://`<your_site_name>.

➢ ***In case of the installation of Parallels Pro Control Panel from Parallels Virtuozzo Containers templates, after adding an IP-based site do the following:***

a When a Virtuozzo container uses the **host-routed network**, after adding an IP-based site the following command should be executed as root on **Virtuozzo Hardware Node**:

```
vzctl set N—ipadd IP –save
```

Where:

- ***N*** – Virtuozzo container identifier
- ***IP*** – IP address of the recently-added IP-based site.

b When **bridged network** is used no additional actions are necessary.

Previewing a New Domain

If your site is new, the DNS information for the site may not have had time to resolve; however, you can still preview the Web page content (on page 137) and CGI script functions (on page 137) of the site.

Note: Once the DNS information for your new site resolves, you can go directly to the actual site by entering the following URL in the **Address** field of your Internet browser: `http://`<site_name>`.com/`.

➢ ***To preview Web page content:***

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

http://<server *IP address*>/<*domain_name*>.com/

where:

<server IP address> is the control panel server's IP address

<domain_name> is the fully qualified name of the domain

➢ ***To preview the CGI scripts:***

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 control panel server's IP address

<domain_name> is the fully qualified name of the domain

<ScriptAlias> is the CGI script directory for the domain

Working with Existing Sites

In this section:

Viewing Site Information

You can view and manage your existing sites from the Sites Manager.

The Sites Manager displays your existing sites in the **Site List**.

➢ ***To view your existing sites:***

In the shortcuts section of the Home page, click **List Sites** (**Sites** section). The **List Sites** form opens displaying your existing site.

The columns in this form include:

- **Site** - The name of the site
- **Status** - The current status of the site
- **Type** - Whether the site is an IP-based site or a name-based site
- **IP Address** - The IP address of the site
- **Actions** - Allows you to perform the following actions on the site.

  - View the site’s bandwidth traffic reports (on page 146)

  - Update the site’s settings (on page 139)

  - Suspend or reactivate the site (on page 140)

  - Remove the site (on page 140)

From the **List Sites** form, you can also Connect to a specific site (on page 140).

Updating Site Settings

You can modify the settings of an existing site to switch between IP-based sites and name-based sites, assign a different Service Plan, toggle services, change the allocated disk space, or change the maximum number of email users.

Important: When you convert a name-based site to an IP-based site, you can offer the Secure Web (SSL) service that enables the Site Administrator to perform secure Web operations.

However, when you convert an IP-based site to a name-based site, the Secure Web (SSL) service is disabled preventing further secure Web operations on the site. If the site availed the service before the update, you must notify the Site Administrator of further unavailability of the service.

➢ ***To update your existing site settings:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to change and in the **Actions** column, click . The **Edit Site** form opens.

3 Use the Service Plan Options Information to help you make changes to the form.

> **Note:** Changing the name in the **Site Name** field does not automatically change the names of the other servers on the domain, such as the Web server or the mail server. If you change the name in the **Site Name** field, make sure the names of the other servers still apply.

4 Click **Update Site**.

Logging onto the Site Administrator Control Panel

Parallels Pro Control Panel Automatic login also called auto-login does not require you to know the Site Administrator's user name and password. You are automatically logged in using the Site Administrator's account information. you into the Site Administrator control panel when you click on a site name. Auto-login is especially useful if the Site Administrator has forgotten the login password, and requires you to access (on page 140) the Site Administrator control panel and reset the current password. As a Site Administrator you can also perform other administrative tasks. While you work as a Site Administrator, your preceding sessions remain active for a duration of 60 minutes. If no activity is noted during this period, the sessions expire. As you perform multiple roles, stacked login ensures that your multiple sessions remain easily accessible and functional.

Connecting to a Specific Site

➢ ***To connect to a specific site:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to connect to and in the **Sites** column, click the underlined name of the site, for example, click `store.acme.com`.

3 A confirmation window opens, informing you that you are automatically logging (on page 139) in as the Site Administrator for the specific site.

4 Click **OK**.

Suspending and Reactivating Sites

Suspending a site makes it unavailable for use but does not remove it from the server.

You can reactivate any site you suspend. To remove the site completely from the server, you must delete it (on page 140).

➢ ***To suspend a site:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to suspend and in the **Actions** column, click . A confirmation window opens.

3 Click **OK** to suspend the site.

It may take a few minutes for the system to complete the operation.

➢ ***To reactivate a site:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to reactivate and in the **Actions** column, click . A confirmation window opens.

3 Click **OK** to reactivate the site.

It may take a few minutes for the system to complete the operation.

Removing Sites

➢ ***To remove a site:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to remove and in the **Actions** column, click .

3 In the confirmation window, verify the site you are removing, then click **OK**.

Securing Sites Using SSL Certification

In this section:

About SSL Certification

If your site stores sensitive data, such as customer profiles, we recommend that you secure your site. To secure a site, you need a Secure Sockets Layer (SSL) certificate.

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.

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

Securing your site is a four-step process.

Step 1: Generating an SSL certificate request (on page 142)

Step 2: Sending the request to a Certificate Authority (CA) (on page 143)

Step 3: Loading the SSL certificate onto your domain (on page 143)

Step 4: Restarting the Web server (on page 144)

Generating an SSL Certificate Request

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

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

You are now ready to go to Step 2, sending the certificate request to a Certificate Authority (on page 143).

Requesting a Certificate from a Certificate Authority

You must generate a certificate request before you can send the request to a Certificate Authority.

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

1. Generate an SSL certificate request. (on page 142)
2. Copy the encrypted request onto your local system clipboard.
3. Open another Internet browser, and go to the Web site of the Certificate Authority you want to use, for example, VeriSign.
4. In the appropriate window of the Certificate Authority’s Web site, paste the encrypted certificate request and follow the Certificate Authority’s instructions for submitting it.
5. The Certificate Authority will send you an SSL certificate, usually through email.

After you receive the certificate from the Certificate Authority, go to step 3, uploading the certificate onto your domain (on page 143).

Uploading the Certificate on the Domain

After you receive the SSL Certificate, load the certificate onto your domain.

➢ ***To load the certificate:***

1. Generate the SSL certificate request and send the request to the Certificate Authority (on page 143).
   The Certificate Authority emails you the SSL certificate.
2. Open the email from the Certificate Authority, and copy the contents onto your local system into a text authoring utility, such as Notepad.
3. Once you have copied the contents into a text authoring utility, leave the utility open on your desktop.
4. Start the server and log on as the Server Administrator.
5. In the shortcuts section of the Home page, click **Import SSL Certificate** (**Web Server/Databases** section). The **Save SSL Certificate** window opens.
6. Copy the server certificate information from the text authoring utility and paste it into the **Server Certificate** text box.
7. 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 text authoring utility does not provide you the certificate.
8. Click **Import**.
9. To make security effective on your domain, restart the Web server. The domain is not secure until you do so.

Restarting the Web Server

Once you save the SSL certificate on your domain, you must restart the Web server on which the domain resides.

Restarting the Web server is a required step. Your domain is not secure until the Web server is restarted.

Viewing Bandwidth Usage Reports

In this section:

Overview of Bandwidth Usage Reports

Bandwidth usage reports are helpful for monitoring network traffic on a site. You can use the information from these reports to manage your plans and billing needs. You can view the bandwidth usage reports for resellers and sites without requiring to log in as a Reseller Administrator or a Site Administrator.

Bandwidth usage reports are updated every five minutes. The reports include cumulative network traffic statistics for the current monitoring session, which spans one month. You can specify the start day of the monitoring session for a site. You set the start day as part of the Service Plan options you select when you create the site.

Note: Bandwidth statistics may not be available for new sites for up to five minutes after the new sites are created. Also, you will not see statistics until there is traffic on the new sites. The information is updated every 2 hours.

Once per day, an email message is sent notifying you of sites that are over their assigned bandwidth usage limits. If no sites are over the limit that day, you will not receive a notification that day.

You can:

- View current site bandwidth usage report for resellers (on page 191)
- View past site bandwidth usage report for resellers (on page 191)
- View bandwidth usage reports for a specific reseller (on page 192)
- View current site bandwidth usage reports (on page 145)
- View past site bandwidth usage reports (on page 146)
- View bandwidth usage reports for a specific site (on page 146)

Viewing Site Bandwidth Usage Reports

In this section:

Viewing Current Site Bandwidth Usage

You can view bandwidth usage for all of your sites for the current monitoring session. The information shown includes all bandwidth usage from the start of the monitoring session to the current day. If the site is new, the information shown includes only statistics starting from the day the site was created to the current day.

Note: Bandwidth statistics may not be available for new sites for up to five minutes after the new sites are created. Also, you will not see statistics until there is traffic on the new site. The information is updated every 2 hours.

➢ ***To view current bandwidth usage reports:***

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

2 The **Usage Reports** page opens listing all the sites that have usage report statistics available.

The columns in this form include:

- **Site -** The name of the site. The site name is linked to a detailed statistical report on the site.
- **Bandwidth -** A bar graph showing how much bandwidth is used in comparison to how much is assigned to the site.
- **Status -** Indicates whether the service is enabled or disabled.
- **Used -** The number of megabytes of bandwidth already used by the site during the current one month period.
- **Quota-** The maximum number of megabytes of bandwidth assigned to the site for the current one month period.
- **Available-** The amount of megabytes difference between the number of bytes of bandwidth assigned to the site and the number of bytes of bandwidth already used.
- **% Used -** The Difference amount shown as a percentage.

You can also view current usage report for a particular site (on page 146).

Viewing Past Site Bandwidth Usage

Once the current monitoring session ends, information about bandwidth usage for the month is moved to the **Last Usage Reports** form. This form shows a summary of the amount of network traffic that occurred for all of your sites during the last monitoring session.

Note: Bandwidth statistics may not be available for new sites for up to five minutes after the new sites are created. Also, you will not see statistics until there is traffic on the new site. The information is updated every 2 hours.

➢ ***To view past site bandwidth usage reports:***

1. In the shortcuts section on the Home page, click **Bandwidth Usage** (**Reports** section).
2. The **Usage Reports** page opens listing all the sites that have usage report statistics available.
3. On the **Usage Reports** menu, click **Last Usage Reports**.

   The **Usage Reports** form opens listing sites and a summary of their bandwidth usage for the time-period selected. The columns in this form include:

   - **Site -** The name of the site.
   - **Bandwidth -** A bar graph showing how much bandwidth is used in comparison to how much is assigned to the site.
   - **Used -** The number of megabytes of bandwidth already used by the site during the current one month period.
   - **Status -** Indicates whether the service is enabled or disabled.
   - **Quota -** The maximum number of megabytes of bandwidth assigned to the site for the current one month period.
   - **Available -** The amount of megabytes difference between the number of bytes of bandwidth assigned to the site and the number of bytes of bandwidth already used.
   - **% Used -** The difference amount shown as a percentage.

You can view past usage report for a particular site (on page 146).

Viewing Bandwidth Usage Reports for a Specific Site

You can view detailed bandwidth usage for a specific site. The report, by default, shows bandwidth usage by all services, from the start of the monitoring session to the current day. You can also browse through past reports by selecting the time period (on page 146) for which you want to view the usage report. The time period is based on the bandwidth monitoring cycle defined for the site at the time of creating the site.

Note: Bandwidth statistics may not be available for new sites for up to five minutes after the new sites are created. Also, you will not see statistics until there is traffic on the new site. The information is updated every 2 hours.

➢ ***To view bandwidth usage details for a specific site:***

1 On the left navigation bar, click **Bandwidth Reports.** The **Usage Reports** form opens displaying all the sites that have usage report statistics available.

2 In the **Site** column, locate the site whose report you want to view, and click the underlined name of that site, for example, click **store.acme.com**.

The **Usage Report** form for that site opens. The upper section of the form shows the bandwidth usage for the entire site (on page 146). The lower section shows details of bandwidth usage by individual services (on page 146) on the site.

About entire site bandwidth usage statistics

The columns in this section include:

- **Bandwidth -** A bar graph showing how much bandwidth is used by the site.
- **Statistics last updated** - The date (in `yyyy/dd/mm` format) on which the bandwidth usage report was last updated.
- **Total Used Bandwidth -** The bandwidth (in megabytes) already used by the site for the selected month.
- **Allowed Quota -** The maximum bandwidth (in Megabytes) assigned to the site for the selected month.
- **Available Quota -** The amount of megabytes still available after finding the difference between the number of bytes of bandwidth assigned to the site and the number of bytes of bandwidth already used.

About individual services bandwidth usage statistics

The columns in this section include:

- **Service -** The name of the service using bandwidth on the site.
- **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.
- **POP** - 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 services distinct from any of the above-mentioned services, they are qualified as other services. For example, if you have configured a service, RSH, bandwidth consumed by traffic on this server will be classified under **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 the site.
- **Incoming -** The number of megabytes of Used bandwidth this service used for incoming network traffic.
- **Outgoing -** The number of megabytes of Used bandwidth this service used for outgoing network traffic.
- **Total -** The sum total number of megabytes of Used bandwidth this service used.
- **% of All -** The Total amount of bandwidth used by this service in comparison to other services, shown as a percentage.

Viewing past bandwidth usage reports

You can choose to view the bandwidth usage report for the site for a given time-period. The time-period is based on the bandwidth monitoring cycle defined for the site at the time of creating the site.

To view past reports, click the arrow in the **View Monthly Reports** list, and select the time period.

Enabling Log Analysis for Sites

In this section:

Introduction to Log Analysis

Every web 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

About 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. By default, Webalizer does not enable incremental processing.

Why do you need incremental processing

Log files grow to very large sizes, over a period of time. A relatively small web site that has several thousand visitors a month will have approximately 25 megabytes of log files. Processing large log files can thus be intensive on time and resources.

Incremental processing aids faster processing of log data by fragmenting large files into smaller data entities, without compromising on data. This is achieved by saving and restoring necessary information to a disk file (by default, webalizer.current, located in the output directory of the application), so that data between runs is preserved and log processing resumes without any loss of detail.

For example, when you run Webalizer, it stores all the log data in a special disk file; this information also includes the time stamp of the log record, last processed. When you run webalizer the next time, it scans the data in the existing disk file, reads the timestamp, and generates reports only for those that were logged after the timestamp.

Caveats of incremental processing

Incremental processing requires you to adhere to the following guidelines.

Ensure that Webalizer configuration options are not changed between runs, as this could cause corruption of the data that encapsulates the state of the previous run.

If you need to change configuration options, it is advisable to do it at the end of the month after normal processing of the previous month and before processing the current month.

Using Webalizer to Analyze Server Logs

In this section:

Introduction to Webalizer

Webalizer is a free log file analysis tool that generates highly detailed usage summaries for Web and FTP servers in easily comprehensible graphical and tabular formats. The logs are a statistical summary of user traffic on your server.

Webalizer reports are generated at a scheduled time in accordance with the configuration options that you set for the site at the time of creating the site.

Note: The webalizer.conf file for the Web/FTP server is located in the respective Webalizer directories (Web/FTP) within the site's file system.

Features of Webalizer

Some of the unique features of Webalizer are:

1. Fast processing of log files
2. Log files, over a period of time, grow to very large sizes. A relatively small web site that has several thousand visitors a month will have approximately 25 megabytes of log files. 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).
3. Portable
4. 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.
5. Configurable reports
6. Webalizer can be configured with custom options at any time by modifying the Webalizer configuration file.
7. Incremental processing of logs
8. Incremental processing (on page 150) 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
2. 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.
3. Combined log format

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

5 Xferlog format

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

7 Squid proxy logs

8 Squid logs record access information, system configuration errors and resource consumption (for example, 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 152).

When a log report is requested, Webalizer performs the following actions to produce the report.

1. Reads the Webalizer configuration information (contained in the webalizer.conf file) for the site. Webalizer can read both GZ and ZIP log file formats. If it gets a GZ or ZIP format, it decompresses the file on the fly.
2. Creates an output directory to store the log reports. If no directory is specified, the current working directory is used.
3. Reads the history file (contains totals for previous months) for the site, if it exists.
4. If incremental processing (on page 150) of logs is enabled, then it looks for a data file, named webalizer.current, that contains information about the previous run.
5. Processes the server log file. If the log file contains information for multiple months, a separate HTML file is created for each month.
6. Creates the usage summary (encapsulated in the index.htm file). The usage summary shows totals by month, and links to the HTML page of each month.
7. A new history file is saved to disk, which contains the totals generated by Webalizer during the current run.
8. If incremental processing is enabled, a data file (webalizer.current) is written, which captures necessary information about the current run.

For more information about Webalizer, visit the Home page of Webalizer (http://www.mrunix.net/webalizer/).

Webalizer Reports Overview

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

Web Server log report

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

The Web server log report is located in the corresponding Webalizer directory within the site's file system.

FTP Server log report

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

The FTP server log report is located in the corresponding Webalizer directory within the site's file system.

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

Report classifications

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 (on page 153) and FTP (on page 156) server) about user traffic for the month.

About Web Server Reports

Webalizer provides a detailed summary of monthly usage traffic on your Web server. Given below is a brief description about each tabulated report.

Monthly Statistics

The **Monthly Statistics** report provides the total and average quantification of site usage patterns for a given month.

Hits by Response Code

A response code signifies the completion status of each request. The **Hits by Response Code** report is primarily useful to personnel who maintain sites. It conveys information on the response evidenced for each request, whether the request resulted in successful transfer of information or led to failed responses in the form of bad requests, page not found, and request time-outs.

Daily statistics

Daily statistics provides a graphical (**Daily Usage**) as well as a tabulated (**Daily Statistics**) summary of Web server usage for the given month.

- **Daily usage**

  This report is a graphical illustration that comprises three key slices conveying 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

- **Daily statistics (for a given month)**

  Daily statistics presents a day-by-day account of the number of hits, files, pages, visits, sites and KBytes of activity observed on the server for the given month.

Hourly statistics

Hourly statistics provides a graphical (**Hourly Usage**) as well as a tabulated (**Hourly Statistics**) summary of Web server usage for the given month.

- **Hourly usage**

  This report is a graphical illustration of the number of pages, files and hits clocked hourly on the server for a given month.

- **Hourly statistics (for a given month)**

  Hourly statistics presents an hourly total and average account, of the number of hits, files, pages, and KBytes of activity observed on the server for the given month.

URLs

URLs present the list of top URLs visited by users, sorted by hits and the amount of data transferred (Kbytes).

- **Top URLs**

  The **Top URLs** report presents the list of top 30 URLs that logged maximum hits on the server. The number of top URLs, you want listed, can be set when you configure Webalizer. The default is 30.

- **Top URLs by KBytes**

  The **Top URLs by KBytes** report presents the list of top 10 URLs that recorded the maximum amount of data transfer from the server. The number of top URLs, you want listed, can be set when you configure Webalizer. The default is 10.

Entry

The **Entry** report presents the list of top pages that are the first to be requested by users when they visit the site.

- **Top entry pages**

  An entry page is the URL of the first page requested. The Top Entry Pages report is a statistical synopsis of the hits and visits logged for the top 10 page URLs, sorted by maximum hits received. The default list is limited to 10 and can be changed when you configure the Webalizer.

Exit

The **Exit** report presents the list of top pages that are the last to be visited by users before they leave the site.

- **Top exit pages**

  An exit page is the page URL of the last page visited, before the user exits the site. The Top Exit Pages report is a statistical synopsis of the hits and visits logged for the top 10 page URLs, sorted by maximum hits received. The default list is limited to 10 and can be changed when you configure the Webalizer.

Sites

The **Sites** report presents the list of top sites visited by users, sorted by hits and the amount of data transferred (Kbytes).

- **Top sites**

  The **Top Sites** report presents the list of top 30 sites (sorted by the maximum number of hits), that made requests to your server. The number of hits, files, KBytes, and visits logged for the hostname of the server that made the request is listed. The default list is limited to 30 and can be changed when configuring the Webalizer.

- **Top sites by Kbytes**

  The **Top Sites by KBytes** report presents the list of top 10 sites (sorted by the maximum amount of KBytes), that made requests to your server. The number of hits, files, KBytes, and visits logged for the server that made the request is listed. The default list is limited to 10 and can be changed when configuring the Webalizer.

Referrers

The **Referrers** report provides a list of top page URLs that led users to your site.

- **Top Referrers**

  The **Top Referrers** report presents the list of top referral pages that directed users to your site.

Search

The **Search** report presents the list of top 20 Search engines that listed your site, along with the search query used to bring up your site.

Agents

The **Agents** report presents the list of top browsers used to make requests to your server.

- **Top Agents**

  Agents are simply browsers that make requests to your Web server. used to request information. The **Top Agents** report lists browsers most popularly used to request information from your Web server.

Countries

The **Countries** report presents, in graphical and tabulated format, the list of top countries from where maximum number of requests originated.

Note: By default, the DNS option is turned off in the Webalizer configuration file. The Countries option therefore does not provide the adequate report.

- **Top countries**

  The Top Countries report presents the top 30 countries that have logged the maximum number of hits on your server. The report lists the number of hits, files and KBytes that characterize the request. The default list is limited to 30 and can be changed when configuring the Webalizer.

About FTP Server Reports

Webalizer provides a detailed summary of monthly usage traffic on your FTP server. Given below is a brief description about each tabulated report.

Monthly Statistics

- The **Monthly Statistics** report provides the total and average quantification of site usage patterns for a given month.

Hits by Response Code

- A response code signifies the completion status of each request. The **Hits by Response Code** report is primarily useful to personnel who maintain sites. It conveys information on the response evidenced for each request, whether the request resulted in successful transfer of information or led to failed responses in the form of bad requests, page not found, and request time-outs.

Daily statistics

Daily statistics provides a graphical (**Daily Usage**) as well as a tabulated (**Daily Statistics**) summary of FTP server usage for the given month.

- **Daily usage**

  This report is a graphical illustration that comprises three key slices conveying 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

- **Daily statistics (for a given month)**

  Daily statistics presents a day-by-day account of the number of hits, files, pages, visits, sites and KBytes of activity observed on the server for the given month.

Hourly statistics

Hourly statistics provides a graphical (**Hourly Usage**) as well as a tabulated (**Hourly Statistics**) summary of FTP server usage for the given month.

- **Hourly usage**

  This report is a graphical illustration of the number of pages, files and hits clocked hourly on the server for a given month.

- **Hourly statistics (for a given month)**

  Hourly statistics presents an hourly total and average account, of the number of hits, files, pages, and KBytes of activity observed on the server for the given month.

URLs

URLs present the list of top URLs visited by users, sorted by hits and the amount of data transferred (Kbytes).

- **Top URLs**

  The **Top URLs** report presents the list of top 30 URLs that logged maximum hits on the server. The number of top URLs, you want listed, can be set when you configure Webalizer. The default is 30.

- **Top URLs by KBytes**

  The **Top URLs by KBytes** report presents the list of top 10 URLs that recorded the maximum amount of data transfer from the server. The number of top URLs, you want listed, can be set when you configure Webalizer. The default is 10.

Sites

The **Sites** report presents the list of top sites visited by users, sorted by hits and the amount of data transferred (Kbytes).

- **Top sites**

The **Top Sites** report presents the list of top 30 sites (sorted by the maximum number of hits), that made requests to your server. The number of hits, files, KBytes, and visits logged for the hostname of the server that made the request is listed. The default list is limited to 30 and can be changed when configuring the Webalizer.

- **Top sites by Kbytes**
- The **Top Sites by KBytes** report presents the list of top 10 sites (sorted by the maximum amount of KBytes), that made requests to your server. The number of hits, files, KBytes, and visits logged for the server that made the request is listed. The default list is limited to 10 and can be changed when configuring the Webalizer.

Users

The **Users** report provides the user names of the users who have visited your FTP server. The default list is limited to 20 and can be changed when configuring the Webalizer.

- **Top users**

  Top users presents the list of top 20 users who have requested information from your FTP server.

Countries

The **Countries** report presents, in graphical and tabulated format, the list of top countries from where maximum number of requests originated.

Note: By default, the DNS option is turned off in the Webalizer configuration file. The Countries option therefore does not provide the adequate report.

- **Top countries**

  The Top Countries report presents the top 30 countries that have logged the maximum number of hits on your server. The report lists the number of hits, files and KBytes that characterize the request. The default list is limited to 30 and can be changed when configuring the Webalizer.

Log Report Field Descriptions

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

Caption	Indicates
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	The URL of the page requested, typically with any of the following extensions, .htm, .html, .cgi. **Note:** Not all entities on the page qualify, for example, audio clips or graphics that link to non-page URLs will not be a part of this statistical representation.
Visits	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 host names 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 cannot configure Webalizer using the control panel.

Webalizer reports are generated in accordance with the options set in the Webalizer configuration file.

Note: The configuration file is called `webalizer.conf` and placed in the respective Webalizer directories (Web/FTP) inside the site's file system.

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

➢ ***To change the configuration options:***

1 Log on to the server using the Telnet or SSH remote login service.

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

```
ssh <server_name>
```

For example, if you have a server by the host name `example`, then type `ssh example`

- If you are using Telnet, type the following:

```
telnet <server_name>
```

2 To assume **root** privileges for the site, using the following command.

```
su
```

3 Change your working directory to the home directory of the site using the following command.

```
/usr/sbin/chroot /home/virtual/<site name>
```

where:

`/usr/sbin/chroot` is the command to change your working directory to the home directory of the site

`/home/virtual/`***<site name>*** is the absolute path to the site's home directory

Important: When you use this command, you must leave a space between the command `/usr/sbin/chroot` and the directory path `/home/virtual/`***<site name>***, otherwise it will result in an error.

4 At the command prompt, type the following command to modify the configuration file.

- To modify the configuration file of Web server

```
vi /etc/webalizer/web/webalizer.conf
```

- To modify the configuration file of FTP server

```
vi /etc/webalizer/ftp/webalizer.conf
```

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.

5 Change the configuration options as needed.

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

```
:wq
```

7 To view the report, run (on page 162) Webalizer.

Running Webalizer

Webalizer is scheduled to run daily at 4.02 AM. You can override this schedule to generate reports as and when you need to generate them.

➢ ***To run Webalizer manually, follow these steps.***

1 Log on to the server using the Telnet or SSH remote login service.

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

```
ssh <server_name>
```

For example, if you have a server by the host name `example`, then type `ssh example`

- If you are using Telnet, type the following:

```
telnet <server_name>
```

2 To assume **root** privileges for the site, using the following command.

```
su
```

3 Change your working directory to the home directory of the site using the following command.

```
/usr/sbin/chroot /home/virtual/<site name>
```

where:

`/usr/sbin/chroot` is the command to change your working directory to the home directory of the site

`/home/virtual/`***<site name>*** is the absolute path to the site's home directory

Important: When you use this command, you must leave a space between the command `/usr/sbin/chroot` and the directory path `/home/virtual/`***<site name>*,** otherwise it will result in an error.

4 Run the Webalizer, by typing the following at the command prompt.

```
/usr/bin/webalizer -c /etc/webalizer/web/webalizer.conf
```

where:

`/usr/bin/webalizer` is the command to run Webalizer

• `c` indicates the configuration file to be used

`/etc/webalizer/web/webalizer.conf` is the absolute path to the Webalizer configuration file

If successful, Webalizer generates the reports in the respective output directories.

- The output directory for Web server reports is:

```
/var/www/html/webalizer/web
```

- The output directory for FTP server reports is:

```
/var/www/html/webalizer/ftp
```

To view the reports, log into the site and in the shortcuts section of the Home page, click on **Webalizer reports** (**Reports** section).

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

For AWStats service implementation, the package `awstats-6.8-1.noarch.rpm` is used.

In this section:

Introduction to 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.

AWStats Reports Overview

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.

Enabling AWStats

By default, AWStats is disabled in your system. You can enable it globally in service plans or for a particular site.

➢ ***To enable AWStats in a service plan:***

1 In the shortcuts section of the Home page, click **List Plans** (**Sites** section).

2 Locate the Service Plan you want to update and in the **Actions** column, click . The **Edit Service Plan** form opens.

3 Scroll down to the **Monitoring** section and check the box in the **AWStats Log Analyzer** column.

4 Use the Service Plan Options Information to help you make changes to the form.

5 Click **Update Plan**.

➢ ***To enable AWStats for a particular site:***

1 In the shortcuts section of the Home page, click **List Sites** (**Sites** section).

2 Locate the site you want to change and in the **Actions** column, click . The **Edit Site** form opens.

3 Scroll down to the **Monitoring** section and check the box in the **AWStats Log Analyzer** column.

Click **Update Site**.

Configuring AWStats for Sites

AWStats reports must be configured from the command line interface. You cannot configure AWStats using the control panel.

AWStats statistics is available in the directories:

- /home/virtual/***<siteN>***/fst/var/www/html/awstats/web - Web server statistics
- /home/virtual/***<siteN>***/fst/var/www/html/awstats/ftp - ftp server statistics

  Here, ***<siteN>*** is site number, for example, site 1, site 2, site 3 and so on.

AWStats reports are generated in accordance with the options set in the AWStats configuration file. AWStats configuration files are stored in the following directories inside the site's file system:

- /home/virtual/***<siteN>***/fst/etc/awstats/awstats.ftp.***<siteN>***.conf
- /home/virtual/***<siteN>***/fst/etc/awstats/awstats.***<siteN>***.conf
- /etc/httpd/conf/***<siteN>***/awstats

You can modify the configuration options to change the default behavior of AWStats reports.

AWStats directory is protected and by default the site administrator user has access to it:

- `/home/virtual/`***<siteN>***`/fst/etc/awstats/.passwd`
- `/home/virtual/`***<siteN>***`/fst/var/www/html/awstats/.htaccess`

➢ ***To change the configuration options:***

1 Log on to the server using the Telnet or SSH remote login service.

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

```
ssh <server_name>
```

For example, if you have a server by the host name `example`, then type `ssh example`

- If you are using Telnet, type the following:

```
telnet <server_name>
```

2 To assume **root** privileges for the site, using the following command.

```
su
```

3 Change your working directory to the home directory of the site using the following command.

```
/usr/sbin/chroot /home/virtual/<siteN>
```

where:

`/usr/sbin/chroot` is the command to change your working directory to the home directory of the site

`/home/virtual/`***<siteN>*** is the absolute path to the site's home directory

---

Important: When you use this command, you must leave a space between the command `/usr/sbin/chroot` and the directory path `/home/virtual/`***<siteN>***, otherwise it will result in an error.

---

4 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
```

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.

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, run AWStats.

Running AWStats

AWStats is scheduled to run daily at 4.02 AM. You can override this schedule to generate reports as and when you need to generate them.

➢ ***To run AWStats manually, follow these steps:***

1 Log on to the server using the Telnet or SSH remote login service.

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

```
ssh <server_name>
```

For example, if you have a server by the host name `example`, then type `ssh example`

- If you are using Telnet, type the following:

```
telnet <server_name>
```

2 To assume **root** privileges for the site, using the following command.

```
su
```

3 Change your working directory to the home directory of the site using the following command.

```
/usr/sbin/chroot /home/virtual/<siteN>
```

where:

`/usr/sbin/chroot` is the command to change your working directory to the home directory of the site

`/home/virtual/`***<siteN>*** is the absolute path to the site's home directory

Important: When you use this command, you must leave a space between the command `/usr/sbin/chroot` and the directory path `/home/virtual/`***<siteN>***, otherwise it will result in an error.

4 Run AWStats by typing the following at the command prompt:

- for gathering statistics:

```
/usr/bin/perl /usr/local/awstats/wwwroot/cgi-bin/awstats.pl -
config=$<siteN> -update
```

- for generating html files:

```
/usr/bin/perl /usr/local/awstats/wwwroot/cgi-bin/awstats.pl -
config=$<siteN> -output -staticlinks >
/var/www/html/awstats/web/index.html
/usr/bin/perl
/usr/local/awstats/tools/awstats_buildstaticpages.pl -
awstatsprog=/usr/local/awstats/wwwroot/cgi-bin/awstats.pl -
config=$<siteN> -output -staticlinks -
dir=/var/www/html/awstats/web
```

Here ***$<siteN>*** is

- ***<siteN>*** for Web server
- `ftp.`<siteN> for ftp server.

If successful, AWStats generates the reports in the respective output directories.

- The output directory for Web server reports is:

```
/var/www/html/awstats/web
```

- The output directory for FTP server reports is:

```
/var/www/html/awstats/ftp
```

To view the reports, log into the site and in the shortcuts section of the Home page, click on **AWStats reports** (**Reports** section).

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 all the sites hosted on the server. The report is useful in tracking the usage status of all the sites and identifying the sites that are approaching or exceeding the allocated limit. You can use this information to prevent issues caused by insufficient disk space.

The report displays the following usage information for all the sites hosted on the server.

- **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.

Your resellers can view the disk usage information for the sites they create. However, they cannot set the threshold for their sites. When a site reaches or exceeds its usage limits (on page 171), an email notification is sent to the Site Administrator.

Types of usage limits

The usage limits operational on a site are as follows:

- **Threshold**. The threshold is a percentage value of the allocated quota for a site. The default threshold is **80** percent of the allocated quota. The current threshold is displayed at the top left corner of the reports page. You can set the threshold (on page 173) at any time. When a 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 a site is **3** MB short of reaching the allocated quota. You can change the critical limit (on page 173) at any time. When a site reaches or exceeds its critical limit, an email notification is sent to the Site Administrator.
- **Hard limit**. The hard limit is the amount of disk space allocated to a site. You can set this limit when you create the site.

Important: It is important that measures be taken to avoid disk space consumption in excess of a 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 **Site Disk Usage** (**Reports** section).

The following information is displayed:

- **Status** - The current usage status for the site. The status is indicated by the following buttons:

  - Indicates that the usage level is below the threshold.

  - Indicates that the usage level exceeds the site’s threshold.

  - Indicates that the usage level exceeds the quota allocated to the site.
- **Site** - The name of the site.
- **Site Owner** - The owner of the site.
- **Usage** - A bar graph showing how much disk space is used in comparison to how much is assigned to the site.
- **% Used Quota -** 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 maximum amount of disk space (in megabytes) allocated to the site.

Setting the Usage Limits

You can modify the threshold (on page 173) and critical limit (on page 173) for the sites hosted on your server. These limits are common to all the sites hosted on the server.

➢ ***To set the threshold:***

1 Log in as the root user to the Parallels Pro server.

2 Update the value of the attribute **quota_threshold** in the configuration file by typing the following command:

```
eplconf set quota_threshold=<value>
```

where ***<value>*** is the new threshold value

3 Restart the epld daemon.

```
service epld restart
```

➢ ***To set the critical limit:***

1 Log in as the root user to the Parallels Pro server.

2 Update the value of the attribute **quota_critical_limit** in the configuration file by typing the following command:

```
eplconf set quota_critical_limit=<value>
```

where <value> is the new value for the critical limit

3 Restart the epld daemon.

```
service epld restart
```

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 the email address you specify in the **Administrator Email** field.

➢ ***To email the report:***

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

CHAPTER 10

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 (on page 176) (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 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 DNS network protocol.

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.

Review the following related topics for more information:

- IDN compatibility requirements for applications (on page 178)
- Using IDNs with email addresses (on page 181)
- Using remote access services to connect to IDN domains (on page 182)

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 176) of the domain name to access the domain. To view the ASCII-encoded representation, click the link show **text name next** to the IDN.

If you are using the Microsoft Windows platform, you need to install (on page 183) 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

  Version: 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 http://www.verisign.com/products-services/naming-and-directory-services/naming-services/internationalized-domain-names/page_002201.html.

Previewing or Connecting to an IDN Domain

You can preview or 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 176) of the domain name to access the domain. To view the ASCII-encoded representation, click the link show *text name next* to the IDN.

Previewing an IDN domain using IDN representation

Your Web browser must be IDN-compliant (on page 178) to enable domain previews using its IDN representation.

➢ ***To preview a domain:***

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

```
http://<server IP address>/<idn_domain_name>.com/
```

where:

<server IP address> is the control panel server’s IP address

<idn_domain_name> is the fully qualified IDN representation of the domain

For example:

To preview the domain `fargbolaget.nu` hosted on the server `1.2.3.4`, type:

```
http://1.2.3.4/fargbolaget.nu/
```

Previewing an IDN domain using ASCII-encoded representation

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

➢ ***To preview a domain using its ASCII-encoded representation:***

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

```
http://<server IP address>/<ascii_domain_name>.com/
```

where:

<*server IP address*> is the control panel server's IP address

<*ascii_domain_name*> is the fully qualified ASCII-encoded representation of the domain

For example:

To preview the domain `fargbolaget.nu` hosted on the server `1.2.3.4` using its ASCII-encoded representation `xn—frgbolaget- q5a.nu`, type:

```
http://1.2.3.4/xn--frgbolaget-q5a.nu/
```

Connecting to an IDN domain using IDN representation

Your Web browser must be IDN-compatible (on page 178) to connect to a domain using its IDN representation, otherwise you will be unable to connect to the domain.

➢ ***To connect to a domain using its IDN representation:***

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` hosted on the server `1.2.3.4`, 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.

➢ ***To connect to a domain name using its ASCII-encoded representation:***

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

http://<ascii_domain_name.com>/

where ***<ascii_domain_name.com>*** is the ASCII-encoded representation of the domain name

For example:

To connect to the domain fargbolaget.nu hosted on the server 1.2.3.4 using its ASCII-encoded representation xn—frgbolaget- q5a.nu, type:

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

Using IDNs in Email Addresses

You can use the IDN representation of a domain name in email addresses if your browser is IDN-compatible (on page 178).

Important: If your application is not IDN-compliant, you must use the ASCII-encoded representation (on page 176) of the domain name to access the domain. To view the ASCII-encoded representation, click the link show **text name next** to the IDN.

When you specify the email address of the Site Administrator while creating a domain ***<idn_domain>***.com, you may enter the email address siteadmin@<idn_domain>.com in the **Email Contact** field.

Example

To specify the email address for the Site Administrator admin1 of the domain fargbolaget.nu, type the email address as follows:

admin1@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 specify the email address for the Site Administrator `admin1` of the domain `fargbolaget.nu` using its ASCII-encoded representation `xn—frgbolaget-q5a.nu`, type the email address as follows:

```
admin1@xn--frgbolaget-q5a.nu
```

Using Remote Access Services to Connect to IDN Domains

If your application is IDN-compliant (on page 178), 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 176) of the domain name to access the domain. To view the ASCII-encoded representation, click the link **show text name** next to the IDN.

➢ ***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.

➢ ***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
```

2 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.

C H A P T E R 1 1

Managing Resellers

In this chapter:

About Resellers

Resellers are individuals or companies who want to sell sites on their own without having to maintain server hardware and software.

The Reseller option creates new business opportunities and allows you to expand your customer base with minimum interaction and support to the end-customer. You allocate a fixed number of sites to a reseller and control the disk quota and mail users that your reseller may create. You also create Reseller Plans to easily allocate and market the Reseller plans.

Once you allocate disk quota and set the number of sites and users that resellers can employ, resellers can sell and distribute these sites to their customers. This flexibility allows resellers to assign maximum resources for a large customer, using the balance for smaller customers. Resellers have their own administrative control panel where they can log on and maintain their customers. They perform many of the service provider tasks, except for server level tasks like starting and stopping services.

You perform the following actions using the Reseller Manager:

- Configuring Reseller options (on page 188)
- Viewing the site list of a Reseller (on page 189)
- Removing a Reseller (on page 190)

Logging Onto the Reseller Administrator Control Panel

Parallels Pro Control Panel Automatic login also called auto-login does not require you to know the Reseller Administrator’s user name and password. You are automatically logged in using the Reseller Administrator’s account information. you into the Reseller Administrator control panel when you click on a reseller account. Auto-login is especially useful if the Reseller Administrator has forgotten the login password, and requires you to access the Reseller Administrator control panel and reset the current password. As a Reseller Administrator, you can also perform other administrative tasks. While you work as a Reseller Administrator, your Server Administrator session remains active for a duration of 60 minutes. If no activity is noted during this period, the session expires and logs you out of the Server Administrator control panel. As you perform multiple roles, stacked login ensures that your multiple sessions remain easily accessible and functional.

➢ ***To log on as the Reseller Administrator:***

1. In the shortcuts section of the Home page , click **List Resellers** (**Resellers** section).
2. In the **User Name** column, click the name of any reseller.

   A dialog box opens and confirms that you want to log on at the Reseller Administrator level.
3. Click **OK**. The **Reseller Administrator** shortcuts page opens, which lists the tasks you can perform as the Reseller Administrator.

Working with the Reseller Manager

In this section:

Viewing Reseller Information

You can view the list of resellers currently hosted on the server and manage their accounts from the Reseller Manager window.

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

In the shortcuts section of the Home page , click **List Resellers** (**Resellers** section). The **Reseller List** page opens displaying the following information:

- **Status** - The current status of the reseller
- **User Name**: The user name of the reseller
- **Disk**: The used and allocated disk quota (in Megabytes)
- **Bandwidth**: The used and allocated bandwidth (in Megabytes)
- **Name-based**: The number of name-based sites allocated to the reseller
- **IP-based**: The number of IP-based sites allocated to the reseller
- **Users**: The total number of users that a reseller can create.
- **Zone Management**: Whether zone management capability is enabled or disabled for the reseller
- **Actions**: Allows you to perform the following actions on the reseller account:

   - View (on page 189) the list of the IP-based sites and name-based sites hosted by the reseller

   - Update (on page 188) reseller settings

   - Remove (on page 190) a reseller

Adding Resellers

You can create reseller accounts using the Reseller Manager. You establish the number of users, sites and other hosting resources that a reseller is enabled to support.

➢ ***To add a reseller:***

1 In the shortcuts section of the Home page , click **Add Reseller** (**Resellers** section).

2 In the **User Name** field, enter a user name for the Reseller Administrator.

Note: The user name should not exceed a maximum of **60** characters and should not include any of the following character: " \ / [] : . ; | = , + * ? < >.

3 In the **Full Name** field, enter the complete name of the Reseller.

Note: The full name should not exceed **255** characters.

4 In the **Password** field, enter a password for the Reseller Administrator (should not exceed **60** characters).

Note: Passwords are case-sensitive.

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

6 Select the **Enabled** check box to enable the reseller account.

7 In the **Email** field, enter the email address of the Reseller Administrator. Any email notifications will be sent to this email address.

8 In the **Allocated Disk Quota** field, enter the total disk space (in Megabytes), to be allocated to the reseller.

9 In the **Maximum Number of Users** field, enter the maximum number of users that can be added by a reseller.

10 In the **Allocated Bandwidth Threshold** field, enter the upper limit of network traffic (in Megabytes) that the reseller is allowed to have.

11 In the **IP-based Sites** field, enter the maximum number of IP-based sites that can be created by the reseller.

Note: Entering '**0**' in the **IP Based Sites** field will not allow the reseller to create any IP based site.

12 In the **Name-based Sites** field, enter the maximum number of name-based sites that can be created by the reseller.

Note: Entering '**0**' in the **Name Based Sites** field will not allow the reseller to create any name-based site.

13 Select the **Allow High Security Sites Only** check box if you want to enable only high security sites for the reseller.

14 Select the **Enable Zone Management** check box if you want to enable zone management capability for the reseller. If enabled, the **DNS** option is displayed in the shortcuts section of the Reseller Administrator control panel, using which the reseller can manage the zones of the sites created on his account; he can also enable the Site Administrators to manage the zones of their site.

15 Click **Save**.

Updating Reseller Account Settings

➢ ***To update existing reseller account settings:***

1 In the shortcuts section of the Home page , click **List Resellers** (**Resellers** section).

2 Locate the reseller whose settings you want to update and in the **Actions** column, click .

3 Update the reseller settings as required.

4 Click **Update**.

Viewing Reseller Site Information

You can view and manage sites hosted on each reseller account using the Reseller Manager.

➢ ***To view the list of sites hosted on a reseller account:***

1 In the shortcuts section of the Home page , click **List Resellers** (**Reseller** section). The Reseller List page opens displaying the list of existing reseller accounts.

2 Locate the reseller whose site information you want to view and in the **Actions** column, click . The Site List page opens displaying the following information:

- **Status**: The status of the site
- **Site**: The name of the site
- **Disk**: The disk space used by the site (in Megabytes)
- **Bandwidth**: The bandwidth used by the site (in Megabytes)
- **Type**: The type of site - IP-based or name-based, indicated by the appropriate icon

  IP symbolizes IP-based sites

  NB symbolizes name-based sites
- **Users**: The total number of user accounts created for the site
- **Actions:** Allows you to perform the following actions on the site:
  - Update reseller site settings (on page 189)
  - Remove sites (on page 190)

Updating Reseller Site Settings

➢ ***To update the settings of a site hosted on a reseller account:***

1 In the shortcuts section of the Home page , click **List Resellers** (**Reseller** section). The **Reseller List** page opens displaying the list of existing reseller accounts.

2 Locate the reseller whose site settings you want to update and in the **Actions** column, click . The **Site List** page opens displaying the list of sites hosted on the reseller account.

3 Locate the site whose settings you want to update and in the **Actions** column, click .

4 Use the Service Plan Options Information to help you make changes to the form.

5 Click **Update Site**.

Removing a Reseller Site

➢ ***To remove a site:***

1 In the shortcuts section of the **Home page**, click **List Resellers** (**Reseller** section). The **Reseller List** page opens displaying the list of existing reseller accounts.

2 Locate the reseller whose site you want to remove and in the **Actions** column, click . The **Site List** page opens displaying the list of sites hosted on the reseller account.

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

4 In the confirmation window, verify the site you are removing, then click **OK**.

Removing a Reseller

Important: When you delete a reseller, you automatically assume ownership of all the sites formerly owned by the reseller. After deletion, when you restore the site, the site continues to exist under your ownership, unless the site is modified to transfer ownership back to the reseller.

➢ ***To remove a reseller:***

1 In the shortcuts section of the Home page , click **List Resellers** (**Resellers** section).

2 Locate the reseller you want to remove and in the **Actions** column click .

3 In the confirmation window, verify the reseller you are removing, then click **OK**.

Viewing Reseller Bandwidth Usage Reports

In this section:

Viewing Current Bandwidth Usage Report for Resellers

You can view bandwidth usage reports (on page 144) for the current monitoring session for all of your reseller accounts. The information shown includes bandwidth usage from the start of the monitoring session to the current day.

The report includes:

- The current usage summary for all resellers
- The current usage summary for each reseller

➢ ***To view current bandwidth usage reports:***

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

2 Click **Current Usage Report for Resellers**. You can view the following usage information.

   - **Current Usage Report For All Resellers**. This report displays a consolidated usage summary for all of your reseller accounts.
   - **Current Usage Report For Each Reseller**. This report displays the usage summary for each reseller account.

   The columns in these reports include:

   - **Reseller -** The name of the reseller. Click the reseller name to view the bandwidth usage details for the reseller.
   - **Bandwidth -** A bar graph showing how much bandwidth is used in comparison to how much is assigned to the reseller.
   - **Status** (not displayed for **All Resellers**) - The current status of the reseller. The status is indicated by the following buttons:

      - Indicates that the reseller account is enabled

      - Indicates that the reseller account is disabled

   - **Used -** The number of megabytes of bandwidth consumed by the reseller during the current one month period.
   - **Quota -** The maximum number of megabytes of bandwidth allocated to the reseller for the current one month period.
   - **Available -** The bandwidth available to the reseller.
   - **% Used -** The difference amount shown as a percentage.

You can also view current usage report for a particular reseller (on page 192).

Viewing Past Bandwidth Usage Report for Resellers

Once the current monitoring session ends, information about bandwidth usage for the month is moved to the Last Usage Reports form. This form shows a summary of the amount of network traffic that occurred for all of your resellers during the last monitoring session.

The report includes:

- The past usage summary for all resellers
- The past usage summary for each reseller

➢ ***To view past bandwidth usage reports for resellers:***

1 On the left navigation bar, click **Bandwidth Reports.**

2 On the Usage Reports menu, click **Last Usage Reports for Resellers**. You can view the following usage information.

   - **Last Usage Report For All Resellers**. This report displays a consolidated usage summary for all of your reseller accounts.
   - **Last Usage Report For Each Reseller**. This report displays the usage summary for each reseller account.

   The columns in this form include:

   - **Reseller -** The name of the reseller. Click the reseller name to view the bandwidth usage details for the reseller.
   - **Bandwidth -** A bar graph showing how much bandwidth is used in comparison to how much is assigned to the reseller.
   - **Status** (not displayed for **All Resellers**) - The current status of the reseller. The status is indicated by the following buttons:

     - Indicates that the reseller account is enabled

     - Indicates that the reseller account is disabled
   - **Used -** The number of megabytes of bandwidth consumed by the reseller during the specified period.
   - **Quota -** The maximum number of megabytes of bandwidth assigned to the reseller.
   - **Available -** The amount of megabytes difference between the number of bytes of bandwidth assigned to the reseller and the number of bytes of bandwidth already used.
   - **% Used -** The difference amount shown as a percentage.

You can view the usage report for a particular reseller (on page 192).

Viewing Bandwidth Usage Reports for a Specific Reseller

You can view detailed bandwidth usage for a specific reseller. The report, by default, shows bandwidth usage by all sites of the reseller, from the start of the monitoring session to the current day. You can also browse through past reports by selecting the time period for which you want to view the usage report. The time period is based on the bandwidth monitoring cycle defined for the site at the time of creating the site.

Note: Bandwidth statistics may not be available for new sites for up to five minutes after the new sites are created. Also, you will not see statistics until there is traffic on the new site. The information is updated every 2 hours.

➢ ***To view bandwidth usage details for a specific reseller:***

1 On the left navigation bar, click **Bandwidth Reports.** The **Usage Reports** form opens displaying all the resellers that have usage report statistics available.

2 Click **Current Usage Report for Resellers** if you want to view reports for the current monitoring session or click **Last Usage Reports for Resellers** if you want to view past reports.

3 In the **Reseller** column, locate the reseller whose report you want to view, and click the underlined name of that reseller.

The **Usage Report** form for that reseller opens. The upper section of the form shows the bandwidth usage summary for the reseller (on page 192). The lower section shows details of bandwidth usage for each site (on page 192).

About bandwidth usage summary for the reseller

The following information is displayed:

- **Bandwidth -** A bar graph showing how much bandwidth is used by the site.
- **Maximum Allowed sites** - The maximum number of sites you can create.
- **Total Sites Created** - The maximum number of sites created for your account.
- **Bandwidth Consumed By Sites** - The number of sites consuming bandwidth.
- **Total Used Bandwidth** - The amount of bandwidth used by the sites on your account.
- **Allowed Quota** - The maximum bandwidth (in megabytes) allocated to you.
- **Available Quota -** The amount of megabytes still available after finding the difference between the number of bytes of bandwidth assigned to you and the number of bytes of bandwidth already used.

About bandwidth usage summary for each site

The columns in this section include:

- **Site -** The name of the site. The site name is linked to a detailed statistical site report (on page 146).
- **Bandwidth -** A bar graph showing how much bandwidth is used in comparison to how much is assigned to the site.
- **Status** - The current usage status of the site. The status is indicated by the following buttons:

   - Indicates that the usage level is below the threshold.

   - Indicates that the usage level exceeds the threshold set for the site.

   - Indicates that the usage level exceeds the quota allocated to the site.
- **Used -** The number of megabytes of bandwidth already used by the site during the current one month period.
- **Quota -** The maximum number of megabytes of bandwidth assigned to the site for the current one month period.
- **Available -** The bandwidth available to the site.
- **% Used -** The difference amount shown as a percentage.

Viewing past bandwidth usage reports for a reseller’s site

You can choose to view past bandwidth usage report (on page 146) for the reseller’s sites for a given time-period. The time-period is based on the bandwidth monitoring cycle defined for the site at the time of creating the site.

To view past reports for a reseller’s site, click the site name.

C H A P T E R 1 2

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.

- Complete data (on page 199)
- Reseller data (on page 203)
- Site data (on page 206)

Note: You must have FTP access (on page 198) to export and import files.

Known issues in export and import

- The MySQL password is exported as metadata; however, the password is not imported when you migrate sites between servers.
- Site statistics is not exported.

Preparing for Export and Import

Before you export or import data, review the preparatory information (on page 196) and the recommended tips (on page 196) 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 198) 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 server renders the site inaccessible. Do not use non-variable Site IDs in Web content. Use Environment variables enable scripts to 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 198) 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 export and import files. 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 servers installed on IIS are configured to support the “MS-DOS” directory listing style while the control panel follows the “Unix” directory listing style. 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 the 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 Complete Export

A complete export backs up the following data.

- Server configuration information such as server security information and system login information is exported.
- The configuration information of reseller accounts and all the sites hosted on the reseller account are exported. (if available)
- The site user accounts and service configuration information and related files are exported.

When you do a Complete export, the following archives are created.

- A compressed file (.gz), that contains the server configuration information
- A compressed file (.gz) for each reseller account

A compressed file (.gz) for each site hosted on the server The naming convention of an exported file is as follows:

<server_hostname>_complete_<export_type>_<YYYY>_<Month>_<date>_<Hours>_Minutes> **`.tar.gz`**

Where:

<server_hostname> is the name of the control panel server
<export_type> indicates the type of export (Complete)
<YYYY>_<Month>_<date>_<Hours>_Minutes> is the time-stamp when the data is exported.

For example, exporting the server *example.com* on Jan 06, 2003 at 11.30 creates the following file:

`example.com_complete_complete_2003_January_06_11_30.tar.gz`

What is exported

The following files and directories are exported.

- Customizations
  - `/usr/lib/ensim-python/site-packages/vh3/custom/anonftp.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/apache.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/cgi.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/mod_perl.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/openssl.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/proftpd.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/custom/ssi.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/subdomain.py`
  - `/usr/lib/ensim-python/site-packages/vh3/custom/tomcat4.py`

- `/etc/appliance/customization/site_remove_disabled`
- `/etc/appliance/customization/corner.gif`
- `/etc/appliance/customization/logo.gif`
- `/etc/appliance/customization/display.ini`
- `/etc/appliance/customization/stylesheet.dtml`
- `/etc/appliance/customization/appliancemenu.dtml`
- `/etc/appliance/customization/resellermenu.dtml`
- `/etc/appliance/customization/sitemenu.dtml`
- `/etc/appliance/customization/usermenu.dtml`
- `/etc/appliance/customization/editVirtDomain.sh`
- `/etc/appliance/customization/virtDomain.sh`
- `/etc/appliance/customization/virtDomain.tar`
- `/etc/appliance/customization/disableVirtDomain.sh`
- `/etc/appliance/customization/enableVirtDomain.sh`
- `/etc/appliance/customization/deleteVirtDomain.sh`
- `/etc/appliance/customization/resellernotify_mail.txt`
- `/etc/appliance/customization/bwnotify_mail.txt`
- `/etc/virtualhosting/ipranges`

- Server security certificate information
  - `/etc/httpd/conf/ssl.crt`
  - `/etc/httpd/conf/ssl.key`
  - `/etc/httpd/conf/ssl.csr`
  - `/etc/httpd/conf/ssl.crl`
  - `/etc/httpd/conf/ssl.prm`
  - `Email access information`
  - `/etc/mail/access`

`/etc/mail/access.db` The following information is exported as metadata:

- DNS information comprises the DNS settings configured for the zone along with zone information for the site.
- Reseller configuration information comprises information such as the reseller's user name and password, customization information such as the reseller logo and style sheets, selected Service Plan and user details. The reseller configuration information is located in the **/home/reseller/<reseller id>** directory.
- 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`
- Databases
  - `/var/lib/mysql/`
  - `/var/lib/pgsql/`
- 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
  - ***<Document root of the Web server>***/squirrelmail/config/ensim_config.php
- SSH authentication information
  - /etc/ssh.pamlist
- Telnet authentication information
  - /etc/telnet.pamlist
- Bandwidth statistics
- Scheduled export settings
  - /etc/cron/*.*

About Reseller Export

A Reseller export creates the following archives.

- A compressed file (.gz) for each reseller. This file contains the reseller configuration information.

A compressed file (.gz) for each site The naming convention of an exported file is as follows:

<server_hostname>_<reseller_name>_<export_type>_<YYYY>_<Month>_<date>_<Hours>_<Minutes>`.tar.gz`

Where:

<server_hostname> is the name of the control panel server
<reseller_name> is the name of the reseller being backed up
<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 reseller *r1* on the server *example.com* on Jan 06, 2003 at 11.30 creates the following file:

```
example.com_r1_reseller_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.
- Reseller configuration information comprises information such as the reseller's user name and password, customization information such as the reseller logo and style sheets, selected Service Plan and user details. The reseller configuration information is located in the **/home/reseller/<reseller id>** directory.
- 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`
- Majordomo
  - `/usr/lib/majordomo/wrapper`
- 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 Control Panel
  - ***<Document root of the Web server>***`/squirrelmail/config/ensim_config.php`
- SSH authentication information
  - `/etc/ssh.pamlist`
- Telnet authentication information
  - `/etc/telnet.pamlist`

About Site Export

A Site export backs up the The site user accounts, service configuration information and related files are exported.

. You can perform a selective (selected sites) or comprehensive (all sites) export.

When you export a site, the following archive is created.

A compressed file (.gz) for each 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
`<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 control panel 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`
- Majordomo
  - `/usr/lib/majordomo/wrapper`
- 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

- ***<Document root of the Web server>***`/squirrelmail/config/ensim_config.php`
- SSH authentication information
  - `/etc/ssh.pamlist`
- Telnet authentication information
  - `/etc/telnet.pamlist`
- Files not owned by group `adminxyz` (for example, `admin123`) or `root`

Exporting Data

Tip: Export the Complete, Reseller and Site backups in different directories for easy identification of the archive when you import.

Example. Export the Complete backup to an `complete_export` directory, the Reseller backup to a `reseller_export` directory and the Site backup to a `site_export` directory.

Important: Any data or configuration change made after you export is lost if your system crashes or the files get corrupted. Further, while the server and the sites hosted on the server are accessible during an export, modifications to files or email messages received during this period may not be exported.

To export data, in the shortcuts section of the Home page, click **Export** (**Tools** section). The **Export** form opens.

You need to choose the type of export, provide necessary FTP account details, and other miscellaneous information.

WIZARD STEP 1. CHOOSE THE TYPE OF EXPORT

1 In the **Type of Export** area, select one of the following option buttons.
   - Complete (on page 199)
   - Resellers (on page 203)

     Click the arrow in the **Resellers** list and choose one of the following.
     - **All** - To export all reseller accounts on the server
     - **<name of the reseller>** - To export a particular reseller. Press CTRL and the left mouse button to select multiple resellers.

     Note: An **All** reseller export is not the same as a **Complete** backup. The server configuration information is not exported in an **All** reseller export.
   - Sites (on page 206)

     Click the arrow in the **Sites** list and choose one of the following.
     - **All** - To export all the sites hosted on the server
     - **<name of the site>** - To export a particular site.

     Press **Ctrl** and the left mouse button to select multiple sites.

WIZARD STEP 2. ENTER FTP INFORMATION

1 In the **FTP Server** field, enter the name of the FTP server you want to use as the export server.

2 In the **FTP Login** field, enter the user name of your account on the FTP server.

3 In the **FTP Password** field, enter the password of your account on the FTP server.

4 In the **FTP Location** field, enter the complete path to the export directory on the FTP server. If you leave the field blank, the data is 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.

WIZARD STEP3. ENTER MISCELLANEOUS INFORMATION

1 In the **Maximum Export File Size** field (Optional), enter the maximum size of the export file. Click the arrow in the **Unit** field and select the appropriate quantifying unit (Megabytes or Gigabytes).

Important: 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 export server, the files are 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** is the name of your export file.*

2 In the **Email** field, enter the email address at which you want to receive export status notifications.

3 Click **Export**.

The status of the export is conveyed in an email notification sent to the address specified in the **Email** field.