
SWsoft, Inc.

Plesk File Server

Administrator's Guide

Plesk 7.5 Reloaded



(c) 1999-2005

ISBN: N/A
SWsoft Inc
13755 Sunrise Valley Drive
Suite 325
Herndon
VA 20171 USA
Tel: +1 (703) 815 5670
Fax: +1 (703) 815 5675

Copyright © 1999-2005 by SWsoft, Inc. All rights reserved
Distribution of this work or derivative of this work in any form is prohibited unless prior written permission is obtained from the copyright holder.
Linux is a registered trademark of Linus Torvalds.
ASPLinux and the ASPLinux logo are registered trademarks of SWsoft, Inc.
RedHat is a registered trademark of Red Hat Software, Inc.
Solaris is a registered trademark of Sun Microsystems, Inc.
UNIX is a registered trademark of The Open Group.
MS Windows, Windows 2003 Server, Windows XP, Windows 2000, Windows NT, Windows 98, and Windows 95 are registered trademarks of Microsoft Corporation.

Contents

Preface	5
About This Guide	5
Documentation Conventions.....	5
Typographical Conventions.....	5
General Conventions	6
Feedback.....	6
Using Plesk™ File Server	7
File Server Interface Basics	7
How to Access File Server.....	9
How to Configure File Server Preferences	9
Managing Users	11
Managing Shares	12
Managing Broadcast Interfaces.....	13
How to Limit Access to File Server.....	14
Index	15

Table of Figures

Figure 1: File Server management page	9
Figure 2: List of shared resources	12

CHAPTER 1

Preface

In This Chapter

About This Guide.....	5
Documentation Conventions.....	5
Feedback	6

About This Guide

This Guide provides detailed instructions on how to use the Plesk™ File Server, a new module that allows the administrator to manage shared resources on the server directly from the control panel.

Documentation Conventions

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

Typographical Conventions

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 QoS tab.
	Titles of chapters, sections, and subsections.	Read the Basic Administration chapter.
<i>Italics</i>	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.	These are the so-called <i>shared VPSs</i> . To destroy a VPS, type <code>vzctl destroy <i>vpsid</i></code> .
Monospace	The names of commands, files, and directories.	Use <code>vzctl start</code> to start a VPS.

<code>Preformatted</code>	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	<code>Saved parameters for VPS 101</code>
Monospace Bold	What you type, contrasted with on-screen computer output.	# rpm -V virtuozzo-release
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

General Conventions

Be aware of the following conventions used in this book.

- Chapters in this guide are divided into sections, which, in turn, are subdivided into subsections. For example, **Documentation Conventions** is a section, and **General Conventions** is a subsection.
- When following steps or using examples, be sure to type double-quotes ("), left single-quotes ('), and right single-quotes (') exactly as shown.
- The key referred to as RETURN is labeled ENTER on some keyboards.

The root path usually includes the `/bin`, `/sbin`, `/usr/bin` and `/usr/sbin` directories, so the steps in this book show the commands in these directories without absolute path names. Steps that use commands in other, less common, directories show the absolute paths in the examples.

Feedback

If you spot a typo in this guide, or if you have thought of a way to make this guide better, we would love to hear from you!

If you have a suggestion for improving the documentation (or any other relevant comments), try to be as specific as possible when formulating it. If you have found an error, please include the chapter/section/subsection name and some of the surrounding text so we can find it easily.

Please submit a report by e-mail to userdocs@sw-soft.com.

CHAPTER 2

Using Plesk™ File Server

The File Server module enables Plesk administrators to share directories on a network directly from the control panel. Using the Plesk File Server, you can share access to a directory on your server, grant access to this directory to specific users or hosts, and assign read-only or write permissions for this directory. File Server uses the Microsoft SMB (Server Message Block) protocol to share resources on a Samba server for network users.

For the Plesk™ File Server, the Samba server (version 2.2.x or 3.x) must be installed and properly configured.

In This Chapter

File Server Interface Basics	7
How to Access File Server.....	9
How to Configure File Server Preferences	9
Managing Users	11
Managing Shares.....	12
Managing Broadcast Interfaces.....	13
How to Limit Access to File Server.....	14

File Server Interface Basics

The Plesk File Server interface is generally the same as that of other Plesk pages. Please, read the instructions below to familiarize yourself with the Plesk interface basics.

A Plesk page includes the following elements:

- 1** *top area* contains the logo image
- 2** *navigation pane* contains navigation items and the context help area
- 3** *work area* contains the groups of available operations (based on the current context), input forms, lists, and other similar interface elements

The *Plesk work area* includes all interface elements located to the right of the navigation pane. The work area displays the options available for the shortcut selected in the navigation pane. For example, if you select the **Modules** shortcut in the navigation pane, the work area will display all currently installed Plesk modules.

Path bar is a chain of links indicating your current location within the Plesk system. It is located at the top of the Plesk work area. By clicking these links, you can jump to one or more levels up. You can also use the **Up Level** button located in the upper right corner of each screen to return to the previous page.



Lists of objects. You may have a considerable number of objects, such as users, shares, etc., handled by your Plesk module. To facilitate working with different lists of objects, use the **Search** and **Sorting** options.

To search through a list, enter the search pattern into the **Search** field, and click **Search**. All matching items will be displayed in a reduced list. To show the entire list of objects, click **Show All**.

To sort a list by a certain parameter in either ascending or descending order, click on the parameter's name in the column heading. The order of sorting will be indicated by a small triangle displayed next to the parameter's name.

To remove an entry from the list, check the boxes at the end of the list and click **Remove Selected**.

How to Access File Server

To access the File Server, click the  Modules shortcut in the navigation pane and, in the Modules group, click the  Samba File Server Configuration icon.

The page that opens is the File Server management page from where you can perform all File Server operations. This page has five tabs: Status, Shares, Users, Interfaces, and Access. Each of these tabs contains tools for managing shared resources, file server properties, network interfaces, and users and computers who will have access to the shared directories.

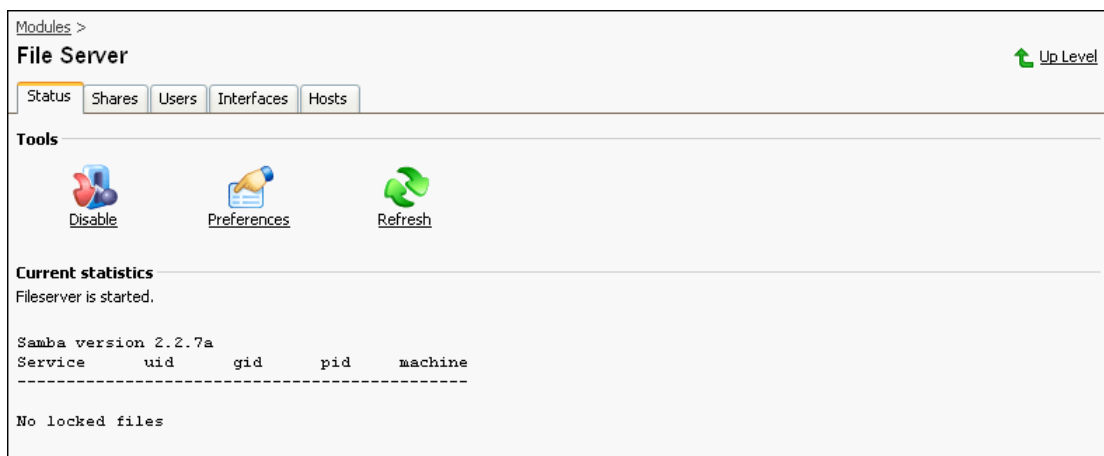


Figure 1: File Server management page

How to Configure File Server Preferences

On the **Status** tab (Modules --> File Server --> Status), you can perform the following actions:

- disable your file server
- view and edit file server preferences
- view the current usage of shared resources
- refresh server statistics

To disable your file server:

Click the **Disable** button in the **Tools** section of the **Status** tab.


To view the current status of your file server, open the **Status** tab. In the **Current statistics** section, you can see whether your file server is started or stopped. The statistics on the current connections to shared directories is provided in the table with the following columns:

Share – name of the shared resource

Host – name of the remote host currently connected to the shared directory

User – user name who is currently connected to the shared directory

To view and edit the file server preferences:

- 1 Click the  Preferences button in the **Tools** section of the **Status** tab. The page that opens displays the preferences of your file server.
- 2 To change the workgroup for your server on the Microsoft network, click in the **Workgroup** field and enter the name of a workgroup. The **Description** field contains an optional description of your file server. You can edit the description, if needed.
- 3 You can also configure the following security parameters for your Samba server:

- **Authentication mode.** Select one of the following security modes:

Share - in this security mode, the user authenticates himself/herself separately for each share. The user sends a password along with each tree connection (share mount). Passwords are meant to be associated with each share, independent of the user.

User - this security mode is based on verifying the username and password. The server can either accept or reject the username/password combination. At this stage the server has no idea what share the client will eventually try to connect to, so it bases the accept/reject decision only on the username/password and the name of the client machine.

Server - in Server Security Mode, the Samba server receives the username/password from the client and sends a session setup request to the machine designated as the password server. If the password server is in user-level security and accepts the password, Samba accepts the client's connection. The client sends all passwords in encrypted form. This security mode requires the use of a password server (see **Authentication server**).

Domain - in Domain Security Mode, the Samba server has a domain security trust account (a machine account) and causes all authentication requests to be passed through to the domain controllers. In other words, domain security has basically the same concept as server security mode, with the exception that the Samba server becomes a member of a Windows NT domain. This means that the Samba server can participate in things such as trust relationships.

ADS - in this mode, the authentication procedure is performed through an Active Directory domain. Samba in this security mode can accept Kerberos tickets.

- **Authentication server.** If you set the security mode to either Server, Domain, or ADS, you will need to specify the password server (or the authentication server). For user and share modes, the password server is not required.

In this field, enter the NetBIOS name of the SMB server used as a password server, on which the Samba server will check the entered passwords. You can list multiple NetBIOS names separated with a space. This allows Samba to attempt a session setup request to each machine in the list in order until a server is contacted. This means that the next machine on the list is contacted only if the previous machine was unavailable.


You must use only the NetBIOS name of the password server (not the IP address), and Samba must have a way of resolving the name to an IP address in order to attempt the connection.

To create a local account for all users that access the Samba server and disable the password field, set this field to the asterisk character (*).

- **Encrypt password.** Select **Yes** if you want to store passwords used to authenticate users in encrypted form or **No** if password encryption is not required.
- **Guest account.** In this drop-down box, select the system user whose rights will be granted to users logged on under the guest account. If you have no guest account on your server, select the **no guest account** option. If you need a guest account for anonymous users, it is advised that you select the **nobody** option.

For details on the Samba security configuration options, please refer to the relevant Samba documentation.

To refresh data on the current connections to your file server:

Click the  Refresh button on the **Status** tab. The list of current connections and file server status will be refreshed.

Managing Users

On the **Users** tab (**Modules --> File Server --> Users**), you can perform the following actions:

- view a list of users who can have access to the shared directories on your server
- add new users to the list
- edit the user data

You can view users that can have access to the shares on the **Users** tab. All users are listed in a table with the following columns:

Name displays the user's login;

System user shows the system user account this File Server user belongs to;

To add a new user to the list of available users:

- 1 On the **Users** tab, click the **Add New User** button.
- 2 You will be taken to the **Editing user information** page on which you should specify the following parameters:

System user - select the corresponding system user from the drop-down box the new user will belong to

Name - user name (login) that will be used to access a share

Password - password used to access a share

Password confirmation - confirm the password

All these fields are mandatory.

Note: You can add only one File Server user for each Unix system user!

To edit the user data:

- 1 In the list of users on the **Users** tab, click the user name you want to edit.
- 2 You will be taken to the **Editing user information** page that is the same as that for creating a new user. Change the parameters as needed.

- 3 Click OK to apply changes or Cancel to cancel the operation.

Managing Shares

On the **Shares** tab (Modules --> File Server --> Shares), you can perform the following actions:



- view a list of all shared resources
- add new shares
- edit the properties of existing shares

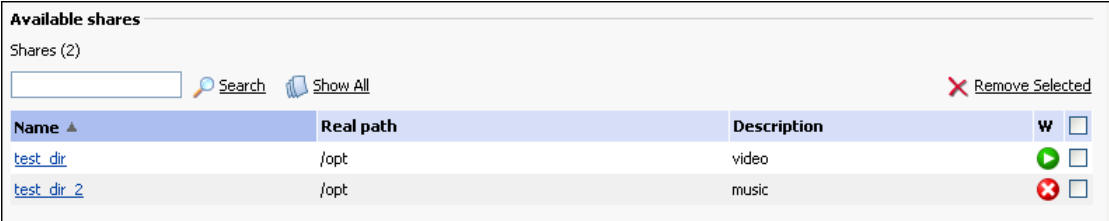
You can view a list of existing shared resources on the **Shares** tab. The list contains the following information about each share:

Name displays the name of the shared resource;

Real path shows the path to the shared resource;

Description contains the description of the shared directory as specified during its creation

(W)rite permissions whether users can add new files to this directory. The  icon means that write permissions are set for this directory. The  icon means that the directory is read-only.





Name ▲	Real path	Description	W
test_dir	/opt	video	 <input type="checkbox"/>
test_dir_2	/opt	music	 <input type="checkbox"/>

Figure 2: List of shared resources

To add a new shared resource:

- 1 Click the **Add New Share** button on the **Shares** tab to open the **Editing properties of the shared directory** page.
- 2 On this page, in the **Preferences** group of fields, enter the name of the shared directory (**Name** field), full path to the directory you want to share (**Real path** field) and its description (**Description** field). If you want to give write permissions on this directory to network users, select the **Writable** check box.
- 3 To select the users that will have access to the shared directory:

Select the **Any user** option button if you want to grant access to the shared directory to all network users;

OR

Select the **Selected only** option button to grant access to the shared directory only to specified users. Select the users that will have access to this directory from the **Available users** list by using the **Add** and **Remove** buttons. If access is allowed for some users, they should specify their login and password to access this folder.

Note: If you want to add other users to the **Available users** list, you must first add them using the **Add New User** button on the **Users** tab. See **Managing Users** (on page 11) on how to add new users.

Click **OK** to apply changes or **Cancel** to cancel the operation.

To edit the properties of a share:

- 1 In the list of shares, click the name of the shared directory you want to edit.
- 2 You will be taken to the **Editing properties of the shared directory** page that is the same as that for creating a new share. Change the necessary parameters.
- 3 Click **OK** to apply changes or **Cancel** to cancel the operation.




Managing Broadcast Interfaces

By default, broadcast mode is disabled for all network interfaces mainly for security reasons. Broadcast mode enables sending data packets to the broadcast address. However, you can manually prevent your File Server from sending broadcast packets to specified network interfaces.


On the **Interface** tab you can:

- View existing network interfaces
- Enable/disable broadcast mode on specific interfaces.



All existing network interfaces are automatically displayed in the list of interfaces on the **Interface** tab. The list is organized as a table with the following columns:

- **(S)tatus** - Icon indicating the status of the network interface. The  icon shows that the broadcast mode for the interface is enabled, the  icon shows that the broadcast mode is disabled for this interface, and the  icon means that broadcast mode for this interface was enabled but now the interface is physically unavailable (was removed or corrupted).
- **Interface name** - Name of the interface, for example, eth0, eth1, etc.
- **IP Addresses** - All IP addresses and subnet addresses that work on this interface.

To enable broadcast mode for an interface:

Click the  icon in the **Status** column of the table listing interfaces. The selected interface will be set to work in broadcast mode.

To disable broadcast mode for an interface:

Click the  or  icons in the **Status** column of the table. Broadcast mode will be switched off for the selected interface.

How to Limit Access to File Server

If you want to enhance the security of your file server, you can regulate what hosts or networks will have access to your shared resources. Connections from other hosts will be refused by your file server. To manage access to your file server, open the **Access** tab.

On the **Access** tab, you can perform the following actions:

- View current access rules
- Add new hosts/networks that will have access to your file server
- Remove hosts/networks or edit their addresses

You can view all hosts and networks that have access to your file server in the table on the **Access** tab. If the list is empty, all hosts can access your file server. This is the default option.

To allow access to your server only from a specific range of hosts:

- 1** On the **Access** tab, click the **Add New Host/Network** button.
- 2** On the **Add host** page that opens, in the **Network/Host address** field, enter the IP address of the host you want to allow access (for example, 123.123.123.1) or the range of hosts (for example, network address/subnet mask written as 123.123.123.0/255.255.255.0).
- 3** Click **OK**.

This will only allow the specified hosts to successfully connect to the shared resources on your file server. All connections from other hosts will be refused by the file server.

If you already have some hosts in the list and want to edit their addresses:

- 1** Click the address of the host in the list of allowed hosts.
- 2** You will be taken to the **Edit host** page on which you can edit the host IP address or subnet mask (for multiple hosts) in the **Network/Host address** field.
- 3** Click **OK** to apply changes.

To remove an address from the list:

- 1** Select the checkbox on the right corresponding to the host address you want to remove and click **Remove all**.
- 2** On the next page, check the box to confirm removal of the selected hosts and click **OK**. To cancel the removal operation, click **Cancel**. If you remove all networks from the list, all hosts will be automatically allowed access to the file server.

Index

A

About This Guide • 5

D

Documentation Conventions • 5

F

Feedback • 6

File Server Interface Basics • 7

G

General Conventions • 6

H

How to Access File Server • 9

How to Configure File Server Preferences • 9

How to Limit Access to File Server • 14

M

Managing Broadcast Interfaces • 13

Managing Shares • 12

Managing Users • 11

P

Preface • 5

T

Typographical Conventions • 5

U

Using Plesk™ File Server • 7