

---

SWsoft, Inc.

# Plesk 7.6 For Windows Reconfigurator

## User's Guide

(Revision 1.1)

**PLESK**

(c) 1999 - 2006

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

*Copyright © 1999-2006 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.*  
*MS Windows, Windows 2003 Server, Windows XP, Windows 2000, Windows NT, Windows 98, and Windows 95*  
*are registered trademarks of Microsoft Corporation.*

---

# Contents

<b>Preface</b>	<b>4</b>
Documentation Conventions.....	4
Typographical Conventions.....	4
Feedback.....	5
<b>Introduction</b>	<b>6</b>
<b>Performing Common Tasks</b>	<b>7</b>
Changing Server IP Addresses.....	8
Moving Virtual Hosts .....	9
Changing Location of Plesk Backup Files.....	10
Changing Location for Storing User Mailboxes .....	11
Repairing Plesk Installation .....	12
Correcting Disk Permissions .....	14
<b>Appendix. Security settings defined during repair</b>	<b>16</b>
Security Settings for Plesk Folders .....	16
Security Settings for Domain Folders.....	17
Security Settings for Domains with Forwarding Hosting .....	20
Security Settings for Subdomain Folders.....	20
Security Settings for Web User Folders.....	24
<b>Glossary</b>	<b>25</b>

---

## CHAPTER 1

# Preface

## In This Chapter

Documentation Conventions.....	4
Typographical Conventions .....	4
Feedback .....	5

---

## 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 <b>QoS</b> tab.
	Titles of chapters, sections, and subsections.	Read the <b>Basic Administration</b> 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> . <code>msiexec /i &lt;name of the aforementioned *.msi file or GUID&gt;</code>
Monospace	The names of commands, files, and directories.	Install Plesk into the "c:\plesk bin" directory
Preformatted	On-screen computer output in your command-line sessions; logs; source code in XML, C++, or other programming languages.	05:31:49 Success. Admin John Smith was added.

---

## 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 that we could find it easily.

Please submit a report by e-mail to [userdocs@swsoft.com](mailto:userdocs@swsoft.com).

---

## CHAPTER 2

# Introduction

Plesk Reconfigurator is a utility designed to assist you with the following tasks:

- Changing IP addresses the Plesk server is running on. This is useful when, for instance, you are moving your Plesk box to a new datacenter, and need to reconfigure Plesk to run on new IP addresses.
- Moving the directory where virtual hosts reside to another location on the same or another partition. This may be useful when there is not enough disk space on the current partition to house new virtual hosts, and you wish to move them all to a new larger volume.
- Moving the directory where Plesk backup files are stored to another location on the same or another partition. This should be used when, for instance, there is not enough disk space on the current partition to house new backup files, and you wish to move them all to a new larger volume.
- Moving the directories that store user mailboxes and all relevant data to another location on the same or another partition. Use this option when there is insufficient amount of disk space on the current partition to serve a larger amount of mailboxes, and you wish to move them all to a new larger volume.
- Repairing Plesk installation. You can use this to correct the problems with mail delivery caused by the changes made to DNS server addresses, restore internal accounts required for proper functioning of Plesk, Plesk services, and set the proper security settings for files and folders created and used by the Plesk software.
- Correcting disk permissions. This option allows correcting root directory permissions in case they are misconfigured and cause improper Plesk functioning.

## CHAPTER 3

# Performing Common Tasks

This chapter describes ways of performing typical tasks with Plesk Reconfigurator.

Plesk Reconfigurator is a standalone Windows application (as opposed to web-browser based ones, e.g. Plesk). You can find it in the Start menu, under the Programs > SWsoft Plesk > Plesk Reconfigurator entry.

The following window opens:



*Figure 1: Plesk Reconfigurator title page*

Each item in the menu corresponds to a task, which can be performed using Plesk Reconfigurator. The following sections describe them in detail.

## In This Chapter

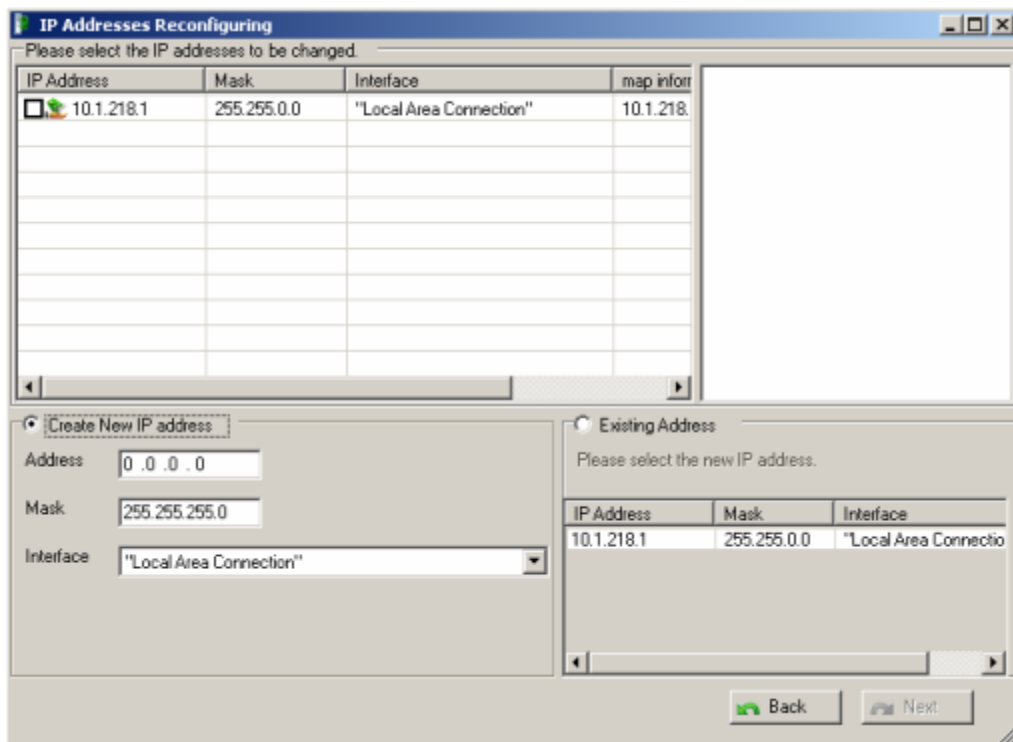
Changing Server IP Addresses.....	8
Moving Virtual Hosts.....	9
Changing Location of Plesk Backup Files .....	10
Changing Location for Storing User Mailboxes .....	11
Repairing Plesk Installation .....	12
Correcting Disk Permissions.....	14

## Changing Server IP Addresses

This option allows you to change IP addresses the Plesk server is running on. This is useful when, for instance, you are moving your Plesk box to a new datacenter, and need to reconfigure Plesk to run on new IP addresses.

To change server's IP address:

- 1 Run Plesk Reconfigurator.
- 2 Select the Change Server IP Addresses option. The following window opens:



*Figure 2: Changing server IP addresses*

- 3 Select the IP address that you wish to change. A list of domains hosted on this IP will be displayed in the window to the right.
- 4 To map the selected IP address to another one, not yet existing on the network interface, select the Create New IP Address option, specify the IP address, network mask, and select the network interface name. To map the selected IP address to another address, already existing on the network interface, select the Map to Existing IP Address option, and select the desired address.
- 5 Click Next. All records in the Plesk database will be updated, network adapters settings will be changed (the old IP addresses will be removed), FTP and WWW servers will be reconfigured, and DNS records will be updated.

If the operation fails due to some reason, all changes are rolled back.

**Note:** When connected to the server via the remote desktop connection, a change of your server's IP address will terminate your session.

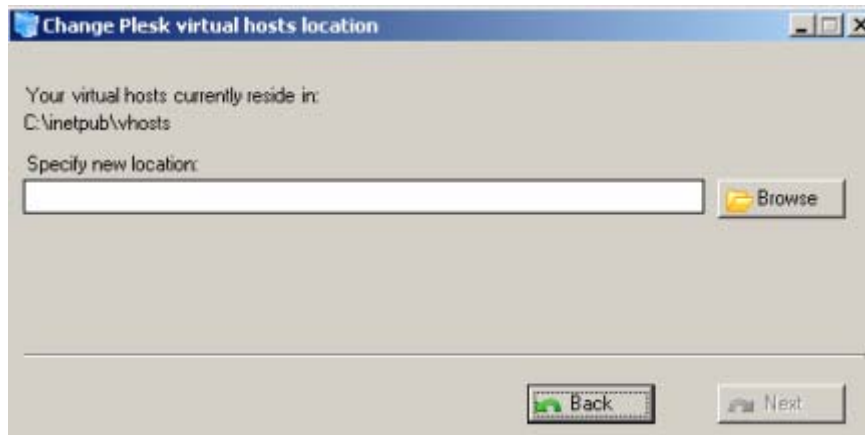
---

## Moving Virtual Hosts

This option allows moving the directory where virtual hosts reside to another location on the same or another partition. This may be useful when there is not enough disk space on the current partition to house new virtual hosts, and you wish to move them all to a new larger volume.

To move the virtual hosts directory:

- 1 Run Plesk Reconfigurator.
- 2 Select the **Change Virtual Hosts location** option. The following window opens:



*Figure 3: Moving virtual hosts*

- 3 Specify the destination directory name. If the directory does not exist, it will be created.
- 4 Click **Next**.

During this operation all Plesk services will be restarted.

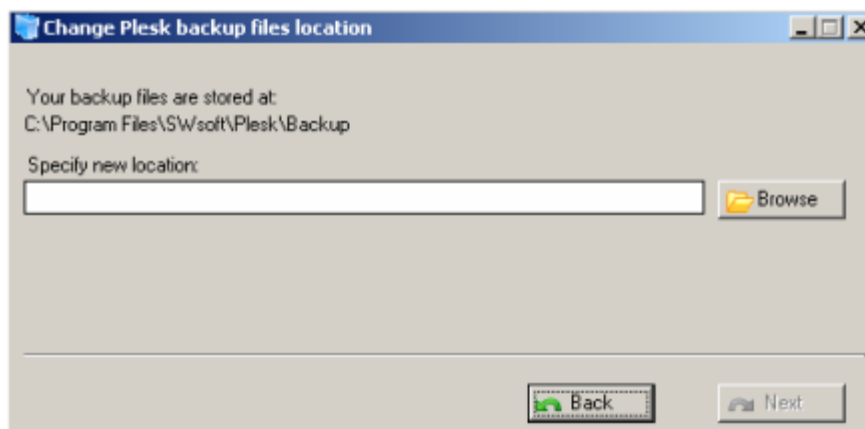
---

## Changing Location of Plesk Backup Files

This option allows moving the directory where Plesk backup files are stored to another location on the same or another partition. This should be used when, for instance, there is not enough disk space on the current partition to house new backup files, and you wish to move them all to a new larger volume.

To move the backup files directory:

- 1 Run Plesk Reconfigurator.
- 2 Select the Change Plesk Backup Data location option. The following window opens:



*Figure 4: Changing location of Plesk backup files*

- 3 Specify the destination directory name. If the directory does not exist, it will be created.
- 4 Click Next.

During this operation all Plesk services will be restarted.

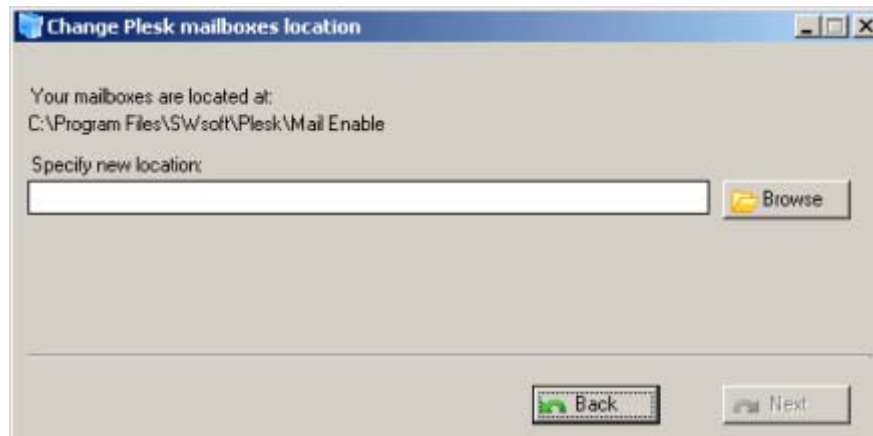
---

## Changing Location for Storing User Mailboxes

This option allows moving the directories that store user mailboxes and all relevant data to another location on the same or another partition. Use this option when there is insufficient amount of disk space on the current partition to serve a larger amount of mailboxes, and you wish to move them all to a new larger volume.

To move the user mailboxes directories:

- 1 Run Plesk Reconfigurator.
- 2 Select the Change Plesk Mail Data location option. The following window opens:



*Figure 5: Changing location for storing user mailboxes*

- 3 Specify the destination directory name. If the directory does not exist, it will be created.
- 4 Click Next.

During this operation Plesk mail and control panel services will be restarted.

## Repairing Plesk Installation

This option allows repairing Plesk installation. Use it to correct the problems with mail delivery caused by the changes made to DNS server addresses, restore internal accounts required for proper functioning of Plesk, Plesk services, and set the proper security settings for files and folders created and used by the Plesk software as well as user quotas.

To repair Plesk installation:

- 1 Run Plesk Reconfigurator.
- 2 Select the Repair Plesk installation option. The following window opens:

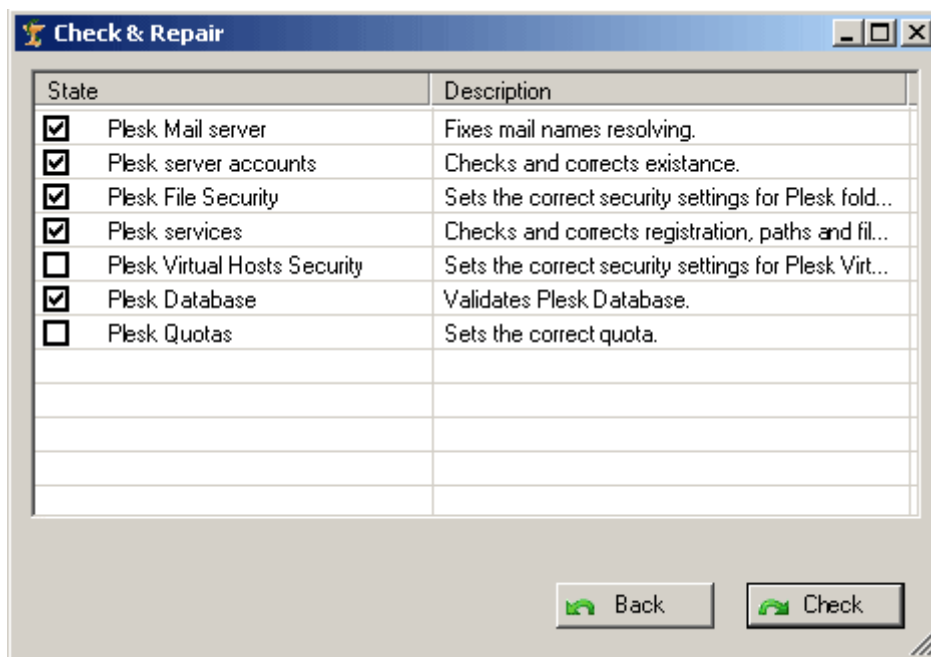


Figure 6: Repairing Plesk installation

- 3 Select the check boxes corresponding to repairing actions you want to perform. See the table below for explanation of each option.
- 4 Click **Check**. Plesk Reconfigurator corrects the problems with mail delivery caused by the changes made to DNS server addresses, restores internal accounts required for proper functioning of Plesk, Plesk services, and sets the proper security settings for files and folders created and used by the Plesk software as well as user quotas.

**Table 1. Check & Repair options**

Option	What is done
Plesk Mail Server	DNS settings from network adapter(s) are applied to the mail server used in Plesk ; localhost network name is added to relay list.

<p>Plesk Server Accounts</p>	<p>During the full repair, Plesk Reconfigurator determines whether there are users "psaadm", "tomcat4", and "ASPNET", and groups "psacln" and "psaserv", and creates them if they are not present. Members of the psaserv group are restored while that of the psacln group are not. It also ensures that the psaserv group includes the accounts: "ASPNET", "LOCAL SERVICE", "NETWORK SERVICE", and "IUSR_&lt;computer name&gt;" (Internet Guest Account).</p> <p>The Reconfigurator utility also checks Plesk's system accounts (including Internet accounts for anonymous access to domains) and IIS settings for anonymous domain access.</p>
<p>Plesk File Security</p>	<p>Plesk Reconfigurator checks permissions for folders %plesk_dir%, %SystemRoot%\temp, %plesk_vhosts%, %plesk_vhosts%\default, %plesk_vhosts%\sqladmin, %plesk_vhosts%\webmail, %plesk_vhosts%\skel. Also, for folders %plesk_dir%, %SystemRoot%\temp permissions for their content are checked.</p>
<p>Plesk Services</p>	<p>For each service, the Reconfigurator attempts to detect and correct the path to its binary file and account under which it is started. All unregistered services are properly registered with the determined paths. All inactive services are started, and have the startup type changed to Automatic. If the Bind service is disabled via Plesk control panel and is not registered in the system, it does not get registered, and if it is running, the Reconfigurator stops it and changes its startup type to Disabled. It also ensures that the Plesk control panel service logs on as "psaadm".</p>
<p>Plesk Virtual Hosts Security</p>	<p>The utility checks if a discretionary access control list (DACL) of an object includes all the necessary security identifiers (SID), and if it does not, an object DACL is overwritten, but if it does – the Reconfigurator checks if there are no Deny type access control entries (ACE) different from those set by Plesk. It also checks if DACL includes all the necessary ACEs (their access rights are not checked), and if it does, all Deny type access control entries different from those set by Plesk and all unresolved SIDs are removed from the DACL, and a DACL is merged with the proper one set by Plesk. See Appendix (see page 16) for the detailed description of what is checked.</p> <p>Also, Reconfigurator restores host structure and recreates removed users and groups along with checking that they belong to correct groups.</p>
<p>Plesk Database</p>	<p>Plesk Reconfigurator cleans the Repository table of inner Plesk database. Also, it checks application vaults' state.</p>
<p>Plesk Quotas</p>	<p>Plesk Reconfigurator checks that files in domain folders belong to domain, subdomain or web user of the corresponding domain (if they belong to someone else, Plesk may report wrong disk space quota usage)</p>

## Correcting Disk Permissions

This option allows correcting root directory permissions in case they are misconfigured and cause improper Plesk functioning (e.g. they prohibit Plesk to run its utilities with the necessary permissions).

To correct the root disk permissions:

- 1 Run Plesk Reconfigurator.
- 2 Select the Correct disk permissions option. The following window opens:

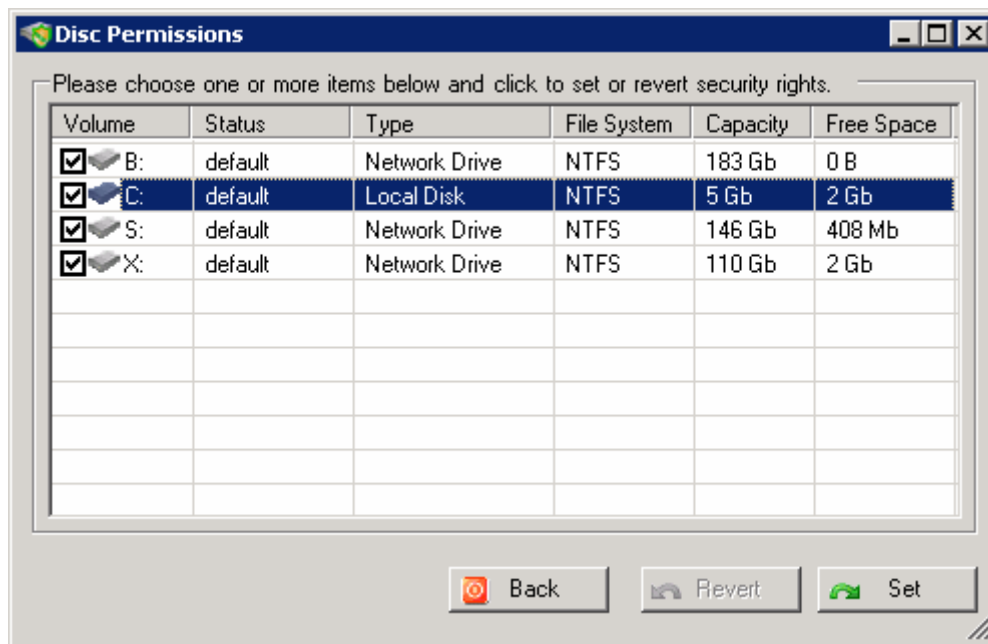


Figure 7: Setting root disk permissions page

- 3 Using check boxes in the **Volume** column, select the drives for which you wish to correct permissions.
- 4 Click **Set** to set the correct permissions for the selected drives. This operation may take some time.

The permissions for the following groups of users are set this way:

- Administrators - full control over this folder, subfolders and files.
- SYSTEM - full control over this folder, subfolders and files.
- Everyone - read and execute permission for this folder only.

If you set permissions with Plesk Reconfigurator and the results do not satisfy you, you can go back to the original settings. To do this, repeat the aforementioned procedure but press **Revert** instead of **Set**.



## CHAPTER 4

# Appendix. Security settings defined during repair

The following sections present tables that contain information on security settings Plesk Reconfigurator uses for restoring your Plesk installation.

## In This Chapter

Security Settings for Plesk Folders .....	16
Security Settings for Domain Folders .....	17
Security Settings for Domains with Forwarding Hosting .....	20
Security Settings for Subdomain Folders.....	20
Security Settings for Web User Folders.....	24

---

## Security Settings for Plesk Folders

The following security settings are defined for Plesk folders:

Path	Account	Access
%PLESK_DIR%	System	Full Control
	Administrators	Full Control
	Psaadm	Read & Execute
%PLESK_VHOSTS% (include only these subfolders: .skel, default, sqladmin, webmail)	System	Full Control
	Administrators	Full Control
	Psacln	Read & Execute
	Psaserv	Read & Execute
%PLESK_DIR%\var\cgitory	Psaadm	Read & Execute
	Psacln	Read & Execute
%PLESK_DIR%\tmp	Psaadm	Full Control
	Psacln	Read & Execute
%PLESK_DIR%\admin\sessions	Psaadm	Full Control
%PLESK_DIR%\admin\logs	Psaadm	Full Control
%PLESK_DIR%\admin\conf	Psaadm	Full Control
%PLESK_VHOSTS%\ .skel	Psaadm	Full Control
%PLESK_DIR%\admin\bin	Psacln	Read & Execute

<MySQL folder>	PsacIn	Read & Execute
%systemroot%\temp	System	Full Control
	Administrators	Full Control
	Network service	Read Data & Delete
	PsacIn	Read & Execute
	Psaserv	Read & Execute
%PLESK_DIR%\etc	Psaserv	Read & Execute

## Security Settings for Domain Folders

The following security settings are defined for domain folders:

Path	Type	Name	Permissions	Objects
<domain.name>	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		<FTP/FrontPage user>	Read	Files only
			Read & Execute	Directories only
<domain.name>\httpdocs	Allow	System	Full control	
		Administrators	Full control	
		IUSR_<domain user>	Read	Files only
			Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	
Full control			Subfolders and files	
<domain.name>\httpdocs\picture_library	Deny	<FTP/FrontPage user>	Write Attributes, Write Extended Attributes, Delete Folder & Files, Change Permissions	This folder
			Allow	System
	Allow	Administrators	Full control	This folder, subfolders and files
		IUSR_<domain user>	Read	Files only

		user>	Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
		Psaadm	Read	Files only
			Read & Execute	Directories only
<domain.name>\cgi-bin	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		IUSR_<domain user>	Read & Execute	This folder, subfolders and files
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
Full control	Subfolders and files			
<domain.name>\private	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended	This folder
			Full control	Subfolders and files
<domain.name>\vault_scripts	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		psaadm	Read	Files only
			Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files

<domain.name>\anon_ftp	Allow	System	Full control	This folder, subfolders and files		
		Administrators	Full control	This folder, subfolders and files		
		<FTP/FrontPage user>	Read	Files only		
			Read & Execute	Directories only		
<domain.name>\anon_ftp\pub & <domain.name>\anon_ftp\incoming	Allow	System	Full control	This folder, subfolders and files		
		Administrators	Full control	This folder, subfolders and files		
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder		
			Full control	Subfolders and files		
<domain.name>\error_docs, <domain.name>\statistics, <domain.name>\statistics\webstat, <domain.name>\statistics\ftpstat & <domain.name>\statistics\anon_ftpstat	Allow	System	Full control	This folder, subfolders and files		
		Administrators	Full control	This folder, subfolders and files		
		IUSR_<domain user>	Read	Files only		
			Read & Execute	Directories only		
		<FTP/FrontPage user>	Read	Files only		
			Read & Execute	Directories only		
		<domain.name>\webusers & <domain.name>\subdomains	Allow	System	Full control	This folder, subfolders and files
				Administrators	Full control	This folder, subfolders and files
<FTP/FrontPage user>	Read			Files only		
	Read & Execute			Directories only		
\<domain.name>\statistics\logs	Allow	System	Full control	This folder, subfolders and files		
		Administrators	Full control	This folder, subfolders and files		
		IUSR_<domain user>	Read	Files only		
			Read & Execute	Directories only		
		<FTP/FrontPage user>	Read	Files only		

		user>	Read & Execute	Directories only
		Psaadm	Read	Files only
			Read & Execute	Directories only

---

## Security Settings for Domains with Forwarding Hosting

The following security settings are defined for the domains that are on forwarding hosting:

Path	Type	Name	Permissions	Objects
<domain.name> , <domain.name>\httpdocs , <domain.name>\statistics <domain.name>\statistics\logs	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		psaserv	Read	Files only
			Read & Execute	Directories only

---

## Security Settings for Subdomain Folders

The following security settings are defined for the subdomain folders:

Path	Type	Name	Permissions	Objects
<subdomain.name>	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		<FTP/FrontPage user>	Read	Files only
			Read & Execute	Directories only
		<subdomain user>	Read	Files only
			Read & Execute	Directories only

<subdomain.name>\httpdocs	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		IUSR_<domain user>	Read	Files only
			Read & Execute	Directories only
		IUSR_<subdomain user>	Read	Files only
			Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
		<subdomain user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
<subdomain.name>\cgi-bin	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		IUSR_<domain user>	Read & Execute	This folder, subfolders and files
		IUSR_<subdomain user>	Read & Execute	This folder, subfolders and files

		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
		<subdomain user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
<domain.name>\private	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files

		<subdomain user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
<domain.name>\vault_scripts	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		psaadm	Read	Files only
			Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
		<subdomain user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder

			Full control	Subfolders and files
--	--	--	--------------	----------------------

## Security Settings for Web User Folders

The following security settings are defined for the web users' folders:

Path	Type	Name	Permissions	Objects
<webuser.name>	Allow	System	Full control	This folder, subfolders and files
		Administrators	Full control	This folder, subfolders and files
		IUSR_<domain user>	Read	Files only
			Read & Execute	Directories only
		IUSR_<webuser>	Read	Files only
			Read & Execute	Directories only
		<FTP/FrontPage user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files
		<web user>	Traverse Folder, List Folder, Read Attributes, Read Extended Attributes, Create Files and Folders, Read Permissions	This folder
			Full control	Subfolders and files

## CHAPTER 5

# Glossary

*DACL (Discretionary Access Control List)*

Part of the security descriptor for an object. The DACL can be applied to a newly created object in order to restrict access to the object.

*ACE (Access Control Entry)*

An individual entry in an access control list (ACL). An access control entry (ACE) contains an SID and describes the access rights to a system resource by a specific user or group of users. Each object has a set of all ACEs, which is used to determine whether an access request to the object is granted.

*SID (Security Identifier)*

A value, unique across time and space, that identifies a process in the security system. SIDs can either identify an individual process, usually containing a user's logon identifier, or a group of processes.

*ACL (Access Control List)*

An ordered list of access control entries (ACEs).

*ACCESS RIGHT*

A permission granted to a process to manipulate a specified object in a particular way (by calling a system service). Different system object types support different access rights, which are stored in an object's access control list (ACL).

*SECURITY DESCRIPTOR*

A data structure used to hold per-object security information, including the object's owner, group, protection attributes, and audit information.