



---

4PSA Central Login 1.2.0  
for Plesk 7.x Reloaded  
User's Guide

Manual Version 0.22

For suggestions regarding this manual contact:

[docs@4psa.com](mailto:docs@4psa.com)

© Copyrights 2002 – 2005 Rack-Soft, LLC. All rights reserved

Distribution of this work or derivative of this work is prohibited unless prior written permissions is obtained from the copyright holder.

Plesk is a Registered Trademark of SWsoft, Inc.

Linux is a Registered Trademark of Linus Torvalds.

RedHat is a Registered Trademark of Red Hat Software, Inc.

FreeBSD is a Registered Trademark of FreeBSD, Inc.

All other trademarks and copyrights are the property of their respective owners.

## Table of Contents

<b>Chapter 1. About 4PSA Central Login 1.2.0 .....</b>	<b>4</b>
1. 4PSA Central Login 1.2.0 Features .....	4
<b>Chapter 2. The Administration Module.....</b>	<b>5</b>
1. Login History .....	5
Search Login Logs.....	5
History Results .....	5
2. Servers Management .....	6
Adding a New Server.....	6
Deleting a Server.....	8
Editing a Server.....	8
3. Settings .....	8
4PSA Central Login Reports.....	8
Login Settings .....	8
Language Settings .....	9
<b>Chapter 3. The Authentication Module.....</b>	<b>9</b>
1. Installing the Authentication Module.....	9
2. Customizing the Authentication Module.....	10
Modifying the index.php File .....	11
Modifying the forgot_index.php File .....	11
3. Language Settings for the Authentication Module .....	11
<b>Appendix A. Server Compatibility.....</b>	<b>13</b>

## Chapter 1. About 4PSA Central Login 1.2.0

4PSA Central Login 1.2.0 is a server-level application that provides a single login interface to multiple Plesk servers owned by a business. The application consists of a single administrator-only module that deals with general product administration, **monitoring and logging login attempts**, and a fully customizable authentication module for Plesk servers.

### 4PSA Central Login 1.2.0 Features

4PSA Central Login 1.2.0 offers the following features:

- Plesk integrated
- Works with all account types (client, domain user, mail user)
- Clients can login to any Plesk server directly from your business web page
- Servers and logins management interface
- Works with all types of Plesk servers
- Provides full logs history
- All input forms/pages are fully editable!
- Forget password support for all accounts types
- Implements timeout and attempt features (Plesk like)
- Works with servers located in multiple data centers
- Configurable to deny the admin login
- No server selection necessary
- Tested with over 35 production servers simultaneously
- Language packs capabilities

## Chapter 2. The Administration Module

The 4PSA Central Login administration module can be accessed after you login to Plesk 7.x Reloaded using the admin account. In order to open the 4PSA Central Login interface click the [4PSA Central Login](#) link available in the Custom navigation menu located on the left side of the Plesk interface.

The 4PSA Central Login tool bar is available on top of the application's interface. The tool bar provides an easy method for the server administrator to view a detailed history of the login attempts, manage servers, view a report about 4PSA Central Login, modify login options and change language settings.

### 1. Login History

4PSA Central Login keeps records of all the login attempts performed through the central authentication area in its database.

In this area (click the **Logs** button available in the tool bar) the records provide detailed information about the login attempts and can be displayed based on the chosen search criteria.

#### Search Login Logs

In this area the server administrator can search the login logs and choose the search criteria. The following criteria are available:

**From** and **To** - Search for log records between two dates in year-month-day format

**Outcome** - Search for logs with a specified result, which can be success or failure

**Show** - Limit the number of results to view in one page

#### History Results

Based on the chosen search criteria, 4PSA Central Login displays the logs that matched these criteria. Every log entry consists of five fields:

**Login** - The login name used in the login attempt by the client

**Client IP address** - The IP address of the machine the client attempted to login from

**Server IP address** - If the login attempt was successful, this is the IP address of the server on which the user has logged in

**Date** - The system date and time when the login attempt occurred (day month year, hh:mm:ss)

**Outcome** - The outcome of the login attempt, which can be success or failure  
The log records can be sorted by login name, client IP address, server IP address, date, and outcome by clicking the table header links.

In order to update the window with the latest logged records, click the [Refresh](#) link. In order to clear all log history records, click the [Clear history](#) link.

## 2. Servers Management

In this area (click the **Servers** button available in the tool bar) the server administrator can add new servers to the 4PSA Central Login database, modify the details for a particular server or delete servers from the application's database.

The server administrator can view a list of all managed servers. For every server the following details are available:

 - By clicking this icon, 4PSA Central Login will display a connectivity report for the chosen server. This report contains the following information:

**Server IP address** - The IP address of the server

**Connection status** - Information about the test connection to this server which means that a test connection could or could not be established

**Hint** - This field is available only if a test connection could not be established to the server. 4PSA Central Login displays several reasons that may cause the error in connection and what to do in order to establish a connection.

**Hostname** - The hostname of the server

**Server IP address** - The IP address of the remote server

**OS** - The operating system installed on the remote server

**Plesk version** - The version of the Plesk software installed on the remote server. Chose correctly the Plesk version installed on the remote server, otherwise the login functions may not work.

### Adding a New Server

Adding a new server to the 4PSA Central Login system is an operation that implies two steps. First you have to enter server parameters in the Server Management area. The second step is to allow MySQL connections on the remote server from the central login server.

To add a new server, you must provide the following details in the Server Management area:

**Hostname** - The name of the server you want to add to 4PSA Central Login

**Server IP Address** - The IP address of the server you want to add to 4PSA Central Login

**Administrator's password** - The password of the administrator account ("admin") on the server you want to add to 4PSA Central Login

**OS** - The operating system of the remote server

**Plesk version** - The Plesk version installed on the remote server. Choose correctly the Plesk version installed on the remote server, otherwise the login functions may not work.

After providing these details, click the **Add** button and the new server will be added to the 4PSA Central Login servers list.

The next step is to allow MySQL connections on the remote server from the central login server. In order to do this, copy the `clogin.sh` shell script on the remote machine, then run the following command in your favorite shell:

```
# sh path_to_clogin_sh/clogin.sh
```



#### Note

You must run the `clogin.sh` shell script logged in as "**root**".

You will be prompted for the IP address of the Central Login server, and after you enter this address the process will continue automatically.

The process of adding a new server is completed. Users will now be able to log in on that server using the 4PSA Central Login system.

In order to add a Windows Plesk server to Central Login system, you have to execute the `clogin.exe` script.



#### Note

Both scripts are available in the Central Login installation archive, in the same directory with `install.sh`.

### Deleting a Server

To delete a server from the list, check the corresponding checkbox on the chosen server row and click the [Remove Selected](#) link. The server administrator can delete multiple servers at the same time.

### Editing a Server

The server administrator can modify the information available for existing servers. In order to edit these details, click the chosen server hostname in the list. In the new page that will open the following server details can be modified: the hostname, the IP address, the administrator's password, the operating system, and the Plesk version.

To save the changes, click the **Update** button. To return to the previous page without saving it, click the [Up Level](#) link.

## 3. Settings

In this area (click the **Settings** button available in the tool bar) the server administrator can view a report about 4PSA Central Login, modify login options and change language settings.



#### Note

Before running 4PSA Central Login for the first time you must adjust these settings.

### 4PSA Central Login Reports

In this area the server administrator can view which version of the 4PSA Central Login is installed on the server.

### Login Settings

In this area the server administrator can control several important parameters of the 4PSA Central Login system.

**Allow admin login** - If enabled, the system will accept "admin" as a valid login name. If disabled, the user "admin" will not be allowed to log in through the 4PSA Central Login system.

**Invalid login attempts** – This field displays the maximum number of invalid login attempts allowed. Once a user has exceeded this value he is locked out for the time specified in the **Invalid login lock time** field.

**Invalid login lock time** – This is the lockout time (in minutes) for an user once the invalid login attempts counter has reached its maximum limit. Upon completion of the lockout time the invalid login attempts counter is reset and the user is again allowed to login to the Plesk server.

### Language Settings

The **Language** option allows the server administrator to select the language that will be used by 4PSA Central Login's interface.

## Chapter 3. The Authentication Module

The Authentication module controls the central login process. This module includes the central login interface which is used by hosting clients.

The Authentication module is packed as a separate archive in your 4PSA Central Login distribution and it has to be installed separately on the hosting company website. The form files (files visible to clients in the login process) can be modified to fit into the hosting company's website design.

### 1. Installing the Authentication Module

In order to install the Authentication module you have to unpack its archive in the SSL web files directory of the domain that will hold the central login interface. The Authentication module **must be installed on the same server** on which you have installed the Administration module. In order to do this, you must follow the steps detailed below:

1. Unpack the Authentication module archive by running the following command in your favorite shell

```
# tar -zxvf central_form.tar.gz
```

This will extract the contents of the archive into the current directory.

2. In your favorite editor open the file `read.php` from the **admin** directory and locate the line

```
$database_password = 'my_psa_password';
```

Replace the text `my_psa_password` with the password used to connect to the **psa** database (the password for the “admin” user on the server where the Authentication module will be installed).



#### Note

The steps above can be performed in Microsoft Windows as well on your local computer. Please note that commands are for \*nix only.

3. Using a FTP client upload the module files and directories to the preferred `installation_directory` on your server.

The Authentication module is installed and can be accessed at `https://domain_name/installation_directory/index.php`. You will find details below on how to customize the Authentication module files in order to include the login form directly on your website page.

## 2. Customizing the Authentication Module

The Authentication module is fully customizable and allows you to change the central login interface based on your preferences.



#### Note

Customizing the central login interface requires basic HTML knowledge.

In order to create a custom login interface you will have to modify two files from the Authentication module: `index.php` and `forgot_index.php`.

### Modifying the index.php File

This file controls the central login interface. The interface layout is entirely customizable based on your preferences. However the following restrictions apply to the HTML code:

The **action** property of the main login form must be `process.php`

The **method** property of the main login form must be `POST`

The **name** property of the Login input field must be `uname`

The **name** property of the Password input field must be `pass`

As you can see, you can create an entirely new page as long as it sends the `uname` and `pass` parameters to `process.php` using the `POST` method.

### Modifying the forgot\_index.php File

This file controls the interface for retrieving lost passwords by e-mail. The interface layout is entirely customizable based on your preferences. However the following restrictions apply to the HTML code:

The **action** of the password retrieval form must be `forgot.php`

The **method** property of the password retrieval form must be `POST`

The **name** property of the Login input field must be `uname`

The **name** property of the E-mail input field must be `email`

As you can see, you can create an entirely new page as long as it sends the `uname` and `email` parameters to `forgot.php` using the `POST` method.

## 3. Language Settings for the Authentication Module

The language for the Authentication module is controlled through the `language.php` file located in the **admin** directory of this module. In order to change the language for the Authentication module you will have to follow these steps:

1. In your favorite editor open the `language.php` file located in the **admin** directory of the Authentication module.
2. Translate the English text that appears on the right side of the equal sign (=) between single quotes (') into the desired language.



### Note

If the translated text contains single quotes (') they must be escaped by placing a backslash (\) in front of them, like in the example below:

'Don\'t forget to escape single quotes in the translated text.'

The field `{hostname}` will be automatically replaced by context-sensitive information. Deleting or even changing this field will result in incomplete phrases being displayed in the interface and may cause undesired operation.

The `language.php` file is a PHP file so it must follow the syntax rules of the PHP programming language.

## Appendix A. Server Compatibility

4PSA Central Login for Plesk 7.x Reloaded is compatible with Plesk 7.x Reloaded installations only.

You have to download the build based on the operating system installed on your machine.

The file `central_login_buildXXX_Plesk7x.tar.gz` provides compatibility with the following operating systems:

- RedHat Linux 7.3
- RedHat Linux 9
- RedHat Enterprise Linux 2.1
- RedHat Enterprise Linux 3.0
- RedHat Enterprise Linux 4.0
- Fedora Linux Core 1
- Fedora Linux Core 2
- Fedora Linux Core 3
- FreeBSD 4.8
- FreeBSD 4.9
- FreeBSD 5.2.1
- FreeBSD 5.3
- Suse 9
- Suse 9.1
- Mandrake 10
- Debian 3.1

Using the Plesk 7.x version of 4PSA Central Login you will be able to connect to any Plesk 5, Plesk 6, Plesk 6.5, Plesk 7, Plesk 7 Reloaded and Plesk 7.5 Reloaded server on the market.