CLOUD CALLING™

VOIPNOW® PROFESSIONAL

4PSA Central Login 3.0.0

for Plesk 10.0.0 and newer versions

User's Guide

For more information about 4PSA Central Login, check:
http://www.4psa.com

User's Guide

Manual Version 84829.9 at 2008/12/04 18:27:57

For suggestions regarding this manual contact:

docs@4psa.com

Table of Contents

Preface 4

Who Should Read This Guide 4

Chapter 1. The Administration Module 5

Login History 5
- Searching Logs 5
- History Results 6

Servers Management 6
- Adding a New Server 7
- Deleting a Server 8
- Editing a Server 8

Settings 9
- 4PSA Central Login Reports 9
- Login Settings 9
- Language Settings 9

License Management 10

Chapter 2. The Authentication Module 12

Installing the Authentication Module 12

Customizing the Authentication Module 13
- Modifying the index.php File 13
- Modifying the forgot_index.php File 14

Language Settings for the Authentication Module 14

Chapter 3. Contact and Support 15

Preface

Who Should Read This Guide

This User's Guide must be read by the administrator of the Plesk server infrastructure.

Chapter 1

The Administration Module

The 4PSA Central Login administrator module can be accessed by logging in the Plesk with the admin account. To access the 4PSA Central Login interface, in the Custom navigation menu click the 4PSA Central Login link.

The 4PSA Central Login toolbar is available on top of the application's interface. The toolbar makes it easy for the server administrator to perform the following operations:

- View a detailed history of the login attempts.
- Manage servers.
- View a report on 4PSA Central Login.
- Modify login options.
- Change the language settings.

Login History

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

In this area, you can find detailed information regarding the login attempts. You can use the available search criteria to view only certain records. To access this area, click the Logs tab.

Searching Logs

In this section, the server administrator can search the login logs using the following criteria:

- From and To - Search for log records between two dates (in year/month/day format).
- Outcome - Search for logs with a specified result. The available options in this drop-down list are:
  - Success - For successful logins.
  - Failed - For failed login attempts.
  - Don't care - Select this option if you do not want to use this parameter to influence the search results.
- Show - The number of results displayed in one page.

History Results

Based on the search criteria you provided, 4PSA Central Login displays the logs that matched these criteria. For every log in the list, the following information is available:

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

Servers Management

In this area, 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.

To access this section, click the Servers button available in the toolbar.

The server administrator is able to view a list of all the managed servers. For every server in the list, the following information is displayed:

- - 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 - It shows if a connection could or could not be established with the server.
  - 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 have caused the connection error and the options available for establishing 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

To add a new server to the 4PSA Central Login system, follow these steps:

1. In the Server Management area, fill in the server details:
   - 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.
   - Use MySQL encryption - Enable if you want to connect to the server using SSL. You must run PHP 5 or newer on the server and the remote server MySQL must be compiled with OpenSSL support.
   - MySQL password – The password used by the 'admin' account to login at MySQL on the server you want to add to 4PSA Central Login.

     Note

     To obtain the MySQL password, please follow these steps:

     a. Log in as root to the server you want to add to 4PSA Central Login using your favorite SSH console (e.g.: Putty).

     b. Run this command:

     ```
     cat /etc/psa/.psa.shadow
     ```

     c. The string returned by the previous command is the MySQL password that you should use in **MySQL password** field.

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

- Plesk admin interface runs on port - If this server Plesk administrator interface runs on a different port, change this setting.

2. Click the Add button to add the new server to the 4PSA Central Login servers list.
3. Allow MySQL connections on the remote server from the central login server. 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 first log in as root in order to run the clogin.sh shell script.

4. You will be prompted for the IP address of the Central Login server. Enter this address and the process will continue automatically.

After the process of adding a new server is completed, users will be able to log in to 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, select the check box corresponding to the respective server 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. To edit these details, follow these steps:

1. In the servers list, click the server hostname link. A new page opens allowing you to modify: the hostname, the IP address, the administrator's password, the operating system, and the Plesk version.

2. To save the changes, click the Update button. To return to the previous page without saving it, click the Up Level link.

Settings

In this area, the server administrator is able to view a report on 4PSA Central Login, modify login options and change language settings.

To access this section, click the Settings button available in the toolbar.

Note

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

4PSA Central Login Reports

In this section, the server administrator is able to view which version of the 4PSA Central Login is installed on the server.

Login Settings

In this section, 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 admin user 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 a user who exceeded the maximum number of login attempts. Upon completion of the lockout time, the invalid login attempts counter is reset and the user is allowed to login to the Plesk server.

Language Settings

Language - Here, all installed language packs are displayed. The interface will use the language pack setup in your account preference in Plesk. If this

language pack is not available, the system will use English as default. You can use only languages that have been installed in the Plesk interface.

License Management

In this area, you can manage the 4PSA Central Login license. The product requires a license key in order to work. The license key will be generated by 4PSA based on the server IP and Plesk version installed on the server.

You can use the following fields and controls to update or monitor your license:

- License key status
  - Your server IP - This is the main IP address of your server. The license key must be specifically issued for this IP otherwise it will not work.
  - License key status - The status of the currently loaded license key.
- Upload license key
  - License file - You can use this form to upload the license key to the server.

> **Note**
>
> If you can access other pages in 4PSA Central Login, this means that your license is valid and you do not have to upload a new one.

- Get license key from licensing server - This form can be used to query the licensing server, using the activation code for your license key This function can only be used when there is a license key loaded on the server. The first time you install the product you will be required to upload the license key.
- License by activation code - This form can be used to query the licensing server, using the activation code of your license key.
- License key properties - This section contains details about the current license.
  - Key number - The number of the license key.
  - Key ownership - The type of the license key ownership.
  - Maximum number of domains - The maximum number of allowed domains.
  - License key must autorenew before - The date when the license key expires and must be renewed.

- Key renewed on - Last key renewal date

Note

The Owned and Leased licenses automatically renew before the **License expire date**.

Chapter 2

The Authentication Module

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

The Authentication module is packed as a separate archive in your 4PSA Central Login distribution and it must 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.

Installing the Authentication Module

To install the Authentication module, you must 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. To do this, follow the steps detailed below:

1. Log in as root to the server where 4PSA Central Login is installed using your favorite SSH console(e.g. Putty).
2. Unpack the Authentication module archive by running the following command in your favorite shell:

   ```
   #> cp /usr/local/clogin/central_form.tar.gz \/var/www/vhosts/domain_name/httpsdocs

   #> cd /var/www/vhosts/domain_name/httpsdocs

   #> tar -zxf central_form.tar.gz
   ```

3. Find the mysql password. To do this, please type:

   ```
   #> cat /etc/psa/.psa.shadow
   ```

   Your password will be displayed on the screen as follows:

   ```
   #> cat /etc/psa/.psa.shadow

   pjieIw0W57c=
   ```

   The password in our example is:

   ```
   pjieIw0W57c=
   ```

4. In your favorite text editor, open the file config.php from the admin directory (e.g. /var/www/vhosts/domain_name/httpsdocs/admin/config.php) and locate the line:

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

5. Replace the my_psa_password with the password used to connect to the 4PSA database (the password from the command cat /etc/psa/.psa.shadow).

> **Note**
>
> The steps above can also be performed in Microsoft Windows on your local computer. Please note that commands above are for Unix only.

6. The Authentication module is now installed and can be accessed at

   `https://domain_name/clogin_interface/index.php`

Customizing the Authentication Module

This section offers you details on how to customize the Authentication module files in order to include the login form directly on your website page. 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.

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 the `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 the email parameters to forgot.php using the POST method.

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. To change the language for the Authentication module, follow these steps:

1. In your favorite text 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

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

If the translated text contains single quotes (') you must add a backslash (\), 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 operations.

Chapter 3

Contact and Support

For online help and support please visit:

- Support Zone: https://help.4psa.com
- Knowledge Base: http://kb.4psa.com
- Documentation: http://help.4psa.com/docs/

For mailing addresses and phone numbers from our offices:

http://www.4psa.com/contactus

If you have any question, do not hesitate to contact us.