

Panda  
**ManagedOfficeProtection**

Basic Administration Guide  
Service Provider Console



<b>Introduction</b> .....	<b>3</b>
<b>Information, inquiries and services</b> .....	<b>4</b>
Useful links .....	4
<b>Chapter 1. Service Providers Web Console</b> .....	<b>5</b>
To access the console.....	5
Preferences .....	5
Default view.....	5
Remote connection for support.....	5
<b>Chapter 2. Client groups</b> .....	<b>6</b>
How to create a client group.....	6
<b>Chapter 3. Users and permissions</b> .....	<b>8</b>
How to create new users.....	8
Types of permissions .....	9
<b>Chapter 4. Language settings</b> .....	<b>10</b>
<b>Chapter 5. Status</b> .....	<b>11</b>
Protection status .....	11
Export the list of clients.....	12
Error details.....	12
Export the list of errors.....	13
License management.....	13
Licenses used .....	13
License expiry date .....	13
<b>Chapter 6. Updates</b> .....	<b>14</b>
<b>Chapter 7. Reports</b> .....	<b>15</b>
Types of reports .....	15
Sending reports.....	15

---

## Copyright notice

© Panda Security 2009. All rights reserved.

Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, C/ Gran Vía Don Diego Lopez de Haro 4, 48001 Bilbao (Vizcaya) SPAIN.

## Trademarks

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other product names may be registered trademarks of their respective companies.

© Panda Security 2009. All rights reserved.  
0309-PMOP-503

## Introduction

Protecting IT networks against malware and all other Internet threats means companies have to spend a lot of time and resources to deploy, install and manage security on computers.

Panda Managed Office Protection (PMOP) has brought about a drastic change in this situation as it allows the protection to be configured and installed online and be complemented with in-depth, constant monitoring of the IT network.

In fact, the user is the cornerstone of PMOP. Each user is assigned groups of clients. Depending on the permissions assigned to them, users can manage their groups to a greater or lesser extent. Groups are made up of clients, and these, in turn, have a series of computers the protection is installed on. Finally, a protection profile is applied to each computer.

Security management is centered around the Service Providers Web Console, which is structured into six areas:

- Status: shows basic information about clients
- Client groups: allows clients to be organized into groups.
- Users: allows users to be created managed and assigned permissions.
- Settings: where the language of the protection can be configured.
- Updates: for managing the automatic updates of clients' protection.
- Reports: You can generate jobs for sending reports to clients.

Panda Security offers security as an integrated service for clients, in the form of PMOP. This Help will allow you to get the most out of PMOP and increase your clients' security and satisfaction quickly and easily. Welcome to PMOP.

# Information, inquiries and services

---

## Information, inquiries and services

Along with the products themselves, Panda Security offers you help files and documentation to extend the information, resolve queries, access the latest updates and benefit from other services. You can also keep up-to-speed on the latest IT security news. Visit the Panda Security website to access all the information you need.

### Useful links

[-Main page](#): all the Panda Security information at your disposal.

[-Documentation](#): All the latest product documentation and other publications.

[-Tech Support](#): clear up any questions you have about infections, viruses, and Panda Security products and services, with continuous and fully up-to-date information, any time of day, all year round:

[-Evaluation software](#): Panda Security offers you free trial software of the solution you want.

[-Products](#): check out all the features of all Panda Security products. You can also buy them or try them without obligation.

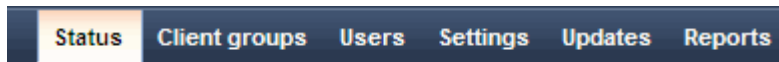
## Chapter 1. Service Providers Web Console

### To access the console

Enter the Login email and Password.

Accept the terms and conditions in the License agreement (you will only be asked to do so once).

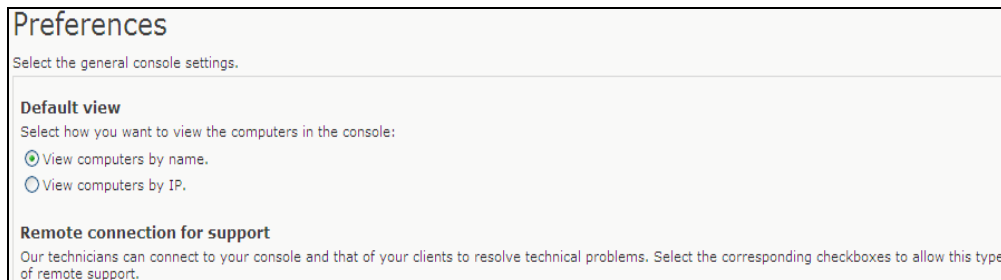
You will then see the main console window, from where you can access each of the areas of PMOP: [Status](#), [Client groups](#), [Users](#), [Reports](#), [Settings](#), and [Updates](#).



To create users and assign them access permissions and management privileges, click Users.

To establish the general console configuration, click **Preferences**.

### Preferences

A screenshot of the 'Preferences' page. The title is 'Preferences'. Below it is the instruction 'Select the general console settings.' There are two sections: 'Default view' with the instruction 'Select how you want to view the computers in the console:' and two radio button options: 'View computers by name.' (selected) and 'View computers by IP.'; and 'Remote connection for support' with the instruction 'Our technicians can connect to your console and that of your clients to resolve technical problems. Select the corresponding checkboxes to allow this type of remote support.'

This screen lets you configure aspects which affect the general configuration of your Web console.

### Default view

Select if you want the computers to be displayed by name or IP address.

### Remote connection for support

Panda Security makes its technical service teams available to you to help you resolve incidents that affect your Web console and your clients' management consoles.

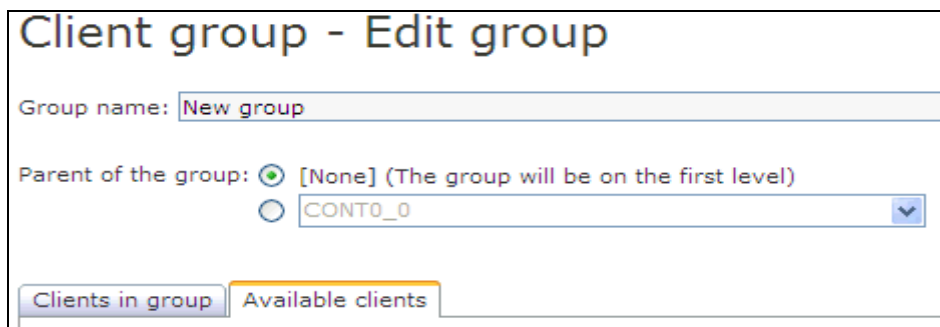
## Chapter 2. Client groups

Clients are organized in groups in the Web console. These groups are displayed in the Client groups window. To access this window, click Client groups in the console's main window.



Click any of the groups to display the **Client group- Edit group** window. Here you will see the group's name, its clients, its licenses and the types of licenses contracted.

### How to create a client group



1. Click the **Create new group** link in the **Client group** window.
2. Enter a name for the group.
3. Parent of the group. Use the first option to place the group on the first level of the tree. Use the second option if you want the group to depend on any of the existing groups in the tree.
4. Click **Settings** if you want to use the search tool. You can search for clients according to the type of license they have.
5. The **Available clients** tab shows a list of the clients that are visible to users (depending on their permissions) and do not belong to the group that the user is editing. Together with the clients you can see the number of contracted licenses and their type. Select the client(s) to integrate into the group.
6. Click **Assign**. Make sure the selected clients appear in the **Clients in group** tab.

If you want to move a client from one group to another do it from here. Select the client(s) that you want to move, and click **Move**.

Go back to the **Client group** main window and you will see that the group you created is at the corresponding level in the group tree. If you remove any of the groups, all their data will also be eliminated.

You can only delete empty groups, that is, groups that do not contain any clients or subgroups. Once you select the group to delete, click **Delete**.

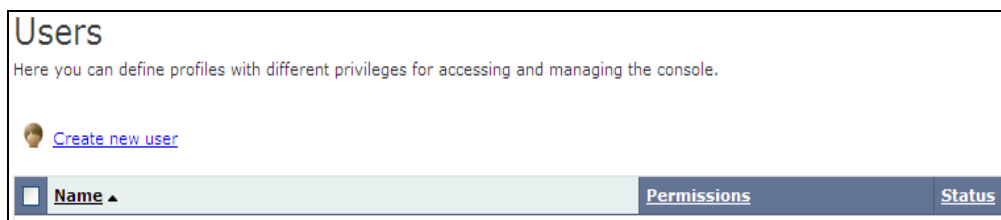
## Chapter 3. Users and permissions

### How to create new users

#### Default user

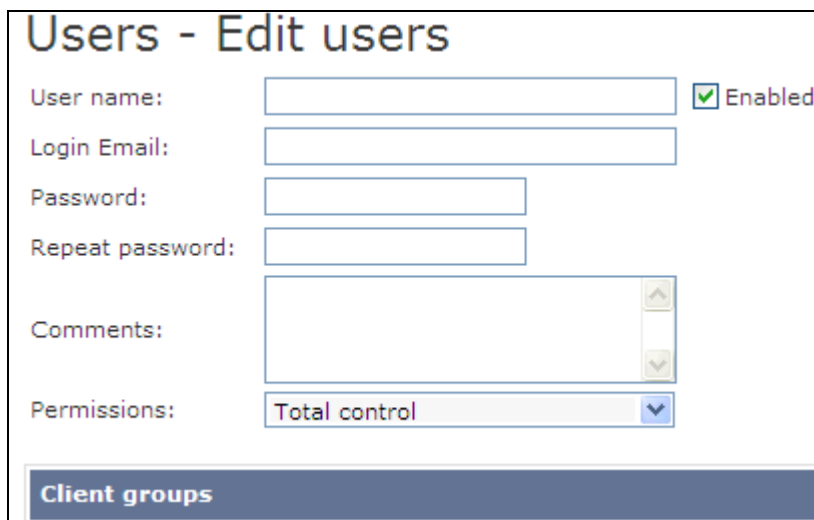
The first time you log in to the console you will use the PMOP default user. This user cannot be deleted and has total control permissions.

#### Users window



The **Users** window distributes information in three columns: **Name**, **Permissions** and **Status**. As you create users, these appear in the list, along with the type of permissions that you have given them and their status (enabled or disabled). Click a user's name to access the **Users - Edition** window. There you can see the user details and the clients groups whose security they can manage.

Go to this window if you want to create a new user.

The screenshot shows the 'Users - Edit users' form. It contains several input fields: 'User name', 'Login Email', 'Password', and 'Repeat password'. There is a checkbox for 'Enabled' which is checked. Below these is a 'Comments' section with a text area and up/down arrows. At the bottom, there is a 'Permissions' dropdown menu set to 'Total control' and a 'Client groups' section.

1. Click Create new user to access the Users - Edition window. Fill out the User name, Email, Password and Repeat password fields.
2. You can add information in the Comments section.
3. In the Permissions menu, select the type of permission to assign to the user:
4. Select the group(s) available to the user in Client groups.
5. Click **OK**.

6. In the main Users window, check that the user has been created and that the name, permission and status appear correctly in the list.
7. To remove a user, select the corresponding checkbox and click Delete.

### Types of permissions

PMOP offers three types of permissions. Depending on the permissions assigned to each user they will be able to manage the security of the groups under their responsibility to a greater or lesser extent.

Type of permission:	The user can:
Total control	Manage configuration of all groups. Assign clients to groups. Move clients from one group to another. Manage all users created on the system. Access all clients' Web consoles with total control permissions. Manage automatic updates of the end client profiles. Manage report send jobs.
Security administrator	Modify their user credentials. Manage groups and eliminate the groups they have permissions over. Access the Web consoles of the clients they have permissions over, with total control permissions. Manage automatic updates of the end client profiles. Create report send jobs for clients of the groups accessible to them.
Monitoring	Modify their user credentials. They cannot create, delete or modify any information in the Web console. Access the groups assigned to them and view the clients of the groups they have permissions over. They cannot create or modify report send jobs.

## Chapter 4. Language settings

From the **Settings** menu of your Web console you can change the language of your clients' protection.

Select the default language of the protection:

Language:

Select the clients to apply the selected language to:

Only my clients

All clients

Select the client profiles to apply the selected language to:

Only the default profile (DEFAULT) for new clients

All profiles created so far and the default profile (DEFAULT) for new clients

Select the language in the drop-down menu, and choose the corresponding checkbox depending on the profiles to which you want the language change to apply.

There are two options:

1. That the language change only affects the default profile for new clients.
2. That the language change affects all profiles created until now as well as the default profile for new clients.

Then click **OK**. The change of language will be reflected in your clients' Web console.

## Chapter 5. Status

### Protection status

Once you have specified the groups, users and permissions, the **Status** window will give you an overview of your clients' status.

In the top of the window you will see the **Notifications** section, which displays messages about new product versions or technical incidents.

You may want to filter lists so that they only display information about certain clients depending on how many or what type of licenses they have or how close their licenses are to expiring. You can use the search tool for this, which you can access through **Settings**.

In addition to the default search, you can apply filters and define a new search. Then click **Find** and you will get a list of clients. Click **Settings** if you want to use the search tool.

You can also monitor a group's protection by selecting it from the tree in the **Groups** column. The right-hand panel will display the available information in the following columns:

#### Client

Shows a list with the clients' names. Click a client's name to go to its console.



Direct access from the client Web console to the Service Providers console is only available to users with security administrator or total control permissions. Users with monitoring permissions won't have access permissions. To find out more about permissions, go to the section [Types of permissions](#).

#### Group

Shows the name of the group to which the client belongs.

#### Licenses

Type and number of licenses contracted by the client, number of licenses used and expiry date. In the case of clients with several maintenance contracts, the **Last expiry** column displays the expiry date of the last contract. For more information about license control and management, go to the section **License management**.

#### Status

Shows the percentage of protection modules with an out-of-date engine or signature file and the percentage of protection modules with errors. When you click on these percentages, you will see the **Updates** window (if the percentage is more than zero).

The **With errors** column displays the percentage of errors in computers administered by the client. To consult all errors, click the percentage and go to the **Error details** window.

You can also click the **View error details** link.

If the number is:	It indicates:
orange	The percentage of out-of-date protection modules is between 20 and 39%
red	The percentage of out-of-date protection modules exceeds 39%

Number of detections on the current day (from 00:00 AM till the present moment) in

- the file system.
- email.
- Internet browsing.
- instant messaging applications.
- items blocked by the firewall.

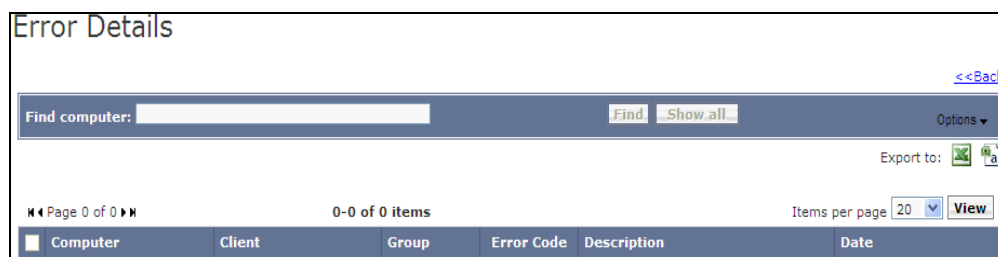
When you place the cursor on the client's name, you will see a yellow tag with information about the client.

### Export the list of clients


The list of clients can be exported, either in Excel or CSV. To do this, click on the corresponding icon next to the text **Export to**. Both formats include a header which specifies the date and time when the file was created, a summary of the search criteria, and the details of the list.

### Error details

This screen displays a list of errors reported by the client computers that you administer.



The information is structured in six columns: **Computer**, **Client**, **Group**, **Error code**, **Description**, and **Date**.

 If you want to go to the help files and documentation about any of the errors that appear in the list, click the corresponding error code.

Users with total control or security administrator permissions can delete entries from the list. To do this, mark the checkbox corresponding to the entry you want to delete and click **Delete**.

Click **Settings** if you want to use the search tool.

In addition to the default search, you can apply filters and define a new search. Then click **Find** to see a list of errors. This search will also be saved for later consultation, and you can edit it or delete it whenever you want.

### Export the list of errors

The list of errors can be exported, either in Excel or CSV. To do this, click on the corresponding icon next to the text **Export to**. Both formats include a header which specifies the date and time when the file was created, a summary of the search criteria, and the details of the list.

### License management

The **Status** window shows information about the number of licenses contracted by each client. The information is as follows:

Licenses contracted  
Licenses used  
License expiry date

PMOP uses a simple color code to inform of licenses used and the proximity of the license expiry date.

#### Licenses used

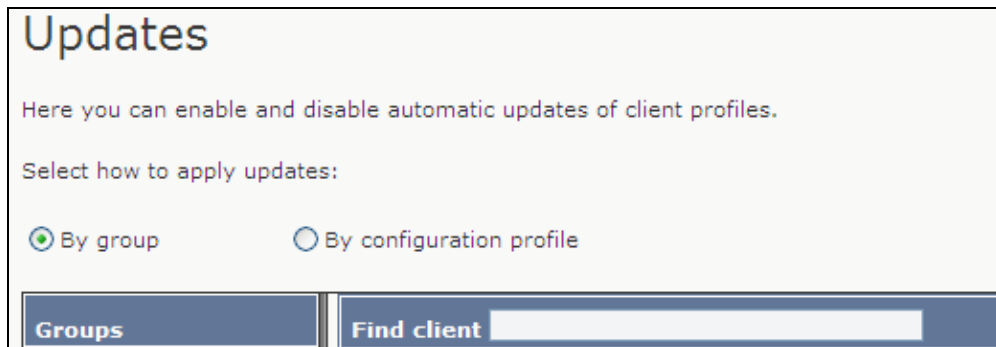
If the color of the number of licenses used is:	It indicates:
orange	85% of the contracted licenses have been used
red	All licenses contracted have been used

#### License expiry date

If the color of the license expiry date is:	It indicates:
orange	There are 30 days or less before license expiry
red	The licenses have expired

### Chapter 6. Updates

To access this window, click **Updates**.



**Updates**


Here you can enable and disable automatic updates of client profiles.


Select how to apply updates:

By group       By configuration profile

**Groups**      **Find client**

From this window you can manage the automatic update of all profiles of your clients.

1. Select the group of clients from the tree.
  2. To the right you will see the names of the clients and the profile they have associated.
  3. If you want to enable automatic updates of the protection of all your clients, select **Protection update**.
  4. If you want to enable automatic updates of the signatures for all your clients, select **Signature update**.
-  To disable the updates mentioned in points 3 and 4, clear the corresponding checkboxes. Both when enabling and disabling, the action will affect all clients that appear on the page. If the list of clients exceeds the space on the page, use the Next-Previous controls at the bottom of the table.
5. To enable the updates just for certain clients, select the corresponding checkboxes.

 It is advisable to assign clients the Monitoring permission for the management of their Web console, as otherwise they could modify management of the updates. Refer to the section Types of permissions.

 Click Apply to activate the automatic updates.

## Chapter 7. Reports

### Types of reports

PMOP generates different types of reports. All of them give information about the security status of the clients' IT network and the items detected over a given period of time.

Also, you can schedule the frequency with which reports will be sent and specify the content and time of sending.

Type of report	Information
Executive	Status of the protection installed and items detected over the last 24 hours. Also, it includes Top 10 lists of computers with malware detected and attacks blocked, respectively.
Status	It gives an overview of the protection status and update level at the time of report generation.
Detections	Describes the detections made in the period of time described in <b>Frequency</b> . It gives information about the computer, group, type of detection, action and date when the detection took place.

### Sending reports

Schedule sending of reports to be able to send them. To do this, select the type of report, its content and the time of sending. You can also select the client the report will refer to and the recipient.

First, select the corporate logo to appear in the bottom left corner of the report. Use the **Change** button if you want to select a different logo. If you don't want a logo to appear, click **Delete**.



In the **Reports** window, click **Schedule sending of reports**. In the **Details of the report send job** section, you can specify who generated the report and the frequency (daily, weekly, monthly, scheduled time).

**Weekly report:** the report will contain information from the last seven days. If the day established for sending reports is Sunday, data will be included from 00:00 on the previous Sunday until the time the report is generated on the current Sunday.

**Monthly report:** tasks cannot be generated for the 30th or 31st of the month. If, for example, you select the 15th of the month, the report generated will include data from 00:00 on the 15th of the previous month until the time the report was generated.

**Full month report:** you cannot select the day and it will always be sent on the first of the month. the report will contain data corresponding to the complete previous month.

In the **Report data** section, you can select the type of report, its content and format. You can also select the language of the report and its logo. You can also specify the client the report will be generated for. To do this:

a) Select, in the **Group** menu, the group of the client for which you want to create the task.

b) Click **Select** to access the **Select client** window. A list is displayed of all clients in the selected group. Select the client or use the **Search** text box.

Click **Edit** if you want to insert a logo in the bottom right corner of the report.

**Message data** section. Fill in the From, To, CC and CCO (if necessary) and Subject fields.

Click **OK**.

**New send job**

**Details of the report send job**

Name:

Created on date/time:

Created by:

Frequency:  Hour:

**Report details**

Group:

Client:

Language:

Format:

Type of report:  Executive  Status  Detection

Content:  License status  Protection status  Detections


Logo:

**Message details**

From:

To:

Click **OK**. The new send job will appear at the top of the list in the **Reports** window.

 There is a limit to the total number of send jobs. To calculate it, multiply the number of types of reports (3) by the number of clients (you can see them in the Status window > Clients column).