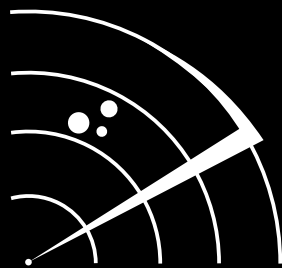


panda

Malware**Radar**



User Guide



Introduction

Panda Malware Radar is an online audit service that automatically identifies threats that are undetected by your current security software. It lets you evaluate the security of your network and generates reports and recommendations that allow you to orient your security strategy. Panda Malware Radar also gives you the option to clean all threats detected.



Audit types

Free trial

The free Panda Malware Radar trial is an online service that lets you audit your IT resources once with no limits on the number of computers scanned.

This type of audit displays a summary of the main results and an example of a detailed report with results for one of the computers.

One-Run Audit

If you buy a One-Run Audit you can scan your company's IT resources once. There are two types of One-Run Audit: **With cleaning of all the malware detected** or **without cleaning the malware detected**.

Once the audit is finished, you'll get two detailed reports: the **executive report** and the **technical report**.

If you would like a One-Run Audit, visit the [Panda Malware Radar web page](#) and buy the licenses you need.

Subscription

When you buy a subscription you can perform an unlimited amount of audits in a given number of computers during the time contracted (one, two or three years).

When each audit is complete you will get two reports: the **executive report** and the **technical report**.

If you want to have unlimited access to the services, visit the [Panda Malware web page](#) and buy the licences you need for the period you prefer.



Preparation

To carry out an audit you have to distribute the Panda Malware Radar scan program on the network.

- To use the automatic distribution tool it is essential that the computer where the tool is to be used has an Internet connection. The automatic distribution tool lets you select the network computers to be audited.
- If you want to audit an isolated network where no computer has an Internet connection, or isolated computers with no Internet connection, you must download the scan program and run it manually on each of the computers to be audited. For more information refer to the **Audits with manual deployment section**. The scan program will not leave any components installed on the computers.

Requirements

Requirements to access the web console:

Internet Explorer 5.5 or later.

Mozilla Firefox 1.5 or later.

Internet connection: direct or through a local area network.

HTTPS connection (port 443).

Requirements on the computer from which deployment is performed:

Operating system: Windows Vista (32 and 64 Bit) /XP Professional (32 and 64 Bit) /2000 Pro /. Windows 2000 /2003 servers (32 and 64 bit).

Processor: Pentium 166 MHz or faster.

RAM: 128 MB.

Hard disk: 70 MB free space.

Browser: Internet Explorer 5.0 or later.

Internet connection.

Access to the Admin\$ resource on the computers to be audited.

Perform the scan with a user that has administrator rights over the computers to be audited.

Requirements on the computers to be audited:

Operating system: Windows Vista (32 and 64 Bit)/ XP /2000 Pro /NT 4.0 /Me/ 98 /95 /. Windows 2003/2000/NT 4.0 servers.

Processor: 486 at 66 MHz or faster.

RAM: 128 MB.

Hard disk: 70 MB free space.

Browser: Internet Explorer 5.0 or later.

Printer and File Sharing for Microsoft networks installed.

To have **Use simple file sharing** disabled (on Windows XP, **Tools > Folder Options > View > Use simple file sharing**).

Disable the Windows firewall or set the exception **File and printer sharing**.

Have administrator rights over the computers to be audited.

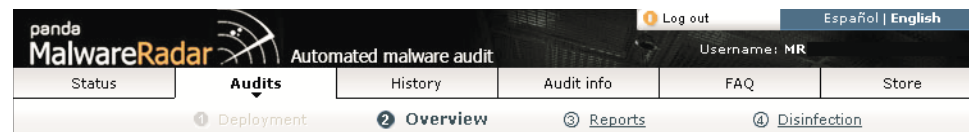


Introduction to the Malware Radar console

To access the Panda Malware Radar console visit the <https://private.malwareradar.com/> page and enter the user name and password sent to you by email when you first registered. Click **Log in** to enter the console.

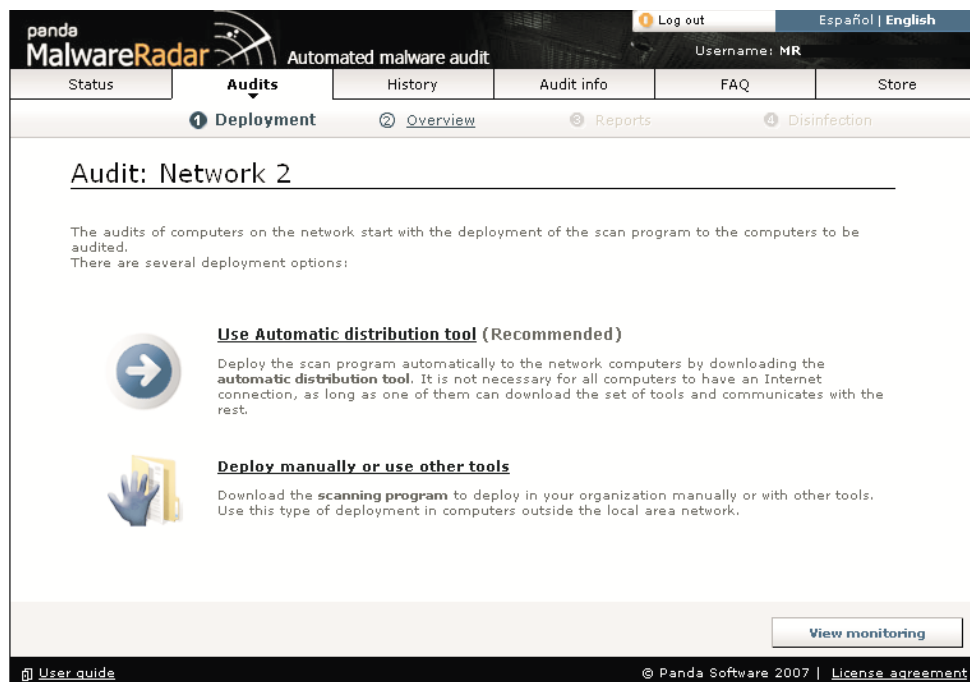
If you don't remember your login details, use the password reminder at www.pandasecurity.com/enterprise/support/details/password/. We will send you a new email with your user name and password.

The Panda Malware Radar console consists of several sections organized into tabs at the top of the console that will help you through the audit process.



The tabs available are as follows:

- **Status:** Displays the possible audits, the status of audits in progress, the alerts...
- **Audits:**
 - **Deployment:** It downloads the **automatic distribution tool** (it must be used on a computer with an Internet connection) or **scan program**. If you want to use your own distribution method you'll need to download the scan program.
 - **Monitoring:** It displays the status of the audit in progress: scanned computers, number of scans finished, malicious code found up to that moment, level of protection of your network, etc.
 - **Reports:** These display detailed information about the malicious software detected (active and latent), security failures, protection level of your network, etc. There are two types of reports with different levels of detail that you can check in the console, or download in PDF or XML.
 - **Cleaning:** This lets you distribute the disinfection program in your network, through the automatic distribution tool or downloading the disinfection program.



After completing the process in each of these tabs, click the next one to continue with the process.

- **History:** A history file of the audits carried out. It lets you create a global report, combining the results of the different audits carried out.
- **Audit Info:** Displays the general statistics with key data about the results obtained by Panda Malware Radar in other companies. In this section it is also possible to access to a glossary of terms.

- **FAQs:** In this section you can find the answer to the most frequently asked questions.
- **Store:** In the store you can buy the audit type you prefer:
 - **One-run audit:** It lets you audit your whole network only once.
 - **Subscription:** It lets you carry out an unlimited number of audits.

You can also contract cleaning during the period contracted (one, two, or three years).



How to carry out an audit in just a few simple steps

The first step to audit a network involves distributing the scan program to each of the computers.

The options available are:

- To use the automatic distribution tool it is essential that the computer where the tool is to be used has an Internet connection.
- If you want to audit an isolated network where no computer has an Internet connection, or isolated computers with no Internet connection, you must download the scan program and run it manually on each one of the computers to be audited. For more information, refer to the **Manual deployment** section. The scan program will not leave any components installed on the computers.
- If you want to use other tools (login script, Tivoli, etc.), you will have to download the scan program and distribute it using the method you want. For more information, refer to the documentation of the tool you want to use.

1.- Accessing the console

To access the Panda Malware Radar console visit <https://private.malwaradar.com/> and enter the user name and password sent to you by email when you first registered. Accept the license agreement and click **Log in** to access the console.

Note: The first time you access the console you will see a security notice asking you to accept a security certificate. When this message appears, click **Yes** to accept the certificate.

2.- Generate a new audit

In the **Status** tab of Panda Malware Radar, you can see all the available audits. Follow these steps to start the process:

The screenshot displays the Panda Malware Radar console interface. At the top, there is a navigation bar with the Panda Malware Radar logo, the text 'Automated malware audit', and user information including 'Log out', 'Español | English', and 'Username: MR'. Below the navigation bar is a menu with tabs for 'Status', 'Audits', 'History', 'Audit info', 'FAQ', and 'Store'. The 'Status' tab is active, showing three main sections: 'My subscription', 'My warnings', and 'My status'. 'My subscription' displays 'Valid until: 4/1/2010' and 'Licenses contracted: 25', with a 'Generate new audit' button. 'My warnings' shows a message: 'There have been no warnings until now'. 'My status' lists three audits: 'Audit {09FBE269A432}: An audit is available' with a 'Start audit' link, 'Audit {1454A907}: An audit is available' with a 'Start audit' link, and 'Audit {1D631D11}: In the process of disinfection' with a 'Monitor disinfection' link. The footer contains 'User guide', '© Panda Software 2007', and 'License agreement'.



1. If you have contracted a **One-Run** audit, click **Start audit**.
2. Specify a name for the audit.
3. Click on **Start now**.

3.- Configuring and downloading the distribution tool

Before distributing the Panda Malware Radar scan program with this tool, there are certain aspects you can configure. To do this, follow these steps:

- If this is the first time you have configured Panda Malware Radar, or you want to enter new settings, click **New configuration**. In the **Configuration name** field, enter a name so that you can identify the settings later.
- If you want to use a configuration that you have previously configured, select it from the list that appears on the left of the screen.

Note: It is essential that the computer on which the distribution tool is to be used has an Internet connection. If you want to distribute the scan program across a network where no computer has an Internet connection, you must use manual deployment.

The screenshot shows the 'Audit: Network 2' configuration window. At the top, there are tabs for 'Deploy', 'Overview', 'Reports', and 'Disinfection'. Below the title, there is a instruction: 'Specify the configuration of the automatic distribution tool or apply one of the existing configurations and click "Start download"'. On the left, a 'Profiles' sidebar shows 'By default' and 'Profile 1' (selected). The main panel has three tabs: 'General', 'Scan', and 'Exclusions'. Under the 'General' tab, there are two radio button options: 'The computers subject to the audit have Internet connection' (selected) and 'Computer without access to the Internet'. Under the selected option, there is a checked checkbox for 'Access to the Internet via proxy' and input fields for 'Proxy', 'Port', 'Username', 'Password', and 'Repeat password'. There are also links for 'New configuration' and 'Delete configuration' at the bottom left. At the bottom right, there are buttons for 'Start download', 'Cancel', and 'Save changes'. The footer contains 'User guide' and '© Panda Software 2007 | License agreement'.

You can configure the following aspects:

- **General tab:** Panda Malware Radar needs to connect to the Internet to send the audit reports to the application. If you use a proxy server to access the Internet, enter the necessary details: the IP address of the server and port. If the server requires authentication, enter the user name and password in the proxy server.



If the computers to be audited do not have an Internet connection, specify a shared resource (on the network) where you want to save the audit report. For example, `\\xxx\reports` (where *XXX* is the name of the computer in which the report in question is saved).

If you want to deploy the scan program to computers with Windows 9x or Windows NT 4, enable the checkbox that allows compatibility with those operating systems.

- **Scan Tab:** Set the parameters for the scan. Among other possibilities, it lets you set the scan you want to carry out (fast or complete).
- **Exclusions tabs:** If you chose the full scan, you can indicate if you want to exclude any folder from the scan. You can also specify types of malware that can be excluded from the cleaning process by enabling the corresponding box.

Once you have established the configuration you want, click **Save changes** and then **Start download**.

4.- Deployment with the automatic distribution tool

When you run the downloaded file the automatic distribution tool will open. This tool lets you select the computers on your network that you want to audit. You can do this in two ways:

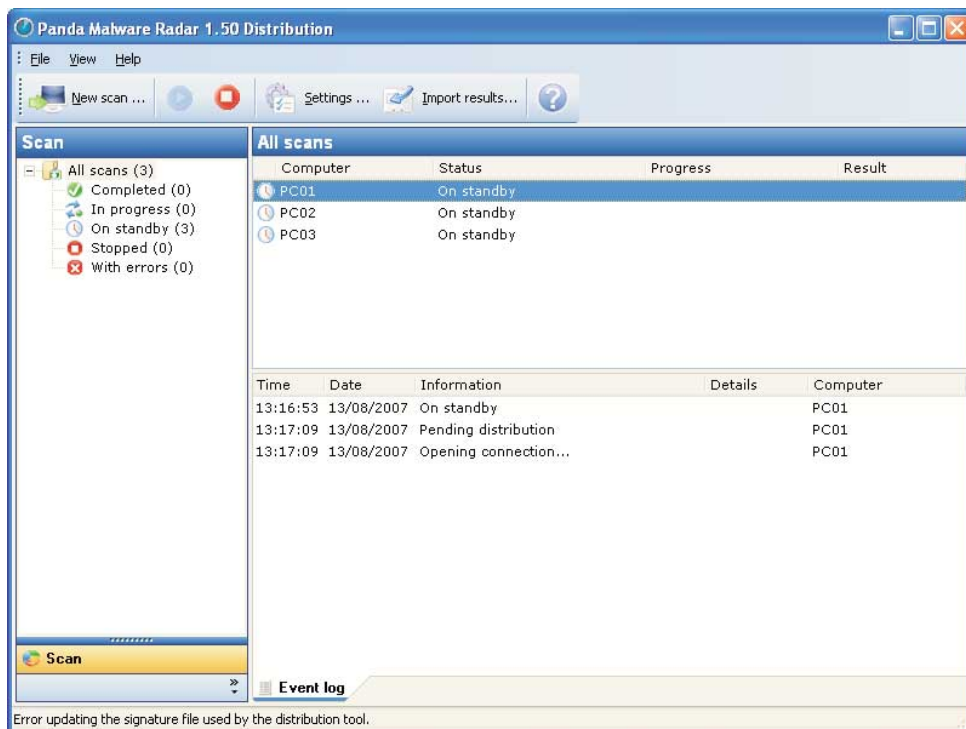
- By selecting the domains or computers that you want to audit from the tree displaying your network structure.
- Specifying the name or IP address of the computers in which you want to launch the audit.

Deployment by domains

1. Click **New Scan**.
2. Select **By domain**.
3. Select the network domains that you want to scan. You can scan all the computers in the domain, or select specific computers by checking the corresponding checkboxes.
4. You can also enter a user name and password with administrator privileges on the computers to be scanned. If you decide not to enter these data now, the application will request them at a later stage. It is advisable to use a domain administrator password. This way you won't have to specify the user name and password of every computer.
5. Click **OK**.

Deployment by IP or computer name

1. Click **By IP or computer name**.
2. Specify the computers to scan. You can indicate the computers' names, IP addresses or IP address range, separating this data with commas. For example: 127.0.0.1, COMPUTER01, 192.0.17.1-192.0.17.128
3. Click **Add**.
4. You can also enter a user name and password with administrator privileges on the computers to be scanned. If you decide not to enter these data now, the application will request them at a later stage. It is advisable to use a domain administrator password. This way you won't have to specify the user name and password of every computer.
5. Click **Scan**.



Panda Malware Radar needs to know the administrator name and password of the computers to which it distributes the scan program. If you want to use default credentials for all computers (for example, a domain password), enter this data in the distribution tool configuration before launching the scan.

Note: If you don't indicate this data before launching the scan, Panda Malware Radar will ask you when it needs them.

Once you've selected the computers, click **Launch scan**.

How to carry out an audit in just a few simple steps

5.- Manual deployment

Panda Malware Radar lets you perform audits on computers without a connection to the Internet or that are out of the networks or in networks where no computer has an Internet connection. If you want to use other distribution tools (SMS, Tivoli, etc.), you must also follow the instructions below.

Notes:

- The Panda Malware Radar distribution tool can only be used on computers with an Internet connection, even if other computers on the network have an Internet connection.
- For information on how to perform distribution with other tools, refer to the documentation of the tool that you want to use.

Follow the steps below:

1. In the **Status** or **Audits** tabs, click **Start audit** (if no audit has already been created, click **Create new audit**).
2. Click **Deploy manually or use other tools** to download the scan program.
3. Click **New configuration** and select **Computers without access to the Internet**. Specify the path to save the audit report. There are two options:
 - You can specify the local path where you want to save the audit for that computer. For example, C:\Reports.
 - If it is a local network, where no computer has an Internet connection, specify a shared resource on the network without an Internet connection in which you want to generate a report. For example, \\xxx\reports (where XXX is the name of the computer in which the report in question is saved).



The screenshot shows the 'General' tab of the configuration window. The 'Configuration name' is 'Profile 1'. Under the section 'The computers subject to the audit have Internet connection', the 'Access to the Internet via proxy' checkbox is checked. Below it are fields for 'Proxy' and 'Port'. The 'The server requires authentication' checkbox is also checked, with fields for 'Username', 'Password', and 'Repeat password'. The 'Computer without access to the Internet' radio button is unselected. Below this is a text box for report location with a note: 'Select the report location for computers without Internet connection (the saved results can be sent later using the remote distribution tool)'.

4. Click **Save changes**.

5. Click **Start download**.

Once downloaded, run the cleaning program on each of the computers to be cleaned. To see the results, copy the .DAT file and the folder with the same name as the .DAT file that will have been generated to a computer with an Internet connection. Then, send it to the Panda Malware Radar servers **using the distribution tool**.

Follow the steps below to download the distribution tool:

1. Go to the **Audits** tab and click **Start audit**.
2. Click **Use Automatic distribution tool**.
3. Select one of the existing settings or create a new one.
4. Make sure that the option **The computers subject to the audit have Internet connection** is enabled. If the connection is through a proxy server, you must also indicate the IP address, port and password (if necessary).
5. Save the changes and click **Start download**.

Import the report by following the steps below:

1. Run the automatic distribution tool and click **Import results**.

The screenshot shows the 'Importing of results' dialog box. It has a title bar with a close button. The main text says 'Importing of results' and 'Specify the location of the folders generated by the audit in computers without local network connection.' Below this is a text input field with a 'Browse...' button. At the bottom, there is a table with two columns: 'Computer' and 'Audit status'. The table is currently empty. At the bottom right, there are 'OK' and 'Cancel' buttons.



2. Click **Browse...** and find the directory that contains the .DAT file and a folder with the same name as the .DAT file.

3. Click **OK** to send the report.

To see the report, go to the **Monitoring** tab in the console and click **View Audit reports**. You can also do this directly through the **Reports** option in the console.

6.- Scan and disinfection monitoring

The second phase of the audits involves monitoring. Monitoring offers information about the status of the scans and is also divided into several groups:

- **Scanning stage:** Displays detailed information about the status of your network: threats detected (active and latent), number of computers affected, protection level, vulnerabilities detected, etc.

Once all the computers on the network have been scanned, click **Finish scan stage**.

Important note: Before the data collection, it is important that no suspicious file remains without having been scanned by PandaLabs. Otherwise, if malware is found, these files will not be disinfected in the cleaning task.

The screenshot shows the Panda MalwareRadar web interface. The top navigation bar includes 'Status', 'Audits', 'History', 'Audit info', 'FAQ', and 'Store'. The main content area is divided into several sections:

- Audit Network 2:** Shows start and close dates, a 'Cancel audit' link, and a 'Finish data collection' button.
- Scanning stage:** Displays a progress bar and a table of malicious code detected.

Type	Active	Latent	PCs affected
Viruses, worms and trojans	0	0	0
Spyware	0	0	0
Adware	0	0	0
Others	0	0	0
Total	0	0	0
- Malicious code detected:** A table showing the protection level of IT resources.

Protection	Computers	Active	Latent
Optimum	0 (0%)	0	0
No optimum protection detected	1 (100%)	0	0
- Critical vulnerabilities:** A table showing the number of vulnerabilities and detections.

Vulnerabilities	Computers	Active	Latent
39	1 (100%)	0	0



- **Scan:** You can see the computers to which the scanning tools have been distributed and the number of scans performed. If you want to know the name of the computers scanned and the network domain, click on the figures to the right.
- **Laboratory study:** PandaLabs, the Panda antivirus laboratory, analyzes suspicious programs and processes. In this section you can find out the number of suspicious files that have been processed in the laboratory, how many have not yet been processed and the computers in which there are suspicious files.
- **Results:** This is the phase of collecting the data generated by the scans. If you have a subscription version or a one-run audit, you can consult the different types of reports to see your organization's status. Click on **View audit reports** (**View disinfection reports**, in the case of cleaning) to see the results.

7.- Reports

It is important to understand and correctly interpret the results in order to correct any risk situation in the network and adequately plan protection strategies.

The screenshot displays the Panda MalwareRadar web interface. At the top, there is a navigation bar with the Panda MalwareRadar logo, the text 'Automated malware audit', and user information including 'Log out', 'Español | English', and 'Username: MR'. Below the navigation bar, there are tabs for 'Status', 'Audits', 'History', 'Audit info', 'FAQ', and 'Store'. The 'Audits' tab is active, and within it, the 'Reports' sub-tab is selected. The main content area shows the title 'Audit: Network 2' and a list of actions:

- ▶ View results online
 - » [View executive report](#)
 - » [View technical report](#)
- ▶ Download results
 - » [Generate executive report](#) Download
 - » [Generate technical report](#) Download
 - » [Generate audit data in xml format](#) Download

You need the Adobe Reader application to view reports. Click [here](#) to download it.
- ▶ Offers to buy

At the bottom of the main content area, there is a note: 'Please contact a Panda sales advisor to find out more about the offers available.' A 'Refresh status' button is located at the bottom right of the main content area. The footer of the page contains 'User guide' and '© Panda Software 2007 | License agreement'.

Results query

If you have a subscription or One-Run audit version you can consult results in the different types of reports:

- **Executive report:** A report on the general situation: number of active and latent threats detected statistics, recommendations, etc.
- **Technical report:** A complete report with all details of the scans in each of the computers audited.
- **Technical disinfection report:** It shows the results of cleaning of your network, and details the number of active and latent threats that have been detected and eliminated, as well as their danger level and location, etc.

When the audit is over, you can send it to the History where you can view the reports again any time you want. The History also allows you to generate consolidated reports with data from the current audit as well as any other audit that might already be in the History.

Download results

Download executive reports and audit data

You can generate an executive report in PDF format and download audit data in XML format. To do this, click the **Generate report** option by the report that you want to download and wait for some seconds until the download link appears.

Download technical report or disinfection report

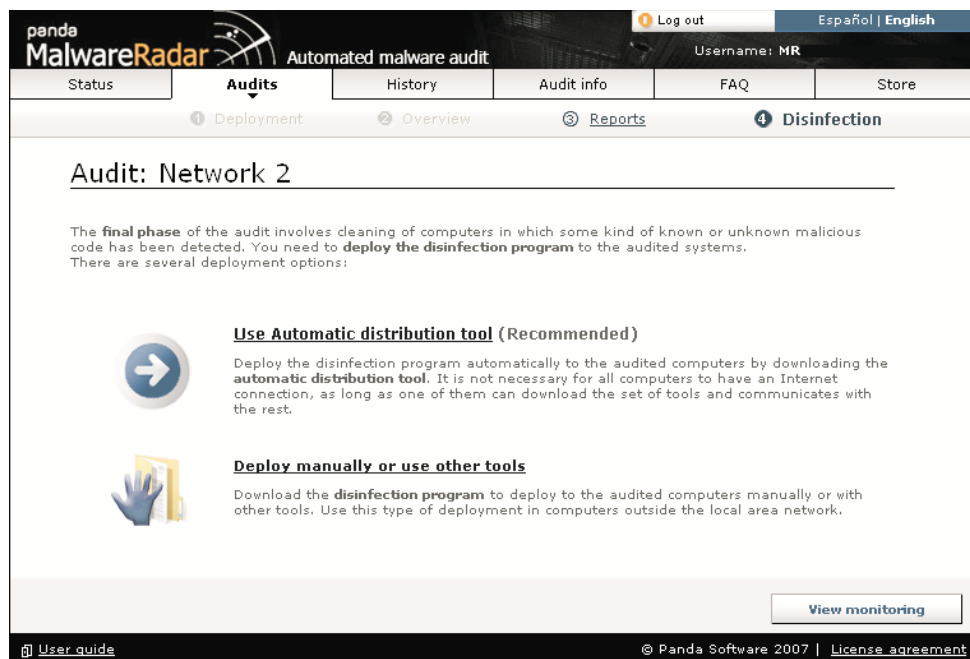
If you want to download a technical report or a disinfection report (in PDF format), you can select the computers on which the report should be generated. This way, you can get the information that you want and avoid overlong reports. To do this, follow the steps below:

1. Click the **Generate report** option by the **Technical report** or **Disinfection report**.
2. Select, from the drop-down list, the computers you want to generate a report on. You can select all the computers, or simply those where malware (with different threat levels), vulnerabilities, etc. were detected.
3. Click **Find** and check the checkboxes that correspond to the computers that you want to view a report on.
4. Click **Generate report**, and wait a few seconds until the download link appears.

8.- Cleaning with the distribution tool

Once you have performed the scan and reviewed the reports, it is time to clean your network. To do this you will have to distribute a disinfection program on your network, following similar steps to those you took to distribute the scan program:

1. Go to the Malware Radar console.
2. In the **Status** window (or the **Audits**) section, click on **Start cleaning**.
3. Specify how you want to distribute the disinfection program: using the automatic distribution tool (recommended on networks with at least one computer with an Internet connection), manually or using other tools.



4. Configure the settings you want. For more information refer to the **Configuration** section.
5. Click **Save changes** and then **Start download**.
6. When you run the downloaded file the distribution tool will open.
7. Click **New disinfection** and select the computers to disinfect (only the computers that were scanned will be displayed).

8. You can also enter a user name and password with administrator privileges on the computers to be disinfected. This is advisable if you know the domain administrator password, as in this case you won't have to enter the credentials for every computer to be disinfected. If you don't specify these data now, Panda Malware Radar will request them when it needs them later on.

9. Click **Disinfect**.

To see the results of the disinfection, go back to the console by following these steps:

1. In the **Status** tab (or the **Audits**) section, click **Monitor disinfection**. This will show the result of the cleaning.
2. Once all the computers have been disinfected, click **Finish disinfection stage**.

Important note: Before finishing the disinfection stage, it's important that no computer remains without being scanned. Once this stage is finished you can't carry out the cleaning again.

3. Click **See the disinfection reports**. For more information, refer to the **Reports** section.

You can also file the audit in the history by clicking on the corresponding button. For more information, refer to the **History** section.



The screenshot shows the Panda MalwareRadar interface. The top navigation bar includes 'Status', 'Audits', 'History', 'Audit info', 'FAQ', and 'Store'. The 'Audits' section is active, showing 'Audit Network 2' with start and close dates from 5/2/2007. The 'Disinfection' results are displayed, indicating that no computers completed the disinfection with warnings. Two tables show 'Disinfected active malicious codes' and 'Disinfected latent malicious codes', both with zero counts across all danger levels (Very high, High, Moderate, Low).

Disinfection Results Summary:

- Computers deployed: 1
- Disinfections complete: 1 (Successfully), 0 (With warnings)
- Disinfections in progress: 0

Disinfected active malicious codes:

Danger level	Successfully	With warnings	PCs affected
Very high	0	0	0
High	0	0	0
Moderate	0	0	0
Low	0	0	0

Disinfected latent malicious codes:

Danger level	Successfully	With warnings	PCs affected
Very high	0	0	0
High	0	0	0
Moderate	0	0	0
Low	0	0	0

9.- Manual cleaning

To perform the cleaning of the computers without an Internet connection, you need to download the **disinfection program** and run it on each of the computers. To do this, follow these steps:

1. Go to the Malware Radar console.
2. In the **Status** window (or the **Audits** section), click on **Start cleaning**.
3. Click **Deploy manually or use other tools**.
4. Specify the path to save the cleaning report. There are two options:
 - You can specify the local path where you want to save the audit for that computer.
 - If it is a local network where none of the computers has an Internet connection, specify a shared resource on the network in which you want to generate a report. For example, `\\xxx\reports` (where XXX is the name of the computer in which the report in question is saved).

Computer without access to the Internet

Select the report location for computers without Internet connection (*the saved results can be sent later using the remote distribution tool*)



5. Configure the settings you want. For more information refer to the **Configuration** section.
6. Click **Save changes**.
7. Click **Start download**.

Once downloaded, run the cleaning program on each of the computers to be cleaned. To see the results, copy the .DAT file and the folder with the same name as the .DAT file that will have been generated to a computer with an Internet connection. Then, send it to the Panda Malware Radar servers **using the distribution tool**.

Follow the steps below to download the distribution tool:

1. Go to the **Audits** tab and click **Start audit**.
2. Click **Use Automatic distribution tool**.
3. Select one of the existing settings or create a new one.
4. Make sure that the option **The computers subject to the audit have Internet connection** is enabled. If the connection is through a proxy server, you must also indicate the IP address, port and password (if necessary).
5. Save the changes and click **Start download**.
6. Run the downloaded file and click **Import results**.



Import the report by following the steps below:

1. Run the automatic distribution tool and click **Import results**.
2. Click **Browse**, and find the directory that contains the .DAT file and a folder with the same name as the .DAT file.
3. Click on **OK** to send the report.



To see the results of the disinfection, go back to the console by following these steps:

1. In the **Status** tab (or the **Audits**), click **Monitor disinfection**. This will show the result of the cleaning.
2. Once all the computers on the network have been disinfected, click **Finish disinfection stage**.
3. Click **See the disinfection reports**. For more information, refer to the section **Reports**.

You can also file the audit in the history by clicking on the corresponding button.

History

The audits that are finished can be stored in a history file. If you already have audits stored in the history, click on the **View** link in the **Results** column for detailed information.

If you want you can create a global report with all the audits carried out. This report has the name of **consolidated report**.

Follow these steps to create a consolidated report:

1. In the audit history table, enable the boxes at the beginning of the lines with information about the audit and click on **Generate consolidated reports**.
2. The consolidated report takes a while to generate, depending on the number of audited computers. Click **Refresh status** occasionally until the **Download consolidated report** button is enabled.
3. Click on **Download consolidated report**.



More information

For more information about Panda Malware Radar, refer to:

- [The Frequently asked questions \(FAQs\) section](#)
(To access this section you need to log in with your user name and password).
- [The program help file](#)
- [Other resources](#)

Tech Support

All the Malware Radar versions include telephone and email support.
You can get the details of the Panda's office in the following email address:
<http://www.pandasecurity.com/about/contact>.