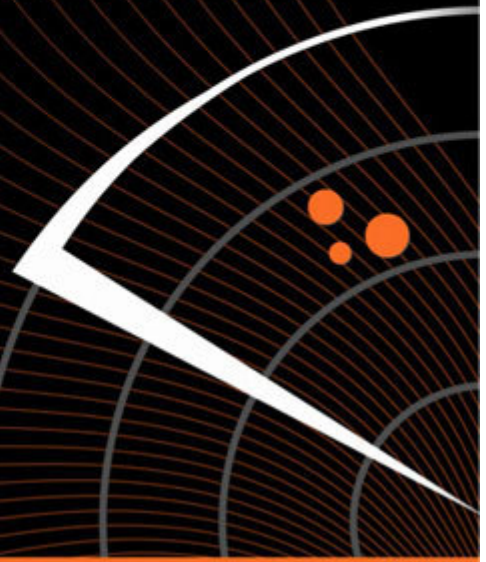


panda
MalwareRadar
Distribution Guide

The logo icon for Panda Malware Radar, featuring a stylized white radar or signal pattern with three small white dots.



Symbols and fonts used in the guide

Icons used in this document:



Note. Provides additional information and useful data.



Warning. Highlights the importance of a concept.



Tip. Useful ideas to help you get the most out of the program.



Reference. Other points that offer more information that you might find useful.

Fonts and styles used in this document:

Bold: Names of menus, options, buttons, windows or dialog boxes.

Code

Names of files, extensions, folders, commandline information or configuration files such as, scripts.

Italics

Names of options related to the operating system, and programs and files with their own name.

Panda Malware Radar distribution guide

The software described in this guide is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

Copyright notice

© Panda Software 2007. 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 Software, c/ Buenos Aires, 12 48001 Bilbao (Biscay) Spain.

Registered trademarks

Panda Software is a trademark or registered trademark belonging to Panda Software. Windows is a trademark or registered trademark of the Microsoft Corporation. Other product names that are mentioned in this guide may be registered trademarks of their respective owners.

© Panda Software 2007

All rights reserved.

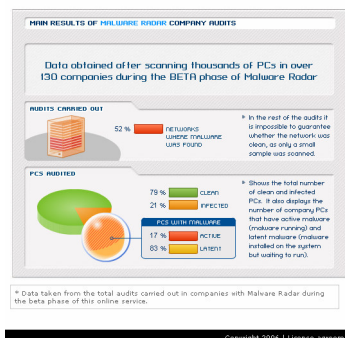
Contents

Panda Malware Radar distribution guide	4
1. Access the Web service	5
2. Create a new audit	6
3. Manage the distribution profiles	8
3.1 Profile creation Wizard	8
3.2 Profile management	8
4. Deploy the scan program to the computers you want to audit.....	9
4.1 Networks with personal firewalls.....	10
4.1.1 Windows XP firewall	10
4.1.2. Other personal firewalls	13
4.2 Distribution in Windows Me/98/95/XP Home.....	13
4.3 Active Directory	14
4.3.1 Assigning logon scripts.....	14
4.3.1 Assigning startup scripts.....	16
4.4 SMS	16
4.4.1 Discovery by login script	17
4.4.2 Discovery of users and groups.....	17
4.4.3 Network discovery	17
4.4.4 Distributing the program using login script.....	17
4.4.5 Remote distribution of the scan program	17
4.4.6 Distributing the software.....	17
4.5 PsExec	18
5. Using the Malware Radar distribution tool	19

Panda Malware Radar distribution guide

Statistics

The following graphs show the most significant data related to the level of protection in companies scanned with Malware Radar®.



Malware Radar is an online service that automatically identifies hidden threats that are undetected by your current security software. It evaluates and reports the status of your network with respect to threats, vulnerabilities and protection levels, including cleaning of detected malware.


In the Web help (which you can consult along with the online service), you will find more information about the characteristics of Malware Radar, audits, subscriptions, cleaning, reports, etc.

This **distribution guide** describes the steps to follow in order to deploy and distribute the **scan program**, which you will have to run in order to audit your network.


Distribution of the scan program is a step prior to monitoring and viewing reports in an audit:

Follow the instructions described in this distribution guide in order to carry out an audit of your network:

1. **Access the Web service.**
2. **Create a new audit.**
3. **Manage the distribution profiles.**
 - 3.1. Profile creation Wizard
 - 3.2. Profile management
4. **Deploy the scan program to the computers you want to audit.**
 - 4.1 In networks with personal firewalls.
 - 4.1.1. Windows XP firewall.
 - 4.1.2. Other personal firewalls.
 - 4.2. Distribution in Windows 95/98/Me.
 - 4.3. Active Directory.
 - 4.4. SMS
 - 4.5. PsExec
5. **Use the Malware Radar distribution tool** (if you have not used one of the other methods of deployment or distribution).

 **Reference:** You will find more information about **monitoring**, viewing **reports**, **disinfection**, etc. in the Web help, which you can consult during each step.

1. Access the Web service

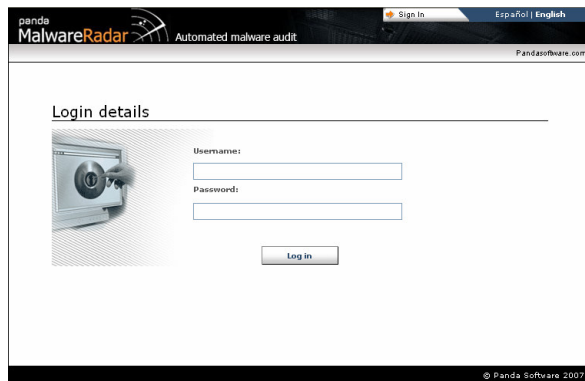
 **Warning:** Before starting the audits, make sure you have a Web browser such as Internet Explorer 5.5 (or later) or Firefox to access the Web service.

To start scanning the computers you want to audit, you need to access the product's Web service.

1. Go to the Panda Malware Radar Web service at the Web address supplied on purchasing the product.

 **Note:** If you have not received the email with the login details or you need more information, you can consult the Panda Malware Radar's tech support website:

2. The first time you access this service you will see a security warning asking you to accept a security certificate. Click on **Yes**.




3. Log on as a registered user of Malware Radar.

1. Enter your **username**.
2. Enter your **password**.
3. Click on **Log in**.

 **Reference:** If you have any problems accessing the service or if you have forgotten your login details, contact Panda Software tech support.

2. Create a new audit

In the **Status > My subscription** section check that you have unused licenses with which to generate a new audit.

 **Note:** If you do not have sufficient licenses for the audit of the computers on your network, you cannot carry out a complete audit. You can get the licenses you need from the website.

In the **My status** and audits section you can check the status of the audits available. Click on the link corresponding to an audit in progress, or if you want to create an audit, follow the instructions below.



There are two methods for creating a new audit and starting the scans, follow these steps:

1. Method

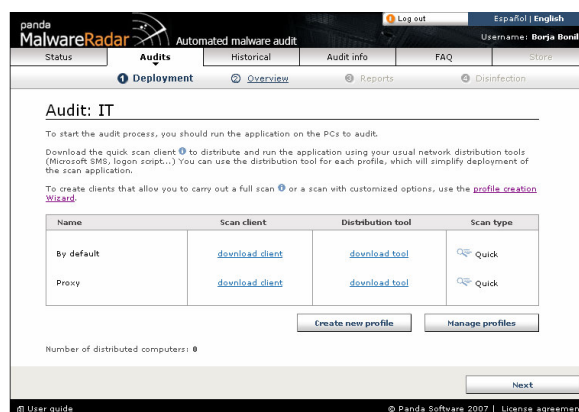
- Go to **My status > My subscription** and click on **Generate new audit**.
- Enter the name of the audit and click on **OK**.

2. Method

- Go to **Audits > My audits** and click on **Create new**.
- Enter the name of the audit and click on **Start audit**.

Malware Radar displays a pre-determined profile. If you prefer, you can create a **profile** that adapts to the configuration of the computers in your network to which the scan client will be distributed (Internet or network connections, proxy authentication if necessary, etc.).

In the next chapter, you'll find more information about creating and managing **distribution profiles**.



To carry out an audit in a domain.

- Check that the computer where the distribution tool is to be used has Internet access and that the user has administration permissions over the computers to which the scan client will be distributed.
- If the product distribution tool is not used, the user of the computer to which the scan client has been distributed must also have administration rights over his/her own computer and access to the Internet.

This Internet access in the scan client will allow the data needed to correctly complete the audit to be sent. If you have used the distribution tool, the remote computers do not need Internet access.

To carry out an audit in a workgroup.

- Follow the instructions above (similar to those for an audit in a domain) and, in addition, bear in mind that the administrator details entered in the distribution tool will be used on starting the scan of the selected computers.

The distribution tool will connect to remote computers for which scans have been requested. If the details initially entered do not have administrator rights over the local computer, you will have to re-enter details that do have administrator rights.

 **Warning:** Remember that computers with **Windows 95/98/Me/XP Home** are not compatible with the distribution tool. In these cases, distribute the scan client through other means (e-mail, FTP, etc.).

Download the tool with the required distribution profile. To do this, click on the **Download tool** button corresponding to the profile you want. If you have not previously created a profile and you want to use the one initially suggested, click on the **Download tool** button corresponding to the default profile. In either of these two ways, you can start deploying the scan client to the network computers you want to audit.

 **Note:** Make sure that these computers are connected in a network and can be accessed from the computer used to run the distribution tool.

If you want to manually distribute the scan client, click on the **Download client** button corresponding to the distribution profile you want or click on the **Download client** button corresponding to the default profile, if no profile has been created and you want to use the one initially suggested. This downloads the file to distribute according to your network configuration and your company's distribution policy (FTP, e-mail, shared folder, login script, other distribution tools such as Microsoft SMS, Tivoli, etc.).

 **Reference:** For more information, refer to the help file or documentation of the distribution tool you want to use.

Whether you are downloading the distribution tool or downloading the default scan client, you can click on profile management to check the configuration of the profile being used.

You can modify the name of the executable programs that you download from the Web service (both the **scan client** and the **distribution tools**).

In order to correctly distribute the scan client to the computers to audit, simply bear in mind the name assigned to the executable file to ensure that references used in the deployment tools (Active Directory, SMS, Tivoli... or Malware Radar) are correct.

3. Manage the distribution profiles

The distribution profiles are a very convenient and organized method for carrying out actions such as: configuring the type of Internet connection (or the place to leave the reports if there is no Internet connection), the type of scan to carry out and the exclusions. In the online help, you will find more information about configuring these operations.

By creating and configuring installation profiles, the installation types can be organized by the characteristics of the users and of the corporate network.

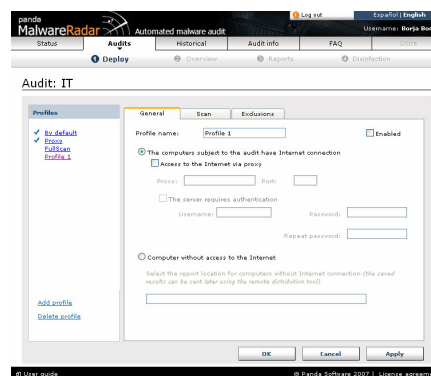
You can configure the scan before downloading. To check the initial settings of the scans, go to profile management in one of the following ways (bearing in mind that at least one audit will have previously been started):

- **Audits > Start audit> Profile management.**
- **Status > (My status section) > Start audit > Profile management.**

In the profile management section, you will find the **default profile** used to create the scan tool. The **Default profile** cannot be modified.

If you want to customize a profile in accordance with the types of scans, or exclusions you want to apply to a certain number of computers, follow these steps:

1. Click on **Profile management**.
2. Click on **Add profile**.
3. Enter the name of the new profile and define the settings you want to use in the computers to which you will distribute the scan tool with this profile:
 - Configure the Internet access settings of the computers to audit (if they have Internet access).
 - Types of scans.
 - Directories excluded from the scan and disinfection.
4. Once the new profile is configured, click on **OK**.



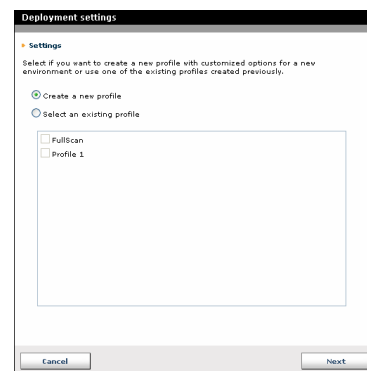
3.1 Profile creation Wizard

Click on the **profile creation wizard** if you want to create clients or distribution tools with customized options.

For more information, refer to the deployment wizard help file available from the product's Web service.

3.2 Profile management

Click on **Profile management** to check and, if necessary, alter the characteristics of one of the available profiles.



Remember the **Default profile** cannot be modified. If you still don't have a profile (except the default profile), you can also click on **Add profile** and follow the instructions at the beginning of this chapter.

4. Deploy the scan program to the computers you want to audit.

Distribute the program to the computers you want to audit using the deployment method that best adapts to the needs of your network:

- **Manual deployment.**

Download the scan client or program to manually deploy the scan across your company. Use this type of deployment in computers outside the local area network.

Manual deployment is simple: Download the scan program and distribute it using the deployment method that best adapts to the needs of your network.

In this chapter, you will find information and practical examples with deployment methods using Active Directory, PsExec, SMS, Tivoli and other tools. You also find out how to configure or disable local firewalls in order to distribute the scan program effectively. For more information, consult the documentation from the developer of the deployment tool used on your corporate network.

If you do not have a file distribution tool on your network, it is not necessary to install any of the tools mentioned above. In this case, use the automatic deployment method summarized in the following point and explained in more detail in the following chapter.

- **Automatic deployment.**

Use the automatic distribution tool in Malware Radar if you do not have a file distribution system on your corporate network. In the following chapter, you will find more information on how to do this.

Automatically distributes the scan clients to the computers connected to the network. It is not necessary for all computers to have an Internet connection, as long as one of them can download the distribution tool and is connected to the same network to which the scan client will be distributed.

Remember that the distribution tool is included in the product's Web service and distributes the scan client to the computers to be audited. Refer to other sections of this guide or the help file for more information.

General methods of distribution

It is not difficult to distribute the scan program to carry out the audit in a homogenous environment. A homogenous working environment is characterized by:

- NT technologies.
- Shared administrative resources.
- The domain administrator is the local administrator of computers.
- Personal firewalls that prevent reception of executable files, such as the scan program, are not enabled (or they are enabled, and exclude file and printer sharing).

In this type of environment, the process is the same as for distributing an executable program to your corporate network computers.

You can choose between **manual deployment** (distributing the scan program using Active Directory, SMS or whatever system you use on your network), or the **automatic system** (available in Malware Radar thanks to the deployment tool).

This chapter describes the installation process for heterogeneous networks in which administrators have one or more of the following items, resources or tools.


- Networks with personal firewalls (Windows XP or other personal firewalls)
- Windows XP Home/Me/98/95
- Active Directory
- SMS
- PSEXEC
- Work groups

4.1 Networks with personal firewalls

If any of the computers in your network to which the scan tool will be distributed have a personal firewall, follow these instructions:

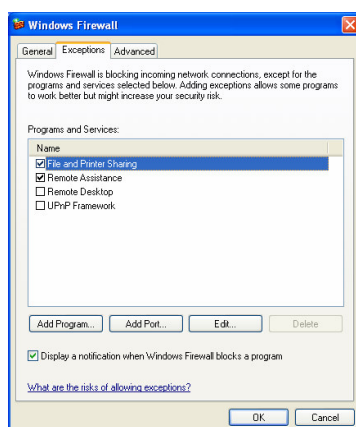
4.1.1 Windows XP firewall

Default installations of Windows XP with SP2 install and enable the personal firewall. In corporate environments where the domain administrator has direct access to shared resources on workstations, the firewall does not prevent distribution of the scan program.

 **Note:** Bear in mind that the scan program is an executable that you can rename and distribute in the form that best adapts to the characteristics of your network. The information below will help you resolve the most common incidents caused by firewalls preventing distribution of the executable file.


One of the fastest ways of distributing the program without needing to disable the Windows XP firewall is as follows:

1. In Windows, disable the option: **Use simple file sharing**. By doing this, the `admin$` resource will be available. In the following section, you will find more information on how to do this.



2. In the Windows XP firewall settings (**Control Panel > Security Center**), enable **File and printer sharing** in the **Exceptions** tab of the **Windows firewall**.

File sharing settings in Windows XP

 **Note: Simple file sharing** means that remote connections to shared resources are only identified as Guest users. You need to disable this option to act as administrators. This is an essential requirement in order to copy and run files on remote computers.

To disable **Simple file sharing in Windows XP Professional**, follow the instructions below:

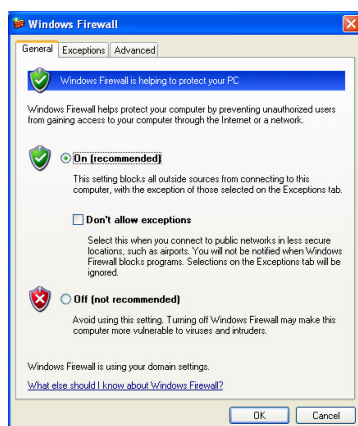
1. Double-click on **My computer**.
2. In the **Tools** menu, click on **Folder options**.
3. Click on the **View** tab and clear the **Simple file sharing** check box.

Configuring the Windows XP firewall to allow distribution of the scan program

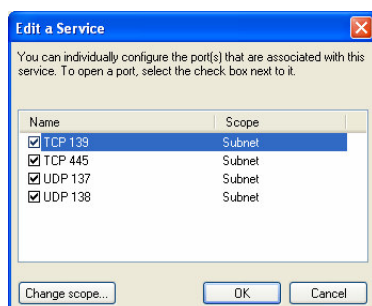
The aim is to allow traffic through TCP ports 139 / 445 and UDP ports 137 / 138. You can enable the **File and printer sharing** option in the **Exceptions** tab in the Windows XP firewall to carry out the task automatically without needing to create an additional rule.

If you want to check that the **File and printer sharing** option is enabled and the necessary ports are configured:

1. In the Windows XP firewall settings (**Control Panel > Security Center**), check that **File and printer sharing** is enabled in the **Exceptions** tab of the **Windows firewall**.



2. To check the ports associated with the **File and printer sharing** service, click on **Edit**.



Disabling the Windows XP firewall in environments with Active Directory

Before starting to distribute the scan program, bear in mind the credentials and tools to use.

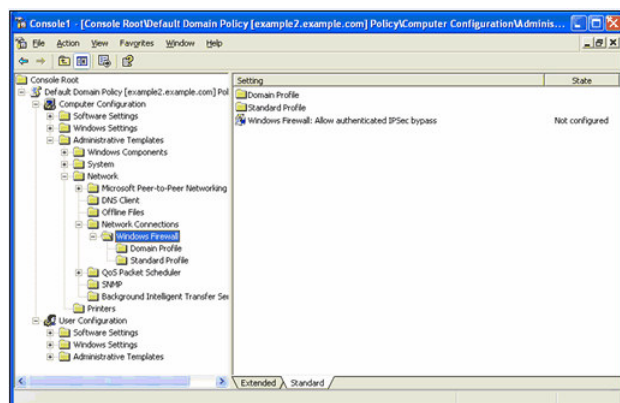
- **Credentials:** Logon a Windows XP SP 2 computer, which is a client of the Active Directory domain, as a member of the **Domain administrators** security group, and open the group policy object you modified in the previous task.
- **Tools:** Microsoft Management Console (MMC) with the **Group policy object editor** installed.

 **Note:** To open a GPO use MMC with the Group policy object editor. Alternatively, you can use the Active Directory users and computers console in a client Windows XP computer by running *adminpak.msi* from the Windows Server 2003 CD.

To edit the Windows firewall settings using group policies, in the appropriate GPOs, use the *Group policy object editor* or the *Active Directory users and computers console*.

To configure the Windows firewall options:

1. In Windows XP SP 2, click on **Start, Run**, type **mmc**, and click on **OK**.
2. In the **File** menu, click on **Add/remove Snap-in**.
3. In the **Standalone** tab, click on **Add**.
4. In the list of *Available standalone snap-ins*, select **Group policy object editor** and click on **Add**.
5. In the **Select group policy object window**, click on **Browse**.
6. Select the group policy object you want to configure and click on **OK**, and then on **Finish**.
7. Use the **Close** button to exit the **Add standalone snap-in** window.
8. Click on **OK** to exit the **Add/remove snap-in** window and return to the administration console.
9. In the console organization tree, open **Computer Configuration, Administrative templates, Network, Network connections and Windows firewall**.



Once you have configured the Windows firewall options:


1. The next update of the group policies will download the new Windows firewall options.
2. They will be applied to computers running Windows XP SP 2.

If you decide to disable the Windows firewall across the network, you will have to configure three groups of options:

- In **Network connections**, change the mode of the *Prohibit use of Internet Connection Firewall on your DNS domain network* policy to **Enabled**.
- In **Windows Firewall > Domain Profile**, clear the **Protect all network connections** check box.
- In **Windows Firewall > Standard Profile**, clear the **Protect all network connections** check box.


 **Notes:**

- The standard profile configuration ensures that the Windows firewall is not used either when connecting to the corporate network, or otherwise.
- To ensure the Windows firewall is not disabled at all times, for example, when computers don't connect to the corporate network, change the status of the options described above to **Enabled**.
- The standard profile options are usually more restrictive than the domain profile options because they don't include applications and services that are only used in a managed domain environment.

 **Warning:** The information offered in this guide about the Windows firewall or distribution methods based on the infrastructure of your network in no way replace the recommendations and documentation provided by the developers of these products.

4.1.2. Other personal firewalls

If you use a firewall from other developers on your corporate network, please refer to the corresponding documentation to disable the protection that prevents the scan tool from being distributed.

 **Warning:** In general, for personal firewalls that could be installed on networked workstations you will have to ensure that NetBios access to port 137, UDP port 139 or TCP port 445 is enabled from the computer on which you run the distribution tool.

4.2 Distribution in Windows Me/98/95/XP Home

For workstations with Windows Home/Me/98/95 there are several alternatives for distributing the scan program:

- **Login Script.** These are codes or programming sequences used to start up the computer. Batch process files (*BAT*), or script programming languages (*VBS*, *JS*...) can be used to organize to start up computers on networks within a corporate environment.
- **Direct execution** (locally). Where there are few workstations, you can share files in a network directory and access them from each computer. Where there is a large number of workstations, it is better to opt for automatic file distribution, using the deployment method established on your network (Active Directory, SMS, etc.).

If you do not have automatic file distribution on your network, use whatever system you normally use to distribute a file of this type: FTP, email, CD-ROM or DVD with the program, etc.

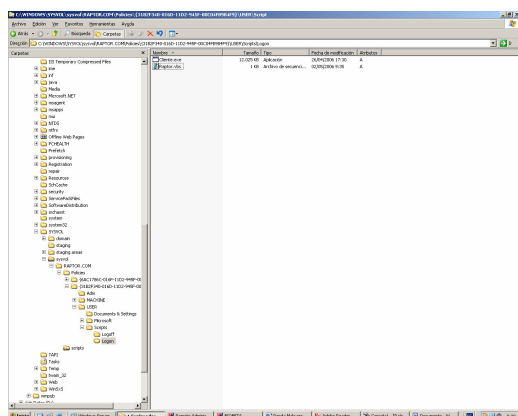
Remember that the name of the scan program file can be changed once downloaded from the Web service. Simply remember the name assigned to the file so that when it is distributed, the administrator or end user of the computer run it without any further complications, bearing in mind that they must have permissions for the Windows XP Home/Me/98/95 computer.

4.3 Active Directory

Distribution of the scan tool using Active Directory is one of the most reliable methods in correctly structured and configured Windows networks.

This section explains the options offered by Active Directory for distributing the tool. Remember that the information in this guide about using third-party distribution tools is not intended to replace the information provided by the corresponding developer.

You can use the folder corresponding to the specific policy. This folder will be displayed when you click on **Browse**.



 **Warning:** Only the domain administrator can configure scripts in a domain controller.

It is advisable to use the **Logon/Logoff** options. If you use the *Computer Configuration*, Logon/Logoff policies, the process will run with the *Local System* account, without taking access to network resources into account. This could lead to errors in audits configured to leave reports in network resources.

How to access the Group Policies console:

1. Start the session as a member of the *Domain administrators* security group, the *Organization administrators* security group or the *Group Policy Creator Owners* security group.
2. Open the *Group policy object editor* by clicking on the Windows **Start** button, then click on **Run**, type *gpedit.msc* and click on **OK**.

To edit a group policy object, click on the object and then on **Edit**.

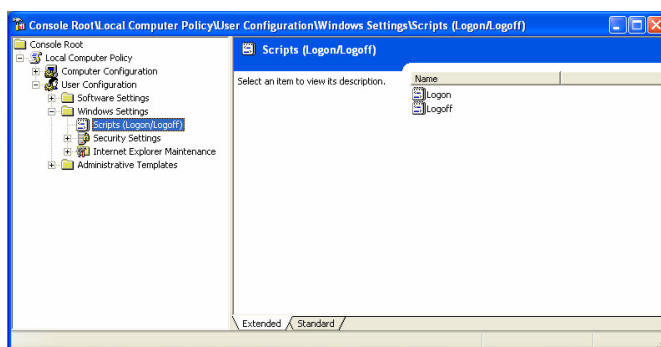
To create a group policy object, click on **New**, type the name of the new object, and then click on **Edit**.

The changes made to the local group policy object will be saved automatically.

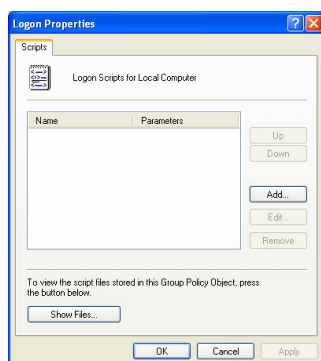
4.3.1 Assigning logon scripts

This is the best option when users have the necessary permissions locally. In this case, follow these instructions:

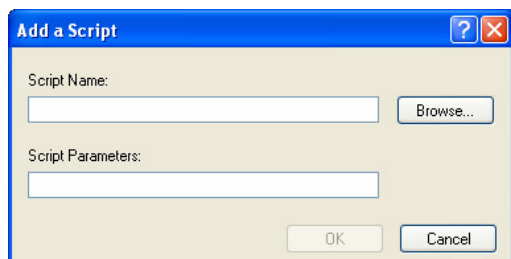
1. Open the *Group policy object editor*.
2. In the console tree, click on **Scripts (Logon/Logoff)** in the path: *Group policy object/User Configuration/Windows settings/Scripts (Logon/Logoff)*.



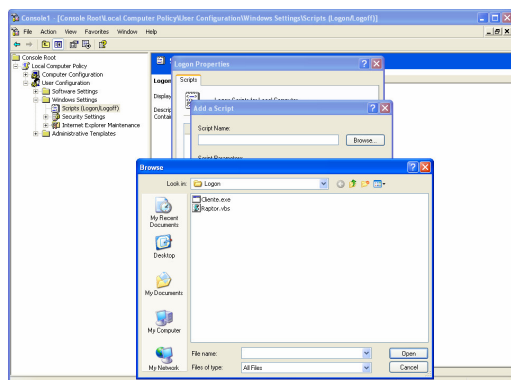
3. In the details panel, double-click on **Logon**.



4. In the **Logon Properties**, click on **Add**.

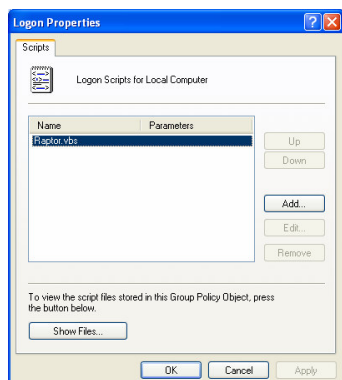


5. In **Add a script**, in **Script Name**, type the path to the script or click on **Browse** to search for the script in the *NetLogon* shared folder on the domain controller.



- In **Script Parameters**, enter the parameters you want in the same way as you would type them on the command line. For example: `//logo` (display banner) and `//I` (interactive mode).

On assigning several scripts, they will be processed in the specified order. To move a file up the list of scripts, select it and click on **Up**. If you want to move it down, select it and click on **Down**.



4.3.2 Assigning startup scripts

This option is recommended for users without local permissions and for which the audit does not require access to network. Configuration is very similar to the previous case.

- Open the *Group policy object editor*.
- In the console tree, click on **Scripts (Startup/Shutdown)** in the path: *Group policy object/Computer Configuration/Windows settings/Scripts (Startup/Shutdown)*.
- In the details panel, double-click on **Startup**.
- In the **Startup Properties** dialog box, click on **Add**.
- In the **Add script** dialog box, do the following:
 - In **Script Name**, type the path to the script or click on **Browse** to search for the script in the *Netlogon* shared folder in the domain controller.
 - In **Script Parameters**, enter the parameters you want in the same way as you would type them on the command line. For example, if the script includes the parameters `//logo` (display banner) and `//I` (interactive mode), type `//logo //I`.



Notes:

- To complete the process, logon as a member of the *Domain administrators* security group, the *Organization administrators* security group or the *Group Policy Creator Owners* security group.
- The startup scripts are executed as *Local System* and have all rights associated in order to do so.
- The server might operate differently, depending on the version and operating system installed, as well as the accounts permissions and the menu settings.

4.4 SMS

Systems Management Server is a distribution tool for Microsoft networks for: hardware and software inventories, controlling licenses, deployment of software (distributing and programming software on the network) and organizing the network. SMS operates on NT Server using MS SQL Server 6.5 (or later) as a database.



SMS, like other developers' distribution tools, should only be used to distribute the scan program in Malware Radar when this type of infrastructure is already activated on your network. The information below does not replace the documentation of the developer.

The **discovery methods** are the different ways that SMS has of completing the database with computers and users. Several methods are available:

4.4.1 Discovery by login script

With this method, SMS modifies the *login scripts* of users in a selected domain so that they run *smsls.bat* on logging on. SMS copies the necessary files to the *NETLOGON* of the domain *PDC*:

- When logging on one of the workstations, the *login script* is run.
- To check that the computer has been detected, run the search from *All Systems*.

4.4.2 Discovery of users and groups

You can program the search for new users and groups every X minutes. In this way, you can check that the searches for *All user groups* and *All users* display all domain users.

4.4.3 Network discovery

If you activate network discovery using the domain and subnet, configure the timer to find more computers on the network.

4.4.4 Distributing the program using login script

Select the login script method and activate it on the object property pages. Edit the previously generated login scripts. When a user authenticates in a workstation, the login script will run automatically to install the scan program.

4.4.5 Remote distribution of the scan program

Select the remote installation method and activate it on the object property pages. Delete the login script of a user (using Windows *User Manager*).

On installing the scan program using SMS, you will see several icons in the Windows Control Panel on the target computer. These icons belong to programs that let you configure and consult the status of the scan program installed on computer.

4.4.6 Distributing the software

SMS allows deployment of software. This is a task scheduler that executes software configured on computers.

The SMS software distribution program is responsible for executing the tasks on computers. There are many options for configuring these tasks according to different scenarios: whether users are logged on or not, the permissions with which the program is to be executed.

The distribution of software is carried out in the section: **Advertised Programs Client Agent**.

In SMS the program to be distributed is a **package** and the computers from which they are distributed are called **distribution points**. Initially, the SMS server has one distribution point, but more can be created in other servers or shared resources.


The steps to follow to distribute the scan program with SMS are:



1. In the *packages* branch, create a new package indicating the location of the scan file (the package).
 2. The scan program you have previously downloaded from the Web service becomes a new installation program with the data needed to run the program.
 3. Add the previously created *distribution point*.
 4. SMS will pass the files to this *distribution point*.
-
5. Create a new *advertisement* to install the package in the collection that contains all workstations with NT.

4.5 PsExec

You can also distribute the scan program using tools such as *PsExec*, a program that allows distribution of executables such as the Malware Radar scan program.

 **Note:** If you're not familiar with the use of this distribution system, use the distribution tool that lets you distribute Malware Radar automatically. The information here will help you use the distribution tool but does not replace the documentation provided by the developer of the application.

Executing PsExec allows you to enter multiple parameters:

```
psexec [\\path [,computers[,..] | @files ][-u username [-p password]][-ns][l][-s|-e][-i][-x][-c [-f|-v]][-d][-w directory][-<priority>][-an,n,...] cmd [arguments]
```

For more details on the PsExec parameters consult the developer's documentation for this distribution program.

Examples of using PsExec to distribute the scan program:

- `psexec \\(name of workstation or server) -c malwaredar.exe`

Command that copies the malwaredar.exe program (or the name that you have given the scan program downloaded from the Web service) and executes it interactively.

- `psexec \\(name of workstation or server) c:\path\malwaredar.exe`

Command that executes the malwaredar.exe program (or the name that you have given the scan program downloaded from the Web service) and in which it has previously copied to the remote computer. In this case, you also specify the path of the program to run.

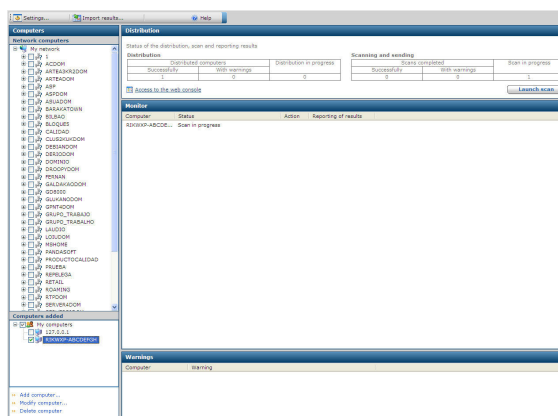
In these two examples, if you omit the name of the workstations or servers to which to copy and run the Malware Radar scan program, it will be run locally, i.e. on the computer using the PsExec tool.

5. Using the Malware Radar distribution tool (if you have not used one of the other methods of deployment or distribution).

Run the distribution tool you have downloaded. The program allows you to add computers to the audit and run the corresponding scan.


The distribution tool window is divided into several sections.

- On the left (**Computers**), you can select the computers to audit.
- In the top right you can **Launch scan**.
- In the centre, you have a monitor indicating the status of the computers.
- At the bottom right, you will see warnings related to the scan process and the audit.



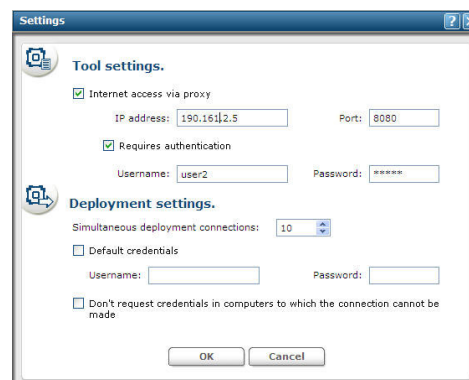
Click on **Settings...** and if necessary, configure access through a proxy server and configure deployment.

You can also add computers using their IP addresses or IP ranges (*format: xxx.xxx.xxx.xxx – yyy.yyy.yyy.yyy*). Separate the initial address in the range from the last address using a hyphen, which appears pre-formatted in this option, for example, 192.168.1.1-192.168.1.254), or using NetBIOS computer names or DNS names.

 **Warning:** If you do not enter the necessary details for deployment or these details are incorrect, the deployment tool will request the necessary details for a specific computer unless you have selected the check box **Don't request credentials in computers to which the connection cannot be established**.

In order to correctly configure the tool.

1. If necessary, enter the proxy server IP address, port and authentication data.
2. To optimize deployment in the corporate network you can limit the maximum number of simultaneous connections. Adapt the number to the capacity of your network.
3. For the deployment of the scan client you can establish login details that will be used in each of the remote computers in which authentication is necessary, such as, workstations in a workgroup that are not authenticated in a domain, in which the administrator has a common username and password.
4. If you don't want login details to be requested in computers to which there is no connection, select the corresponding checkbox. This situation will mean that the scan will not start and computers will therefore not be audited.



 **Reference:** If you want more information about the deployment process and other questions related with the audit, please consult the additional documentation available and the support website.