SecureWave
Sanctuary®
Safeguarding Tomorrow

Sanctuary Client Deployment Guide

Liability Notice

Information in this manual may change without notice and does not represent a commitment on the part of SecureWave.

The software described in this manual is provided by SecureWave S.A. under a license agreement. The software may only be used in accordance with the terms of the agreement.

No part of this publication may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without the prior written permission of SecureWave.

SecureWave claims copyright in this program and documentation as an unpublished work, revisions of which were first licensed on the date indicated in the foregoing notice. Claim of copyright does not imply waiver of other rights by SecureWave.

Trademarks

Sanctuary is a trademark of SecureWave S.A.
All other trademarks recognized.

SecureWave
Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Luxembourg

Phone: +352 265 364-11 (from USA & Canada, dial 011 352 265 364 11)
Fax: +352 265 364-12 (from USA & Canada, dial 011 352 265 364 12)
Web: www.securewave.com

Technical Support hours are Monday to Friday, 8:30 to 18:00 CET/CEST (2:30 AM to 12:00 PM ET/EDT).

You can contact our technical support team at:

+352 265 364 300 (international),
+1 800 571 9971 (US Toll Free),

or by sending an email to support@securewave.com

Published on: March 2006

Contents

Introduction

This guide explains how to use the Sanctuary Client Deployment Tool.

- *Chapter 1: The Client Deployment tool*: gives you a brief overview of the purpose and features of the Sanctuary Client Deployment Tool.
- *Chapter 2: Creating a deployment package*: describes how to create a deployment package.
- *Chapter 3: Installing the Deployment Package on client computers:* describes how to install the deployment package on to client computers.
- *Chapter 4: Managing deployments*: describes how to manage client computers after the client package is deployed.
- In *Appendix A: Opening firewall ports for client deployment* you will find the procedure to open those required ports needed for the client deployment technique described in this document.

Additional Information

In addition to the documents and the online help provided with Sanctuary Device Control, further information is available on our web site.

http://www.securewave.com

This site provides:

- The latest software upgrades and patches (for registered users).
- The very latest troubleshooting tips and answers to FAQs.
- Other general support material that you may find useful.

We regularly update the SecureWave Web site with new information about Sanctuary Device Control.

Explanation of Symbols

The following symbols are used throughout this guide to emphasize important points about the information you are reading:

Special note. This symbol indicates further information about the topic you are working on. These may relate to other parts of the system or be points that need particular attention.

Time. This symbol placed before a paragraph indicates a 'short-cut' that may save you time.

Caution. This symbol means that proceeding with a course of action may result in a risk, e.g. loss of data or potential problems with the operation of your system.

Typefaces

The following typefaces are used throughout this guide:

> This typeface (*italic*) is used to represent fields, menu options, and cross-references.

> This typeface (`fixed width`) is used to represent messages or commands typed at a command prompt.

> This typeface (SMALL CAPS) is used to represent buttons you select.

Support and Contact Information

If you have a query that is not covered in any of the documentation made available by SecureWave, you can contact customer support:

Phone: +352.265364-300 (from USA & Canada, dial 011 352 265 364 300)
+1 800 571 9971 (US Toll Free)
Fax: +352.265364-12 (from USA & Canada, dial 011 352 265 364 12)
Web: www.securewave.com
eMail: support@SecureWave.com

Technical Support hours are Monday to Friday, 8:30 to 18:00 CET/CEST (2:30 AM to 12:00 PM ET/EDT).

Alternatively, you can write to customer support at:

SecureWave Support
Atrium Business Park
23-ZA Bourmicht
L-8070 Bertrange
Luxembourg

Chapter 1: The Client Deployment tool

The purpose of creating Sanctuary Client Deployment packages

Once you have installed and tested your Sanctuary configuration on a few computers, you will want to deploy it on all or most of the computers on your network. If you have a large number of computers to manage, the Client Deployment tool is the easiest way of ensuring that all have the correct package, and of obtaining a list of the machines that already have the client deployed.

If you prefer to use another deployment tool, you should be aware that some of them, by design limitations or errors in their configuration, do not do a completely 'silent' installation and sometimes fail since they are waiting for user input.

If you are installing Sanctuary on Windows XP SP2 machines, you need to open certain blocked ports to be able to do an unattended client installation. Refer to Appendix A: Opening firewall ports for client deployment *on page* 33 *for more details.*

You cannot install Sanctuary Server Edition's client on Windows XP or Windows 2000 Pro machines.

Prerequisites for creating a Sanctuary Client Deployment package

To create and install a deployment package you must meet the following conditions:

- The administrator running the Client Deployment tool is in the Local Administrators group on all targeted computers. (You can also use the command "net use \\<computer>" to log on as an administrator.)
- You must synchronize the clocks of the different computers. You can use Windows Time Service (W32Time, based on Simple Network Time Protocol or SNTP) to maintain date and time synchronization for computers running Windows 2000 or later.

- The operating system where the deployment tool (Deploy.exe) is running must be Windows 2000, Windows XP Professional, or Windows Server 2003.
- If you are running de deployment tool on Windows XP SP2, check Microsoft Knowledge base article 884020 (http://support.microsoft.com/default.aspx?scid=kb;en-us;884020 Programs that connect to an IP address that are in the loopback address range) and, if necessary, install the provided patch.
- The deployment tool will not work under Windows NT4; it is not designed to deploy clients on Windows NT4 computers.
- If there is a firewall between the Sanctuary Client Deployment and the computer where you want to deploy the Sanctuary Clients, open the following incoming ports on the client computers (see *Appendix F* of the Setup Guide):

    1. TCP 33115 (33114 for older versions of SAC)
    2. TCP: 139, 445 NetBIOS
    3. UDP: 137, 138 Browsing

Installing the Client Deployment tool

The *Client Deployment* tool is installed, among others tools, during the setup of the *Sanctuary Console*. Refer to *Chapter 4: Installing the Sanctuary Console* in the *Setup Guide* for more details.

When considering the choice of the computer on which you will install the Client Deployment tool and from which you will start the deployment, consider the following points:

- The deployment of the Sanctuary client on a long list of computers might take some time. You cannot log off the computer during that period.
- The tool makes significant use of the network resources of the computer where you install it.
- NEVER interrupt an ongoing deployment.

Installing packages

The installation process is done in two parts:

1. Create package(s):
   The deployment tool allows you to select client installations (from the CD-ROM, LAN, or local drives). The deployment tool makes a local copy of the client installation and then displays the 'Options – SecureWave Installation Transform' dialog so that you can create an installation transform (.MST) linked to the MSI file.

   ✍ *An installation transform is a customization of the installation which predefines settings for the installed application. Having an installation transform allows the system administrator to apply identical settings to a group of client computers.*

2. Install/Uninstall package:
   You select the target computers and a package then initiates (un)installation. After you set the reboot options, the deployment starts.

The following chapters describe the installation process.

Chapter 2: Creating a deployment package

To create a deployment package, follow these steps:

1. Select *Sanctuary Client Deployment* from the *Start → Programs → Sanctuary Device Control* (or corresponding installed component) menu. The following dialog appears on first use.

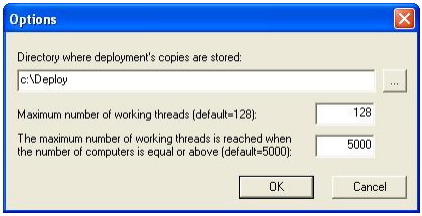

Figure 1: Creating a deployment package: folder to store deployment packages

2. Choose a folder where you would like to store all the deployment packages. You can modify this setting by using the *Options* entry of the *Packages* menu at a later point in time. Do not change other settings.

Do not specify the root directory of the system drive or any other directory where existing files already reside or might be created by other applications.

If the deployment tool is installed on different machines, you might want to specify a shared directory where all instances of the deployment tool can access the company packages.

3. Click OK. The following dialog appears:

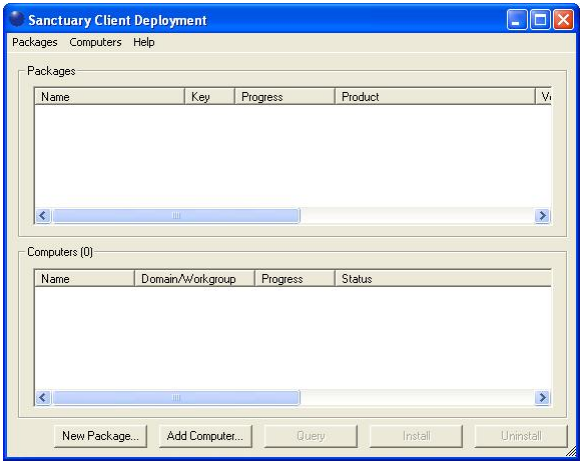

Figure 2: Creating a deployment package: main screen

4. From the *Packages* menu, select *New*. The following dialog is displayed:

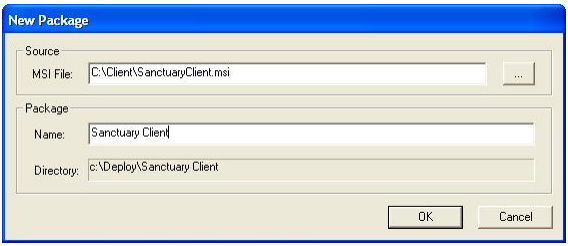

Figure 3: Creating a deployment package: new package

5. Click the ... (ellipsis) button to select an MSI file, typically from the CLIENT folder of the CD-ROM, and type in the name you wish to give to the package. Take note of the directory, we will refer to it as the Deployment Package Folder (C:\DEPLOY in this example).

6. Click OK. The installation files are copied in a subfolder of the destination directory as defined in point 1 (C:\DEPLOY in our example). Then the *Options – SecureWave Installation Transform* dialog appears as shown below:

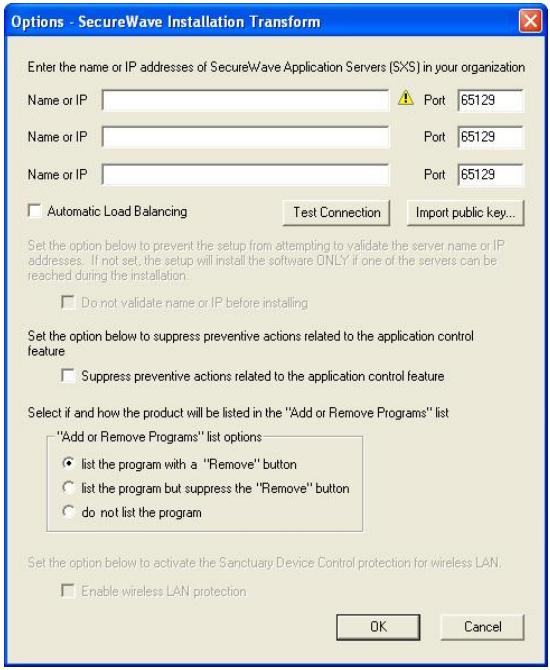

Figure 4: Creating a deployment package: application Server IP or name

You can see two grayed-out options that are only valid if you are installing older versions of our client:

DO NOT VALIDATE NAME OR IP BEFORE INSTALLING. Used to give a Server address or name that is not available at the moment but will be accessible afterwards.

ENABLE WIRELESS LAN PROTECTION. An option available in older clients (v2.8 and before) that has now been superseded by permissions rules.

7. Click IMPORT PUBLIC KEY.

   Select the sx-public.key file located in the %SYSTEMROOT%\SYSTEM32 folder of the *SecureWave Application Server* machine.

If you do not find a sx-public.key file in the %SYSTEMROOT%\SYSTEM32 or the %SYSTEMROOT%\SXSDATA folders of the SecureWave Application Server, it means that your installation is using default keys. You should not deploy the clients in a production environment without having generated your own set of keys. Please refer to Chapter 9: Using the Key Pair Generator *in the* Setup Guide *for more details. Keep in mind that replacing an existing set of keys or implementing customized keys in an environment where encrypted media — if you are using Sanctuary Device Control — are already in use will prevent access to those media altogether.*

Although not recommended, it is possible to deploy the clients on test environments without a customized set of keys. If you do not want to generate custom keys, simply skip this step.

The Sanctuary Clients can now be deployed without specifying a server address(s) that can immediately be validated: the server at the provided address(s) is contacted during the actual setup to make sure the client can communicate with it. If this communication is not achieved, the installation is aborted unless the 'Serverless Mode' option is selected. See next step for more information.

8. Enter the names or IP addresses of the SecureWave Application Servers to which these clients will attempt to connect, using the *Name or IP* fields. If alternative port numbers are required for these connections, then also type in the modified port numbers. If you do not specify any name or address, you are installing in 'SERVERLESS MODE'. While using this mode, the installation routine will not abort if it cannot reach one of the application servers. Alternatively, if you do not leave them empty, at least one of them must be contactable for the installation to continue; the install will rollback if all connection attempts fail. When installing in 'Serverless mode', you can also control policies by exporting them to a special file (polices.dat) and you must also include the license file. See *Chapter 5* of the *Setup Guide* for more information.

   When proceeding without specifying servers, you get the following warning message:

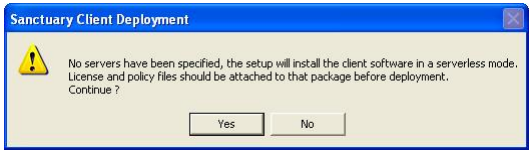

Figure 5: Message when installing in "Serverless mode"

9. Choose whether to select the *Automatic Load Balancing* checkbox. If you select this checkbox, the Sanctuary Client driver attempts to contact one of the servers listed in a random fashion. Alternatively, if you leave *Automatic Load Balancing* unchecked, the Sanctuary Client driver attempts to contact the application servers in the order they are listed.

10. Click on the TEST CONNECTION button to verify the names or IP Addresses you have entered. A confirmation or failure dialog box is displayed. In the case of failure, check the error message for further details about the possible cause of failure (e.g. key pair mismatch, DNS resolution). Here are some examples:

Figure 6: Message when the connection test fails

Figure 7: Message when the connection test fails (key related)

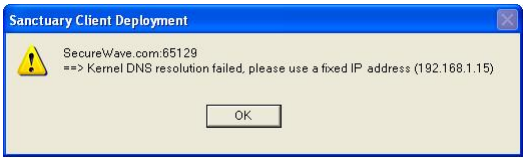

Figure 8: Message when the Kernel DNS resolution fails

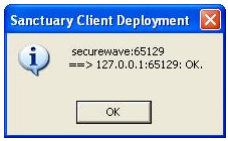

Figure 9: Message when the connection test succeeds

Click OK to clear the message.

11. Select those options controlling how the client driver is shown in the *Add or Remove Programs* Windows' dialog:

    SUPPRESS PREVENTIVE ACTIONS...: Since the client software depends on the licenses you own, it is possible to completely block a computer if you do not export correctly the policies ("serverless" installation) or define them before hand. This is especially true when installing our Sanctuary suite and not authorizing those files belonging to the operating system. To avoid this block out, the program first verifies if there is an update from Sanctuary Device Control to Sanctuary Suite and that this action does not blocks the machine. If this is the case, the installation will not proceed and will rollback. Use this option if you do not want this check done and you are sure that you have correctly defined the policies.

    LIST THE PROGRAM WITH A "REMOVE" BUTTON – The program is listed in the "Add or Remove Programs" Windows' dialog in the 'standard' way; it will include a *Remove* button.

    LIST THE PROGRAM BUT SUPPRESS THE "REMOVE" BUTTON – The program is listed in the "Add or Remove Programs" Windows' dialog but will not include a *Remove* button.

    DO NOT LIST THE PROGRAM – The program will not appear in the "Add or Remove Programs" Windows' dialog.

12. Click on the OK button to close the dialog.

    The new package appears in the Sanctuary Client Deployment packages list:

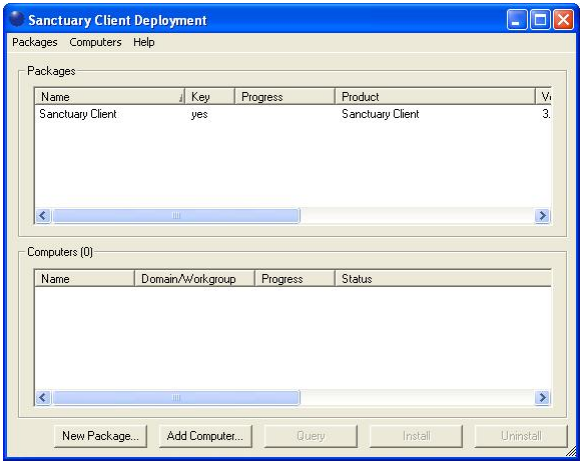

Figure 10: Creating a deployment package: new package created

A small file called *Sanctuary Client.MST* is created in the Deployment package folder (C:\DEPLOY in our example). Select *Options* from the *Packages* menu to check the location of the Deployment package folder on your installation. The specified directory contains subdirectories corresponding to the packages you have just created.

You can see the options of each generated package in the main window:

Name	Key	Progress	Product	Version	Server(s)	Last deployment	License	Policies
Marketing Remote	yes		Sanctuary Client	3.2	securewave:65129		no	yes
Sales Restricted	yes		Sanctuary Client	3.2		Install - 01-11-2006 14h37m19s	yes	no
Sanctuary Client	yes		Sanctuary Client	3.2			no	no

Figure 11: Sanctuary client deployment: package option

If the public key or license (in the case of an installation without servers), is not included in the package, it is displayed, as shown above, with an orange background to warn you. If there is no orange background, the key and license, if applicable, are present and the package is ready to be deployed. It is not recommended to deploy packages without a public key – or license – in a production network.

Chapter 3: Installing the Deployment Package on client computers

A small file called *Sanctuary Client.MST* – created in the previous chapter – is located in the package folder (c:\Deploy in our example). It can be used to install the clients. To proceed with the installation, follow these steps:

1. Select *Sanctuary Client Deployment* from the START → PROGRAMS → SANCTUARY DEVICE CONTROL (or corresponding program's name) menu. The following dialog appears:

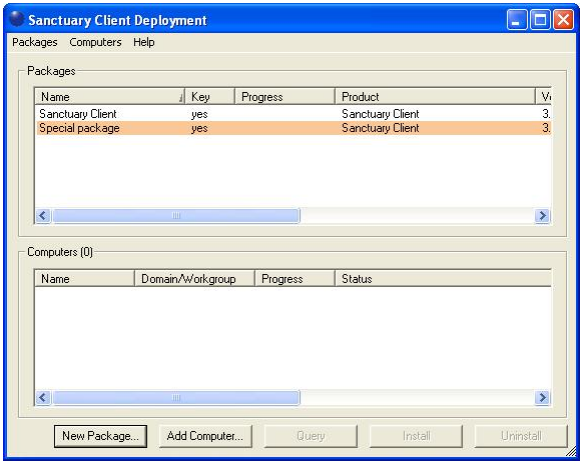

Figure 12: Installing packages: pending package(s)

If the public key or license (in the case of an installation without servers), is not included in the package (see step 7 & 8 in Chapter 2*), the package is displayed as shown above with an orange background to warn the user. If there is no orange background, the key and license, if applicable, are present. It is not recommended to deploy packages without a public key – or license – in a production network.*

2. Click on the ADD COMPUTER button. One of the following dialogs appears, depending of your operating system:

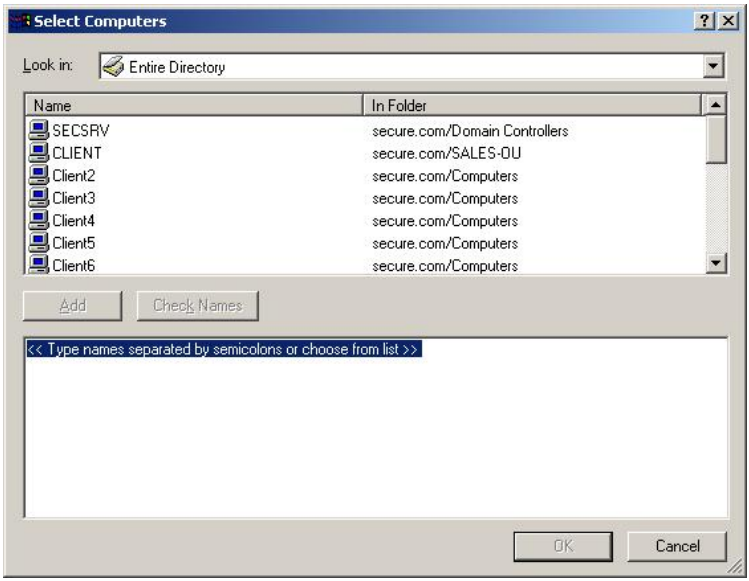

Figure 13: Installing packages: select computer(s) (sample 1)

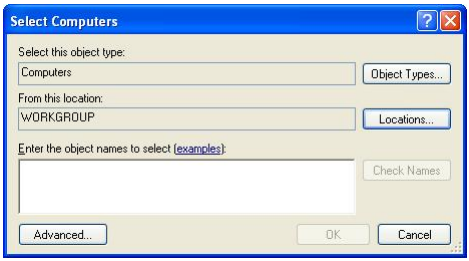

Figure 14: Installing packages: select computer(s) (sample 2)

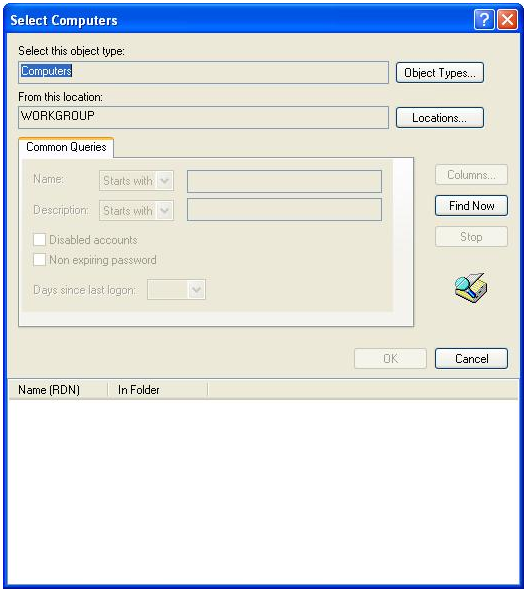

Figure 15: Installing packages: advanced selection dialog

You can also do a Drag & Drop between the external Microsoft Windows Network (from the My Network Places icon) selection dialog.

3. Select the domain you want to search. Then highlight or type the names of the computers you want to add to the list. You can type in multiple names by separating them using a semicolon character ";".

4. Once you have selected the computers you want to add to the list, click OK. The selected computers are now listed in the *Sanctuary Client Deployment* dialog, as shown below.

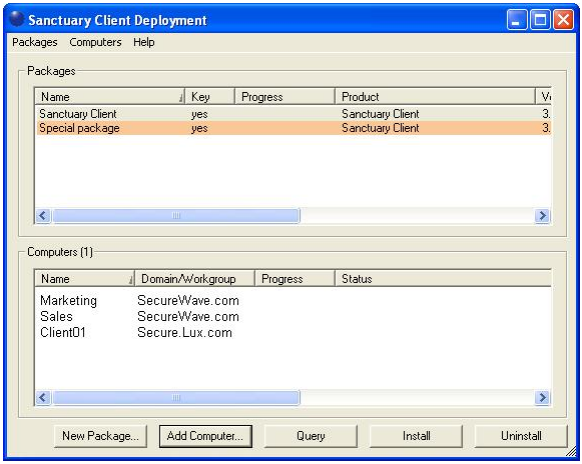

Figure 16: Installing packages: selected computer(s)

If the current or newer version of the client is already installed on a machine you select, it would not be re-installed.

5. Select a package from the *Packages* list.
6. You can optionally select a subset of machines from the *Computers* list.
7. Click INSTALL to start the deployment.
8. If the installation requires a reboot of the client computers, the *Install/Uninstall/Reboot Options* dialog is displayed. Select the options that you decide are appropriate and then click OK.

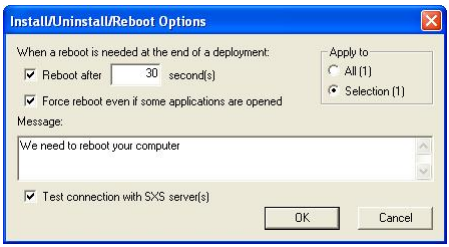

Figure 17: Installing packages: reboot options

You can choose to require a reboot of the client computers after a defined period. You can also enter a text to be displayed to your users.

If a subset of machines was selected from the *Computers* list, the *Apply to* options allow you to select if you want to target only the selected set of computers (*Selection*) or the complete list (*All*).

The *Test connection with SXS servers* option allows you to verify that the application servers defined in the package are up and running before proceeding to the deployment on the client computers. It is a safe precaution to check this option unless you want to do an installation with no servers – optionally controlling the policies with the *policies.dat* file. See *Chapter 5* of the *Setup Guide* for more information.

If the clients are installed while the SecureWave Application Servers are unavailable, they will not be able to obtain permissions – unless they are included with policies.dat – and access to the device/applications will be refused.

By default the client computers are not rebooted at the end of the client installation to avoid interference with the users. However, the client installation requires a reboot – even though the client is installed, it only delivers complete functionality after a reboot. The client un-installation also requires a reboot – the client drivers will stay active until the computer is rebooted.

When you have clicked OK, the *Sanctuary Client Deployment* dialog is displayed indicating the progress of each client installation.

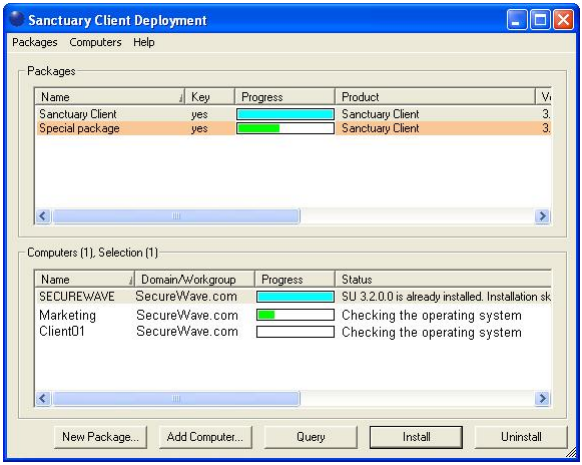

Figure 18: Installing packages: installation progress

9. During deployment, the dialog displays the status for each computer. The progress is shown on the status bar, and the color of the progress bar indicates the state of the task as shown in the following table:

Color		Description
Turquoise		Task completed successfully.
Green		Task in progress with no warning.
Yellow		Task in progress or completed with warnings.
Red		Task in progress or stopped with an error.

Table 1: Installation progress color code

The status column gives you information on the deployment progress for every machine. It reports the error or the warning message when the deployment did not succeed. If the error message reported does not allow you to find the cause of the problem (unknown error, hexadecimal error code), highlight the computer in the list and select *Open Last Log* from the *Computers* menu – or from the contextual menu. The MSI verbose setup log file displayed should contain information on why the setup was aborted and rolled back. You can contact SecureWave's Technical Support Department for further help in analyzing the log file.

Here are some common mistakes to avoid:

- Trying to deploy a client package with a different sx-public.key file than the SecureWave Application Server (Unspecified error)
- Trying to deploy a package while the SecureWave Application Server is offline or cannot be contacted (firewall, wrong IP address) or/and you did not export permissions in *policies.dat* (except when you are trying to do a "serverless" installation – see *Chapter 2: Creating a deployment package* on page *11*)
- Trying to deploy a package on a machine where the client has just been removed without a reboot in between (Error 0x00000643). You must reboot the client machines after uninstalling

The dialog also displays a progress bar for the package being deployed. This progress bar has a mix of green, turquoise, yellow, and red indicating the clients at the various stages of deployment. The progress bar color changes to Turquoise when all tasks are completed successfully as shown. The dialog will eventually have all progress bars filled with diverse colors depending on the result of the different tasks.

When a client deployment is completed, the client computer displays a *System Shutdown* dialog if necessary, as shown below. The message displayed matches the message you type into the *Install/Uninstall/Reboot Options* dialog.

Figure 19: Installing packages: shutdown dialog in the client computer

Chapter 4: Managing deployments

This chapter describes how to manage client deployments packages once they are created with our Client Deployment tool.

The Query button

Once you have installed the Sanctuary Client on some client computers, it is necessary to keep track of where and which packages are installed.

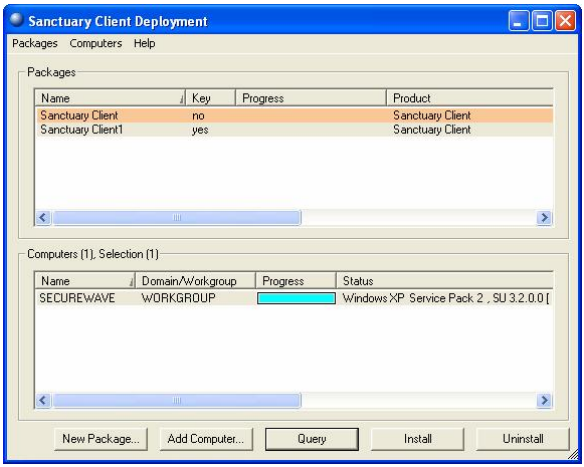

Figure 20: Manage deploy: query

When you the click QUERY button, the *Client Deployment Tool* reports which version of the MSI package is installed on each computer in the list. It also checks if all client drivers are still in place and running and reports the client operating system and version.

> ✍ *This allows you to detect, for instance, if a user has the client installed on their machine but has disabled the drivers.*

The Client Deployment menus

The Packages Menu

The Packages menu has the following items:

Item	Description
New	Allows the user to create a new deployment package, using the process described in *Chapter 2: Creating a deployment package*.
Delete	Deletes the selected deployment package.
Rename	Renames the selected deployment package.
Import public key	Allows the user to choose a public key to be included in the selected deployment package. The dialog shown in *Figure 21* is displayed allowing you to select the public key to be added.
Set Licenses	Opens a dialog where you can import a license to include in the package when it is installed in *Serverless mode*. This is done so that the correct options are installed with the client.
Set Policies	Opens a dialog where you can test the connection with a valid Application Server from where the policies are obtained, and import a public key. See *Figure 22*.
Test Connection	Allows you to verify that the application servers, defined in the package, are up and running before proceeding to the deployment on the client computers. It is not available if you choose the *Serverless Mode* option
Install	Installs the selected package on all computers in the list. (This performs the same function as the INSTALL button as described in step 7 of *Chapter 3: Installing the Deployment Package on client computers*).
Uninstall	Uninstalls the selected package from all machines in the list.
Open last report	Displays a report describing the last install or uninstall, indicating which machines were modified and status (e.g. whether the install was successful or not.)
Options	Allows you to change the root directory where the packages and the application settings are stored.

Table 2: Client deployment menu: packages menu

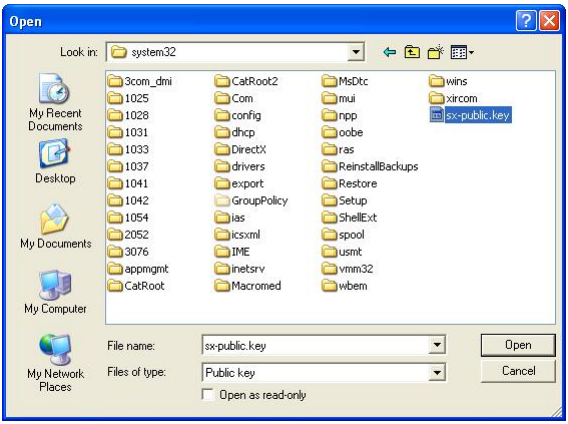

Figure 21: Client deployment menus: import public key

Figure 22: Client deployment menus: set policies

The Computers menu

The Computers menu has the following items.

Item	Description
Add	Displays a dialog allowing you to add one or more computers to the list of computers. This is the same dialog as appears when you click the ADD COMPUTER button.
Remove	Removes the selected computer from the list.
Import	Allows you to import a list of computers from an external ASCII or Unicode text file. The file must be a flat text file with one machine per line. The machine name is optionally followed by the domain name and separated from it only by a "|" sign. Every line looks like this: "ComputerName|DomainName"
Export	Allows you to export a selection of the computers in the computer list to a text file. The file produced is a flat text file with one machine per line. The machine name is followed by the domain name and separated from it only by a "|" sign. Every line looks like this: "ComputerName|DomainName"
Reboot	Forces a reboot of the selected computers in the list of computers.
Query	Performs the same function as clicking the QUERY button (see above). The program will query the client versions and drivers status for every machine in the list. It will also report the operating system version and service pack.
Progress details	It displays an additional window providing details of the install / uninstall / query operation on the selected computers. An example of progress window is shown in *Figure 23*.
Open last log	Opens the log of the last installation. An example log file is shown in *Figure 24*.

Table 3: Client deployment menu: computers menu

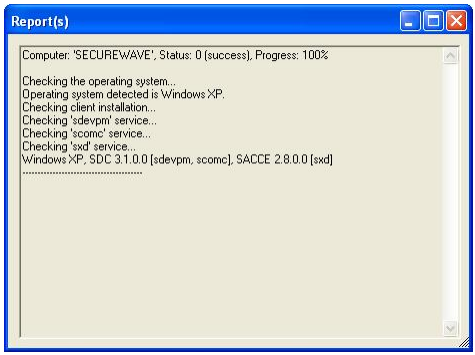

Figure 23: Client deployment menus: progress detail

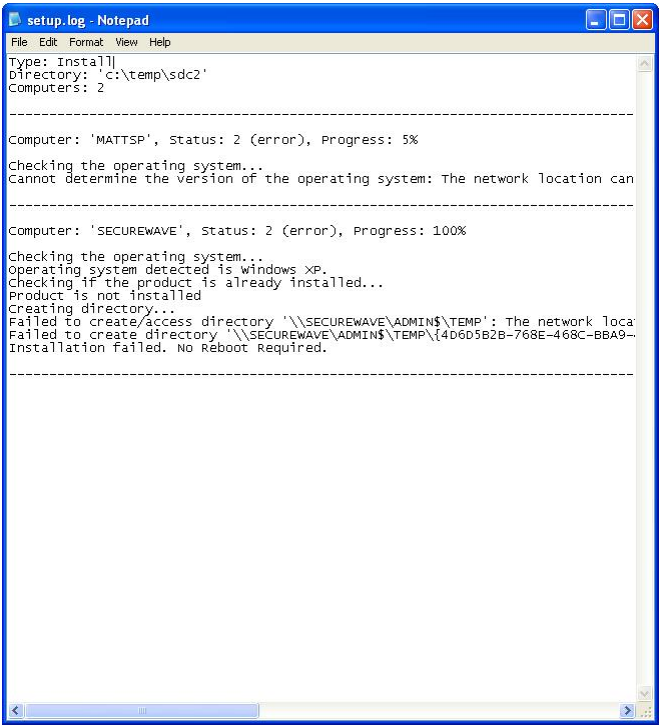

Figure 24: Client deployment menus: log example

Help menu

The Help menu has the following items.

Item	Description
Help	Displays the online help.
About Deploy...	Displays a dialog giving copyright and version information about the Sanctuary Client Deployment tool.

Table 4: Client deployment menu: help menu

Contextual menus

You have two contextual menus to choose from depending on which panel you do a right click:

1. In the *Packages* panel: the available options are those of the *Packages* menu.
2. In the *Computers* panel: the available options are those found in the *Computers* menu.

Figure 25: Package panel contextual menu

Figure 26: Computers panel contextual menu

The Options Screen

If you select the *Options* entry of the *Packages* menu, the following dialog appears, allowing you to modify the Sanctuary Client Deployment options.

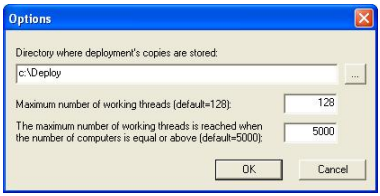

Figure 27: Client deployment menus: options screen

> The first field lets you choose a folder where you would like to store all the deployment packages.

Do not specify the root directory of the system drive or any other directory where existing files already reside or might be created by other applications.

If the deployment tool is installed on different machines, you might want to specify a shared directory where all instances of the deployment tool can access the company packages.

> The maximum number of working threads value defines the maximum number of deployments tasks that the program can perform in parallel. Choosing a lower value will reduce the impact on the computer and network performance. Choosing a higher value will allow faster deployments providing the computer and network resources are still available.

> The third parameter defines the number of computers threshold for which the maximum number of threads will be used. Both parameters are combined to allow you to fine tune the application performances. The relation that links both parameters is explained in *Figure 28*.

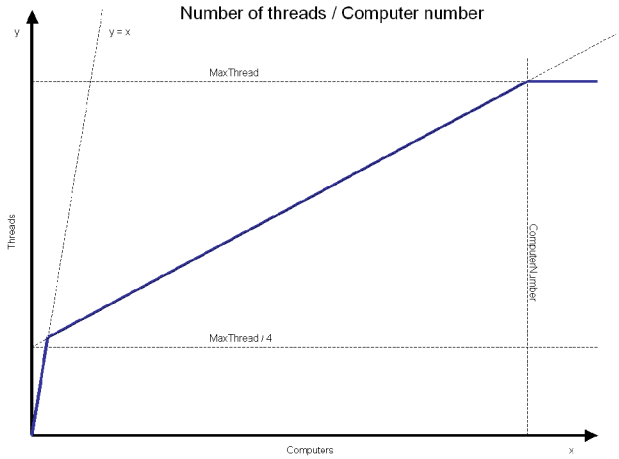

Figure 28: Client deployment menus: number of threads vs. number of computers

Appendix A: Opening firewall ports for client deployment

Microsoft Windows XP Service Pack 2 (SP2) enables the Windows Firewall by default. While this firewall configuration helps secure your system, it can also prevent legitimate software from interacting with the computer.

Many NetBIOS and DirectHost services, such as our deployment tool, rely upon a combination of TCP and UDP network ports, specifically TCP 139, TCP 445, UDP 137, and UDP 138. These services are installed by default on Windows NT 4.0 and Windows 2000 systems, as well as domain-joined Windows XP systems.

With the advent of Windows XP SP2 these services are, by default, no longer available to remote systems. This firewall denies access to these services and prevents connections to all network ports. The defaults settings prevent our installation tool to connect to the remote computers.

With the methods described in this chapter, you can preserve system security while deploying our software in your organization.

You can apply these necessary firewall settings on a computer-by-computer basis, or via an Active Directory domain group policy as explained in the following sections.

To manually open the ports in a computer-by-computer basis

1. *Start → Settings Control Panel → Windows Firewall* (or click SECURITY CENTER and then WINDOWS FIREWALL) and go to the *Exceptions* tab.

   On this tab, you can choose to enable the *File and Print Sharing services* (as well as other listed services). By enabling File and Printer Sharing services, TCP ports 139 and 445, and UDP ports 137 and 138, you can install our client remotely using our deployment tool, while all other (non-selected) services are blocked.

   If the computer resides on a remote IP subnet, you will need to edit the service and choose Subnet as the Scope.

2. Click OK to close the Windows Firewall control panel.

3. Restart the computer to enable these choices.

To open the ports in a computer-by-computer basis with a .bat file

Open your notepad or your favorite text processor and type or copy and paste the following lines:

```
netsh firewall set portopening protocol=UDP port=137
name=SANCTUARY_UDP_137 mode=ENABLE profile=All

netsh firewall set portopening protocol=UDP port=138
name=SANCTUARY_UDP_138 mode=ENABLE profile=All

netsh firewall set portopening protocol=TCP port=139
name=SANCTUARY_TCP_139 mode=ENABLE profile=All

netsh firewall set portopening protocol=TCP port=445
name=SANCTUARY_TCP_445 mode=ENABLE profile=All
```

Save and run on each machine.

To open the firewall ports via an Active Directory Group policy

While it is possible to open ports manually in a small network, this can also be achieved in a larger scale by centrally configuring the Windows firewall using Group Policy. When the XP SP2 machines log on to the network, they will inherit the customized Group Policies, thus opening the Windows Firewall ports required for remote deployment. This is the Microsoft recommended method to manage centrally Windows Firewall settings.

In the following steps, we will modify a domain group policy to open the needed ports:

To avoid compatibility problems ensure that the machine has the latest patches and service packs.

If you are using a Windows Server 2003 with Service Pack 1 computer joined to the domain:

1. Log on as domain administrator.
2. Download and install the .NET framework (required for the next step.)

3. Download and install the Microsoft Group Policy Management Console (GPMC) from Microsoft's Web site.

To create the Group Policy (GPO):

1. Open the Group Policy Management console (Start → Run → gpmc.msc)

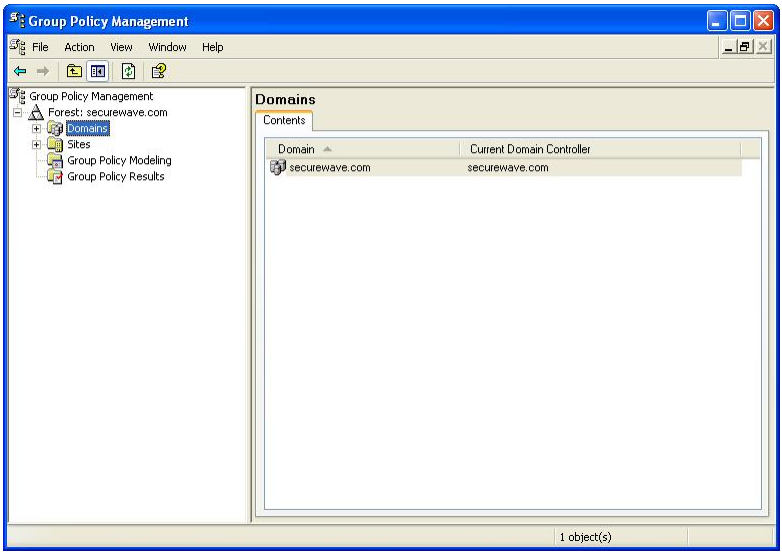

Figure 29. Open firewall ports: select domain and forest

2. Select the Forest and the Domain for which you wish to create a Windows Firewall Policy.

3. Right-click the entry for *Default Domain Policy* and select EDIT.

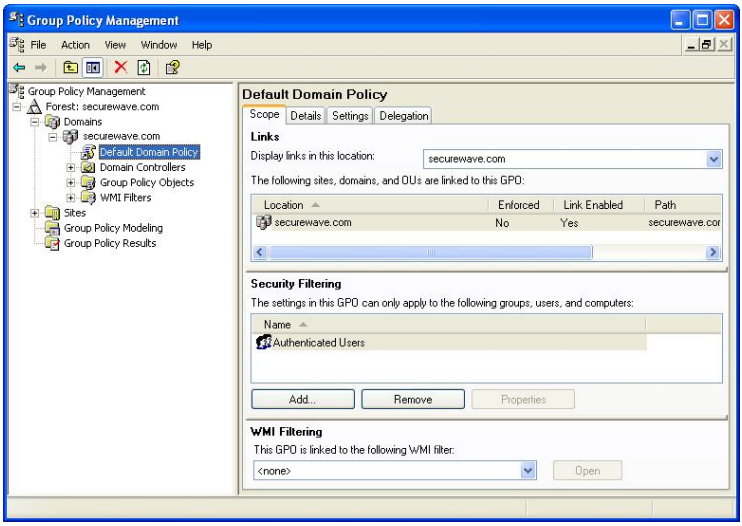

Figure 30. Open firewall ports: edit the Default Domain Policy

4. This will open a *Group Policy* window for the selected domain:

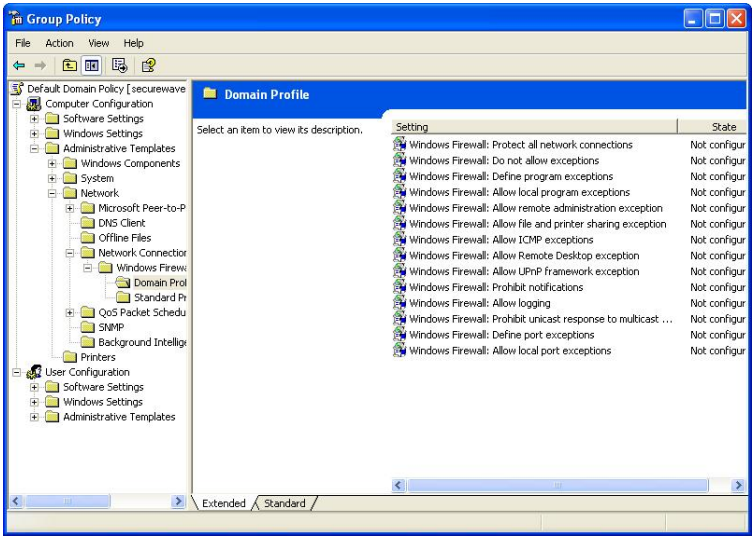

Figure 31. Open firewall ports: modify file and printer sharing exceptions

5. Expand the *Computer Configuration* tree and navigate to the *Administrative Templates* → *Network* → *Network Connections* → *Windows Firewall* → *Domain Profile* folder, as illustrated in the previous figure.

   The simplest way to enable the ports used by our deployment tool is to enable the policy *Windows Firewall: Allow file and printer sharing exception*.

6. Right-click *Windows Firewall: Allow file and printer sharing exception* and select *Properties*. The following dialog appears:

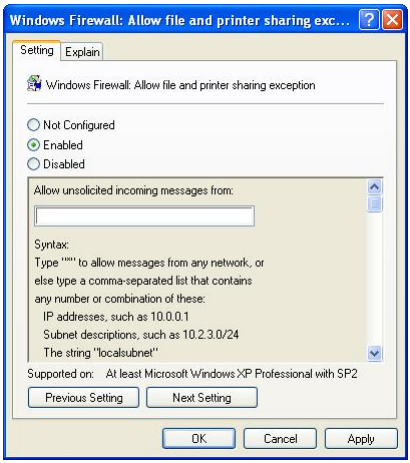

Figure 32. Open firewall ports: enable the required ports

7. Choose *Enabled* and then type *Localsubnet* in the *Allow unsolicited incoming messages from* field.

8. To save these settings click on the APPLY button and then on OK.

Enabling File and Printer Sharing access will open TCP ports 139 and 445, and UDP ports 137 and 138, making them available to other machines on the same local IP subnet. These machines will appear completely blocked for those systems outside of the local subnet.

To improve security

To enhance further the security, you can replace 'localsubnet' in step 7 of the preceding procedure with the specific IP address or addresses (comma separated) of the computers allowed to deploy the client.

Index of figures

Index of tables

Index