]HackingTeam[

Remote Control System

Administration Manual

Summary

1 Introduction

1.1 Offensive security technology

Remote Control System (RCS) is an investigation support tool that performs active and passive interception of data and information related to the activities of the user of a controlled system.

RCS can create, configure, and install a *software agent* that is in turn able to scan, remaining undetected, all activities and operations executed out on a PC (target) or a Mobile Phone and to gather all data and information generated by the system.

The *software agent* is guaranteed to remain operational even when no internet connection is available: the agent will continue gathering information and will be able to act autonomously, following the logic pattern programmed during the configuration process. All gathered data will be uploaded to the *control room* whenever possible.

This feature grants extreme flexibility and allows for data interception in the most adverse conditions.

1.2 Functionality

RCS allows you to intercept, monitor and gather a large number of information on all the activities carried out on a PC or a Mobile Phone, like:

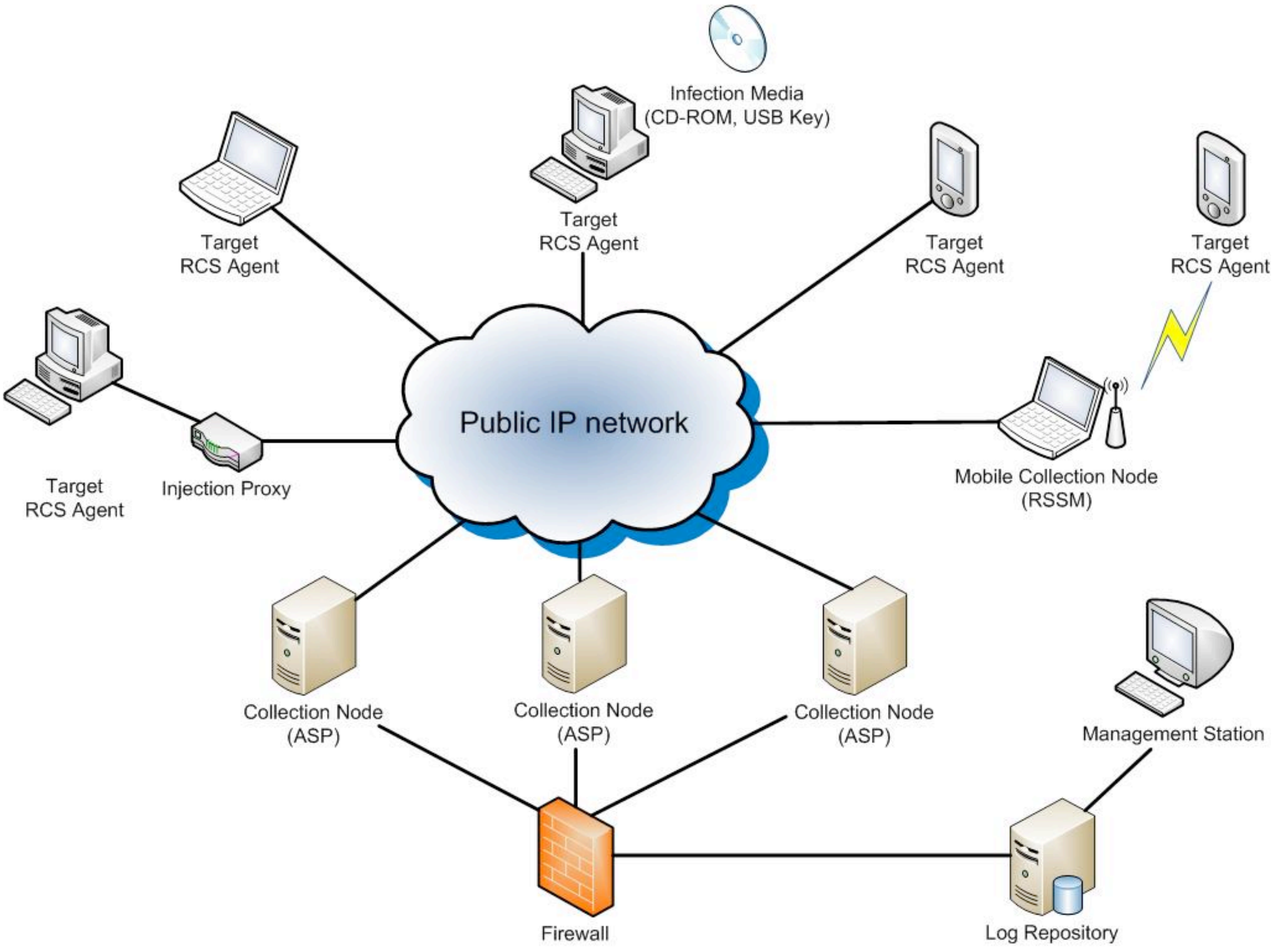
- Websites visited;
- Filed opened/modified/deleted;
- Keys pressed;
- Documents and images printed;
- VoIP phone calls (Skype, WindowsLiveMessenger, YahooMessenger, etc);
- Programs executed;
- Audio surveillance;
- Webcam capture;
- Screen capture;
- Instant Messaging and Chat (Skype, WindowsLiveMessenger, YahooMessenger, etc);
- Clipboard;
- Passwords (i.e.: e-mail account, WindowsLive account, etc);
- Sent and received e-mails;
- Mobile phone calls;
- GPS Position;
- Address book and contacts

1.3 Stealth

A fundamental feature of RCS is the stealth system of the *software agent*: once "installed" on the target, all resources used by the agent will be hidden, rendering it invisible to the most widely spread protection systems and virtually impossible to detect using conventional tools.
Its logic of operation was designed to mimic the user's behaviour, a feature that makes it all the more difficult to detect its activities and tell them apart from those of the user.

2 General Architecture

The following diagram explains the main logic components of the RCS system. In the following paragraphs we'll go through all the necessary information to fully understand the role and the functionality of each key element in the infrastructure.



RCS Aschitecture

2.1 RCS Agent

All surveillance functionalities are implemented in a small software module (RCS *agent*). Once installed on the target PC, the agent will perform all necessary operations to gather evidences without being detected.

The RCS agent was designed with modularity and flexibility in mind: all features and functionalities of the agent can be profiled, added, removed or updated according your needs, even during the course of operations.

The functionality paradigm is based on the concept of *event/action*: the agent is able to monitor the user's activities and, when a certain "event" occurs, react following the "actions" programmed during the set-up process. Thanks to its innovative design, the agent will be able to work autonomously, according to the logic patters programmed during configuration.

All information gathered is stored locally on the target PC in an encrypted repository, hidden to the system. Based on the agent's configuration (programmed by the operator) all gathered data are sent back to the operator through a ciphered connection and removed safely once the upload is complete. The connections are strongly encrypted and mutually authenticated.

The uploading system of the evidences is perfectly able to work in complex network infrastructures (enterprise), in the presence of firewalls, proxies with domain authentication, etc., mimicking the behaviour of a normal user browsing the web.

Thanks to its modus operandi, the RCS agent is able to work in the most extreme conditions.

2.2 RCS Control Station (HCM)

The *HCM* application is the interface through which the operator can configure and deploy the *RCS agents*.

HCM allows the operator to create digital (melted executables, injection proxy) and physical (offline cdrom, usb key) vectors of installation.

The software is able to connect to different log repositories, thus allowing the operator to easily control even the most complex RCS structure.

2.3 Admin Station (RCS Console)

This component is the main user interface of the RCS system.

Using the Admin Station, the operator will be able to:

- Manage users and groups of the RCS system;
- Manage all investigation activities and targets;
- Browse and search the logs database;
- Monitor the state of the RCS agents;
- Check all data and information concerning the system;

Access to the functions mentioned above is regulated by the privileges assigned to the operator. It is so possible to create different profiles:

- Administrators;
- Operatives;
- Evidence Inspectors;

2.4 Collection Node (ASP)

ASP is the reference point for the *RCS agents*. Through this service it is possible to receive the logs gathered by the *agents*, and to upload new configurations and *plug-ins*.

Once the authenticity of the RCS client has been verified, ASP will work as an intermediary towards the DB: this means that it will be possible to link any number of ASPs (even when they are located in different networks) to a single central log repository. The agent will be able to upload its logs and receive the new configurations (stored on the DB) regardless of what ASP server it established contact with.

ASP is the only component in the infrastructure that needs to be visible from the internet: the use of a firewall to profile access to the service is strongly recommended.

ASP also implements security devices such as decoying to another website, in case of attempted access to the service by any client different from an actual *RCS agent*.

2.5 Mobile Collection Node (RSSM)

RSSM is the component that accepts connections from Mobile RCS installations, using point-to-point proximity protocols (BlueTooth, WiFi). Thus it will be possible to retrieve logs from a Mobile RCS Agent, and send new configurations, without forcing it to establish a payment internet connection to the ASP server. Data are stored encrypted on the RSSM device, and it is possible to synchronize them to the ASP server later, using a standard internet connection.

2.6 Log Repository (RCS DB)

The RCS DB is the storage component of all logs gathered by the *agents*, of all current and previous configurations, and of all information used in managing the access to the RCS system (users, groups, profiles, etc.)

On a logical level, the RCS DB is composed of a relational database, whose access is managed and regulated by an application logic that allows the other components (ASP, HCM, etc.) to access all data and information.

The system was designed to protect the content and the integrity of sensitive information (the data gathered by the agents) and to implement all those security devices needed to prevent the adulteration of all gathered information.

2.7 Infection Media

The RCS system is also able to install agents through hardware devices (CD-ROM, USB Key), should direct access to the target machine be impossible. Such devices can execute the infection even if the PC is protected by OS or BIOS password.

Through the infection media, it is also possible to export logs (in the scenario of a target machine that is never connected to the internet) or remove the agent.

2.8 Injection proxy

Injection proxy is a hardware/software system that can inject and modify the data generated during a web session. In different attack scenarios, the system is able to infect, safely and undetected, any Windows executable downloaded from the web on a target PC. When the unknowing user executes the downloaded file, the injected code will silently install the RCS agent.

A description of all possible attack scenarios is provided in the respective paragraph.

3 RCS Installation

In order to function correctly, the system needs several components.

These components must be installed as described below, exactly in this order.

- **Log repository**
  1. RCSDB
  2. RCSCORE
- **Collection node**
  1. RCSASP
- **Admin station**
  1. RCSConsole
- **Control station**
  1. HCM
  2. RCSPE

3.1 Log repository

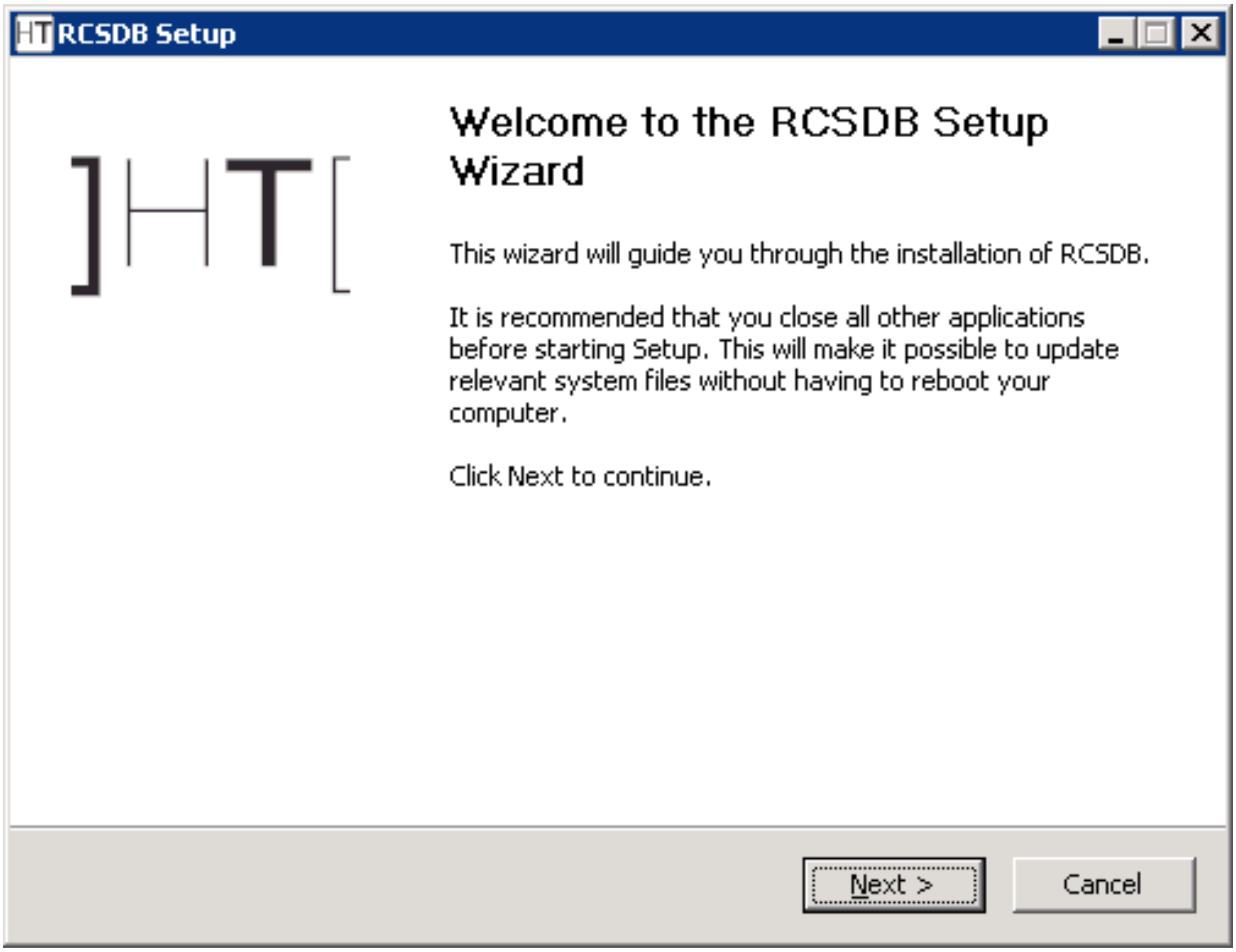
Collection nodes, Admin stations and Control stations must reach Log repository's TCP ports 80 and 4443 (ssl encrypted channel).

3.1.1 RCSDB

The RCSDB package contains all the necessary software for data storage.

The operating system required is Microsoft Windows Server 2003.

The installation file is called RCSDB-<serial>.exe and must be launched using the following procedure.



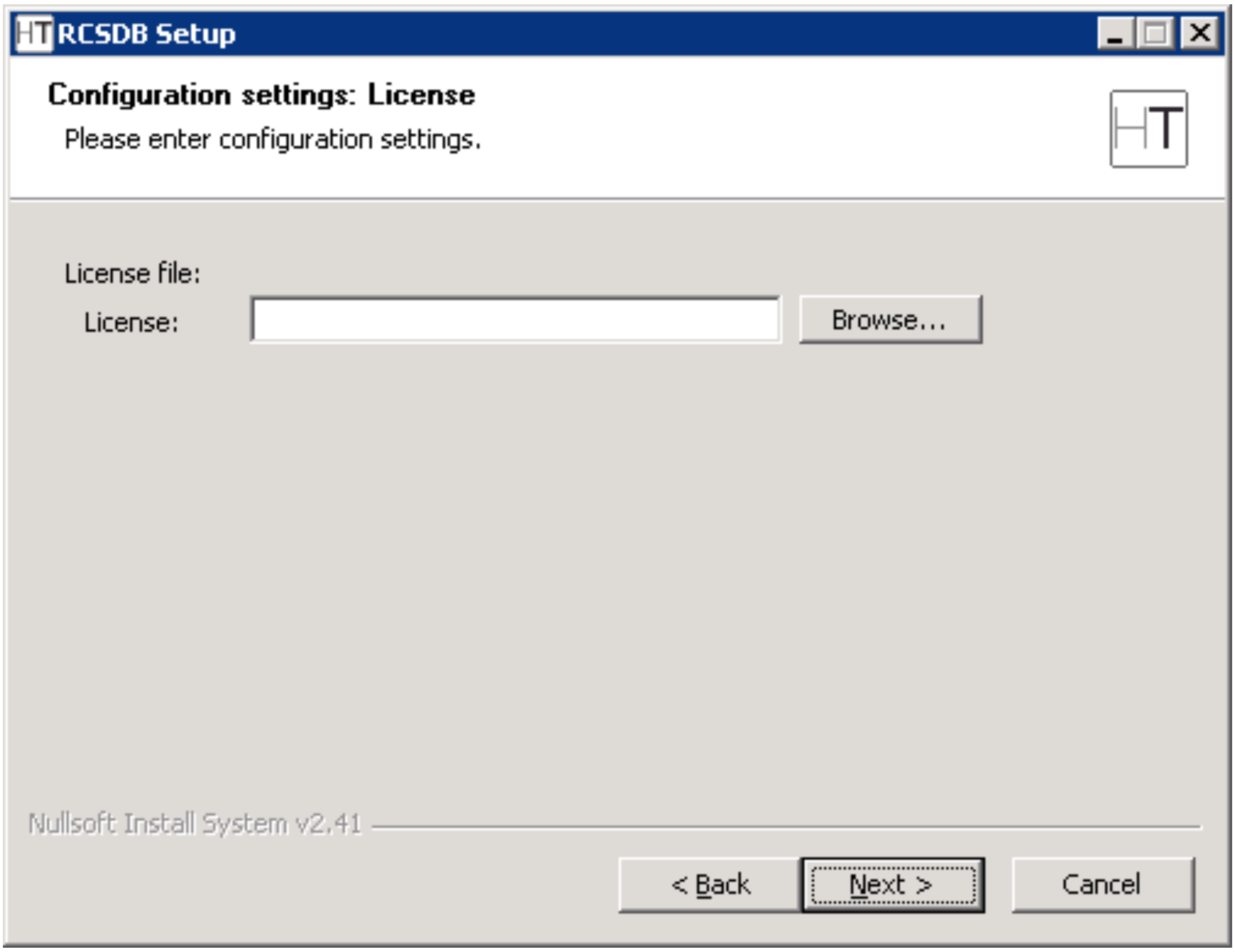
Welcome to the RCSDB Setup Wizard

This wizard will guide you through the installation of RCSDB.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

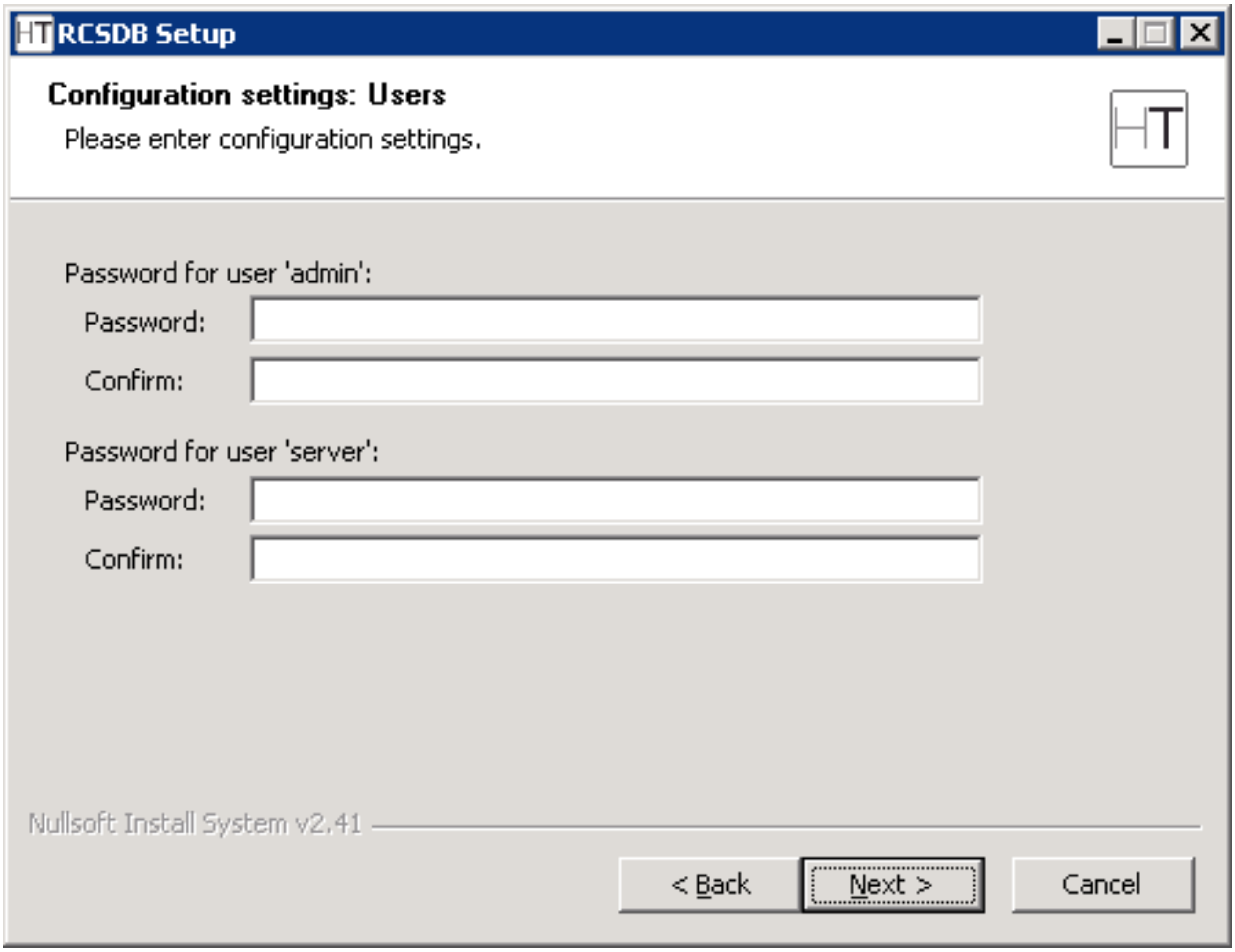
Click Next to continue.

- click on 'Next'



RCSDB Setup
Configuration settings: License
Please enter configuration settings.
License file:
License:
Browse...
Nullsoft Install System v2.41
< Back
Next >
Cancel

- insert the path of the license file
- click on 'Next'



RCSDB Setup

Configuration settings: Users

Please enter configuration settings.

Password for user 'admin':

Password:

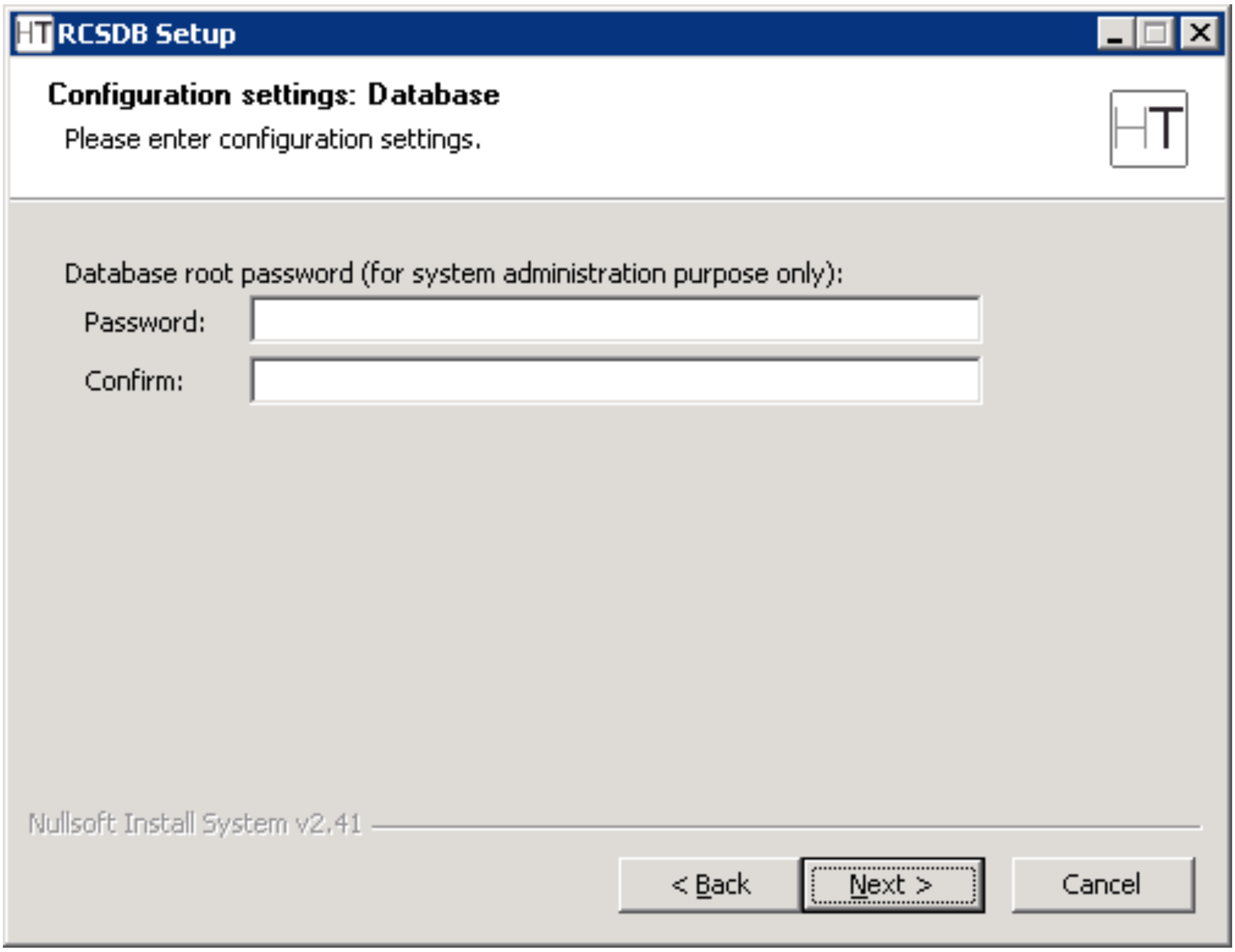
Confirm:

Password for user 'server':

Password:

Confirm:

- insert the password for the ‘admin’ user that will be used to create and configure the system through the RCSConsole
- insert the password for the ‘server’ user that will be used from the other components of the system to interact with the RCSDB
- click on 'Next'



Configuration settings: Database

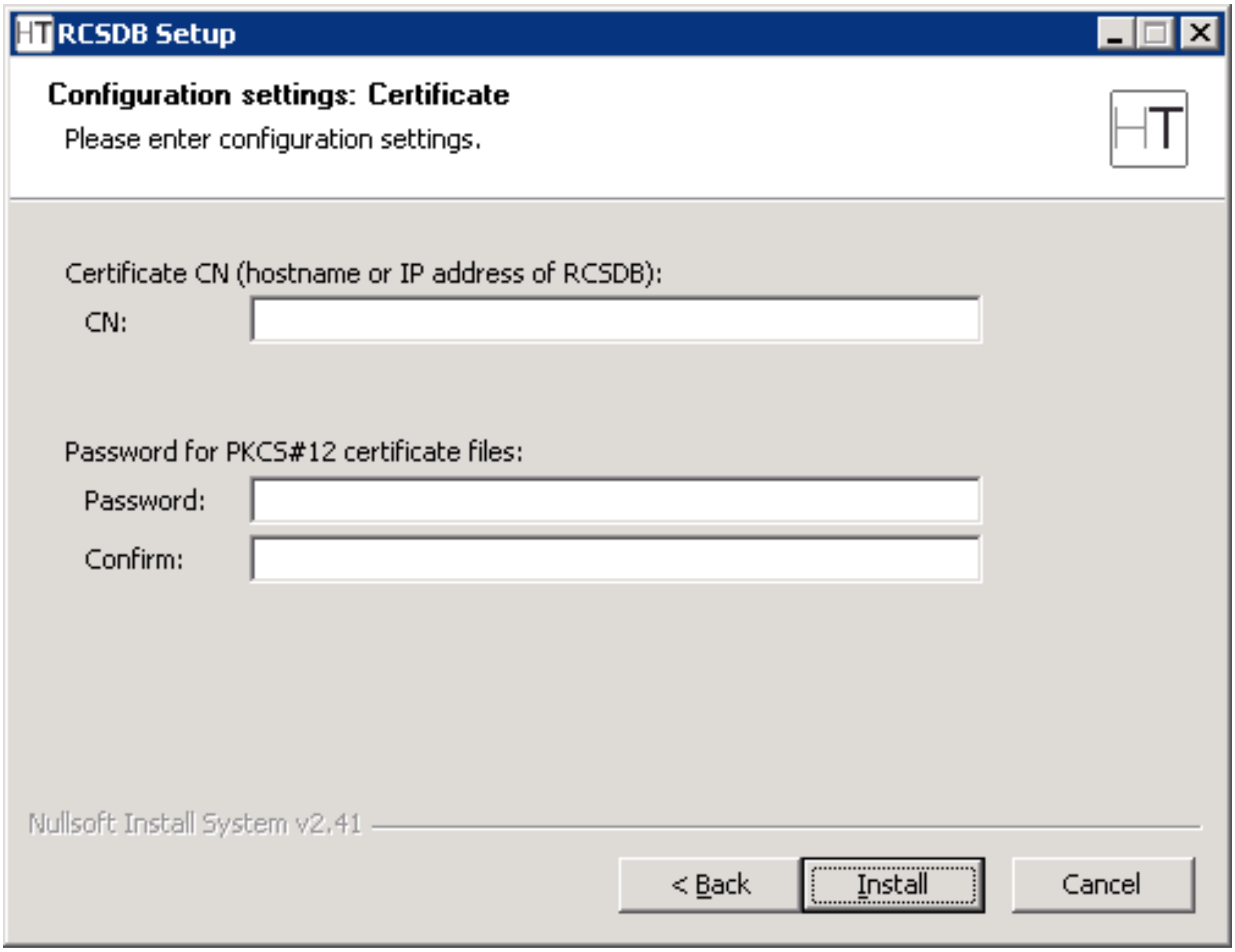
Please enter configuration settings.

Database root password (for system administration purpose only):

Password:

Confirm:

- insert the password that will be used to administer the database
- click on 'Next'



RCSDB Setup

Configuration settings: Certificate

Please enter configuration settings.

Certificate CN (hostname or IP address of RCSDB):

CN:

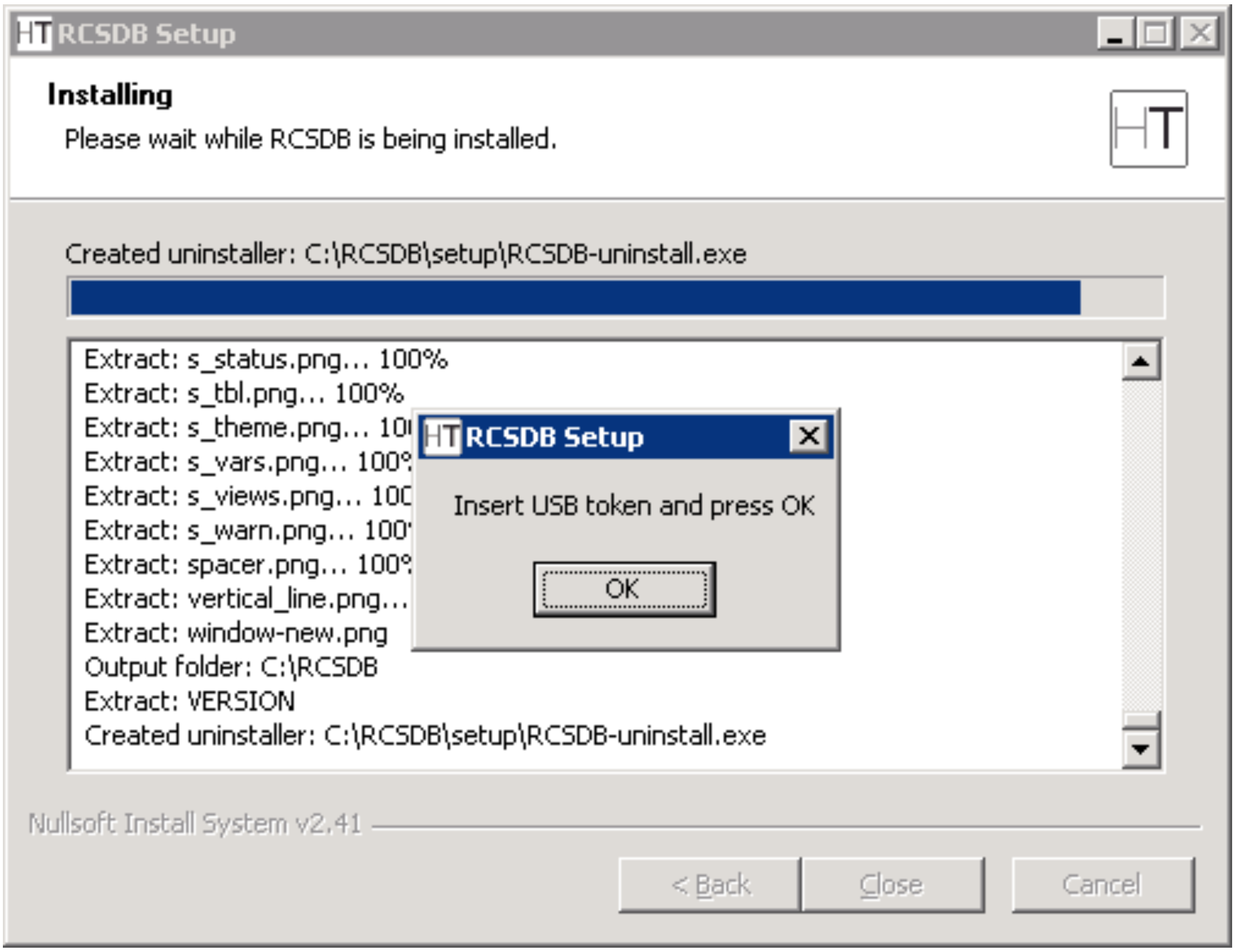
Password for PKCS#12 certificate files:

Password:

Confirm:

Nullsoft Install System v2.41

- insert the hostname of the server
- insert the password for the PKCS#12 certificate files
- click on 'Install'



Installing

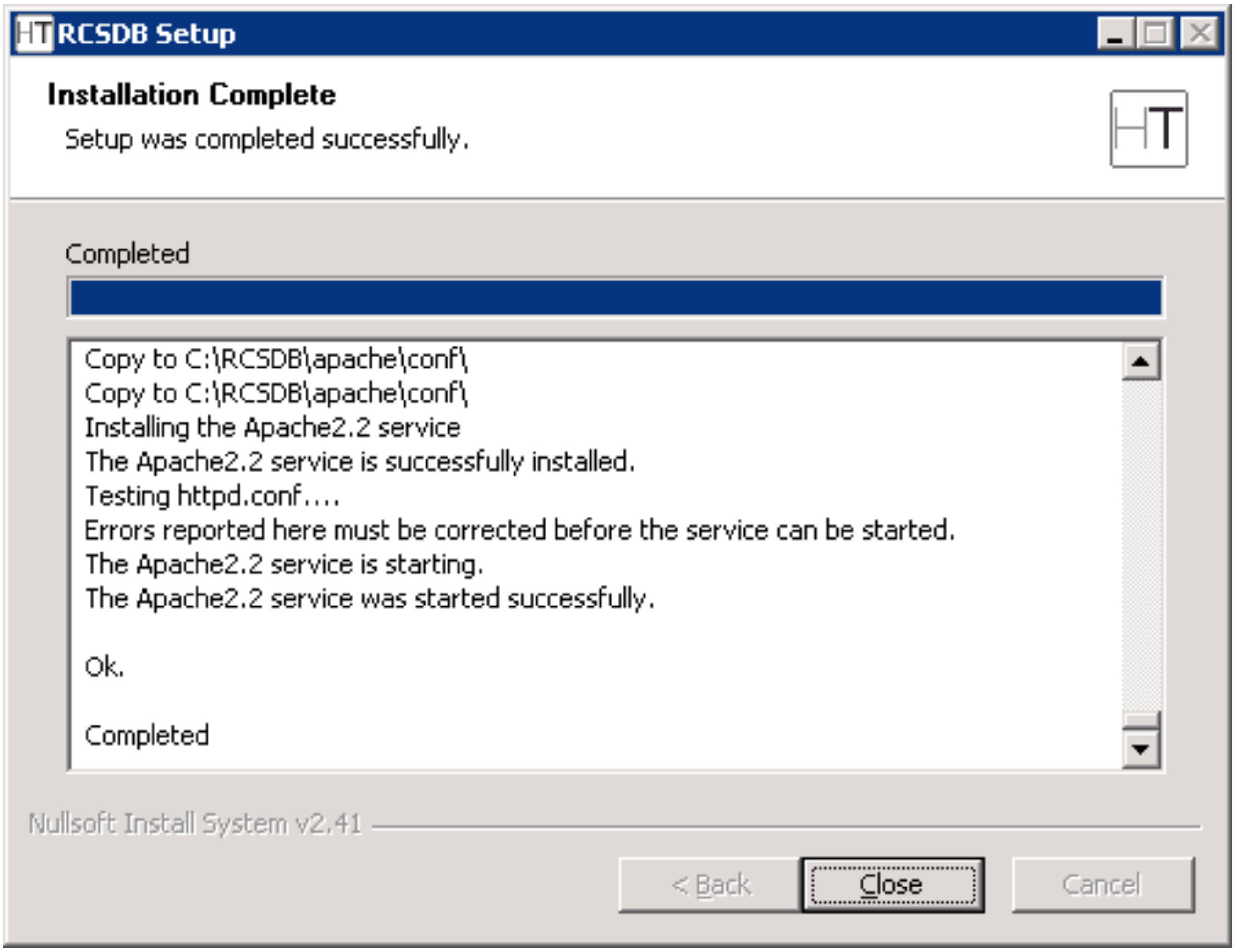
Please wait while RCSDB is being installed.

Created uninstaller: C:\RCSDB\setup\RCSDB-uninstall.exe

```
Extract: s_status.png... 100%
Extract: s_tbl.png... 100%
Extract: s_theme.png... 10
Extract: s_vars.png... 100
Extract: s_views.png... 10
Extract: s_warn.png... 100
Extract: spacer.png... 100
Extract: vertical_line.png...
Extract: window-new.png
Output folder: C:\RCSDB
Extract: VERSION
Created uninstaller: C:\RCSDB\setup\RCSDB-uninstall.exe
```

Insert USB token and press OK

- insert the USB token into a free USB port and click on 'OK'



Installation Complete

Setup was completed successfully.

Completed

```
Copy to C:\RCSDB\apache\conf\
Copy to C:\RCSDB\apache\conf\
Installing the Apache2.2 service
The Apache2.2 service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
The Apache2.2 service is starting.
The Apache2.2 service was started successfully.

Ok.

Completed
```

- wait for the installation process to complete
- make sure that no error occurred during the process
- click on 'Close'

3.1.2 RCSCORE

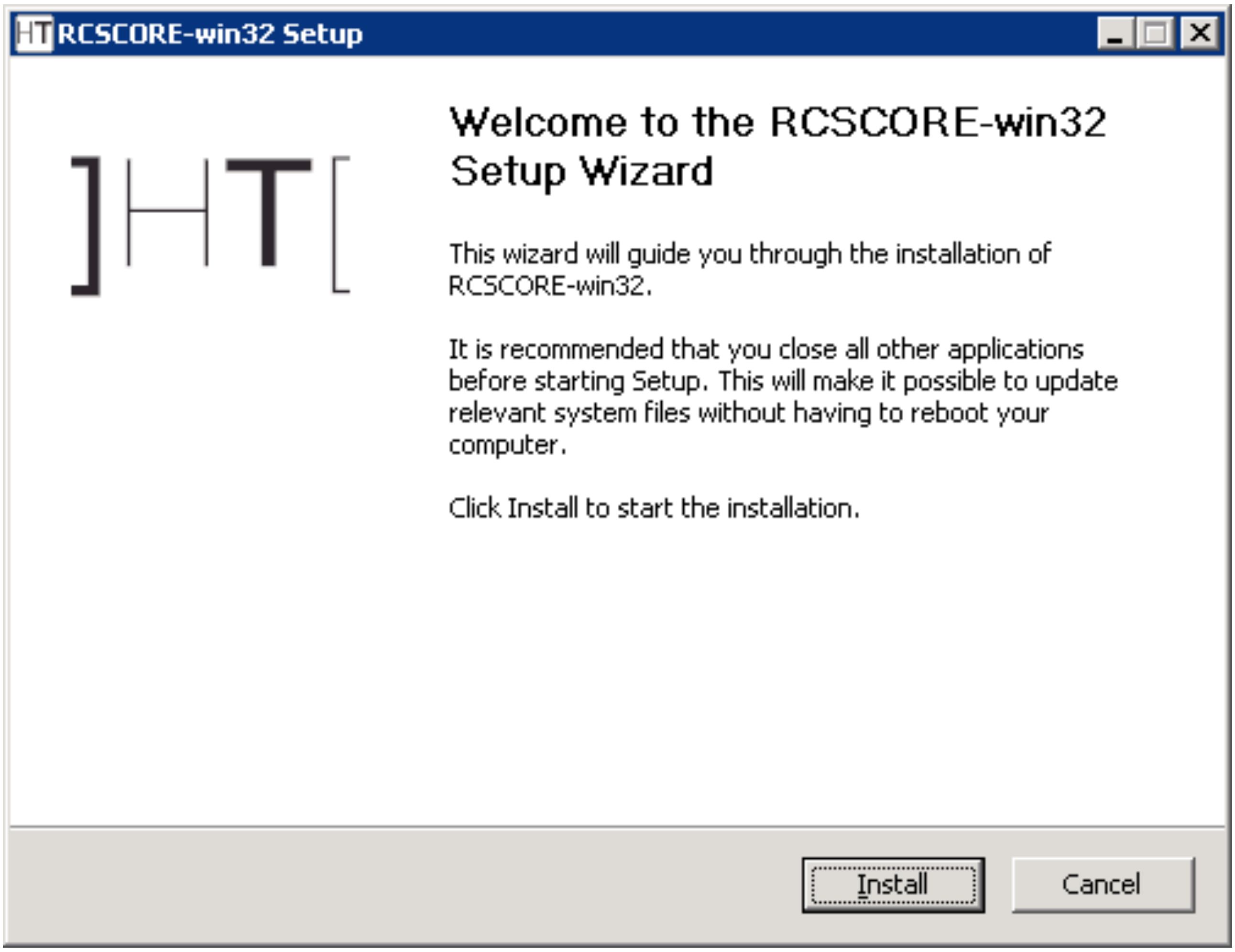
The RCSCORE package contains the client's software.

The operating system required is Microsoft Windows Server 2003.

The installation must take place on the same computer where the RCSDB was installed.

Repeat the procedure for each architecture.

The installation file is called RCSCORE-<architecture>-<serial>.exe and must be launched using the following procedure.



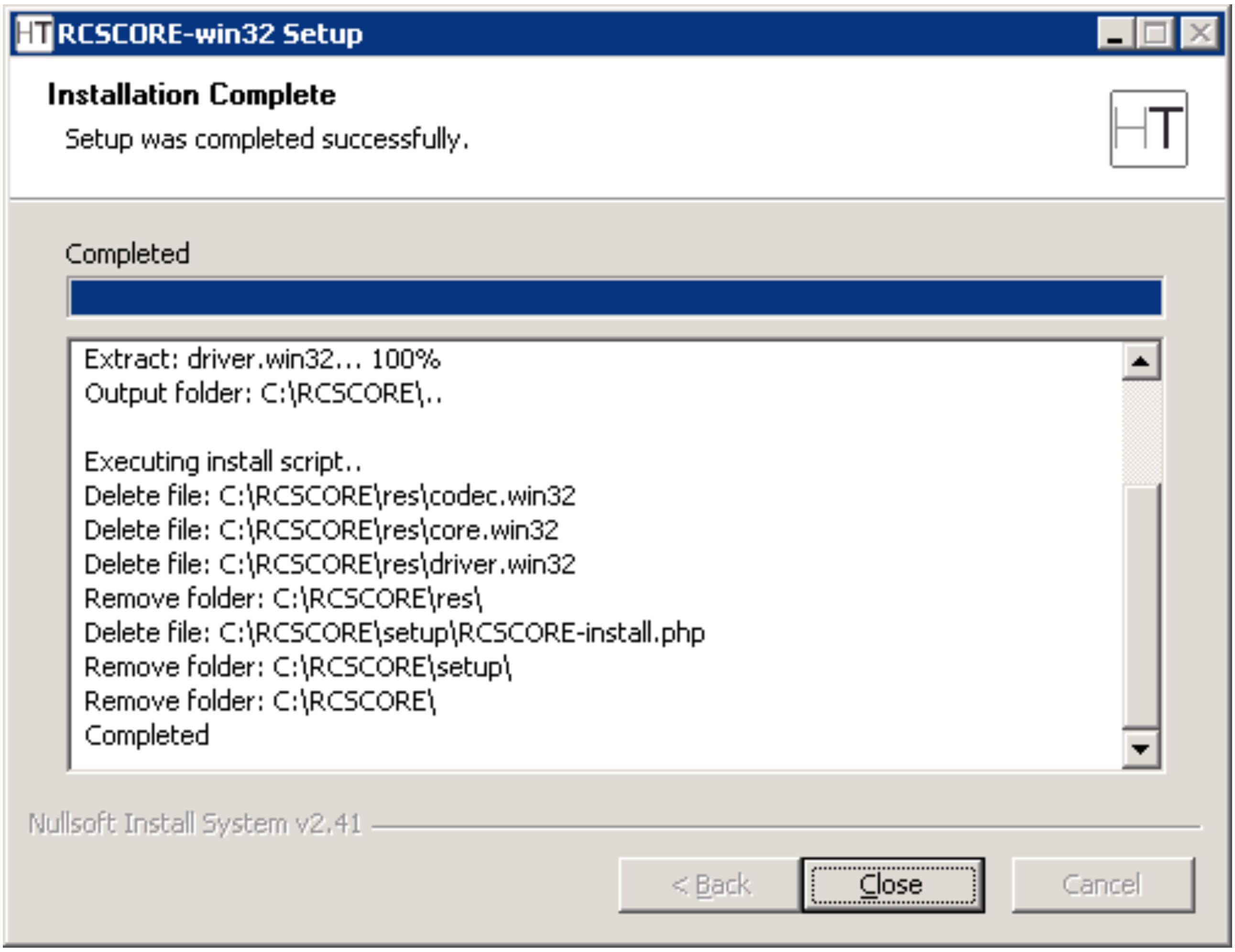
Welcome to the RCSCORE-win32 Setup Wizard

This wizard will guide you through the installation of RCSCORE-win32.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Install to start the installation.

- click on 'Next'



```
Extract: driver.win32... 100%
Output folder: C:\RCSCORE\..

Executing install script..
Delete file: C:\RCSCORE\res\codec.win32
Delete file: C:\RCSCORE\res\core.win32
Delete file: C:\RCSCORE\res\driver.win32
Remove folder: C:\RCSCORE\res\
Delete file: C:\RCSCORE\setup\RCSCORE-install.php
Remove folder: C:\RCSCORE\setup\
Remove folder: C:\RCSCORE\
Completed
```

- wait for the installation process to complete
- make sure that no error occurred during the process
- click on 'Close'

3.2 Collection node

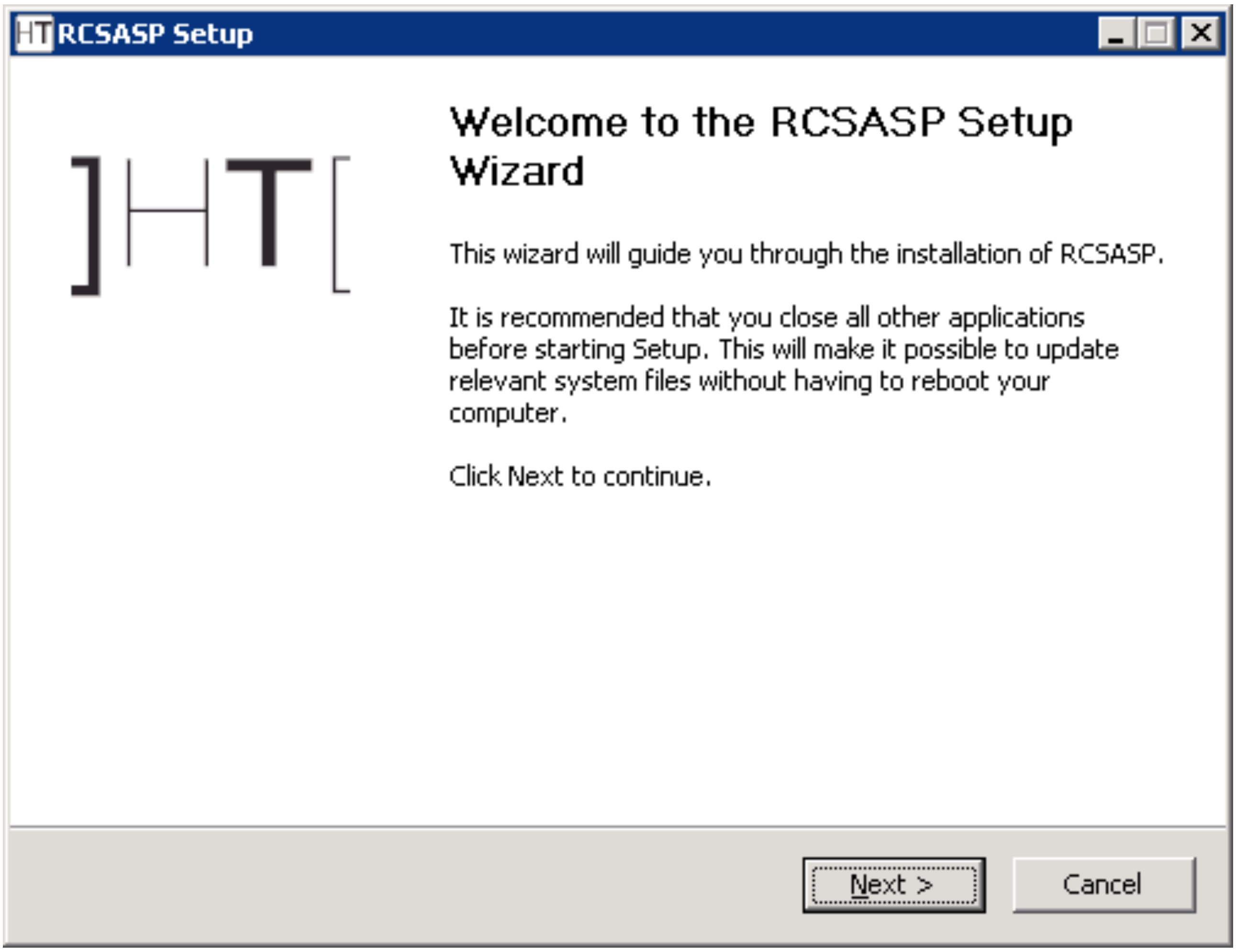
Collection nodes must be reached by RCS Agents on TCP port 443.

3.2.1 RCSASP

The RCSASP package contains all the necessary software for data reception.

The operating system required is Microsoft Windows Server 2003.

The installation file is called RCSASP-<serial>.exe and must be launched using the following procedure.



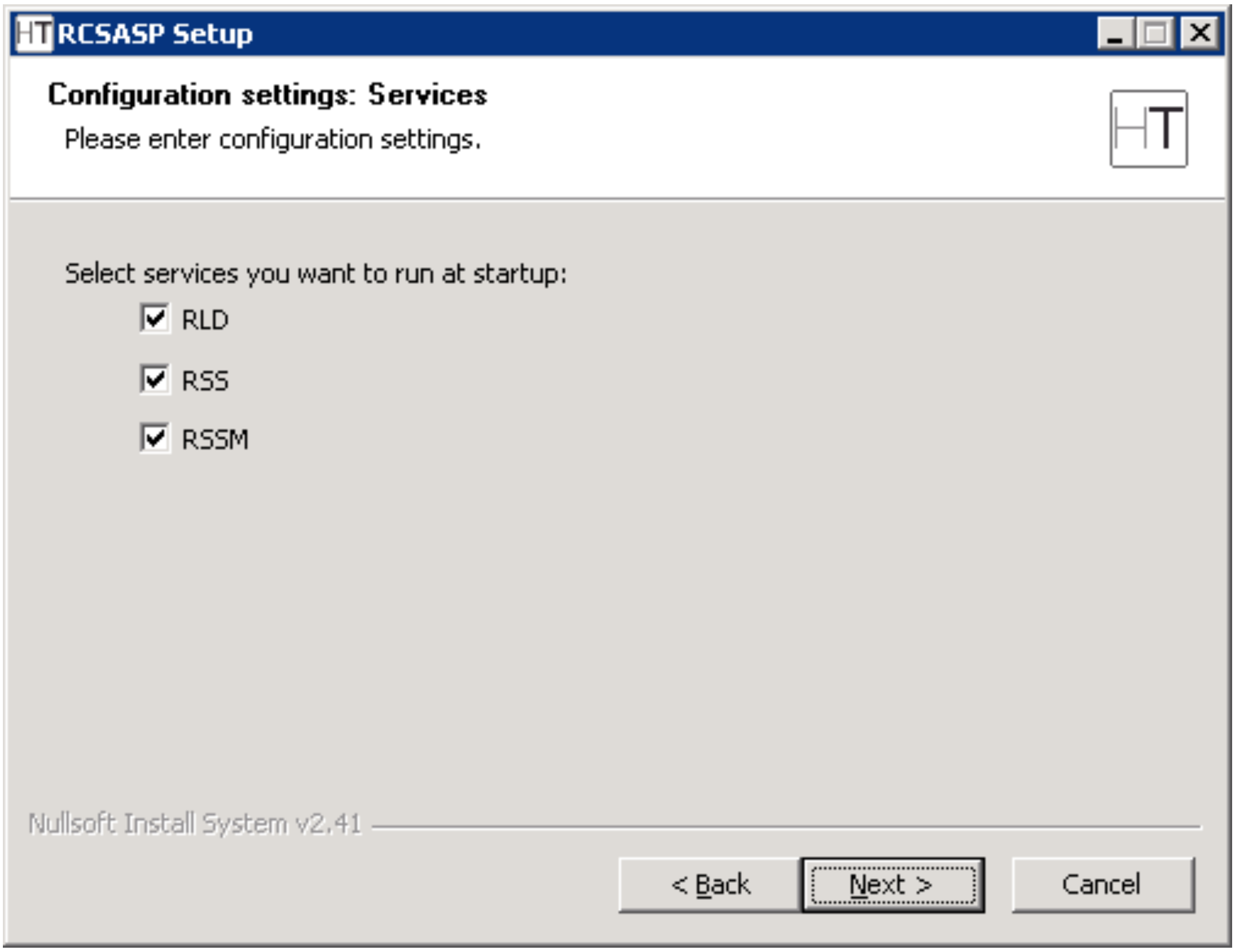
Welcome to the RCSASP Setup Wizard

This wizard will guide you through the installation of RCSASP.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

- click on 'Next'



Configuration settings: Services

Please enter configuration settings.

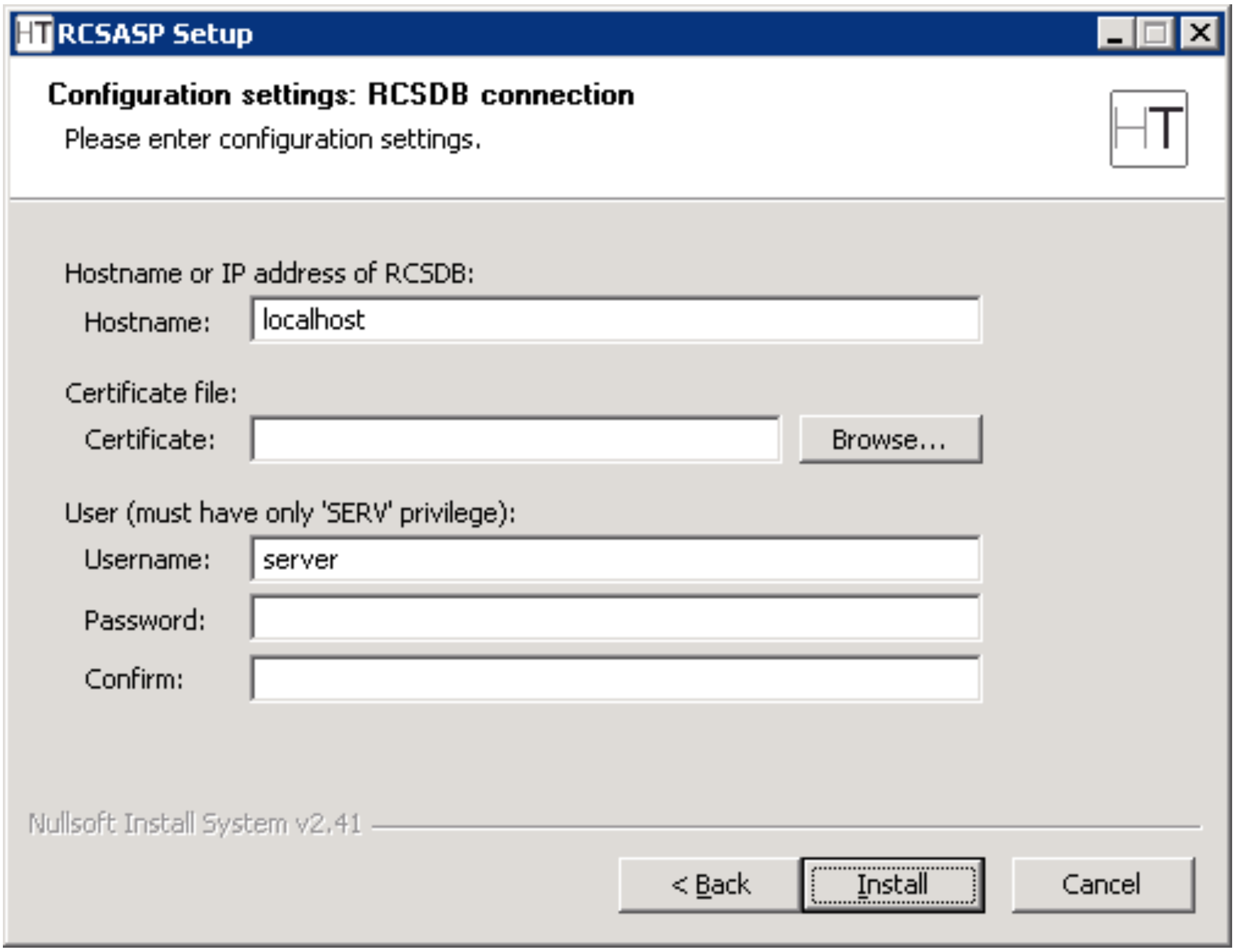
Select services you want to run at startup:

☑ RLD

☑ RSS

☑ RSSM

- select the components to be installed
- click on 'Next'



Configuration settings: RCSDB connection

Please enter configuration settings.

Hostname or IP address of RCSDB:

Hostname: localhost

Certificate file:

Certificate:

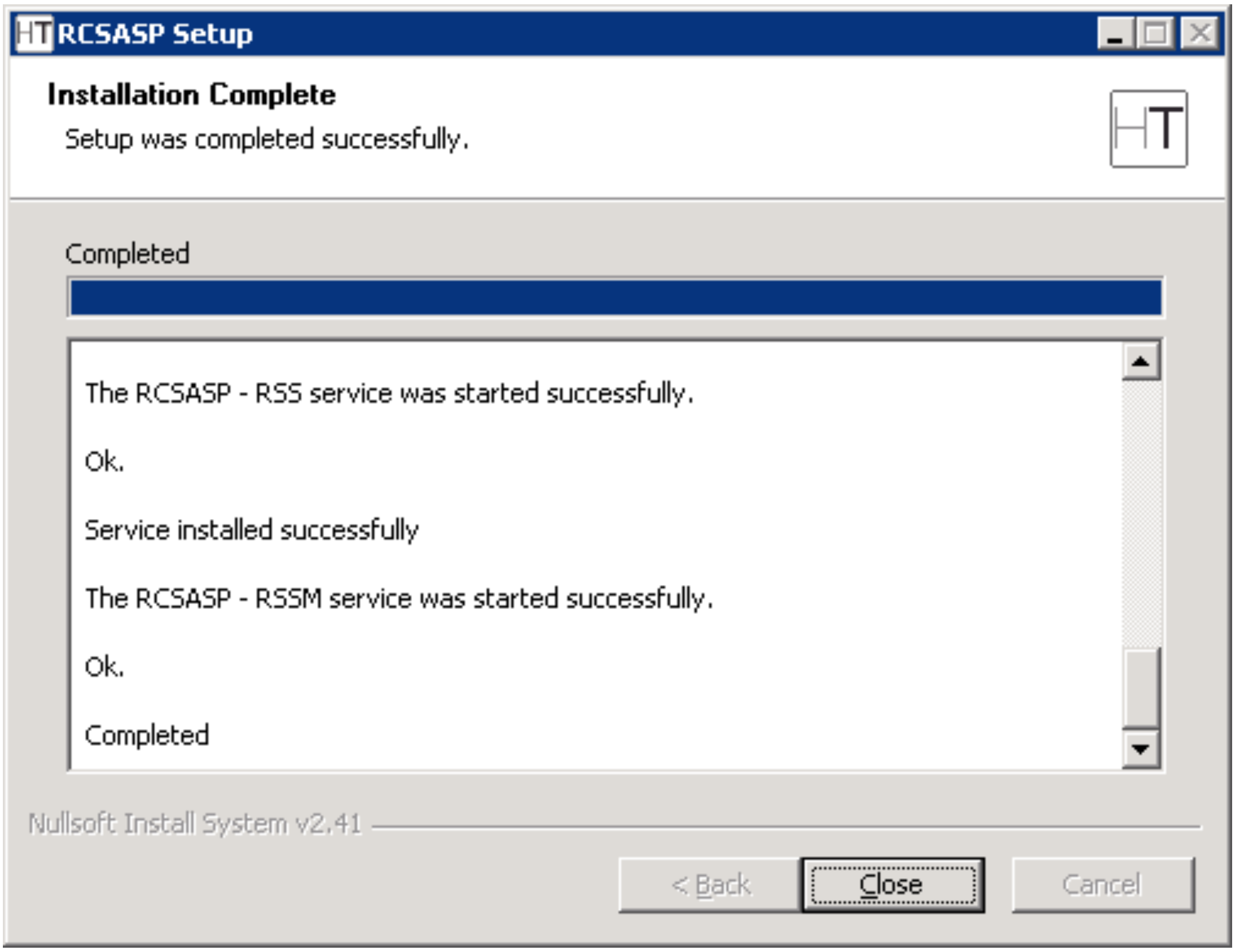
User (must have only 'SERV' privilege):

Username: server

Password:

Confirm:

- modify the server address using the hostname or ip address to interact with
- insert the path of the certificate file (“C:\RCSDB\cert\rcs-client\rcs-client.pem” on the server where RCSDB is installed)
- insert the username and password for the ‘server’ user configured during the installation of the RCSDB
- click on 'Next'



Installation Complete

Setup was completed successfully.

Completed

```
The RCSASP - RSS service was started successfully.

Ok.

Service installed successfully

The RCSASP - RSSM service was started successfully.

Ok.

Completed
```

- wait for the installation process to complete
- click on 'Close'

3.3 *Admin station*

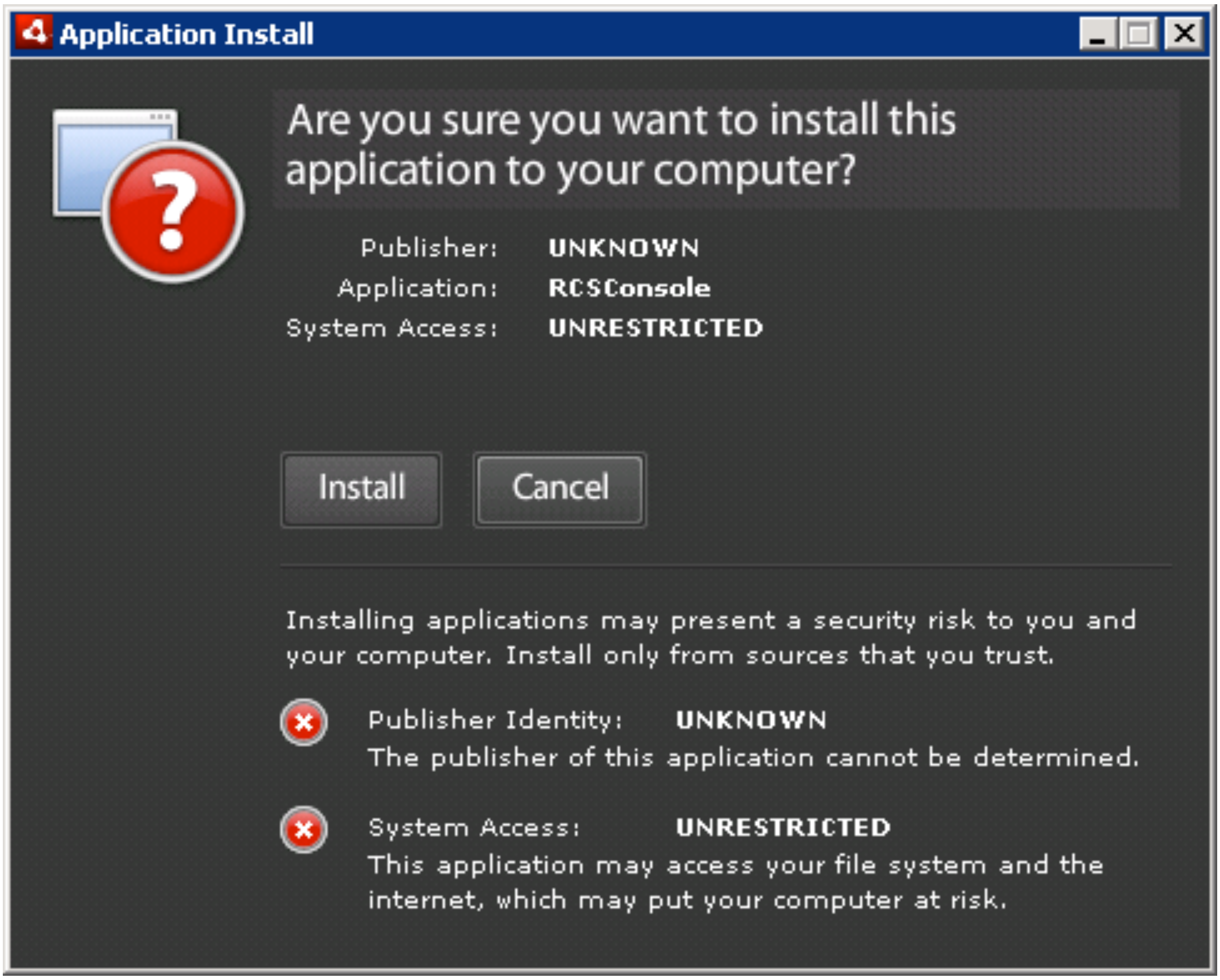
Admin station doesn't act as a server, so it doesn't need open TCP ports.

3.3.1 RCSConsole

The RCSConsole package contains all the necessary software to launch the console of the RCS system.

The Adobe AIR work environment is required (available on http://www.adobe.com/).

The installation file is called *RCSConsole-<serial>.air* and must be launched using the following procedure.



Application Install

Are you sure you want to install this application to your computer?

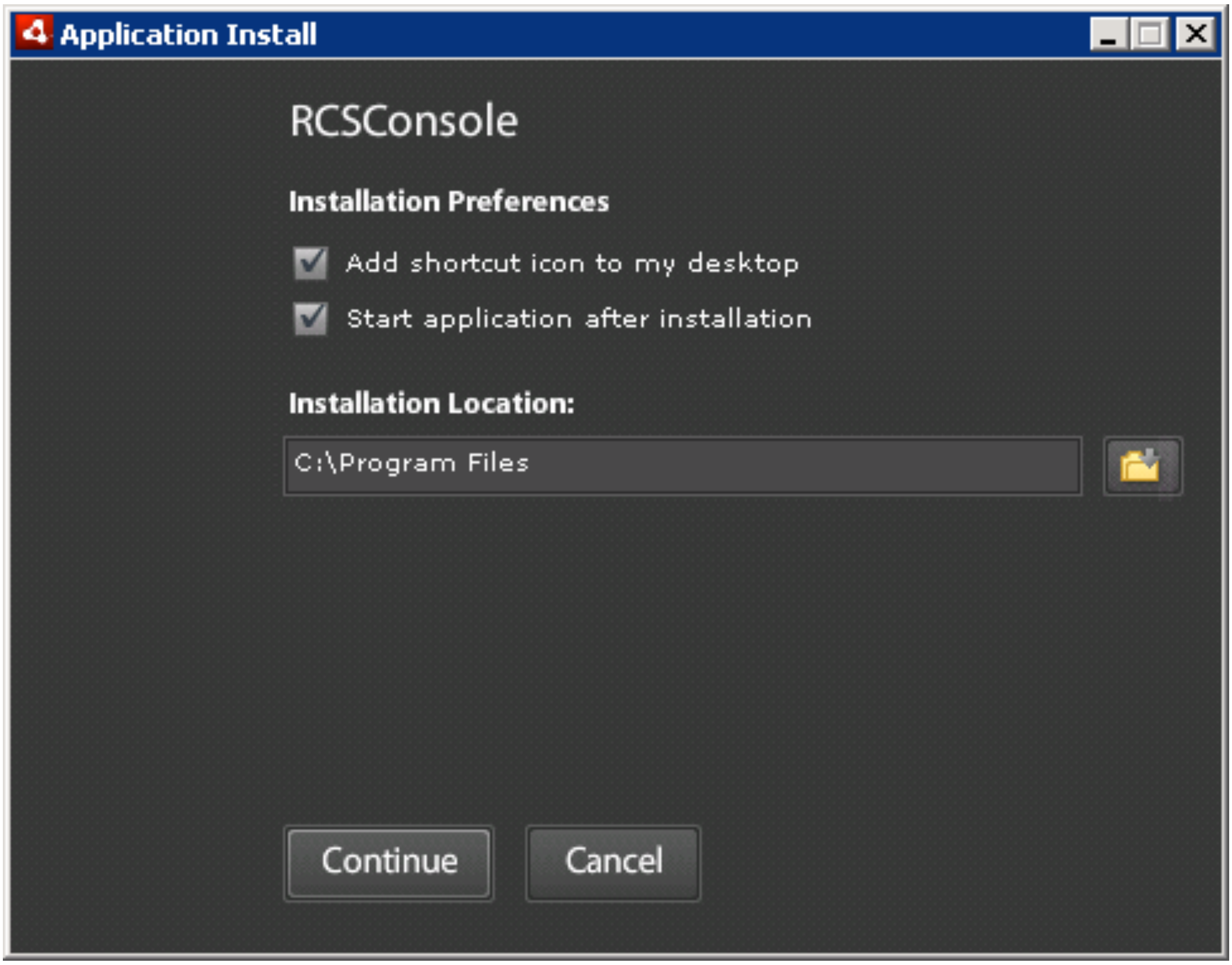
Publisher: UNKNOWN
Application: RCSConsole
System Access: UNRESTRICTED

Installing applications may present a security risk to you and your computer. Install only from sources that you trust.

Publisher Identity: UNKNOWN
The publisher of this application cannot be determined.

System Access: UNRESTRICTED
This application may access your file system and the internet, which may put your computer at risk.

- click on 'Install'



RCSConsole

Installation Preferences

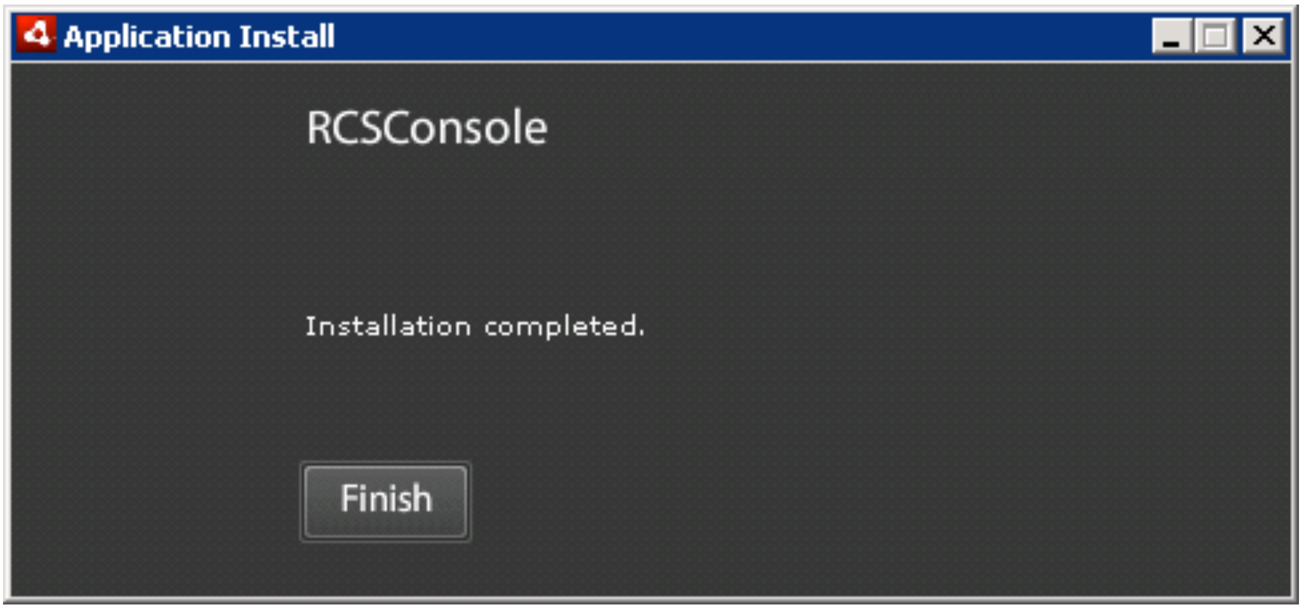
☑ Add shortcut icon to my desktop

☑ Start application after installation

Installation Location:

C:\Program Files

- uncheck 'Start application after installation'
- click on 'Continue'



RCSConsole

Installation completed.

- wait for the installation process to complete
- click on 'Finish'

3.3.2 OS Configuration

In order to properly visualize all the evidences, it’s strongly suggested to install *Arial Unicode MS* font. This will enable the visualization of all unicode and special characters (eg: arrows, backspace, etc.).

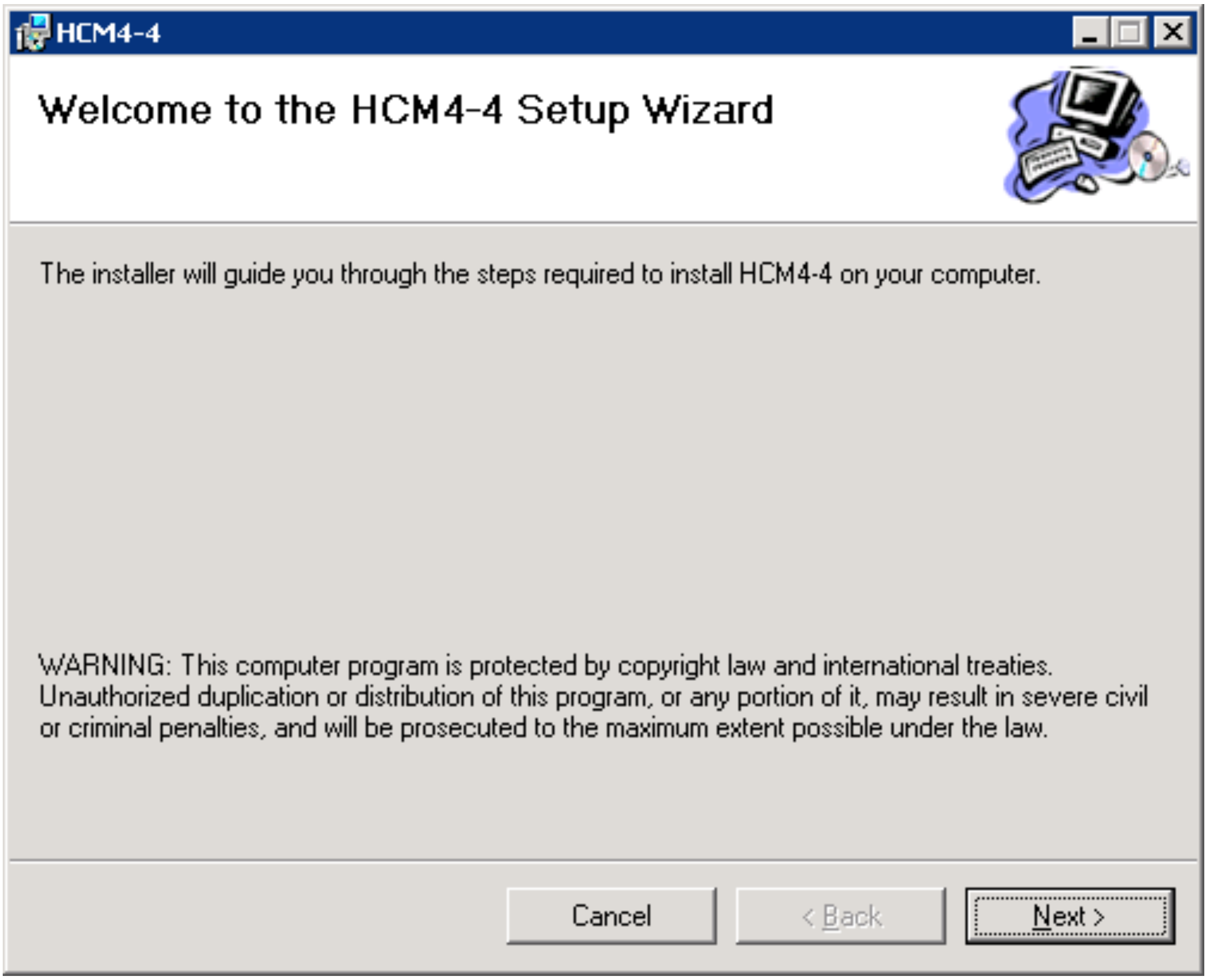
3.4 Control station

Control station doesn't act as a server, so it doesn't need open TCP ports.

3.4.1 HCM

The HCM package contains the necessary software for the configuration of the RCS agents.

The installation file is called HCM-<serial>.msi and must be launched using the following procedure.

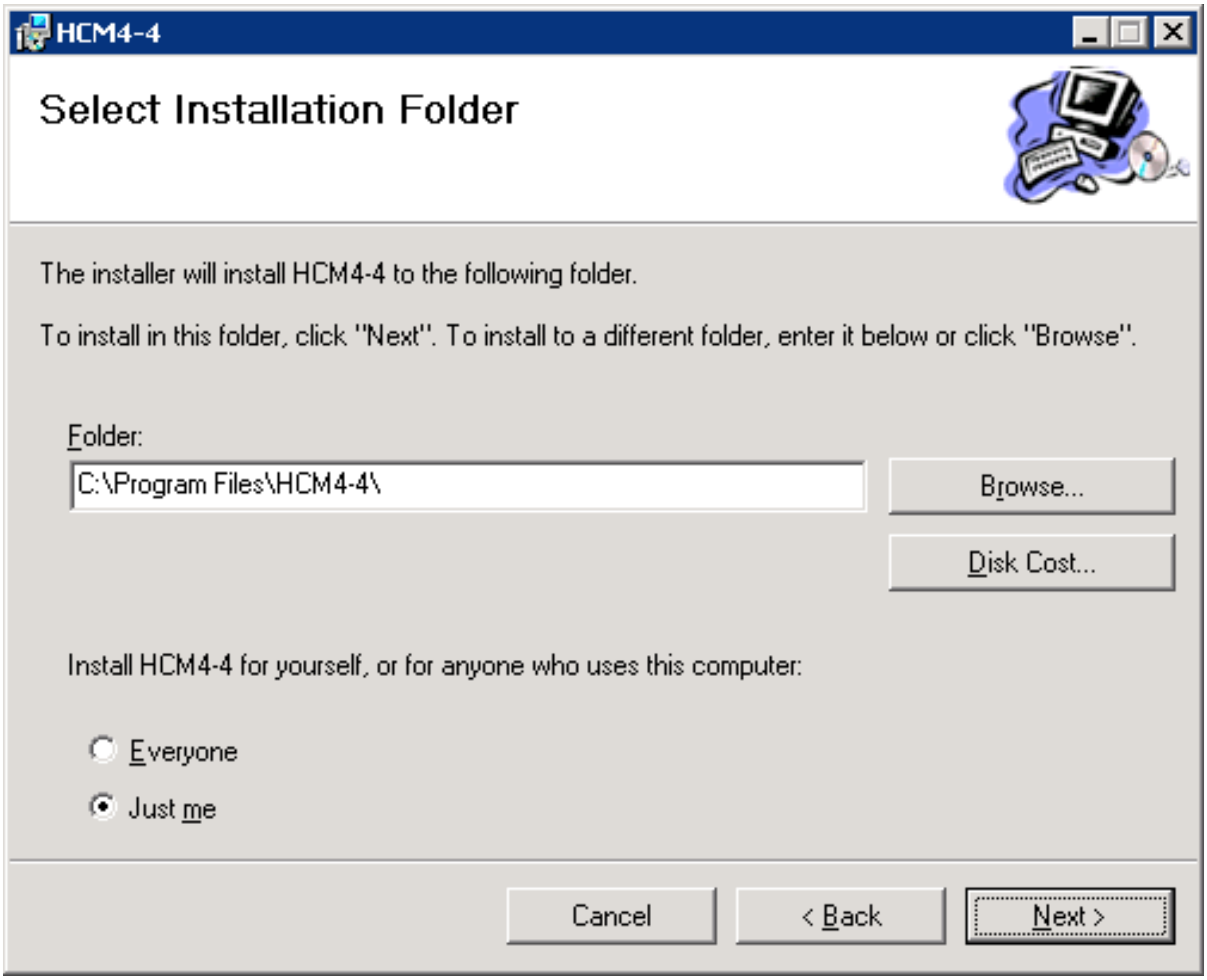


Welcome to the HCM4-4 Setup Wizard

The installer will guide you through the steps required to install HCM4-4 on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

- click on 'Next'



Select Installation Folder

The installer will install HCM4-4 to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

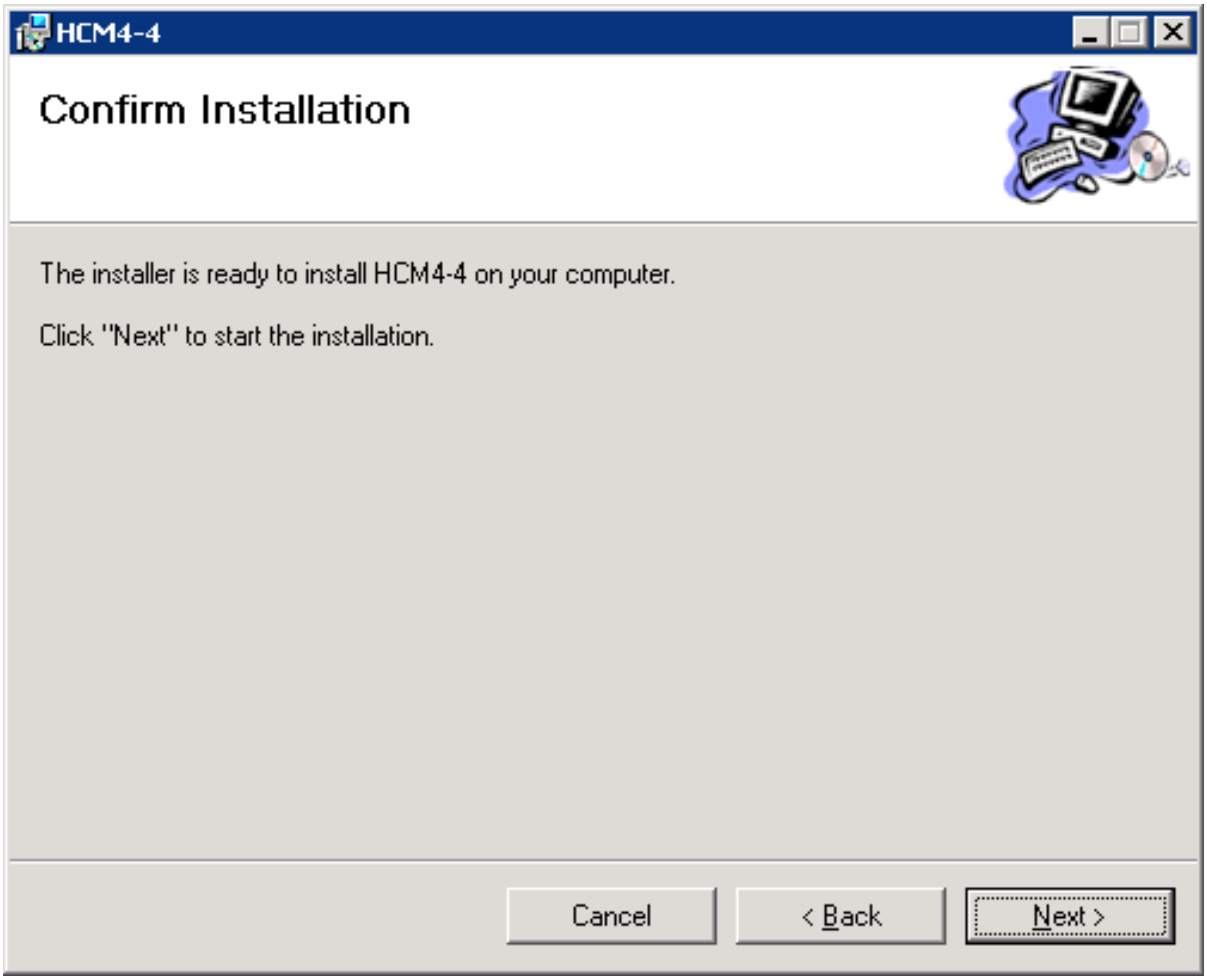
Folder: C:\Program Files\HCM4-4\

Install HCM4-4 for yourself, or for anyone who uses this computer:

○ Everyone

● Just me

- click on 'Next'

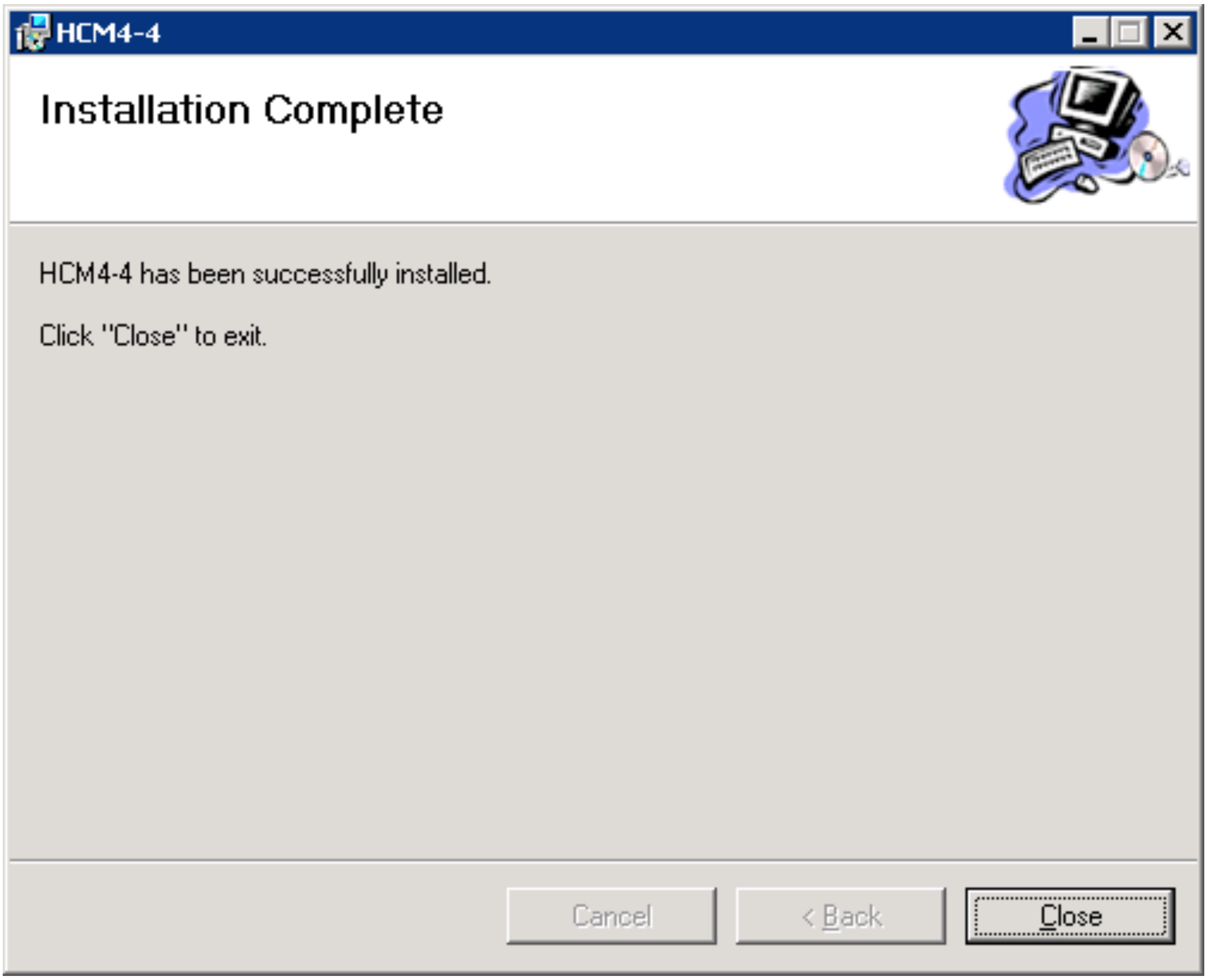


Confirm Installation

The installer is ready to install HCM4-4 on your computer.

Click "Next" to start the installation.

- Click on 'Next'.



Installation Complete

HCM4-4 has been successfully installed.

Click "Close" to exit.

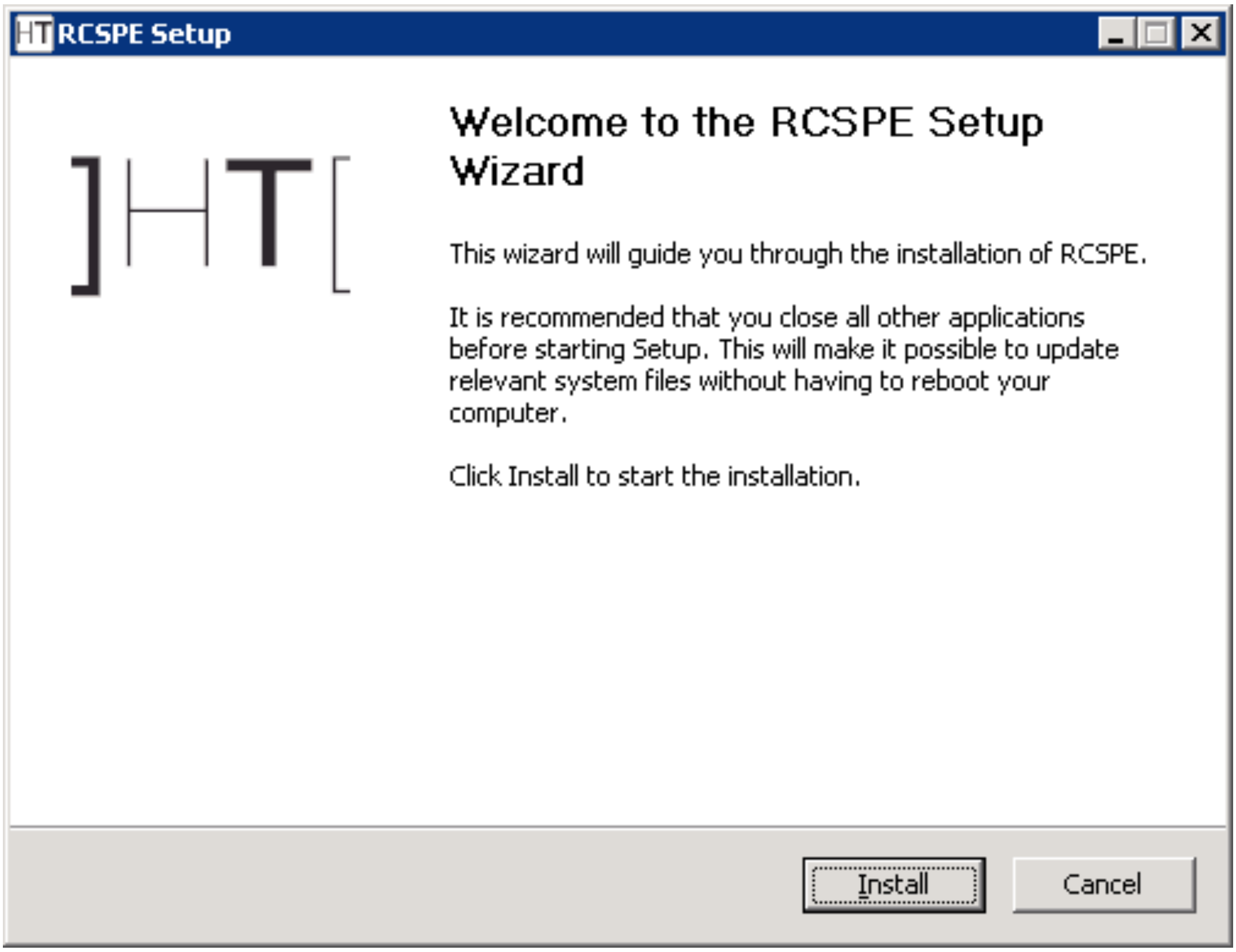
- wait for the installation process to complete
- click on 'Close'

3.4.2 RCSPE

The RCSPE package contains all the necessary software to create the infection vectors (CD/USB).

The installation must take place on the same computer where HCM was installed.

The installation file is called RCSPE-<serial>.exe and must be launched using the following procedure.



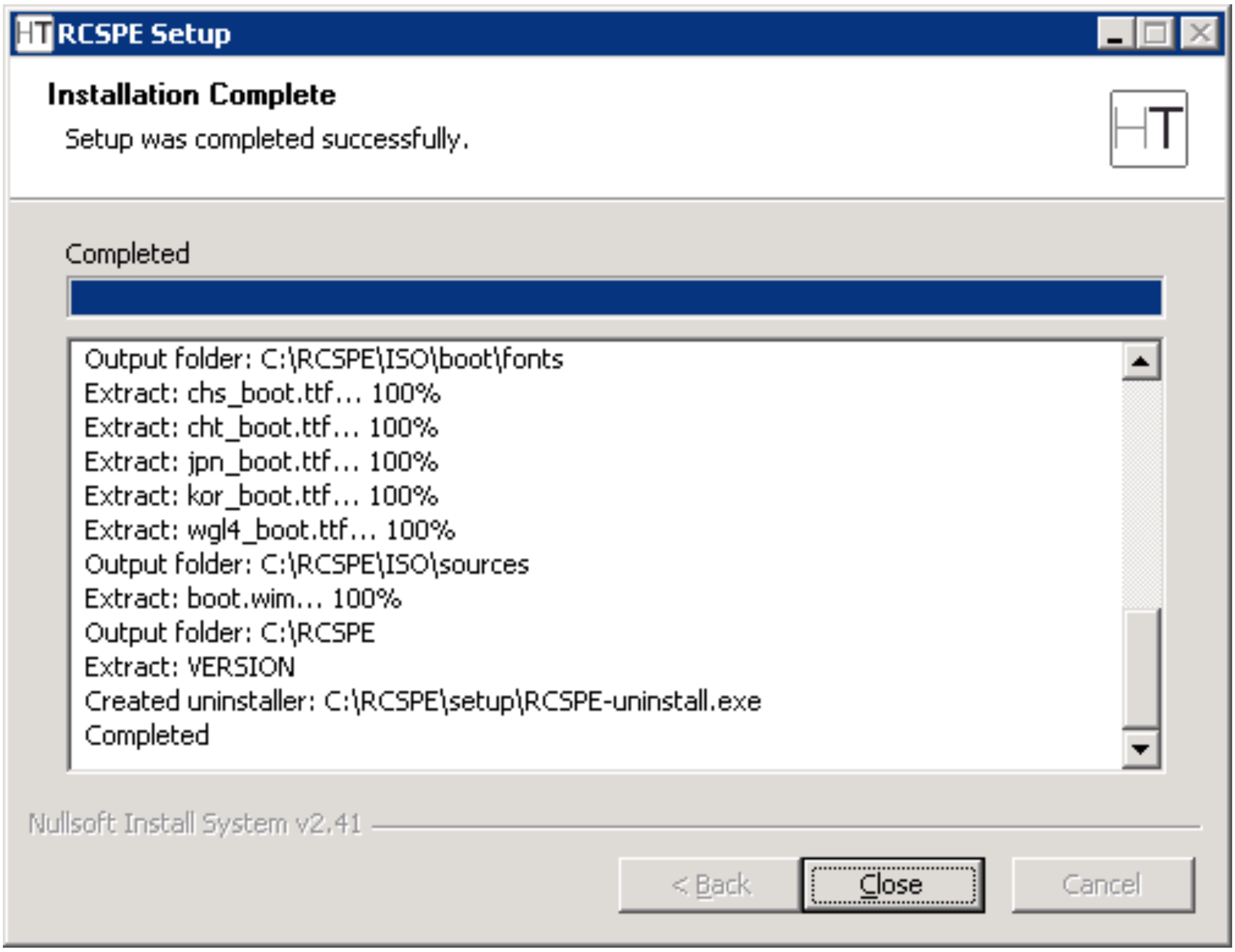
Welcome to the RCSPE Setup Wizard

This wizard will guide you through the installation of RCSPE.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Install to start the installation.

- click on 'Next'


RCSPE Setup
Installation Complete
Setup was completed successfully.
Completed
Nullsoft Install System v2.41
< Back
Close
Cancel

```
Output folder: C:\RCSPE\ISO\boot\fonts
Extract: chs_boot.ttf... 100%
Extract: cht_boot.ttf... 100%
Extract: jpn_boot.ttf... 100%
Extract: kor_boot.ttf... 100%
Extract: wgl4_boot.ttf... 100%
Output folder: C:\RCSPE\ISO\sources
Extract: boot.wim... 100%
Output folder: C:\RCSPE
Extract: VERSION
Created uninstaller: C:\RCSPE\setup\RCSPE-uninstall.exe
Completed
```

- wait for the installation process to complete
- make sure no errors occurred during the installation process
- click on 'Close'

4 Usage

4.1 Functionality Flow

We are going to explain in detail the correct functionality flow of the RCS system.

The flow should be followed exactly as detailed below, and customized according to the needs of the case.

The functionality flow is composed of the following steps:

- *Group creation;*
- *User creation;*
- *Activity creation;*
- *Target creation;*
- *Backdoor creation;*
- *Backdoor configuration;*
- *Infection vector creation;*
- *Evidence visualization;*
- *End of activities.*

4.1.1 Group Creation

This process involves the creation of the groups that will be used in the following steps.

ADMIN-level privileges are needed to execute this step.

The tool used is the RCSConsole.

We recommend the creation of a different group for each group of people dealing with the same activities, creating a new group for every new activity. By assigning the same user to different groups it will be possible to handle existing users (linked to physical persons) in different activities including them in the relative group.

4.1.2 User Creation

This process involves the creation of the users that will be used in the following steps.

ADMIN-level privileges are needed to execute this step.

The tool used is the RCSConsole.

The users are one or more technicians (TECH-level privileges), taking care of backdoor configuration and of the creation of the infection vectors (executable, CD-Rom, USB, etc.), and one or more operators (VIEW-level privileges) tasked with monitoring the evidences once they are archived inside the system.

All users who need to interact with an activity (both newly created and already existing users) will have to be added to the groups designated to that activity.

4.1.3 Activity creation

This process involves the creation of the activities that will be used in the following steps.

ADMIN-level privileges are needed to execute this step.

The tool used is the RCSConsole.

An activity is a complete and complex analysis process that may involve one or more one or more subjects for monitoring. The activity must keep an OPEN state until all the evidence gathering operations are complete. Only then it will be possible to close the activity, thus preventing any further modification. The activity must be associated to the groups created to contain those users who will be able to interact with it.

4.1.4 Target Creation

This process involves the creation of the targets that will be used in the following steps.

ADMIN-level privileges are needed to execute this step.

The tool used is the RCSConsole.

A target is a single entity, part of a specific activity. However, it is possible to associate more than one backdoor to a single target (for instance, for the different devices used by the target).

The target is persistently linked to the activity for which it is created and cannot be re-associated to another activity. The target becomes non-modifiable once the relative activity is closed.

4.1.5 Backdoor Creation

This process involves the creation of the backdoors that will be used in the following steps.

TECH-level privileges are needed to execute this step.

The tool used is the RCSConsole.

A backdoor is a specific installation on a specific device used by the target it is associated to.

The backdoor is persistently linked to the target for which it is created and cannot be re-associated to another target. The backdoor is disabled automatically once the relative activity is closed.

4.1.6 Backdoor Configuration

This process involves the configuration of the backdoors that will be used in the following steps.

TECH-level privileges are needed to execute this step.

The tool used is HCM.

Once the backdoors have been created, it is necessary to configure them to execute the evidence gathering operations and to upload said evidences to the system.

Once the configuration process is complete, it is possible to save the configuration and modify it later using the same procedure.

4.1.7 Infection Vector Creation

This process involves the creation of the infection vectors that will be used in the following steps.

TECH-level privileges are needed to execute this step.

The tool used is HCM.

After a backdoor has been configured, it is time to choose among the different infection vectors that will be used to install the backdoor on the target system.

The creation and use of the vectors may vary according to the selected type. It is possible to create more than one infection vector for the same backdoor. Once installed on the target system, the backdoor will be independent from the infection vector used for the installation.

4.1.8 Installation on target machine

Once the creation of the infection vector is complete, it is possible to install the backdoor on the target system. The installation can take place in different ways:

- "Melted" executable: Just open the file on the target PC (either directly or through hacking or social engineering). The backdoor will be installed automatically, while the no modification to the original executable will be visible to the user (see the paragraph on the "Creation of the infection executable" for further details).
- CD/USB Offline installation: It is possible to boot the target PC from one of these media (it is necessary to have physical access to the computer); the backdoor is installed automatically on the users selected from a list. If the computer cannot be booted (e.g., when the bios is protected by password), it will be possible to directly infect the hard disk linking it with the USB adapter to a laptop on which the Offline Installation CD is executed.
- Injection Proxy: This device can be used to infect the files downloaded by the user on the target PC (see chapter 4.6).
- Installation on Mobile Phones: RCS can be installed on mobile phones by infecting their MMC (see chapter 4.3.4).

  Installation can also be performed manually:
  - If the mobile phone is turned on it can be connected to a laptop pc via ActiveSync/WindowsMobileDeviceCenter. Two files: *autorun.exe* and *autorun.zoo* needs to be copied inside the */Storage Media/2577* directory, it is possible to start the infection either by clicking on the executable or simply restarting the device.
  - If the mobile phone is turned off it is still possible to carry out the infection just by extracting the SD card and copying the backdoor files inside the */2577/* directory. The infection process will start upon reboot or after the re-insertion of the SD card (if the device was already turned on).

4.1.9 Evidence Visualization

This step involves the visualization of the evidence gathered.

VIEW-level privileges are needed to execute this step.

The tool used is the RCSConsole.

The visualization of the evidence allows an operator to have access to all the information received from the backdoors installed on the targets. It is possible to execute queries, save the evidence, create a summary, modify the priority and create public and private notes.

4.1.10 End of Activities

This process involves finalization of the activities executed.

ADMIN-level privileges are needed to execute this step.

The tool used is the RCSConsole.

Once the gathering of the evidences for a given activity is complete, it is possible to close the activity and render it un-modifiable. No new information about the targets will be received, and it will no longer be possible to modify the data associated to the activity. However, it will still be possible to execute all the operations described in the previous step - like the visualization and the creation of the summary.

Closing and activity is an irreversible operation that should only be used in the appropriate case.

All the backdoors related to a closed activity will be automatically uninstalled from the target machine upon next synchronization.

4.2 Admin Station (RCS Console)

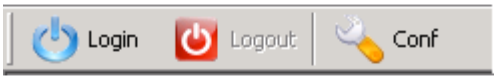
RCS Console usage is described in a different document. Please refer to it for further informations.

4.3 RCS Control Station (HCM)

The HCM system allows the operator to manage and configure the RCS agents through a simple and friendly interface. The software can also create the digital (melted executables, injection proxies) and physical (offline CD-ROM, USB Key) installation vectors.

4.3.1 HCM: Main Control Panel

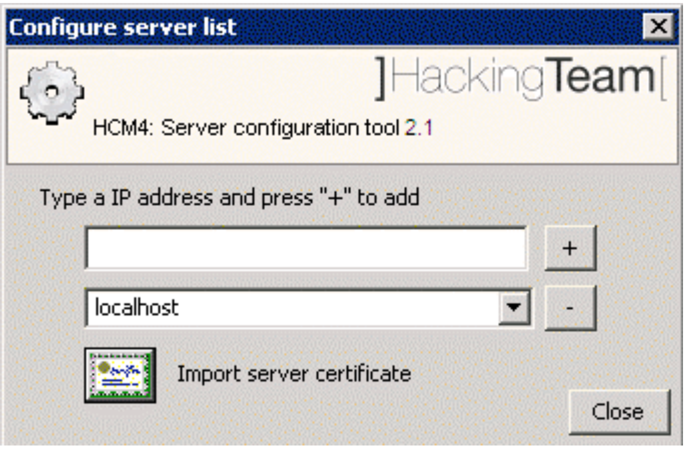
Through the main tool bar, it is possible to log in and out the application and to configure the addresses of the repositories.



Main Toolbar

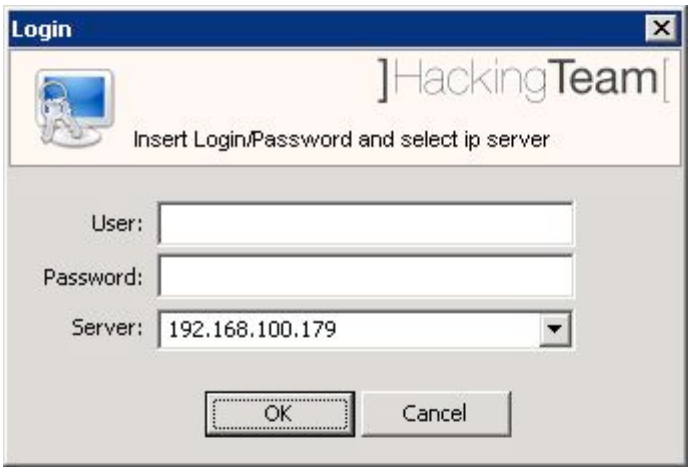
Using the “Conf” button, it is possible to set up the address of a new repository writing the IP address in the field and clicking on the ‘+’ button. To delete a repository, just select it from the drop down list and press the ‘-‘ button.

NOTE: When adding a new repository, importing its certificate is required (click on the certificate icon).


Configure server list
]HackingTeam[
HCM4: Server configuration tool 2.1
Type a IP address and press "+" to add
+
localhost
-
Import server certificate
Close

IP Server Configuration

To log into the application, select the address of the repository you wish to connect to and insert a valid username and password for that repository. Please, note that only users with ‘tech’ privileges can access the HCM (see the paragraph on the creation of users from the Admin Station for further details).



User:

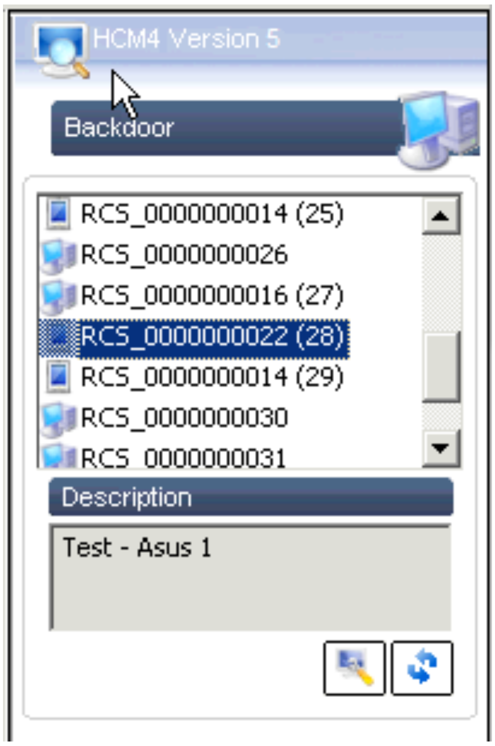
Password:

Server: 192.168.100.179

Login to the Repository

Once the user has been identified, the console will show a lost of the RCS agents on that repository.

4.3.2 HCM: Configuring the RCS Agent



RCS_0000000014 (25)
RCS_0000000026
RCS_0000000016 (27)
RCS_0000000022 (28)
RCS_0000000014 (29)
RCS_0000000030
RCS_0000000031

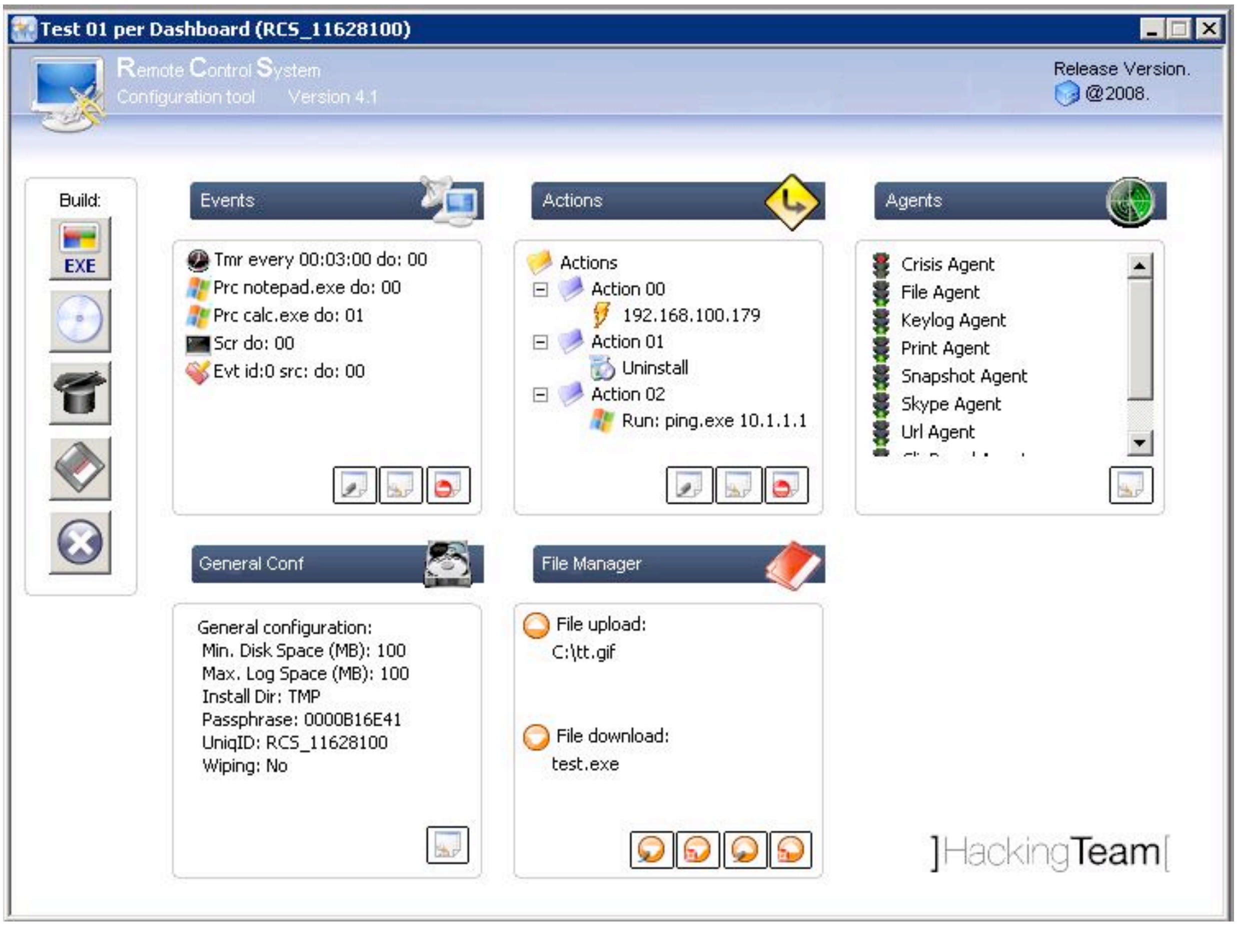
Description

Test - Asus 1

RCS Agents List

Double clicking on an agent (or clicking on the Modify Backdoor button) will open a new window where it is possible to modify the configuration of the selected RCS agent. Agents are identified with different icons depending on the target platform: Desktop/Laptop systems or Smartphone devices.

Through this interface it is also possible to create the infection vectors that will execute the installation of the RCS agent on the target PC or Smartphone.



Tmr every 00:03:00 do: 00
Prc notepad.exe do: 00
Prc calc.exe do: 01
Scr do: 00
Evt id:0 src: do: 00

```
Actions
⊟ Action 00
    192.168.100.179
⊟ Action 01
    Uninstall
⊟ Action 02
    Run: ping.exe 10.1.1.1
```

Crisis Agent
File Agent
Keylog Agent
Print Agent
Snapshot Agent
Skype Agent
Url Agent

General configuration:
Min. Disk Space (MB): 100
Max. Log Space (MB): 100
Install Dir: TMP
Passphrase: 0000B16E41
UniqID: RCS_11628100
Wiping: No

File upload:
C:\tt.gif

File download:
test.exe

Configuration window

The functionality of the RCS agent is based on a "*event/action*" paradigm. This logic is based on the agent's ability to constantly monitor the target system: as soon as one of the preset "events" occurs, the agent will take all the actions it was configured to take.

The configurations created with the HCM are stored in the central repository and sent to the RCS agent as soon as it makes contact (*syncs*) with an ASP server.

4.3.2.1 Event Configuration

The logic of operation is based on the execution of “actions” as soon as certain “events” occur. For instance, it is possible to program the RCS agent to take “snapshots” as soon as an image editing software is started, or send (*sync*) all gathered logs to the server as soon as the screensaver is activated, or disable the most resource-consuming agents when the disk quota is about to be exceeded, as so forth.

Going more into details, the available types of events common to both Desktop and Smartphone agents are:

- Events related to processes/windows (Process);
- Events related to internet connections (Connections);
- Time Events (Timer).

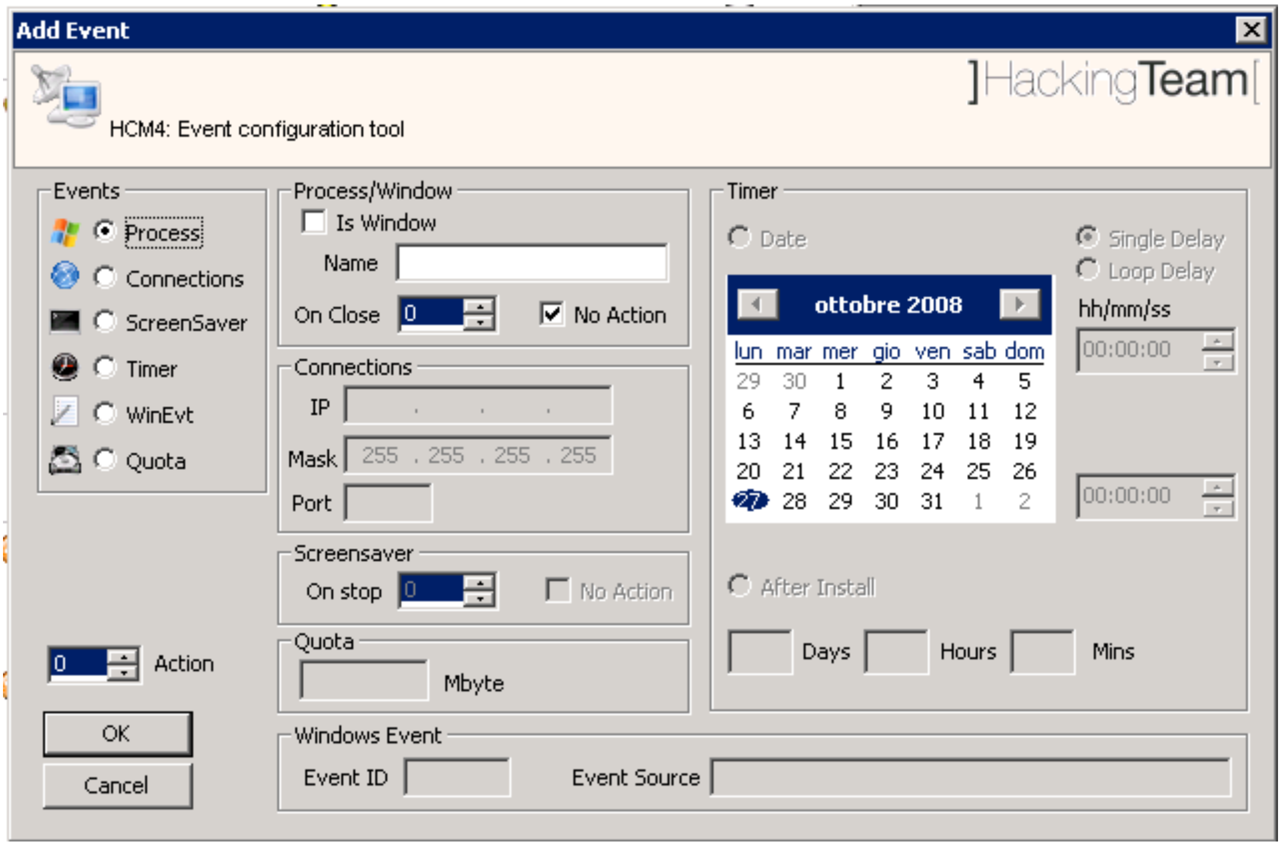
On agents targeted to Desktop or Laptops, it’s also possibile to associate actions to the following events:

- Events related to a specific “Windows System event” (WinEvt);
- Events related to the activation/deactivation of the screensaver (ScreenSaver);
- Disk quota-related events.

Agents targeted to Smartphone devices present the following events:

- SIM change event;
- Incoming SMS message event;
- Events related to geographical location.

Each event is linked to an “action” by a progressive number displayed in the “Action” window.



● Process

□ Is Window

On Close 0 ☑ No Action

Mask 255 . 255 . 255 . 255

On stop 0 □ No Action

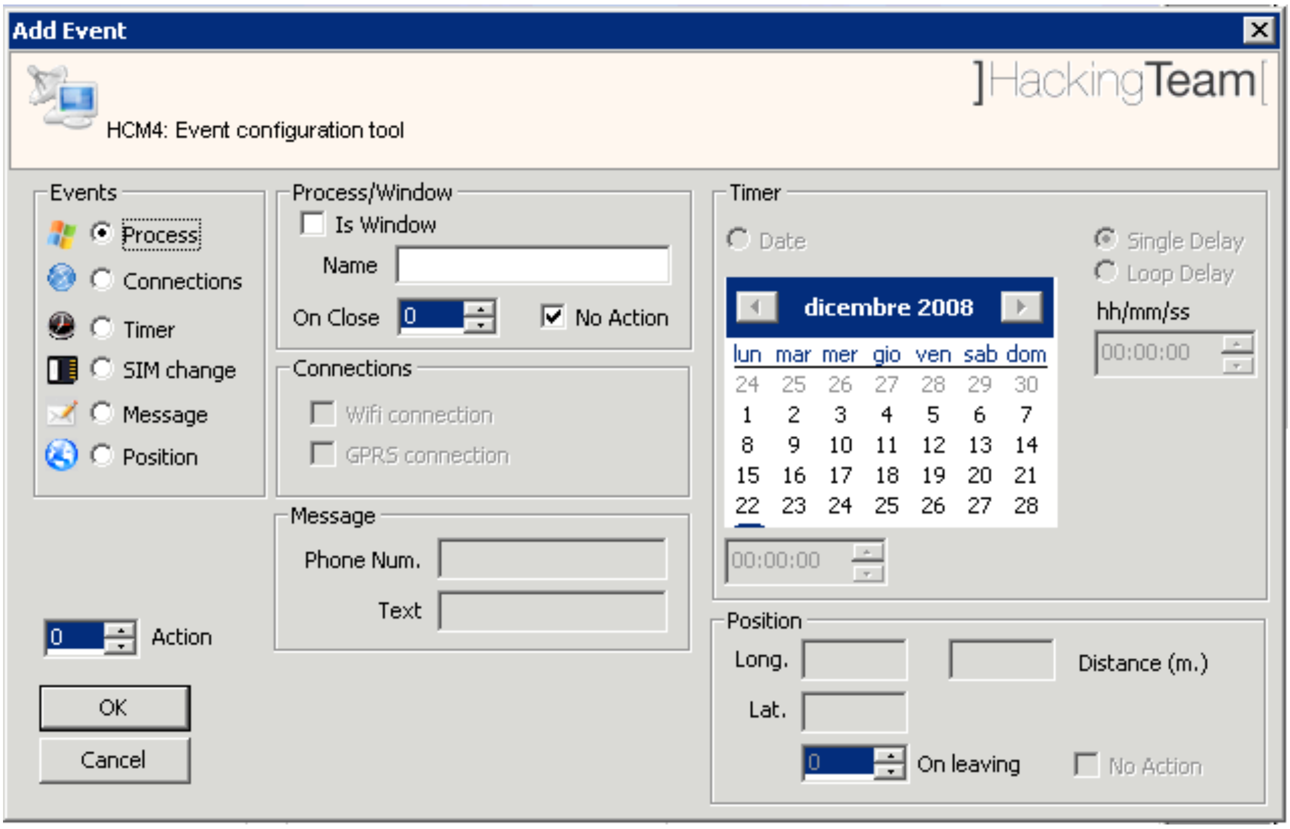
● Single Delay

hh/mm/ss 00:00:00

00:00:00

0 Action

Event Configuration (for Desktop agents)



● Process

□ Is Window

On Close 0 ☑ No Action

● Single Delay

hh/mm/ss 00:00:00

00:00:00

0 On leaving □ No Action

0 Action

Event Configuration (for Smartphone agents)

Creating or modifying an *event* is as easy as clicking on the relative button in the "Events" check or double-clicking on the event itself. The system will immediately open the event management window. Here it is possible to see all the necessary elements to create a new event. The most important elements are:

- The "*Action*" field: allows you to select the action to perform when the event occurs (see next paragraph);
- *Radio-button* "Events": allows you to select the type of event (in the left-hand side of the window) and to set up all the parameters related to the event.

All other parameters are specific to the selected event:

Process/Window

Description: the event is detected when an executable or a window "compatible" with the selected parameters is opened on the target PC.

Parameters:

- *Is Window*: specifies if the string of text in the "Name" field is the name of an executable or a window's header;
- *Name*: the name of an executable (*case insensitive* with the extention ["*.exe*"]) or the header of a window (*case insensitive*). For the names of the windows (that is, if the "is window" field is checked) is is possible to use wildcards (like '*'): it is thus possible to match sub-strings of a window's header (e.g., *"* - Microsoft *"*);
- *On Close*: sets the action to perform when the process is terminated or the window is closed;
- *No action*: sets whether or not to perform an action when the process is terminated or the window is closed.

Connection

Description: the event is detected when a TCP connection is established between the target PC and a specific IP address or subnet.

Parameters:

- *IP*: sets an address or subnet [e.g., "*223.1.2.33*", "*150.11.0.0*"]. If the IP and the Mask fields are set to [0.0.0.0], the event will be detected with any address.
- *Mask*: a network mask that allows matching a host or a network [es. "*255.255.255.248, "255.255.0.0:*"]
- *Port*: sets the TCP port linked to a service [es "*80*", "*443*", "*25*"]. If the Port field is set to "0", the event will be detected with any port.

N.B. Connections to local addresses in the same subnet as the target are not taken into account.

Timer

Description: the event is detected at the end of a set period of time.

Parameters:

- *Date*: sets a specific date (day/month/year) and a specific hour. If the RCS agent is not active at that moment (for example, if the target PC is off) the event is generated at the next activation.
- *Single delay*: an interval of time (hours/minutes/seconds) calculated starting from when the monitored user logs onto the target PC. Use the controls on the top-right corner to set this parameter.
- *Loop delay*: The same as Delay, but the event keeps being triggered cyclically. Use the controls on the top-right corner to set this parameter.
- *After install:* sets a specific time (days/hours/minutes) from the moment the RCS agent is installed on the target PC.

Screensaver

Description: the event is detected as soon as the screensaver is activated on the target PC.

Parameters:

- *On stop*: sets the *action* to perform when the screensaver is deactivated.
- *No action*: sets whether or not to perform the *action* when the screen saver is deactivated.

Windows Event

Description: the event is detected when the relative “windows event” occurs on the target PC.

***Parameters**:*

- *Event id*: sets the numeric id of a “*windows event”.*
- *Event source*: sets the event type (es: System, Application, etc.).

Quota

Description: the event is detected when the total amount of gathered logs reach a certain size.

***Parameters**:*

- *Mbyte*: sets at how many Megabytes the event will be triggered.

SIM Change

Description: the event is detected when the SIM inserted into the Smartphone is changed with a different one.

***Parameters**:*

- *There are no configurable parameters for this event*.

Message

Description: the event is detected when an SMS message coming from a specified number and with a specified text is received.

***Parameters**:*

- *Phone Num.*: indicates the phone number from which the message will be sent. The phone number must be written with the international prefix;
- *Text:* indicates the message body, up to 160 ASCII characters, that will trigger the event.

Position

Description: the event is detected when a specific geographical location is entered or left.

***Parameters**:*

- *Long.* : sets the Longitude relative to the centre of the location.
- *Lat.* : sets the Latitude relative to the centre of the location;
- *Distance :* sets the Distance from the point indicated by Latitude and Longitude. This will act as the radius of the circle that delimits the location to be monitored.
- *On leaving* : sets the Action to be triggered when location is left. Check *No Action* if triggering should happen only upon entrance of the location.

4.3.2.2 Action Configuration

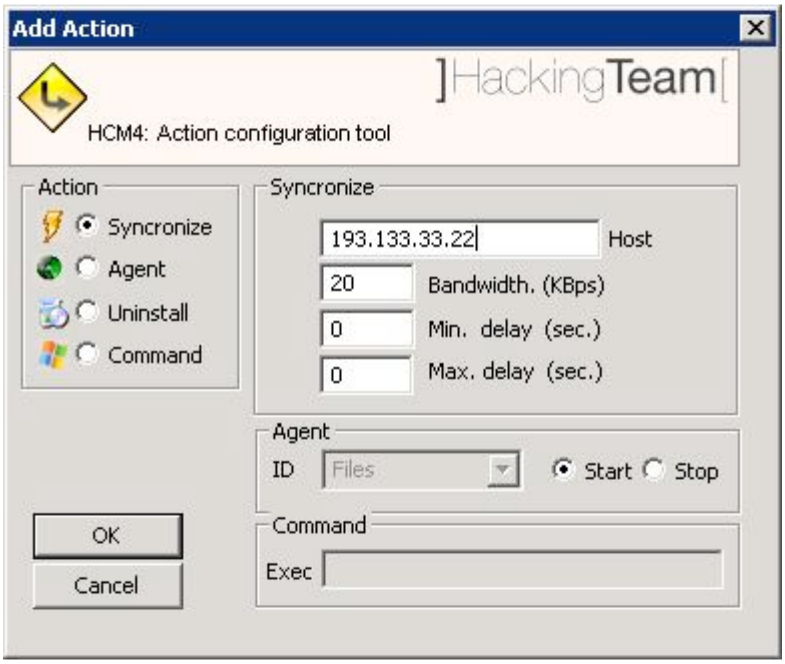
Clicking the “Create Action” button in the “Actions” window will open the dialog box used to create actions. Each action will be identified by an incremental number.

Clicking the “Create Action” button after selecting an existing action (e.g., Action 00, Action 01) it will possible to add a “sub-action”.

Each “*action*” is actually a logic container of “*sub-actions*”: this mechanism allows the RCS agent to execute one or more commands inside the same action.

When an “*event*” is triggered (according to the configuration process described in the previous paragraph) the RCS agent will perform all the “*sub-actions*” contained in the “*action”* associated to the event.

The “Modify Action” and the “Delete Action” buttons allows you to modify or delete an action. Double-clicking on an action has the same function as clicking on “Modify Action”.



Add Action

HCM4: Action configuration tool

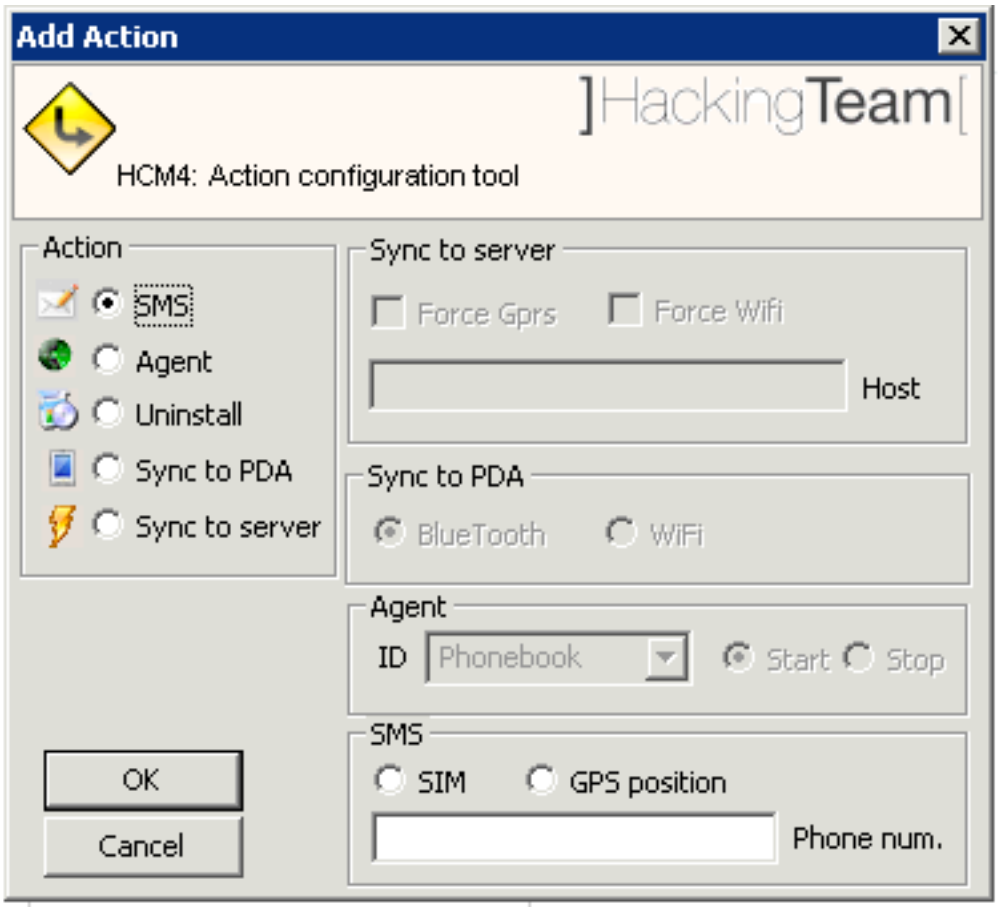
Action
- ● Syncronize
- ○ Agent
- ○ Uninstall
- ○ Command

Syncronize
- Host: 193.133.33.22
- Bandwidth. (KBps): 20
- Min. delay (sec.): 0
- Max. delay (sec.): 0

Agent
- ID: Files
- ● Start ○ Stop

Command
- Exec:

Action Configuration (for Desktop/Laptop agents)



Add Action

]HackingTeam[

HCM4: Action configuration tool

Action
● SMS
○ Agent
○ Uninstall
○ Sync to PDA
○ Sync to server

Sync to server
□ Force Gprs □ Force Wifi
Host

Sync to PDA
● BlueTooth ○ WiFi

Agent
ID Phonebook ● Start ○ Stop

SMS
○ SIM ○ GPS position
Phone num.

Action Configuration (for Smartphone agents)

A selection in the "*Action*" *radio-button* (in the left-hand side of the window) will allow you to configure the parameters of the selected action. According to which action is selected, the parameters are:

Synchronize (on Desktop agents)
Sync to server (on Smartphone agents)

Description: will perform synchronization between the RCS agent and the ASP server. The synchronization process is composed of th following steps:

- Version verification and mutual identification between the RCS agent and the ASP server.
- Time synchronization between the RCS agent and the ASP server.
- Update of the RCS agent's configuration.
- Upload of all the files in the "upload" queue (see the paragraph about the File Manager for further details).
- Download of all the files in the "download" queue (see the paragraph about the File Manager for further details).
- Upload of all logs gathered by the RCS agent.
- Safe removal of the uploaded logs.

Parameters:

- *Host*: sets the IP address (or the name) of the ASP server to synchronize with.
- *Bandwidth*: upper limit to the bandwidth the agent will use to upload data (KiloByte per second [max. 10000 KBs])
- *Min. delay*: lower limit of the random latency between the upload of each log (useful to avoid traffic profiling). Set this value to 0 to apply no lower limit.
- *Max delay:* Upper limit of the random latency between the upload of each log (useful to avoid traffic profiling). Set this value to 0 to apply no upper limit.

Agent (interception modules)

Description: Activates or deactivates a specific “log agent”.

Parameters:

- *ID*: sets the log agent to activate/deactivate.
- *Start*: Activates the module.
- *Stop:* Deactivates the module.

Uninstall

Description: Remove RCS agent

Note: RCS agent will be **totally removed** on the target system.

Command (only for Desktop agents)

Description: executes a system command.

Parameters:

Exec: sets the name of an executable (the use of absolute path names is advised) with the relative parameters, if any (the maximum length of the string is 250 characters). Besides the standard ambient variables, it is possible to use a “virtual” ambient variable *dir* that points to the agent’s own (hidden) installation folder: it is possible to use this special variable when executing commands like the one in the example: `%systemroot%\system32\cmd.exe /c dir > $dir$\result.txt`. This string executes the shell command “dir” and redirects the output on a file inside the hidden log repository in the target PC. The files created with this process can then be downloaded (see the paragraph about the File Manager for further details). It is important to be particularly careful when performing this action because, even though all commands are executed using the RCS agent’s hiding system and are therefore undetectable, any resulting modification to the file system (e.g., files created on the desktop, etc.) will be visible by the user.

SMS (only for Smartphone agents)

Description: Send an SMS with selected informations.

Parameters:

- *SIM*: send message with SIM informations.
- *GPS Position*: send a message with GPS Position.
- *Phone num.* : phone number to send message to. Number must be complete of international prefix.

Sync To PDA (only for Smartphone agents)

Description: Sync to a portable system by means of WiFi or Bluetooth connection.

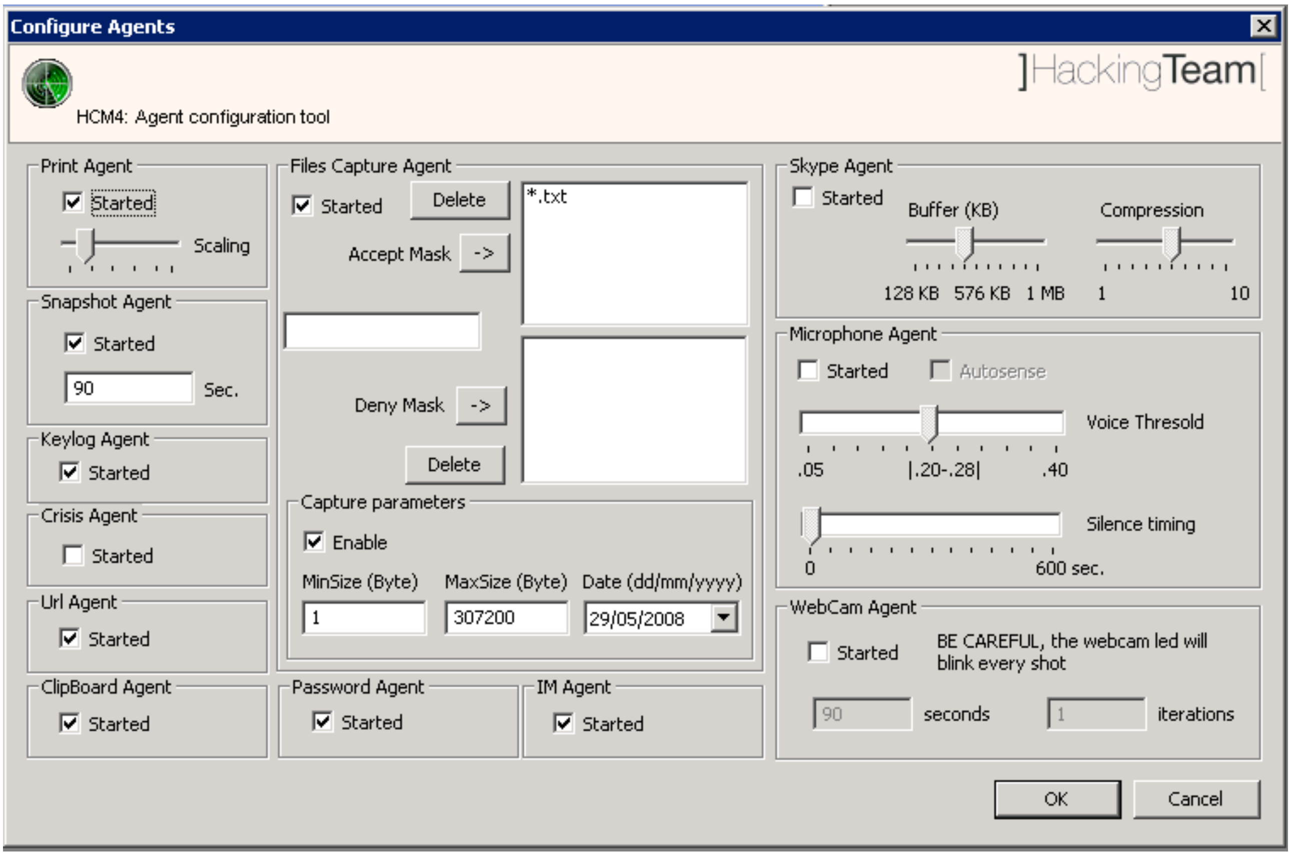
Parameters:

- *Bluetooth*: use a Bluetooth connection to perform syncronization.
- *WiFi*: use a WiFi connection to perform syncronization.

4.3.2.3 *Configuring the interception modules (Agents)*

In this window it is possible to configure the behaviour of the interception modules implemented by the RCS agent.

The modules (also called *log agents* or, simply, *agents*) are tasked with gathering logs on user activity on the target machine.



Configure Agents

HCM4: Agent configuration tool

Print Agent: ☑ Started; Scaling

Snapshot Agent: ☑ Started; 90 Sec.

Keylog Agent: ☑ Started

Crisis Agent: □ Started

Url Agent: ☑ Started

ClipBoard Agent: ☑ Started

Files Capture Agent: ☑ Started; Accept Mask: *.txt; Deny Mask

Capture parameters: ☑ Enable; MinSize (Byte): 1; MaxSize (Byte): 307200; Date (dd/mm/yyyy): 29/05/2008

Password Agent: ☑ Started

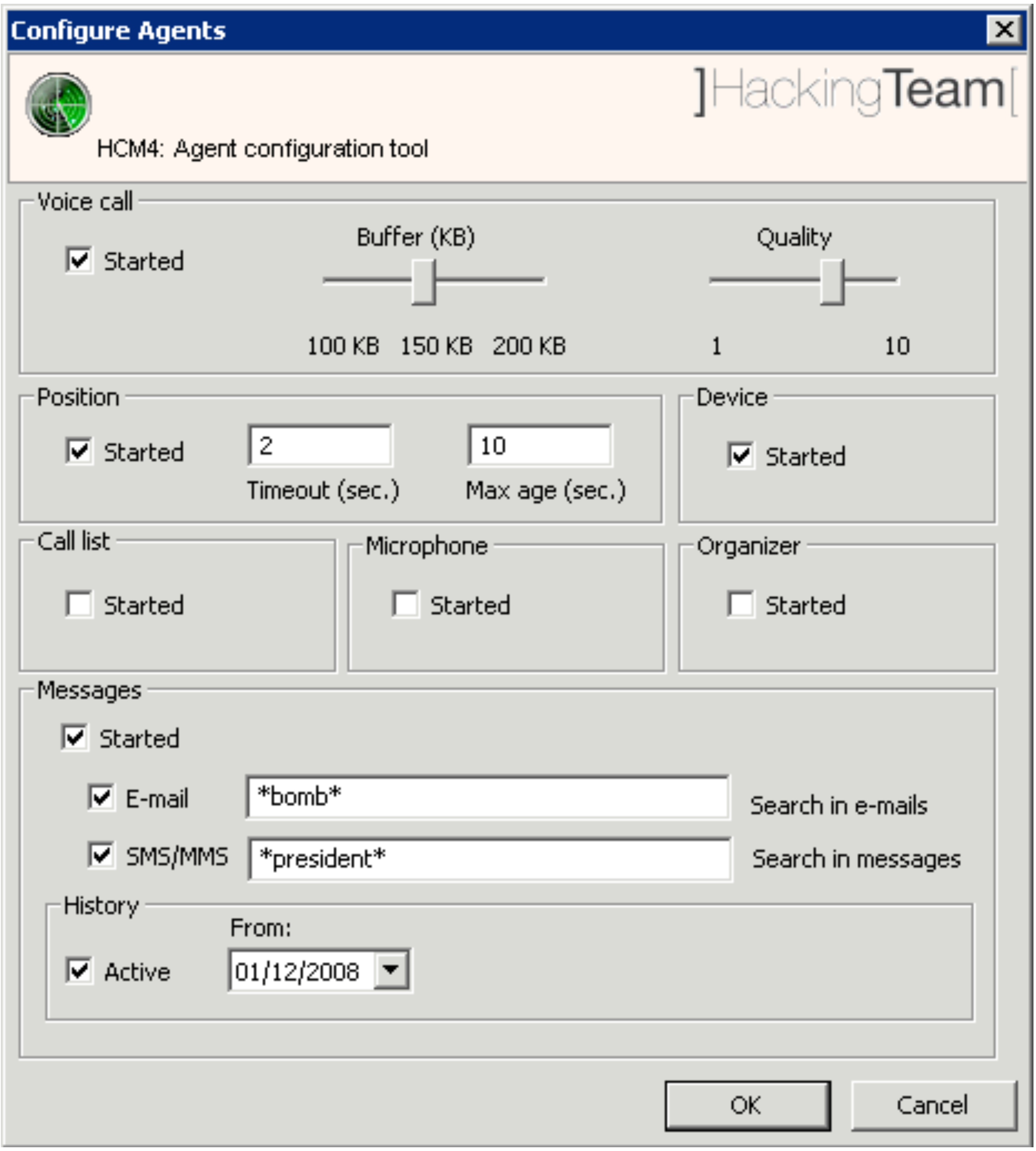
IM Agent: ☑ Started

Skype Agent: □ Started; Buffer (KB); Compression

Microphone Agent: □ Started; □ Autosense; Voice Thresold; Silence timing

WebCam Agent: □ Started; BE CAREFUL, the webcam led will blink every shot; 90 seconds; 1 iterations

Parameters of the Interception Modules (on Desktop agents)



Configure Agents

HCM4: Agent configuration tool

Voice call
☑ Started
Buffer (KB): 100 KB 150 KB 200 KB
Quality: 1 10

Position
☑ Started
Timeout (sec.): 2
Max age (sec.): 10

Device
☑ Started

Call list
□ Started

Microphone
□ Started

Organizer
□ Started

Messages
☑ Started
☑ E-mail: *bomb* Search in e-mails
☑ SMS/MMS: *president* Search in messages

History
☑ Active
From: 01/12/2008

Parameters of the Interception Modules (on Smartphone agents)

The configuration window allows you to define the default status of each module. At start-up the RCS agent reads from its configuration parameters whether to activate a module, based on the respective "*Started*" parameter: if this box is checked, the RCS agent will immediately start the module, otherwise the activation of the module will be triggered by a preset "*event/action*", at which point the agent will start intercepting the corresponding data.

In order to modify an *agent's* (or interception module) parameters, simply click on the corresponding button in the "Agents" control panel or double click on the list. The system will display the agents' management window. The available parameters are:

Print Agent (only for Desktop agents)

***Description*:** Interception module for printed documents.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

Scaling: sets the final quality of the image generated when capturing a printed document. The *slide bar* allows you to set the compression ratio and the quality of the generated images: sliding the cursor to the right end will apply a high level of compression, while sliding the cursor to the right will apply less compression, while generating higher-quality images.

N.B. Using the default value is advised.

Snapshot Agent (only for Desktop agents)

***Description*:** interception module that takes "snapshots" of the target PC's desktop.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.
- *Seconds*: time in seconds between captures.

Keylog Agent (only for Desktop agents)

***Description*:** interception module for keystrokes (both from keyboard or IME device).

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

Url Agent (only for Desktop agents)

***Description*:** Interception module for all visited websites.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

File Agent (only for Desktop agents)

Description: interception module for all the files accessed on the target PC.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.
- *Accept mask*: a list of names (the use of *wildcards* is allowed) that specify which files to trace during the interception activity.
- *Deny Mask:* a list of *exceptions* that specify the *patterns* to exclude from the “accept mask” (e.g., Accpet mask = “*.txt” and Deny Mask = “c:\windows” will trace all text files except those in the “c:\windows” folder).

Capture parameters

- *Enable*: this checkbox allows you to set whether or not to make a physical copy of the traced files. The file will be copied only if all parameters are met (Accept/Deny Mask, Min.size, Max.size, Date).
- *Min. size*: the files that meet the matching parameters (Accept/Deny Mask) are “copied” only if larger than “Min. size” bytes.
- *Max. size*: the files that meet the matching parameters (Accept/Deny Mask) are “copied” only if smaller than “Max. size” bytes.
- *Date*: the files that meet the matching parameters (Accept/Deny Mask) are “copied” only if more recent that the selected date.

VoIP Agent (only for Desktop agents)

Description: interception module for VoIP calls (Skype, WindowsLive, etc.) made from the target PC.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.
- *Buffer*: size in Byte of the capture buffer used when capturing each audio sample.
- *Compression:* level of compression of the audio samples (1=maximum compression, 10=best quality).

N.B. It is strongly advised to use the default values, allowing for a good compromise between file size and audio quality.

Crisis Agent (only for Desktop agents)

Description: if activated, this module blocks some of the functions of a RCS agent, like:

- Synchronization (Synchronize Action);
- Command execution (Command Action).

N.B. Extreme attention is advised in the use of this module. Its employment will block the RCS agent from sending log files. This module was thought as a "Crisis" device designed to protect, inhibiting those functions that may result more detectable. It could be used, for instance, to create a "Process" event able to detect the launch of a specific analysis software, linked to the execution of a "start crisis agent" action. Likewise, the Crisis Agent could then be deactivated by the "OnClose" action of the aforementioned "Process" event.

Microphone Agent

Description: audio surveillance module

Note: on Smartphone agents there are no configurable parameters.

Parameters:

- *Autosense*: If this flag is checked, the agent will try to modify audio mixer settings[1] (mute/unmute, line selection and volume) in order to optimize audio capture, avoiding low volumes or clipped recordings.
- *Voice Threshold*: the Microphone agent tries to record only human voices, avoiding background noise. Voice analysis functions produce an output value: if the value is in the accepted range, the captured chunk is recorded. Suggested range is 0.2-0.28. Higher values will adapt better to female voices but will record more background noise as well.
- *Silence Timing*: This value represents the maximum amount of seconds of silence that the agent will record. If the agent captures only silence for "silence time" seconds, the recording is interrupted. There can be moments of silence in any conversation: if this value is too low, only the "active" part of the conversation will be recorded, suppressing all silence. On the other hand, if the slider is set to the highest value, silence will not be suppressed at all and the audio capture will result in a single continuous recording.

[1] Only if the audio driver allows it.

Clipboard Agent (only for Desktop agents)

Description**:** this module intercepts the text stored in the Clipboard

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

Password Agent (only for Desktop agents)

Description**:** interception module for the passwords stored on the target PC (e.g.: e-mail account, WindowsLive account, etc.)

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

IM Agent (only for Desktop agents)

Description**:** interception module for Chat and InstantMessaging sessions.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.

WebCam Agent (only for Desktop agents)

Description**:** this interception module can take snapshots using the webcam.

Parameters:

- *Started*: sets whether or not the interception module is active when the RCS agent starts up.
- *Seconds*: sets the time in seconds between snapshots.
- *Iterations*: sets the number of snapshots the agent will take from the moment it’s activated.

Voice Call Agent (only for Smartphone agents)

Description: this interception module takes voice calls.

Note: default values are optimal for most scenarios, it is strongly advised to not modify them.

Parameters:

- *Buffer*: size in Byte of the capture buffer used when capturing each audio sample;
- *Compression:* level of compression of the audio samples (1=maximum compression, 10=best quality).

Position Agent (only for Smartphone agents)

Description: this interception module periodically registers the position of the device.

Note: this module needs a smarphone with gps capabilities to work. Actual working depends on the performance of the GPS and on the conditions of use of the device (ie. indoor usage may prevent proper working).

Parameters:

- *Timeout*: The timeout (in seconds) between two requests;
- *Max age:* Maximum valid age for coordinates in cache.

Device Agent (only for Smartphone agents)

Description: this interception module takes generic informations on the device.

Parameters:

- *There are no configurable parameters for this agent.*

Call List Agent (only for Smartphone agents)

Description: this interception module takes the list of calls received, done and rejected.

Parameters:

- *There are no configurable parameters for this agent.*

Microphone Agent (only for Smartphone agents)

Description: this interception module continuously registers sound using the Smartphone microphone.

Note: usage of this agent heavily shortens device's battery duration.

Parameters:

- *There are no configurable parameters for this agent.*

Organizer Agent (only for Smartphone agents)

Description: this interception module takes all the calendar and contact list entries.

Parameters:

- *There are no configurable parameters for this agent.*

Messages Agent (only for Smartphone agents)

Description: this interception module takes all the SMS, MMS and Email messages already stored on the phone and upon reception.

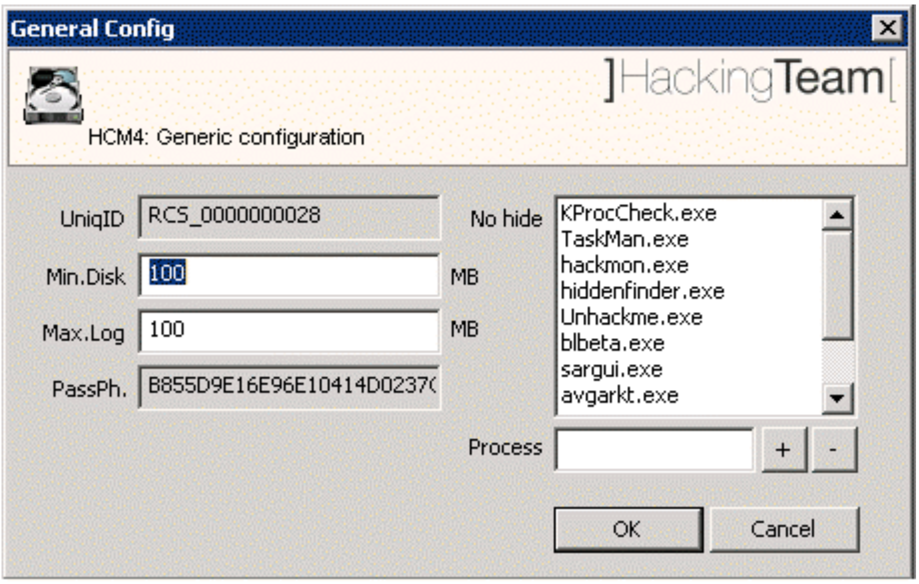
Note: keywords could use one or more “*” (star) character or “?” (question mark) character as wildcards. Star character matches anything, while question mark matches any single character.

Parameters:

- *E-mail: sets a keyword to filter sender e-mail address and subject of the message.*
- *SMS/MMS: sets a keyword to filter sender SMS/MMS phone number and body (for SMS) or subject (for MMS) of the message.*
- History Active: if checked stored messages are collected if matching the E-mail or SMS/MMS filters.
- History From: sets the date from which messages are started to be taken; messages older than the selected date will not be taken.

4.3.2.4 General Configuration

Pressing the “Modify Config” button in the “General Config” panel will give you access to the “General Config” window, where it is possible to set up the general parameters of the RCS agent.



General Config

HCM4: Generic configuration

UniqID: RCS_0000000028

Min.Disk: 100 MB

Max.Log: 100 MB

PassPh.: B855D9E16E96E10414D0237(

No hide:
KProcCheck.exe
TaskMan.exe
hackmon.exe
hiddenfinder.exe
Unhackme.exe
blbeta.exe
sargui.exe
avgarkt.exe

Process:

General Configuration

The parameters are:

- *Max. Log*: the maximum amount of disk space the agent can take before it stops producing logs (this value is calculated in millions of bytes, Max value is ‘4000’).
- *Min. Disk*: the minimum amount of free disk space on the file system of the target PC. If the free available space goes under this value, the RCS agent will stop producing logs (this value is calculated in millions of bytes, Max value is ‘4000’).
- *UniqID*: the unique identifier of the RCS agent, used internally by the RCS system. This identifier contains an additional ID (in brackets) if it’s a secondary instance of a backdoor (see the paragraph about backdoors in the RCS Console manual).
- *PasshPh*: the key used for the encryption of the logs gathered by the RCS agent.

No hide: a list of executables that won’t be infected by the hiding module of the RCS agent. The names of the “.exe” files must match exactly the name of the executable you wish to exclude (the matching process id *case-sensitive*). Pressing the ‘+’ and ‘-‘ keys it is possible to add or remove a name from the list. This can be useful to bypass those anti-rootkit systems that perform differential analysis to detect hidden files and processes.

4.3.2.5 File manager

In this window it’s possible to add/remove one or more files from the Upload/Download queue of the RCS system.

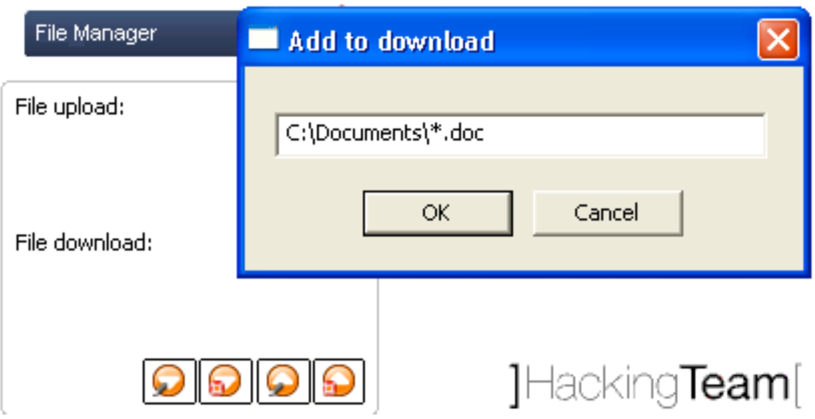
Each RCS agent is able to transfer file both ways (from the RCS server to the target PC and vice versa) during the synchronization process.

This component allows you to manage the Upload (to the target PC) and Download (from the target PC to the RCS server) queues.

Using the four buttons in the panel, it is possible to add or remove a file from the Download queue, and to add or remove a file from the Upload queue.

Downloading a file from the PC target requires the operator to input a filename (of a file located on the target PC) with absolute pathname. It is possible to specify multiple files using *wildcards* like, for instance, io“*c:\Dir\Files\*.doc*”. Besides to standard ambient variable, it is possible to use the virtual variable “$dir$” that points to the repository hidden on the target PC.

The files in the Upload queue are transferred on the target PC at the first synchronization and are stored in the hidden repository of the RCS agent (they can be accessed using the virtual variable “$dir$”).



C:\Documents\*.doc

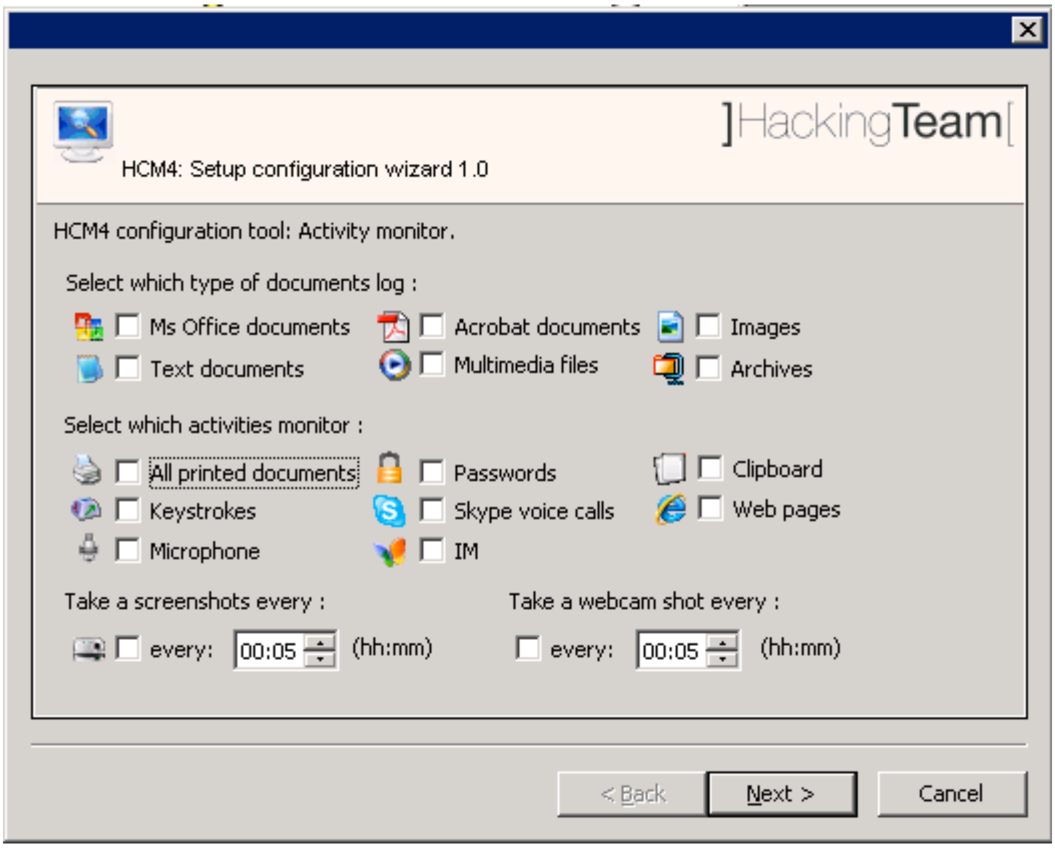
File manager

Note The files are removed from the Upload/Download queue once transfer is complete.

4.3.2.6 The Configuration Assistant

In order to make the configuration process of a RCS agent more easy and direct, pressing the button it is possible to access a guided process that allows the operator to create a basic configuration. It will then be possible to fine-tune the basic configuration using the process described in the previous paragraphs.

Using the Configuration Assistant, the operator can choose the "*activities*" to intercept on the target PC, the type of documents to monitor, when and towards which RCS server to execute the transfer of the logs. The guided procedure is composed of three steps; in the first step, the operator chooses which activities to monitor on the target PC.



HCM4: Setup configuration wizard 1.0

HCM4 configuration tool: Activity monitor.

Select which type of documents log :

□ Ms Office documents □ Acrobat documents □ Images
□ Text documents □ Multimedia files □ Archives

Select which activities monitor :

□ All printed documents □ Passwords □ Clipboard
□ Keystrokes □ Skype voice calls □ Web pages
□ Microphone □ IM

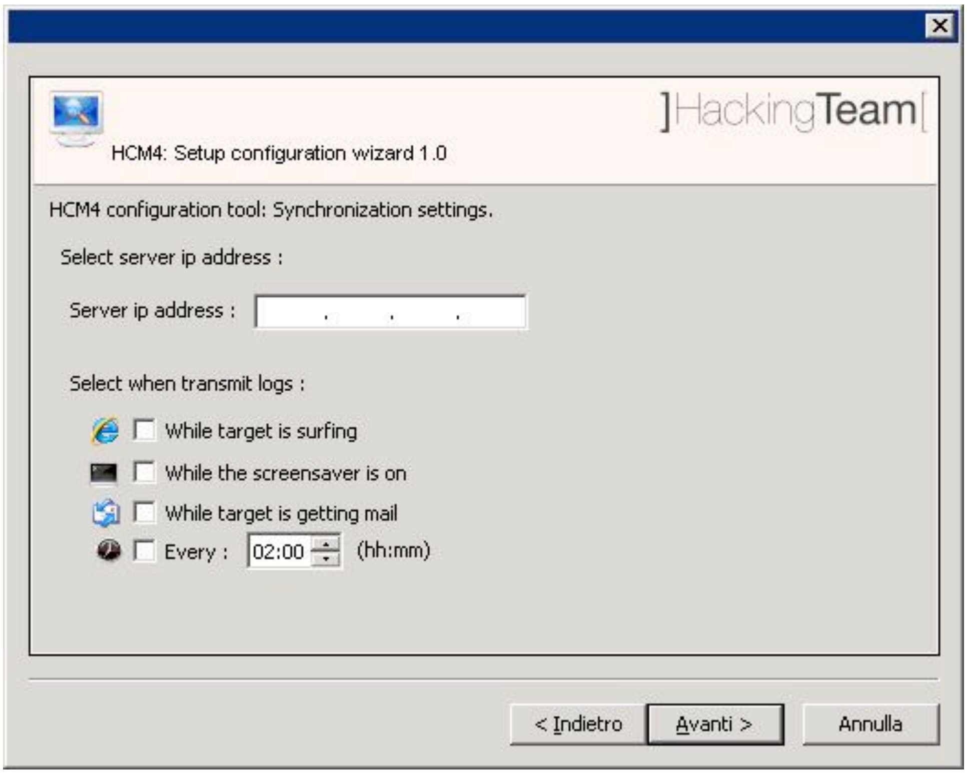
Take a screenshots every :
□ every: 00:05 (hh:mm)

Take a webcam shot every :
□ every: 00:05 (hh:mm)

Configuration Wizard [step 1]

In this window it is also possible to choose which type of document to monitor, and how often - if ever - to take "snapshots" of the screen using the webcam.

In the second window it is possible to set-up the parameters for the synchronization with the RCS server.



HCM4: Setup configuration wizard 1.0

HCM4 configuration tool: Synchronization settings.

Select server ip address :

Server ip address : . . .

Select when transmit logs :

□ While target is surfing

□ While the screensaver is on

□ While target is getting mail

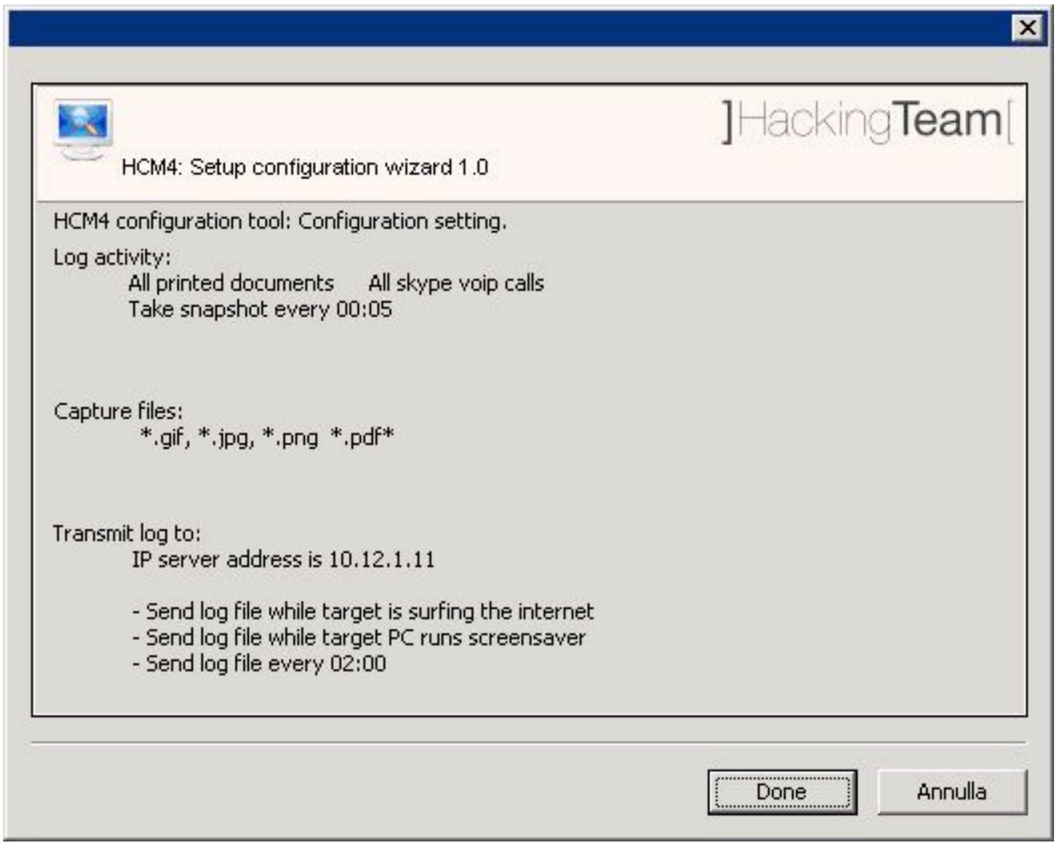
□ Every : 02:00 (hh:mm)

Configuration Wizard [step 2]

In this window it is possible to choose when to execute the synchronization with the RCS server and when. It is possible to select more than one event to trigger the synchronization:

- While the target PC is surfing the Web;
- While the target PC is sending or receiving emails;
- While the screensaver on the target PC is active;
- Every *x* hours/minutes.

In the last window it's possible to review the details of the configuration:



HCM4: Setup configuration wizard 1.0

HCM4 configuration tool: Configuration setting.

Log activity:
All printed documents   All skype voip calls
Take snapshot every 00:05

Capture files:
*.gif, *.jpg, *.png *.pdf*

Transmit log to:
IP server address is 10.12.1.11

- Send log file while target is surfing the internet
- Send log file while target PC runs screensaver
- Send log file every 02:00

Configuration Wizard [step 3]

If you are satisfied with the resulting configuration, clicking on the "*Done*" button will bring you back to the main window. Here it will be possible to modify, if you so wish, all the parameters you have configured with the Assistant, according to the rules and criteria detailed in the previous paragraphs.

It will then be possible to save the configuration and upload it to the RCS agent.

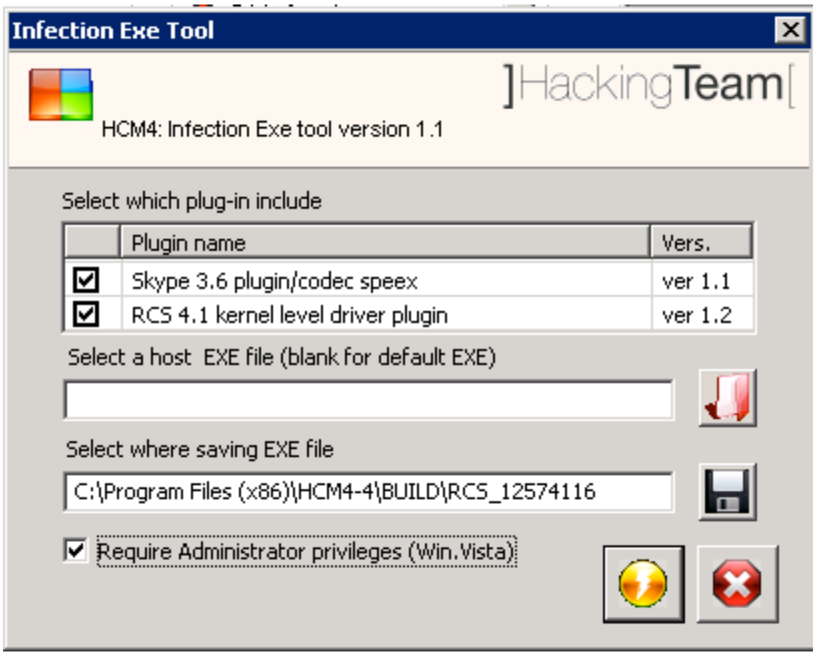
4.3.3 Creation of the infection executable (Melting tool)

Once you have configured the RCS agent, you can create the executable (with .exe extension) that is used to infect the target PC.

The procedure (called 'melting') enables you to create an executable starting from whichever executable file you want. This file should be a Windows executable (in uncompressed, unpacked 'PE format'). The melting tool transforms the original file adding the functionalities of the RCS agent and installs it silently once executed. The resulting file maintains the original functionality of the starting file.

The new executable, once launched on the target PC, silently installs the RCS agent and then executes the original file. This way the user is not aware of what is actually happening.

The components of the RCS agent are encrypted by a polymorphic engine, which introduces anti-reversing and anti-debugging feature to the RCS core.



Infection Exe Tool

]HackingTeam[

HCM4: Infection Exe tool version 1.1

Select which plug-in include

	Plugin name	Vers.
☑	Skype 3.6 plugin/codec speex	ver 1.1
☑	RCS 4.1 kernel level driver plugin	ver 1.2

Select a host EXE file (blank for default EXE)

Select where saving EXE file

C:\Program Files (x86)\HCM4-4\BUILD\RCS_12574116

☑ Require Administrator privileges (Win.Vista)

Melting tool

The right button on the left-hand side of the HCM "Configuration Module" calls up the melting tool.

The procedure requires a starting executable and a target directory where the final executable will be saved (the name of the executable will be identical to the original one).

If the starting executable is not specified, a neutral executable will be used. This executable has no functionalities and its aim is to install the RCS agent silently.

The default destination directory will be the path of the HCM install dir + “BUILD\<Uniq_ID>”. In this case the executable will be called <Uniq_id>.exe (ex: “*RCS_5577758.EXE*”).

Before generating the setup file it’s also possible to choose which plug-in (components that implement additional features to the RCS agent) to embed during the melting.

The console automatically adds the plug-ins based on the agent’s configuration: for example, if the VoIP interception is active by default or if it’s activated during the events / actions configuration process, the plug-in will be added automatically.

NOTE:

Plug-ins can be installed dynamically even after the installation of the RCS agent: simply insert the plug-in (taken from the appropriate sub-folder [see Appendix]) in the queue of upload files. At the first synchronization the plug-in will be transferred to the target PC and will be available at the end-of-sync.

NOTE 2:

The “Require Administrator Privileges” flag is used to modify the host program’s *manifest* in order to request, upon running, the highest user privileges allowed (program’s icon will be visualized with the UAC shield).

This flag has to be checked if the program is going to be run on Windows Vista operating system, and the target user is a member of the Administrators group. In every other case (non-admin user, WindowsXP system, etc.) the flag doesn’t need to be checked (even though it doesn’t compromise program’s functionality).

Anyhow, for some programs, it won’t be possible to modify the *manifest*; In this case, if the flag is checked, HCM will pop up an error message, prompting you to change the host program.

This flag’s state affects the *build* even if it’s used with the injection proxy tool.

4.3.4 Offline Media installation tool

Through the management console it is possible to create the media for the offline installation ("bootable cdrom" or "bootable usb pen drive" for PC, “infected MMC” for mobile phones).

These tools allow the installation of the RCS agent when it is possible to have physical access to the target PC or mobile phone: insert the cd-rom or plug the usb pen drive into target PC turned off, power on the system and boot from one of these devices. The system will start from the media and a simple installation procedure will begin (see chapter 4.54.3.4)

For mobile phones, insert the MMC and turn the device on: the backdoor will be silently installed.

Pressing the appropriate button from the HCM “Configuration Module” launches the media creation process: 💿 for PC or ▭ for mobile phones.

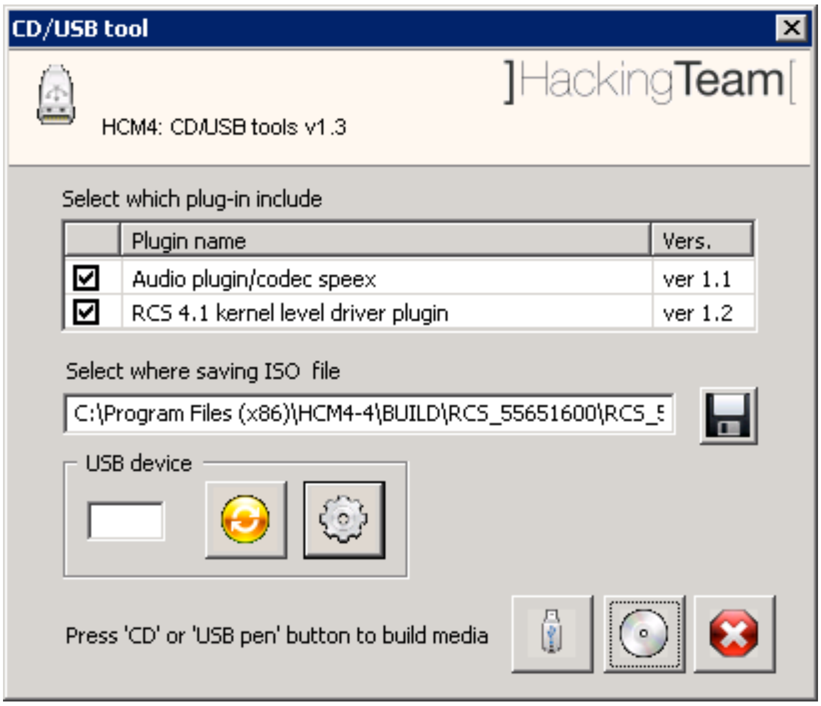
Before being added to the media, the components of the RCS agent are encrypted by a polymorphic engine that introduces anti-reversing and anti-debugging feature to the RCS core.

It is possible to choose which plug-in (components that implement additional features to the RCS agent) embed in the media.

The tool automatically adds plug-ins according to the agent’s configuration: for example, if the Skype module is active by default or if it is activated during the events / actions configuration process, the plug-in will be added automatically.

For the creation of a cd-rom you need to set the file name "ISO" and its destination, while for the USB memory stick and the MMC (once inserted in the PC) you have to select the letter (eg "D:" , "Z:" etc.) on which the USB device or the MMC are mapped. To generate the media, simply press the corresponding button.

The "bootable CD" creation process, produces an ISO9660 image; you can then burn it using a standard cd burning application.



CD/USB tool

]HackingTeam[

HCM4: CD/USB tools v1.3

Select which plug-in include

	Plugin name	Vers.
☑	Audio plugin/codec speex	ver 1.1
☑	RCS 4.1 kernel level driver plugin	ver 1.2

Select where saving ISO file

C:\Program Files (x86)\HCM4-4\BUILD\RCS_55651600\RCS_5

USB device

Press 'CD' or 'USB pen' button to build media

Media installation tool for PC

NOTE:

Before using the media installation tool with the usb drive, you have to prepare the stick (only once per usb drive):

1. *open the media installation tool then press the* 🔄 *button to refresh the drive mappings;*
2. *select the correct removable drive and press* ⚙*, following the on-video instructions.*

To create a Usb media, plug a "prepared" USB stick in your computer and open the media installation tool (you can use the 🔄 button to rescan drives), then select the letter where the drive is mapped and press the button.

Plug-ins can be installed dynamically even after the installation of the RCS agent: simply insert the plug-in (taken from the appropriate sub-folder [see Appendix]) in the queue of upload files. At the first synchronization it will be transferred to the target PC and will be available at the end of the sync.

4.4 Mobile Server Admin

RSSM service handles connections coming from Mobile RCS Agents, and is installed as a part of ASP package on the Collection Nodes. RSSM can also be installed as a standalone service to deploy Mobile Collection Nodes in order to retrieve logs from Mobile RCS Agents using point-to-point proximity connections (BlueTooth, WiFi).

When running RSSM as a standalone Mobile Collection Node, the Mobile Server Admin GUI must be used in order to configure the service and interact with it.

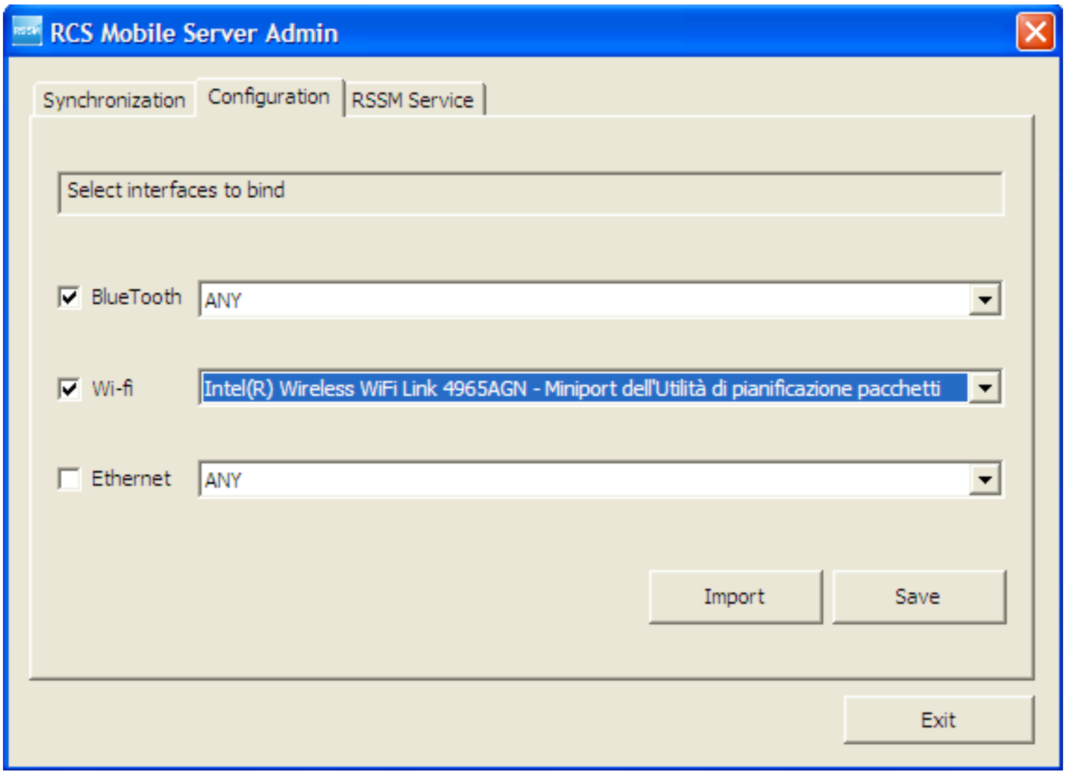
After launching the MobileGUI (in the \RCSASP path) executable, the RSSM Admin GUI will be accessible from the system tray bar by this icon RSSM

4.4.1 Service configuration

Before using the RSSM as a Mobile Collection Node, the service has to be configured. The basic configuration file must be imported from an ASP server running the RSSM component (be sure to install it on the Collection Node if you plan to handle data coming from mobile targets).

To export the configuration file, run the MobileGUI on the ASP server, switch to the *Configuration* tab and click “Export”. Copy the exported file on the Mobile Collection Node and run the MobileGUI. Switch to the *Configuration* panel, click “Import” and select the exported configuration file.

Now the configuration should be modified to activate the proper media.



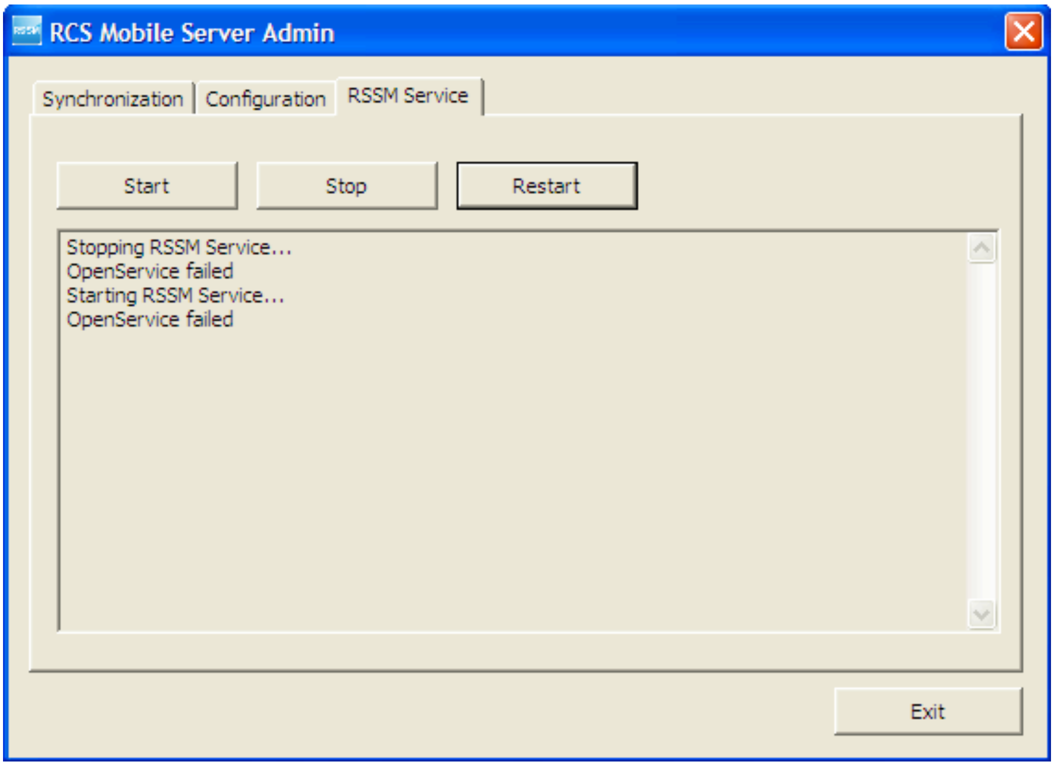
Select interfaces to bind

☑ BlueTooth ANY

☑ Wi-fi Intel(R) Wireless WiFi Link 4965AGN - Miniport dell'Utilità di pianificazione pacchetti

□ Ethernet ANY

After saving the modified configuration, the service has to be restarted (switch to the *RSSM Service* tab). Under some circumstances the program will ask for a reboot.



```
Stopping RSSM Service...
OpenService failed
Starting RSSM Service...
OpenService failed
```

Now the Mobile Collection Node is ready to receive new connections from Mobile RCS Agents. RSSM log file can be used to monitor service activity (paragraph **Error! Reference source not found.**).

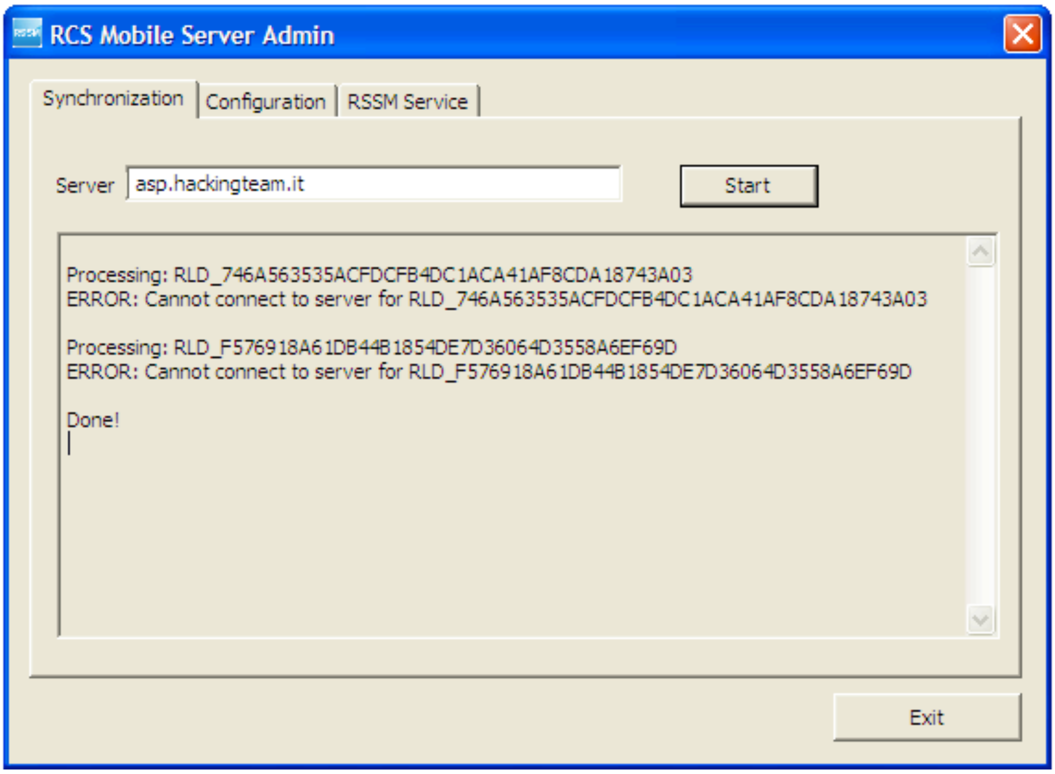
4.4.2 Data synchronization

Mobile Collection Node can synchronize its data with the Log Repository using a standard internet connection.

Synchronization process includes:

- **Logs sending:** All logs collected from Mobile Agents are sent to the Log Repository
- **Configurations retrieving:** New configurations, if available, are downloaded for all the backdoors that synchronized with that Mobile Collection Node at least once. The backdoors will receive the updated configuration files next time they synchronize with the Mobile Collection Node.
- **Uninstalling:** If a backdoor has to be uninstalled (eg: its activity was closed), the Mobile Collection Node will record its status (only for the backdoors that synchronized with that Mobile Collection Node at least once). The backdoor will receive the uninstall command next time it synchronizes with the Mobile Collection Node.

To perform a Synchronization run the MobileGUI and switch to the *Synchronization* tab.



Server asp.hackingteam.it

```
Processing: RLD_746A563535ACFDCFB4DC1ACA41AF8CDA18743A03
ERROR: Cannot connect to server for RLD_746A563535ACFDCFB4DC1ACA41AF8CDA18743A03

Processing: RLD_F576918A61DB44B1854DE7D36064D3558A6EF69D
ERROR: Cannot connect to server for RLD_F576918A61DB44B1854DE7D36064D3558A6EF69D

Done!
```

NOTE: The *Server* field must point to an ASP server running the RSSM service.

4.5 Off-line installer

The offline installation tool (it can be either a Cd-Rom or a USB-Dongle[2]) allows the installation of RCS tools on a computer when physical access is possible. The installation takes place booting the computer from the infection media, so that loading the operative system of the target computer is not necessary. The same media can also be used to uninstall the RCS tool from the computers that were previously infected.

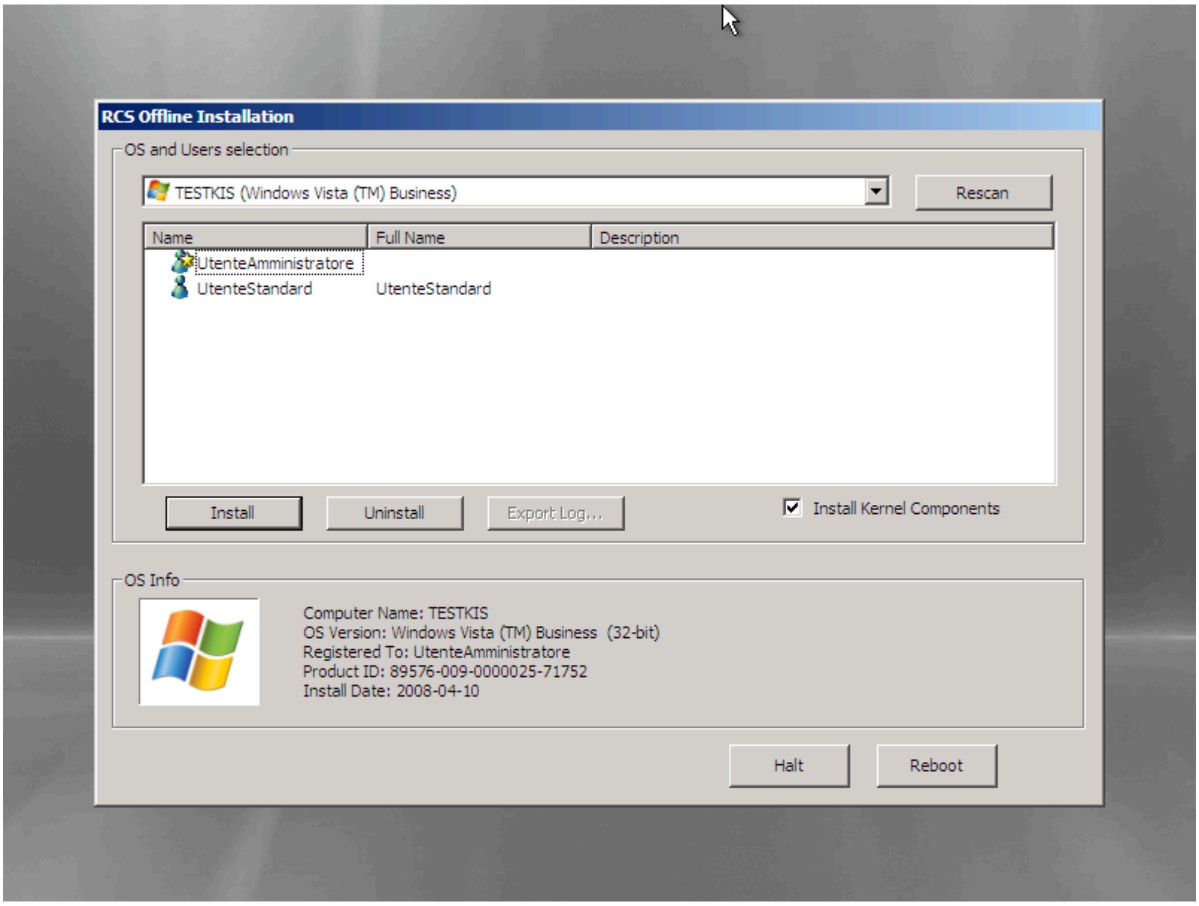
Note Each infection media is associated, in a unique way, to a single backdoor generated by the *configuration module*. A specific infection media will only be capable of uninstalling the backdoor it's been associated to (one of its instances), even though the backdoor was installed on-line (*.exe melting, injection proxy)*, or offline by means of the same infection media.

The installation and the removal of a RCS Backdoor are executed in three simple steps, described below.

[2] For the sake of brevity only the CD-Rom will be referred to in the documentation, although the very same considerations apply to a USB dongle too.

4.5.1 RCS Installation

After booting the target pc from the infection media, a window like the one in the image below will automatically appear on-screen:



RCS Offline Installation

OS and Users selection

TESTKIS (Windows Vista (TM) Business)

Name	Full Name	Description
UtenteAmministratore		
UtenteStandard	UtenteStandard	

☑ Install Kernel Components

OS Info

Computer Name: TESTKIS
OS Version: Windows Vista (TM) Business (32-bit)
Registered To: UtenteAmministratore
Product ID: 89576-009-0000025-71752
Install Date: 2008-04-10

Offline installation tool

We can see, in the top section of the window, a *dropdown list* containing all the operating systems installed on the target computer that were recognized by RCS; in the lower section of the window, we can see a list of all information gathered from the selected operating system (OS Info). The icon on the lower left corner is shown in colors if the selected operating system is supported by RCS, otherwise the icon will be shown in black and white, and it won't be possible to install RCS on that OS.

Select from the dropdown list the OS to infect with a RCS backdoor.

Note If the target device is a removable media, and it's not shown in the dropdown list, it may be necessary to click the *Rescan* button to force a new scan of all the attached devices.

A list of all users for the selected OS can be seen in the middle section of the window. For each user it will be possible to see the system name, the real name and a description, when available. Below there's a list of the icons that identify each user:

- Standard User
- Administrator
- Domain User

If the icon is shown in colors the user is active, otherwise it means that the user has been disabled from the system administrator.

Besides the icons described above, there may be another icon used to represent the status of RCS for that particular user:

- ✓ Correct RCS installation for this user;
- ✗ Corrupted (or not working) installation of RCS for this user;

Select one or more users to infect with RCS, then click the *Install* button. A message will appear, warning about the finalization of the installation process.

From now on it will be possible to power off or restart the target computer clicking the *Halt* or the *Reboot* button.

4.5.2 RCS Uninstall

The uninstall procedure is specular to the one described above. After selecting one or more users infected by RCS, click on the *Uninstall* button. A message will appear on-screen, warning about the finalization of the uninstall process. From now on it will be possible to power off or restart the target computer clicking the *Halt* or the *Reboot* button.

4.5.3 Log Export

In the case of a target PC with no available internet connection, it is possible to export the logs via the offline installation tool. After selecting the user (or users) whose logs have to be exported, the operator will just have to press the Export Log button. An interface window will appear on-screen and it will be possible to select where to save the logs (it is advisable to use a removable media or the USB Key itself).

To Importing the logs into the DB, just copy the folder created during the export process (the name of the folder will be of the kind RLD_XXXXXX) in the \RCSASP\LOGREPO folder located in all Collection Nodes (ASP).

4.6 Injection Proxy

The on-line installation tool (Injection Proxy) allows you to install the RCS software on a system without needing physical access to the computer itself. In order for the installation to be successful it is necessary to be able to actively monitor the internet connection used by the target. The Injection software will thus be able to trace the HTTP connections established by the client, intercept incoming downloads, and inject all executables on-the-fly. When the user launched the downloaded file, the RCS software will be able to silently install itself on the computer.

In the following paragraphs, we will go through all the necessary steps to install, configure and activate the Injection Proxy.

4.6.1 Installing the environment

The softwer is provided in the form of a tar/gzip archive, ready to be installed on computers using Linux operating system. The installation process is composed of the following steps (admin privileges required):

- **Uncompress the archive:** `tar –zxvf jproxy-bin.tar.gz`
- **Install the files:** `make –C jproxy-bin install`
- **Import the backdoors:** (vedere paragrafi successivi)
- **Select the targets:** (vedere paragrafi successivi)
- **Launch the program:** `/usr/local/bin/inject_proxy`[3]
- **Divert the traffic:** (see following paragraphs)

The logs of the infection activities are stored in the files:

- `/var/log/jproxy_infect.log`
- `/tmp/infect_box`

[3] Please, refer to the program's manual and online help for further information on the configuration and execution parameters.

4.6.2 Importing a backdoor

The Injection Proxy system will infect with the RCS software the executables downloaded by the target. Once installed on the target system, RCS will begin to gather logs and to execute actions as specified during the configuration process.
The RCS configurations are created with the *RCS Control Station* (see relevant paragraph); it will be necessary to "import" the configurations created with this tool into the Injection Proxy.

In order to execute the *Import* you must:

- Open the folder where the *RCS Control Station* is installed (es: C:\Program Files\HCM4-4\)
- Open the sub-folder BUILD.
- Copy the folder with the desired backdoor's name into the file system of the linux machine where the Injection Proxy is located. The destination path can be chosen by the user.
- Associate the newly created folder, and the relative backdoor, to the desired target (see following paragraph).

4.6.3 Selecting the targets

The Injection Proxy system is able to import an arbitrary number of backdoors (and relative configurations) from the *RCS Control Station.* It is necessary to provide the Injection System with the necessary information for it to choose which backdoor will be use to infect the files downloaded by a specific target client (you will have to provide the source IP address of the connections).

In order to make the association, you will have to edit the *[Inject]* section of the configuration file */etc/jproxy.conf.* (see paragraph **Error! Reference source not found.**).

Each line in this section identifies a target through a *range* of IP addresses; the character '*' is used as a wildcard (e.g., 192.168.0.* identifies the range of addresses between 192.168.0.0 and 192.168.0.255).

Each line contains also the information that will be used by the Injection Proxy to execute the infection on a specific target:

- **Backdoor Path:** identifies the directory where the desired backdoor is located. A '*' in this field assigns to the target the folder identified by the *default_backdoor* variable.

- **Extension:** identifies the extention (including the '.') of file types that must eb infected. A '*' in this field identifies the files indicated by the *default_extension* variable.
- **Max file size:** sets the maximum size (in bytes) that a file must have in order to be infected.
- **Max infection:** sets the maximum number of files that will be infected for a specific target.

4.6.4 Diverting the Internet Traffic

In order for the Injection Proxy to infect the downloaded files, it is necessary to divert the target's HTTP traffic through the proxy itself. It is possible to redirect the traffic in several ways:

- **Layer3:** the traffic is redirected coming out of the target's LAN, via appropriate modifications to the routing tables of the network system of the target's internet provider.
- **Layer2:** the traffic is redirected before coming out of the LAN, via appropriate hacking techniques or modifications to the configurations of the Layer2 systems (switch).
- **Layer1:** the traffic is physically redirected through the proxy machine, bridging it to the target's uplink cable.

Choosing how to redirect the traffic depends heavily on the context of use. For further information (routs set-up, bridging, etc.), please refer to the jproxy software manual.

5 Troubleshooting

5.1 Log Format

If a component of the system fails, it is possible to inspect the respective logs to point out the cause of the problem.

The critical components generating the logs are ASP and the DB.

5.1.1 ASP

ASP is divided into separate Windows services: RSS, RLD and RSSM

RSS is responsible for managing the connections to the backdoors, while the RLD takes care of deciphering the logs and inserting the data in the DB. RSSM handles connections coming from mobile agents, and can also be used as a standalone mobile collection node.

If no logs are received from any of the backdoors, it is necessary to make sure that these services are functioning correctly. It is possible to check their execution from the list of Windows' services.

If the services are in execution, it is necessary to inspect the logs to point out what's causing the problem.

Each one of these services creates a log called ASPService_RSS.log (for RSS), ASPService_RLD.log (for RLD) and AspService_RSSM.log (for RSSM) in the directory \\RCSASP

The format of the log files is the following:

date hour service [thread_id] : message

Example:

```
2008-10-23 07:29:35 RSS [02136]: StartAspHttps - INIT phase completed
```

If an error occurs, the message will explicitly contain the word 'ERROR" followed by a short description of the error. If the error can be easily identified, solve the problem and reboot the service. If the issue still occurs, please contact tech support.

These files can also be used to monitor the normal activity of the services, because every key function writes inside the file what's happening at any given time.

5.1.2 DB

The database is composed of 3 main elements: MySQL, Apache and PHP.

If the database is not reachable, it is necessary to check that mysql and apache are functioning correctly. These are both Windows services and can be re-booted with the standard procedure.

MYSQL records its activities inside the system's logs.

Apache saves the logs in the file *\\RCSDB\apache\logs\error.log.* All the activities of the PHP layer are recorded here. All XML-RPC methods invoked are recorded in this file. N.B.: this file can reach considerable size with prolonged use of the product. It is advisable to monitor the space on the disk occupied by the database server.

5.2 Activity Trace

Every time an user performs a sensitive operation, such as creation of backdoors or targets, an audit log is generated. Those logs can be browsed by RCS Administrators (with ADMIN privilege) using the RCS Console (see RCS Console documentation).

6 Internals

6.1 ASP Decoy Page

“**DDPH.html**” file (stored in “C:\RCSASP” folder) is a static HTML page that is sent when a client connected to the ASP service is not a RCS agent recognized as "genuine" (eg: a web browser). This feature allows the administrator to hide the ASP service behind a “fake” web server.

You can modify this file to implement a custom web site’s home page.

7 Disaster Recovery

If a critical error occurs, it is possible to restore the correct functionality of the system following these procedures:

7.1 Backup

All the information are stored inside the database. It is necessary to plan some backup procedure for the data. In the case of critical error, it will be possible to restore the whole architecture starting from the data stored in the DB.

In order to backup all data in the DB correctly, execute the command:

```
mysqldump -v --hex-blob --triggers --add-drop-database
--single-transaction -c -f –u root –p rcs > backupfile.dump
```

All the data stored inside the DB will be saved in the specified file. The command will ask the root password used during the installation of the RCSDB package. It is also necessary to backup DB’s license file and configuration file. Both files are stored in the directory: \RCSDB\apache\htdocs\etc (RCSDB.lic and RCSDB.ini).

N.B.: It is always advisable to backup the whole computer where the database is installed: in case of malfunctioning, recovery time will be shorter than manually reinstalling all packages.

7.2 Recovery

In case of malfunctioning, it will be necessary to completely restore the failing component.

7.2.1 ASP

To restore the ASP server, simply reinstall the RCSASP package and provide the IP of the server and the access credentials. No data is stored on the ASP server; all you need is in the DB. This makes for a very fast and simple restore procedure.

7.2.2 DB

If a full backup of the DB computer is available, it is advisable to restore the backup. Otherwise, in order to restore the DB server, it will be necessary to reinstall the RCSDB package and restore the data.
Once the RCSDB package has been reinstalled, it is possible to import all data from the backup created previously. The restore command is:

```
mysql –u root –p < backupfile.dump
```

We have now restored the DB to the exact moment of the backup. In order for the server to work correctly, besides the data of the DB, it will be necessary to restore also the DB's license and configuration files. The RCSDB.lic and RCSDB.ini files must be restored in the directory \RCSDB\apache\htdocs\etc.
Once all data have been restored, it is possible to re-boot the services (mysql and apache) being careful to plug the USB-dongle in the server's usb port.

7.3 Dongle malfunction

In the case of a USB-dongle malfunction, it will be necessary to replace the defective dongle with a new one and replace the license file. The license is univocally linked to the serial number of the dongle itself. Just replace the license file (RCSDB.lic) in \RCSDB\apache\htdocs\etc; replace the broken dongle with the new dongle linked to the new license and re-boot the DB services (apache e mysql).

7.4 Disgrunted employee

If you need to modify the password of an ‘admin’ account, you can operate directly on the DB. Even if the passwords to the other admin accounts have been modified by a malicious account, it will be possible to workaround the problem by operating directly on the database tables. To access the database tables, you can use the *phpmyadmin* application at *http://<server_ip_address>/phpmyadmin* or execute the command *mysql –u root –p* from the console.

All passwords in the database are stored in the ‘user’ table. Each user is linked to the ‘pass’ field that contains the MD5 hash of the password. For this reason, it will be necessary to modify the MD5 hash of a known password.

If the ‘root’ user of the DB is compromised, it is possible to boot the MySQL server in ‘grantless’ mode and restore the ‘root’ user. In order to do this, you will have to follow this procedure:

- Stop the service:

  ```
  net stop MySQL5.0
  ```

- Boot the service (mysqld) using the command:

  ```
  C:\RCSDB\mysql\bin\mysqld-nt --skip-grant-table
  ```

- Connect to the database and modify the root user:

  ```
  mysql -u root -e "UPDATE `user` SET `Password` =
  PASSWORD('newpassword') WHERE `Host` = 'localhost' AND `User` =
  'root'" mysql
  ```

- Shut down the service:

  ```
  mysqladmin shutdown
  ```

- Re-boot the service:

  ```
  net start MySQL5.0
  ```