Tactical Network Injector installation

Introduction

Tactical Network Injector is supplied with pre-installed and set Tactical Device operating system and Tactical Control Center control software. It must be synchronized with RCS server.

IMPORTANT: installation requires the Master Node authentication files and synchronization requires the creation of Network Injector on RCS Console. Be well prepared for installations far from the operating center.

Package content

The package includes a notebook and installation CD.

Installation sequence

The full installation sequence is provided below:

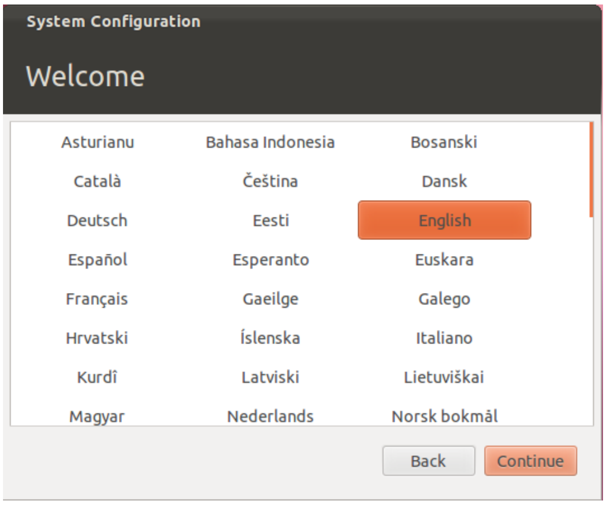
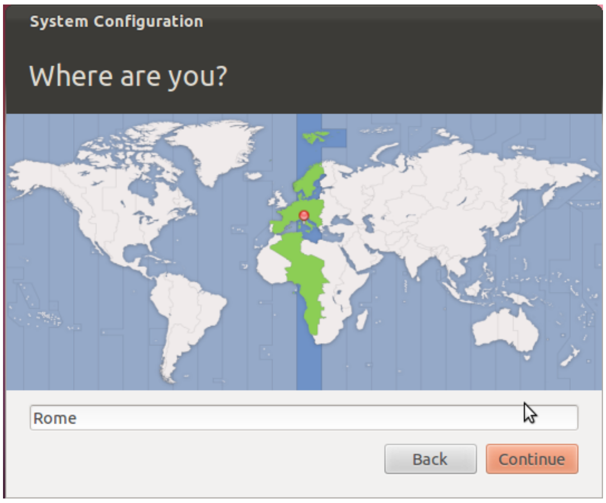
Step	*Action*	*Paragraph*
1	Installing the Tactical Device operating system NOTE: the operating system is already installed at purchase.	*"Operating system installation and settings" below*
2	Synchronizing Network Injector with RCS server	*"First Network Injector synchronization with RCS server" on page 51*
3	Checking Network Injector status	*"Checking Network Injector status" on page 52*

Operating system installation and settings

Tactical Network Injector is supplied installed and ready for use, complete with all the foreseen applications. It can also be installed using a restore disk.

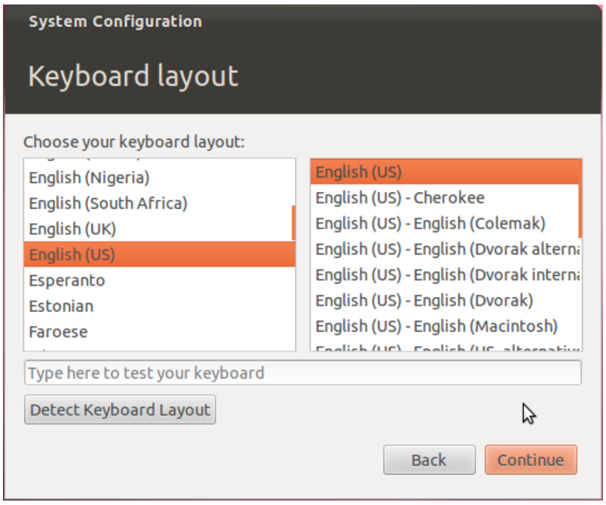
The procedure is described below:

Steps	*Result*
1. Connect the computer to the network using an Ethernet cable and insert the installation CD.	-

Steps	***Result***
2. Select Tactical Device for notebook version installation: operating system installation is launched and the computer shuts down when finished. **IMPORTANT: the computer must remain connected to the internet during the entire installation process.**	-
3. Reboot the notebook; enter the *passphrase* to unlock the encrypted disk. The passphrase for first boot is "firstboot".	-
4. The first setup window appears. 5. Select the language.	 System Configuration Welcome English Asturianu Bahasa Indonesia Bosanski Català Čeština Dansk Deutsch Eesti Español Esperanto Euskara Français Gaeilge Galego Hrvatski Íslenska Italiano Kurdî Latviski Lietuviškai Magyar Nederlands Norsk bokmål Back Continue
6. Select the correct time zone.	 System Configuration Where are you? Rome

Steps ***Result***

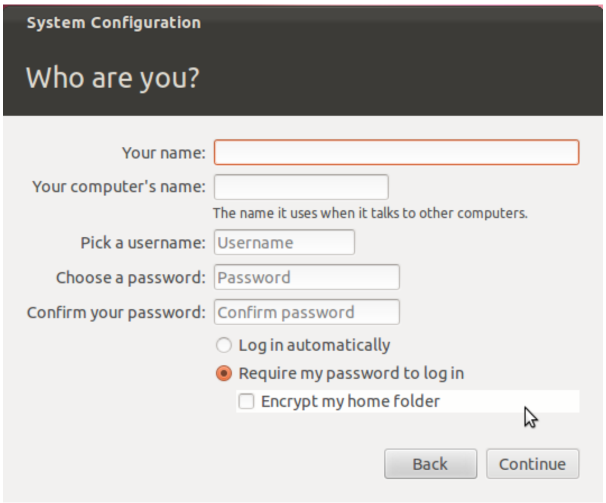
7. The keyboard layout is read. Only change it if necessary.


System Configuration
Keyboard layout
Choose your keyboard layout:
English (Nigeria)
English (South Africa)
English (UK)
English (US)
Esperanto
Estonian
Faroese
English (US)
English (US) - Cherokee
English (US) - English (Colemak)
English (US) - English (Dvorak alterna
English (US) - English (Dvorak interna
English (US) - English (Dvorak)
English (US) - English (Macintosh)
Type here to test your keyboard
Detect Keyboard Layout
Back
Continue

8. Enter user data: operating system setup starts.

WARNING: if you lose your password you must re-install Tactical Network Injector.

IMPORTANT: the entered password becomes the disk encryption passphrase requested each time the notebook is turned on. The password is also requested at user login.


System Configuration
Who are you?
Your name:
Your computer's name:
The name it uses when it talks to other computers.
Pick a username: Username
Choose a password: Password
Confirm your password: Confirm password
○ Log in automatically
● Require my password to log in
□ Encrypt my home folder
Back
Continue

9. The standard login page appears at the end of operating system installation. The Tactical Control Center operating system and control software are installed on the computer.

-

Verifying the IP address

To verify Network Injector IP addresses, open RCS Console, **Monitor** section: the IP address is indicated in the **Address** column for the concerned Network Injector.

Changing the IP address

If the Network Injector IP address changes, a new element is displayed in the RCS Console **Monitor** section. Two elements will thus be included for that Network Injector: one with the new address in green status (running component) and one with the old address in red status. Eliminate the element with the old address.

Uninstall

To uninstall Tactical Control Center, simply remove it from the computer. To uninstall a Tactical Network Injector, simply delete the object in RCS Console and turn off the device.

*See "**Managing the Network Injector**" on page 102*

Other applications installed on Network Injectors

Introduction

Network Injectors come with some helpful third party applications installed.

Applications

Following are the applications installed on Tactical Network Injector and Network Injector Appliance:

ℹ NOTE: for application instructions, refer to the documents issued by the application manufacturers.

Application name	*Description*
Disniff	Tool packet to tap unsafe network traffic
hping3	Network traffic generator
Kismet	Monitoring tool for Wireless 802.11b networks
Macchanger	Network interface MAC address changer tool
Nbtscan	Network scanner for information on NetBIOS names
Netdiscover	Active/passive network address scanner using ARP requests
Ngrep	Network traffic grep
Nmap	Network Mapper
P0f	Passive OS fingerprinting tool
Sslsniff	Man-in-the-middle attack tool for SSL/TLS network traffic
Sslstrip	Man-in-the-middle attack and hijacking tool for SSL/TLS network traffic

Application name	*Description*
Tcpdump	Network traffic analyzer from command prompt
Wireshark	Network traffic analyzer
Xprobe	Remote OS identifier tool

Tactical Control Center and Appliance Control Center commands

Introduction

Some terminal commands are available to manage Tactical Control Center and Appliance Control Center applications.

NOTE: Administrator privileges are required to run commands.

Commands

Commands available for Tactical Control Center and Appliance Control Center are described below:

Tactical Control Center command	*Appliance Control Center command*	*Function*
`tactical`	`appliance`	Starts the application.
`tactical -d` or `tactical --desync`	`appliance -d` or `appliance --desync`	Disconnects the system from the currently synchronized RCS server.
`tactical -l` or `tactical --log`	`appliance -l` or `appliance --log`	Displays current infection process logs. NOTE: the application window must be open.
`tactical -s` or `tactical --show-logs`	`appliance -s` or `appliance --show-logs`	Displays all log files saved in file system.
`tactical - r` or `tactical --report`	`appliance - r` or `appliance --report`	Creates a system report and saves it in the user's Home folder.

Tactical Control Center command	*Appliance Control Center command*	*Function*
`tactical - v` or `Tactical --version`	`appliance - v` or `appliance --version`	Displays the application version.
`tactical -h` or `tactical --help`	`appliance -h` or `appliance --help`	Displays available commands.

First Network Injector synchronization with RCS server

Introduction

The first Network Injector synchronization is necessary to allow communications between Network Injector and the RCS server and to create and send sniffing and infection rules. Once installed and synchronized, Network Injector queries the server every 30 seconds.

Synchronizing a Network Injector with RCS server

The authentication key must be installed and Network Injector synchronized with the RCS server to complete Network Injector installation.

NOTE: authentication key installation is only necessary for the first synchronization.

Following is the procedure for both Network Injector Appliance and Tactical Network Injector:

Step	*Action*
1	From **RCS Console,** in the **System** section, **Network Injector**, click **New Injector**.
2	Enter the required data and click **Save.** *See "Network Injector data" on page 104* **Result**: the Network Injector appears in the list and the new object to be monitored is added to the Monitor section.
3	Select the newly created Network Injector and click **Export Key** **Result**: a .zip file with the authentication key is generated.
4	Save the generated .zip file.
5	From the Appliance Control Center or Tactical Control Center **System Management** tab, **Server Management** section, enter the Anonymizer IP address and communications port. NOTE: the default communications port is 80.

Step	*Action*
6	Click **Import key** and select the previously saved .zip file generated by RCS Console.
7	Click **Configure**. **Result**: Network Injector starts communicating with the Anonymizer.
8	Check Network Injector status in the RCS Console **Monitor** section. *See "Checking Network Injector status" below*

Checking Network Injector status

Introduction

Network Injector synchronizes with the RCS server to download updated control software versions, identification and injection rules and - at the same time - send their logs.

Network Injector status can be monitored from RCS Console.

Specifically:

- in the **Monitor** section: to identify when Network Injector is synchronized and thus request data exchanges.
- in the **System** section, **Network Injector**: to view the logs sent by Network Injector.

Identifying when Network Injector is synchronized

The procedure is described below:

Step	*Action*
1	In the **Monitor** section, select the Network Injector object row to be analyzed. Check the **Status** column: if flagged green, the Network Injector is synchronized. This situation occurs when on Control Center software (Appliance or Tactical): • **Config** was clicked, the operator manually queued for new rules or updates; • **Start** was clicked or an infection is in progress. **IMPORTANT: applied rules and updates can only be received from RCS when Network Injector is synchronized.**

Viewing Network Injector logs

The procedure is described below:

Step	*Action*
1	In the **System** section, **Network Injectors**, select the Network Injector to be analyzed, double-click or click **Edit.** **Result** : a window opens with Network Injector data and saved logs. *See "Network Injector data" on page 104* NOTE: logs are only received and displayed if Network Injector is synchronized.

Additional component installation

Introduction

Shard databases (for large data volumes) and additional Collectors (one per each Anonymizer chain) can be added.

Service call: distributed architecture design must be checked with HackingTeam support service.

Additional component installation requirements

Before installing additional components, complete Master Node and Collector installation.
See "RCS server installation" on page 17.

Installation sequence

The complete additional component installation sequence is described below:

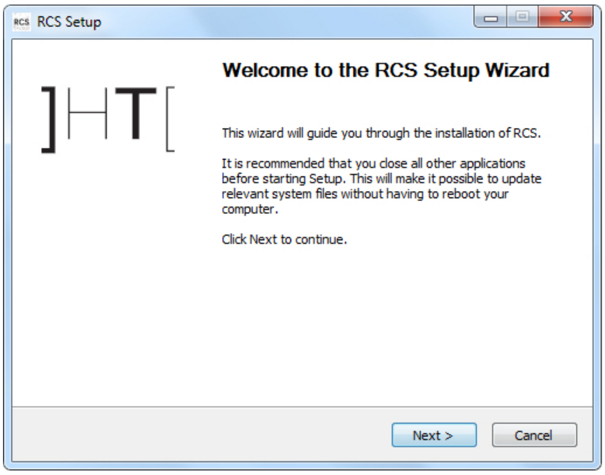
Step	*Action*	*Machine*
1	Prepare that indicated in *installation requirements.*	-
2	Install additional Shard databases.	*server in back end environment*
3	Check installation logs.	
4	Install additional Collectors.	*server in front end environment*
5	Check installation logs.	
6	Check for the installed objects in the **System**, **Backend** and **Frontend** sections.	*RCS Console*

Additional Shard database installation

To install an additional Shard database in back end environment:

Steps ***Result***

1. Insert the CD with the installation package. Run file RCS-version.exe in folder x:\setup: the first wizard window appears.
2. Click **Next**.


RCS Setup

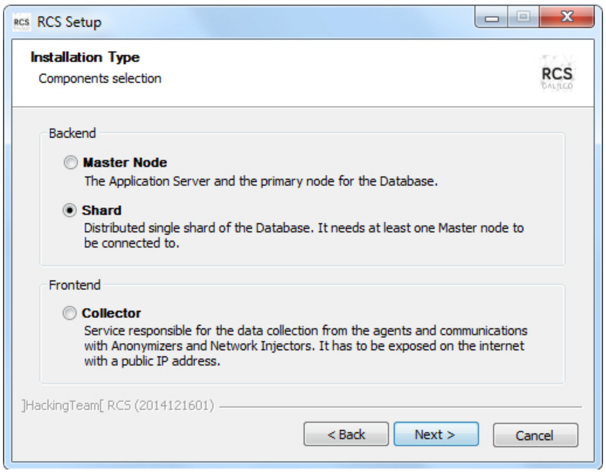
Welcome to the RCS Setup Wizard

This wizard will guide you through the installation of RCS.

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.

3. Select **Shard.**
4. Click **Next**.


RCS Setup

Installation Type
Components selection

Backend

○ **Master Node**
The Application Server and the primary node for the Database.

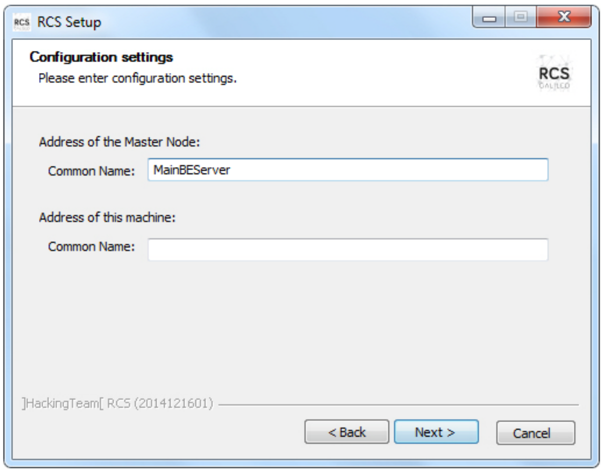
● **Shard**
Distributed single shard of the Database. It needs at least one Master node to be connected to.

Frontend

○ **Collector**
Service responsible for the data collection from the agents and communications with Anonymizers and Network Injectors. It has to be exposed on the internet with a public IP address.

]HackingTeam[RCS (2014121601)

5. Enter the name of IP address of the Master Node server (i.e.: MainBEServer) and machine where Shard is being installed.
6. Click **Next**: when installation has completed, services start and attempt to communicate with Master Node. The server in back end environment is protected and any remote login is redirected

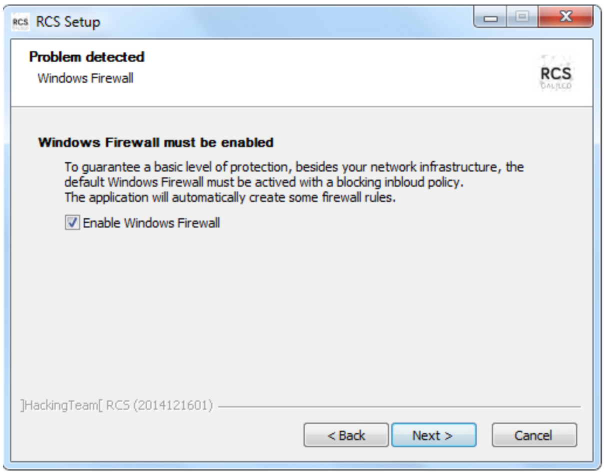
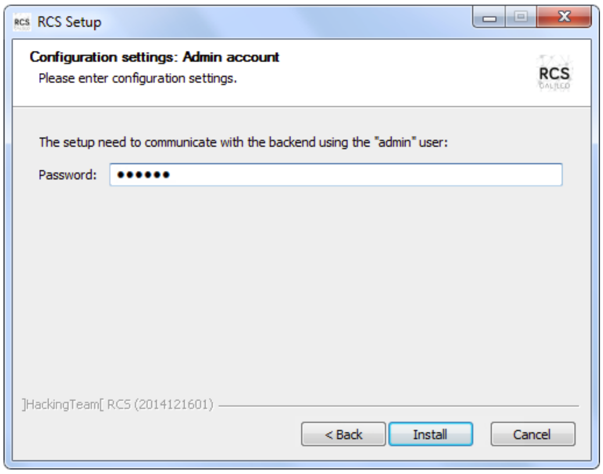

RCS Setup

Configuration settings
Please enter configuration settings.

Address of the Master Node:
Common Name: MainBEServer

Address of this machine:
Common Name:

]HackingTeam[RCS (2014121601)

Steps	*Result*
7. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.	 RCS Setup **Problem detected** Windows Firewall **Windows Firewall must be enabled** To guarantee a basic level of protection, besides your network infrastructure, the default Windows Firewall must be actived with a blocking inbloud policy. The application will automatically create some firewall rules. ☑ Enable Windows Firewall]HackingTeam[RCS (2014121601) < Back Next > Cancel
8. Enter the System administrator's password. 9. Click **Install**: when installation has completed, services are started and are ready to receive data and communicate with the RCS Console.	 RCS Setup **Configuration settings: Admin account** Please enter configuration settings. The setup need to communicate with the backend using the "admin" user: Password: ●●●●●●]HackingTeam[RCS (2014121601) < Back Install Cancel

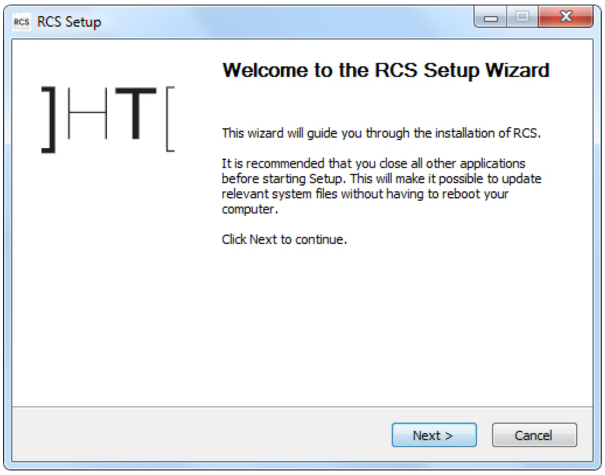
NOTE: if the server name or IP address needs to be changed after installation due to faults, *see "**Editing Master Node settings**" on page 69*.

Additional Collector installation

To install several Collectors in front end environment:

Steps | ***Result***

1. Insert the CD with the installation package. Run file RCS-version.exe in folder x:\setup: the first wizard window appears.
2. Click **Next**.



Welcome to the RCS Setup Wizard

This wizard will guide you through the installation of RCS.

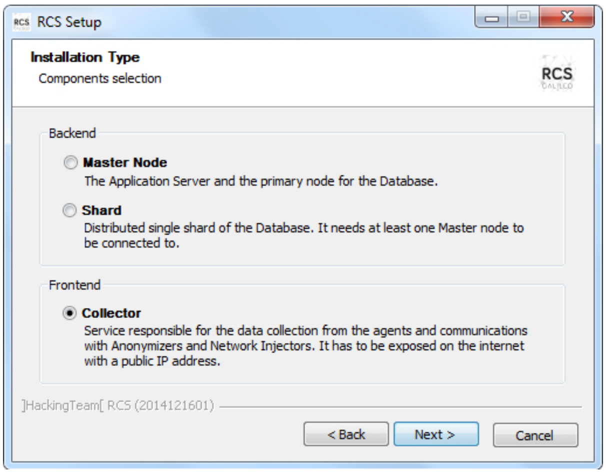
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

3. Select **Collector.**

NOTE: all Collector services are automatically installed.

4. Click **Next**.



Installation Type

Components selection

Backend

○ **Master Node**
The Application Server and the primary node for the Database.

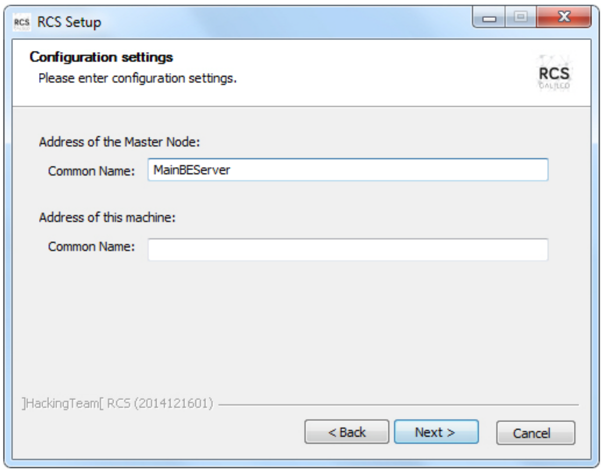
○ **Shard**
Distributed single shard of the Database. It needs at least one Master node to be connected to.

Frontend

● **Collector**
Service responsible for the data collection from the agents and communications with Anonymizers and Network Injectors. It has to be exposed on the internet with a public IP address.

]HackingTeam[RCS (2014121601)

5. Enter the name or IP address of the Master Node server (i.e.: MainBEServer) and machine where Collector is being installed.
6. Click **Next**: when installation has completed, services start and attempt to communicate with Master Node. The server in back end environment is protected and any remote login is redirected



Configuration settings

Please enter configuration settings.

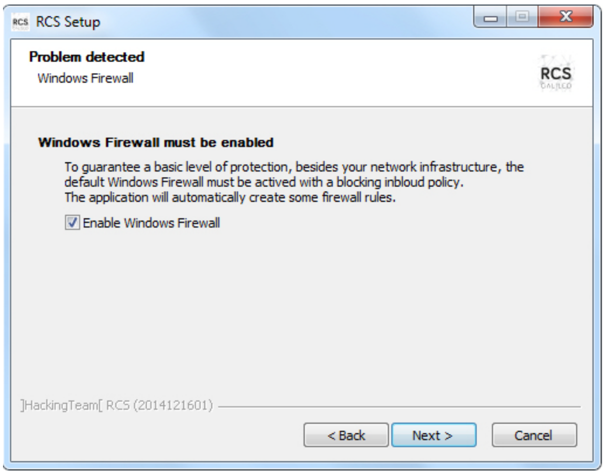
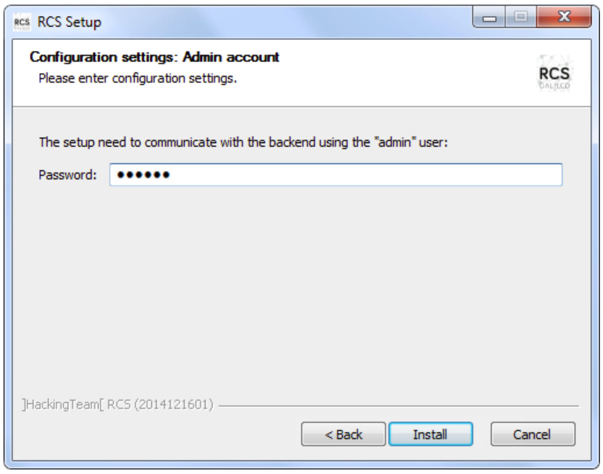
Address of the Master Node:

Common Name: MainBEServer

Address of this machine:

Common Name:

]HackingTeam[RCS (2014121601)

Steps	***Result***
7. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.	 RCS Setup **Problem detected** Windows Firewall **Windows Firewall must be enabled** To guarantee a basic level of protection, besides your network infrastructure, the default Windows Firewall must be actived with a blocking inbloud policy. The application will automatically create some firewall rules. ☑ Enable Windows Firewall]HackingTeam[RCS (2014121601)
8. Enter the system administrator password indicated in Master Node installation. 9. Click **Install**: installation is launched.	 RCS Setup **Configuration settings: Admin account** Please enter configuration settings. The setup need to communicate with the backend using the "admin" user: Password: ••••••]HackingTeam[RCS (2014121601)

Checking service start

Make sure all RCS services are up and running. If services are not running, manually start them. *See "**List of RCS services**" on page 25.*

IMPORTANT: Collector only accepts connections if the Windows firewall is running.

Checking installation logs

If errors occur during installation, check logs and send them to support service if necessary. *See "**System logs**" on page 74*

Check IP addresses

To check all addresses, start the RCS Console, **System** section, **Frontend:** Collector addresses appear on the screen. *See "**Anonymizer installation and settings**" on page 34*

Uninstall

RCS can be uninstalled from the Windows Control Panel.

CAUTION: data is lost when a Shard database is uninstalled. For correct operations, backup data. See "Backup management" on page 98.

NOTE: data will not be lost when a Collector is uninstalled.