]HackingTeam[

RCS 8.3

The hacking suite for governmental interception

System Administrator's Guide

System Administrator's Guide - ver.1.3 MAR-2013

Information ownership

Albeit text and images being selected with the utmost care, HackingTeam reserves the right to change and/or update the information hereto to correct typos and/or errors without any prior notice or additional liability.

Any reference to names, data and addresses of companies not in the HackingTeam is purely coincidental and, unless otherwise indicated, included as examples to better clarify product use.

NOTE: requests for additional copies of this manual or product technical information should be addressed to:

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

Contents

List of diagrams

Glossary

The terms and their definitions used in this manual are provided below.

A

Accounting
Console section that manages RCS access.

acquisition sequence
Group of complex events, actions and acquisition modules that make up the advanced agent configuration.

Administrator
The person who enables user access to the system, creates work groups and defines operations, targets and the type of data to be collected.

Agent
Software probes installed on devices to monitor. They are designed to collect evidence and communicate it to the Collector.

alert rules
Rules that create alerts when new evidence is stored or agents communicate back for the first time.

Alerting
Console section that manages new evidence alerts.

alerting group
Group of users who receive notifications via mail whenever a system alarm is triggered (for example, when the database exceeds available free space limits). Normally this group is not linked to an operation.

Analyst
Person in charge of analyzing the data collected during operations.

Anonymizer
(optional) Protects the server against external attacks and permits anonymity during investigations. Transfers agent data to Collectors.

Audit

Console section that reports all users' and system actions. Used to monitor abuse of RCS.

B

back end

Environment designed to decrypt and save collected information. In distributed architecture, it includes Master Node and Shard databases.

BRAS

(Broadband Remote Access Server) routes traffic to/from DSLAM to the ISP network and provides authentication to the ISP subscribers.

C

Collector

Receives data sent by agents directly or through the Anonymizer chain.

console

Computer on which the RCS Console is installed. It directly accesses the RCS Server or Master Node.

D

Dashboard

Console section used by the Analyst. Used to have a quick overview of the status of the most important operations, targets and agents.

DSLAM

(Digital Subscriber Line Access Multiplexer) network device, often located in the telephone exchanges of the telecommunications operators. It connects multiple customer digital subscriber line (DSL) interfaces to a high-speed digital communications channel using multiplexing techniques.

E

entity

Set of intelligence information linked to a target.

evidence

Collected data evidence. The format depends on the type of evidence (i.e.: image).

evidence alerts

Alerts, usually in the form of emails, sent to analysts when new evidence matches the set rule.

F

factory

A template for agent configuration and compiling.

front end

Environment designed to communicate with agents to collect information and set their configurations. In distributed architecture, it includes the Collector and Network Controller.

I

injection rules

Settings that define how to identify HTTP traffic, what resource should be injected and what method is to be used for the injection.

M

Monitor

Console section that monitors components and license status.

N

Network Controller

Component that checks Network Injector and Anonymizer status and sends them new configurations and software updates.

Network Injector

Hardware component that monitors the target’s network traffic and injects an agent into selected Web resources. It comes in two versions, Appliance or Tactical: the former is for deployment at the ISP, the latter for use on the field.

Network Injector Appliance

Rackable version of the Network Injector, for installation at ISP. See: Tactical Network Injector.

O

operation

Investigation aimed at one or more targets, whose devices will be recipients for agents.

R

RCS

(Remote Control System) the product documented hereto.

RCS Console

Software designed to interact with the RCS Server.

RCS Server

One or more computers, based on the installation architecture, were essential RCS components are installed: Shard databases, Network Controllers and Collector.

S

SSH

(Secure SHell) a network protocol for secure data communication, remote shell services or command execution.

System

Console section that manages the system.

System administrator

The person who installs the servers and consoles, updates software and restores data in case of faults.

T

Tactical Network Injector

The portable version of Network Injector, for tactical use. See: Network Injector Appliance.

TAP

(Test Access Port) a hardware device installed in a network that passively monitors the transmitted data flow.

target

The physical person under investigation.

Technician

The person assigned by the Administrator to create and manage agents.

V

VPS

(Virtual Private Server) a remote server where the Anonymizer is installed. Commonly available for rent.

1

Guide introduction

Presentation

Manual goals

This manual is a guide for the *System Administrator* to:

- correctly install the RCS system and its components
- set up components using the administration console
- understand and resolve any system problems

Information on how to consult the manual is provided below.

Content

This section includes the following topics:

New guide features

List of release notes and updates to this online help.

Release date	*Code*	*Software version.*	*Description*
15 March 2013	System Administrator's Guide 1.3 MAR-2013	8.3	Changed Tactical Network Injector update methods. *See "Tactical Network Injector update" on page 65 .* Changed Network Injector Appliance update methods. *See "Network Injector Appliance update" on page 63 .* Added description of third party software connection rules. *See "Connector management" on page 98 .* The OCR module can index file type evidence content (all formats). *See "OCR module installation" on page 33 .* Added description of the RCS Translate module available with the purchase of a user license and can be installed with support service assistance.
15 October 2012	System Administrator's Guide 1.2 OCT-2012	8.2	Added utility to restart Windows services, *see "Service restart procedures " on page 77 .* Added BareTail for Windows, log code viewer. *See "System logs" on page 74 .* Added incremental backup management and mandatory metadata backup job. *See "What you should know about backup" on page 97 .* E-mail delivery authentication support for alerts. *See "Editing Master Node settings" on page 69 .* Optional OCR module *See "OCR module installation" on page 33* Added fast database management wizard. *See "Wizards in the homepage" on page 85* Sole Tactical Control Center application on Tactical Network Injector.
30 June 2012	System Administrator's Guide 1.1 JUN-2012	8.1	File Manager to delete file packets in the folder C:\RCS\Collector\public. *See "Front end management" on page 90 .*
16 April 2012	System Administrator's Guide 1.0 APR-2012	8.0	First publication

Supplied documentation

The following manuals are supplied with RCS software:

Manual	*Addressees*	*Code*	*Distribution format*
System Administrator's Guide (this manual)	System administrator	*System Administrator's Guide* *1.3 MAR-2013*	PDF
Administrator's Guide	Administrators	*Administrator's Guide* *1.3 MAR-2013*	PDF
Technician's Guide	Technicians	*Technician's Guide* *1.3 MAR-2013*	PDF
Analyst's Guide	Analysts	*Analyst's Guide* *1.3 MAR-2013*	PDF

Print concepts for notes

Notes foreseen in this document are listed below (Microsoft Manual of Style):

WARNING: indicates a risky situation which, if not avoided, could cause user injury or equipment damages.

CAUTION: indicates a risky situation which, if not avoided, can cause data to be lost.

IMPORTANT: offers the indications required to complete the task. While notes can be neglected and do not influence task completion, important indications should not be neglected.

NOTE: neutral and positive information that emphasize or add information to the main text. They provide information that can only be applied in special cases.

Tip: suggestion for the application of techniques and procedures described in the text according to special needs. It may suggest an alternative method and is not essential to text comprehension.

Service call: the operation may only be completed with the help of technical service.

Print concepts for format

A key to print concepts is provided below:

Example	***Style***	***Description***
*See "**User data**"*	*italic*	this indicates a chapter, section, sub-section, paragraph, table or illustration heading in this manual or other publication of reference.
<ddmmyyyy>	<aaa>	indicates text that must be specified by the user according to a certain syntax. In the example <ddmmyyyy> is a date and could be “14072011”.
Select one of the listed servers **[2]**.	**[x]**	indicates the object specified in the text that appears in the adjacent image.
Click **Add**. Select the **File menu, Save data**.	**bold**	indicates text on the operator interface, a graphic element (i.e.: table, tab) or screen button (i.e.: display).
Press ENTER	UPPER CASE	indicates the name of keyboard keys.
See: Network Injector Appliance.	-	suggests you compare the definition of a word in the glossary or content with another word or content.

Product and guide addressees

Following is the list of professionals that interact with RCS.

Addressee	***Activity***	***Skills***
System administrator	Follows the HackingTeam's instructions provided during the contract phase. Installs and updates RCS servers, Network Injectors and RCS Consoles. Schedules and manages backups. Restores backups if servers are replaced. WARNING: the system administrator must have the required necessary skills. The HackingTeam is not liable for equipment malfunctions or damages due to unprofessional installation.	*Expert network technician*
Administrator	Creates authorized accounts and groups. Creates operations and target. Monitors system and license status.	*Investigation manager*

Addressee	*Activity*	*Skills*
Technician	Creates and sets up agents. Sets Network Injector rules	*Tapping specialist technician*
Analyst	Analyzes and exports evidence.	*Operative*

Software author identification data

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
e-mail: info@hackingteam.com

2

RCS (Remote Control System)

Presentation

Introduction

RCS (Remote Control System) is a solution that supports investigations by actively and passively tapping data and information from the devices targeted by the investigations. In fact, RCS anonymously creates, sets and installs software agents that collect data and information, sending the results to the central database to be decrypted and saved.

Content

This section includes the following topics:

All-in-One architecture components

Introduction

RCS is installed at the operating center and proprietary authority's tapping rooms. It can come with special devices (hardware and software) installed at remote organizations such as Internet providers or remote servers. RCS can be installed in *All-In-One* or *Distributed* architecture.

All-In-One architecture layout

All-in-One architecture includes RCS installed on a single server. The logical architecture layout is provided below:

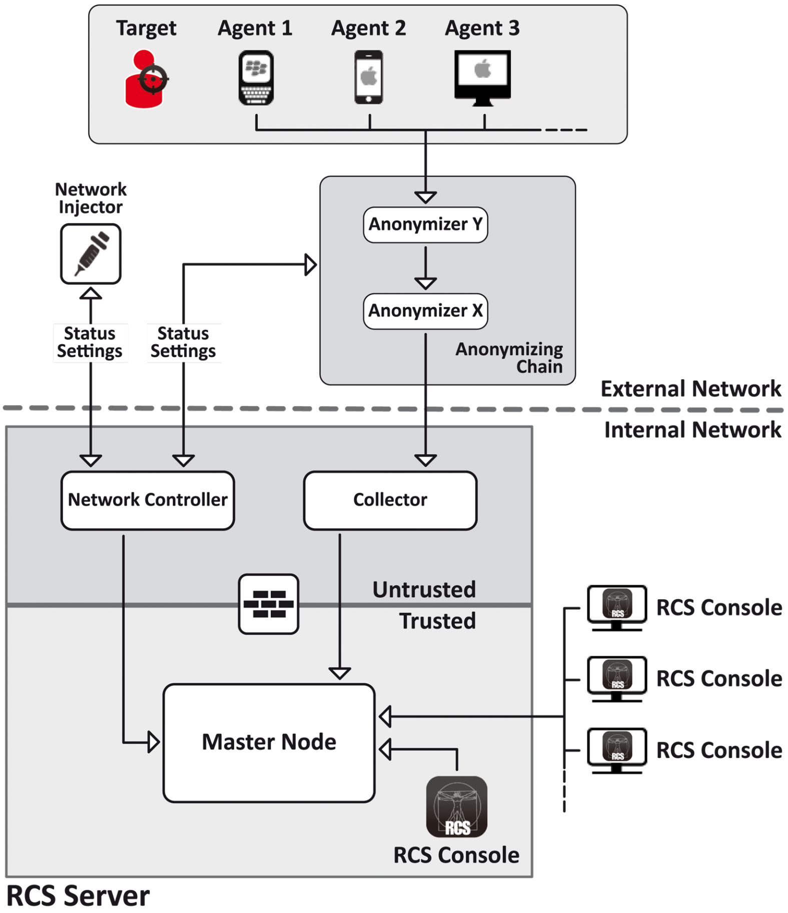


Figure 1: All-In-One RCS architecture: logical layout

All-in-One RCS architecture components

Architecture components are provided below:

Component	*Function*	*Installation*
Agent	Software bugs tap and communicate the investigation target's data and information to an Anonymizer or, if not installed, directly to Collectors.	- *target devices* - *data sources*
Anonymizing chain **Anonymizer**	(optional) geographically distributed Anonymizer groups that guarantee Collector anonymity and redirect collected data to protect servers from remote attacks. It transfers agent data to servers. Several Anonymizers can be set up in a chain to increase the level of protection. Each chain leads to one Collector.	*VPS (Virtual Private Server)*
Collector	RCS server component that collects agent data either directly or through the Anonymizer chain.	*RCS server*
Firewall	Optional but highly recommended, it protects the *trusted* environment were data is processed and saved from the *untrusted* environment where data is collected.	*RCS server*
RCS console	Setup, monitoring and analysis console used by operating center workers.	- *RCS server* - *internal network*
Master Node	Heart of the RCS server, it manages data flows, component status and includes the first Shard database. It includes the Worker service to decode data before saving it in the database.	*RCS server*
Network Controller	(optional) RCS server component, sends settings to Network Injector, Anonymizer chains and constantly acquires their status.	*RCS server*
Network Injector	(optional) Fixed hardware component (Appliance) or notebook (Tactical), it runs sniffing and injection operations on the target's HTTP connections.	- *ISP* - *Wired or Wireless LAN (homes, hotel)*
Target	Investigation targets. Each device owned by the target is a data source and can be monitored by an agent.	-

Distributed architecture components

Introduction

In special cases, RCS can also be installed in *distributed* architecture.

Distributed architecture layout

Software components are installed on several servers in distributed architecture. The architecture layout is provided below:

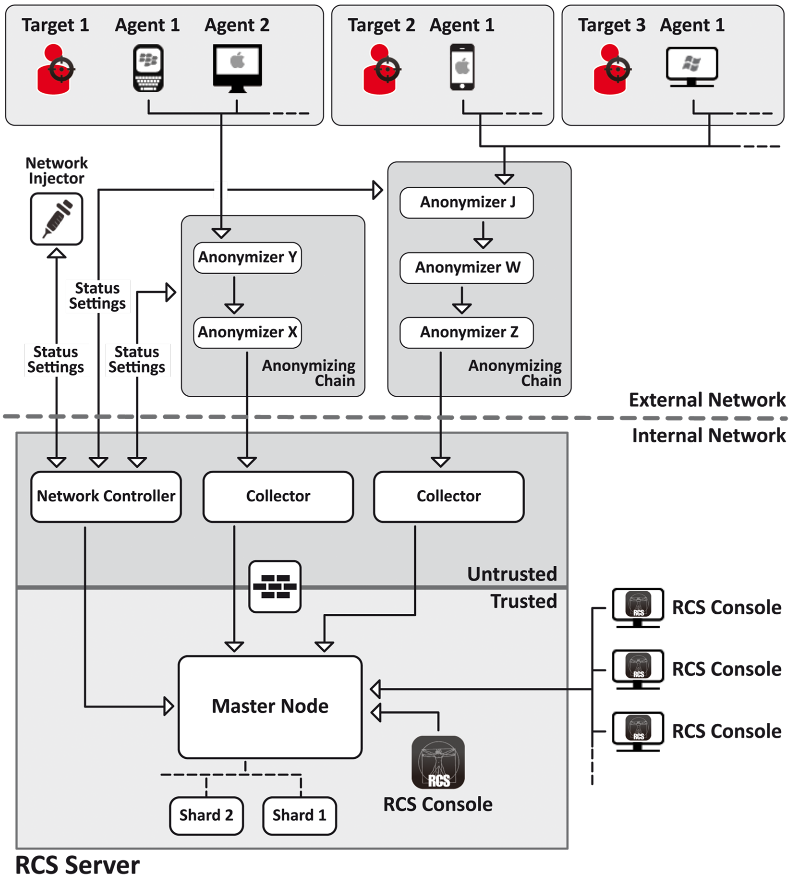


Figure 1: Distributed RCS architecture: logical layout

Distributed architecture components

Following are the difference in components in distributed architecture compared to All-in-One architecture:

Component	*Function*	*Installation*
Collector	One per each Anonymizing Chain, it collects data communicated by the last Anonymizer in the chain. It requires a single license.	*one or more servers in front end environment*
Network Controller	One per architecture, it is included in first Collector installation.	*one server in front end environment*
Shard x	Additional RCS distributed database partitions. Shard 0 is included in Master Node. It includes Worker service to decode data and enter it in the database.	*one or more servers in back end environment*

What you should know about RCS

Operations

RCS system components must be suitably installed at both the operating center and, eventually, an Internet service provider. Typically divided in *front end* environments for all data collection, tapping and monitoring, and *back end* environment for data collection and backup.

Data flow and protection

The RCS server clearly separates activities in *untrusted* environment from those in *trusted* environment. The barrier limit is provided by a resident firewall.

Tapping data is collected in untrusted environment, eventually redirected to protect the addressee's identity (you) and sent to an information collector (Collector). Remote device status and settings are checked by a specific component (Network Controller).

In trusted environment, evidence is managed, set and monitored (Master Node).

Lastly, RCS Console is a client that directly connects to Master Node. It can be installed on any computer to be used by the various RCS users.

*See "**Distributed architecture components**" on previous page .*

Data logging continuity

Agents send collected data to the Collector. If communications fail, connectivity is down or the Collector does not work, agents can save a set amount of data until connectivity is restored. Data that exceed the admitted limit are lost.

If the Collector cannot communicate with Master Node (disservice or maintenance in progress), received data is locally saved on the Collector until Master Node is restored. Once restored, data is automatically sent.

Redirecting login to Collector

The Collectors real function can be hidden, for direct access to data collection service, by redirecting to an unsuspicious page (i.e.: Google, e-commerce site and so on). Redirecting is through a customizable HTML page.

*See "**Files installed at the end of installation**" on page 35*

Digital certificates

Master Node uses HTTPS digital certificates that guarantee communication security between Master Node, Collector, Network Controller and RCS Consoles.

Some agents (Android, Symbian) require specific certificates that must be created and saved in folder \RCS\DB\config\certs.

*See "**Files installed at the end of installation**" on page 35*

Decoding data

Worker service is installed with each Shard and decodes data before it is saved in the database. For distributed databases, each Shard has its own Worker that receives encrypted data from Master Node, decodes it and saves it in the database. The work load is automatically evenly distributed among all Shards in the same cluster.

Differences with previous versions

Differences with the RCS 7.6 version are described below

Glossary

RCS v. 7.6	*RCS 8.0 and higher*
Activity	Operation
Agent	Module
Anonymizer chain	Anonymizing chain
Backdoor	Agent
Backdoor Class	Factory
Collection Node (ASP)	Collector
Injection Proxy Appliance (IPA)	Network Injector Appliance
Log Repository (RCSDB)	Master Node and additional Shard
Mobile Collection Node (RSSM)	Collector
RCSAnon	Anonymizer

3

Installation introduction

Presentation

Introduction

RCS installation is run at first installation or subsequent updates. Installation files are available on the CD included in the package or can be downloaded from the HackingTeam support portal.

Installation requirements

All hardware must already be installed and running according to the system requirements communicated by HackingTeam upon order confirmation.
*See "**Minimum system requirements**" on page 14*

NOTE: Network Injector or Anonymizer installation is optional and will be documented in the following chapters.

Content

This section includes the following topics:

Package content

Package content

RCS is supplied in a package that includes:

- an installation CD
- a USB key with user license
- two USB hardware keys (main and backup)

Service call: all USB keys are supplied with an ID code that must be communicated to support service for all software replacements and updates.

Installation package content (CD or web)

The installation package in the CD or downloaded from the HackingTeam support portal contains the following files where 'x' is the CD root:

Folder	*Included files*	*Description*
x:	ChangeLog.pdf	*Release notes*
x:\doc	RCS_ x.x_ Admin_ y.y_ <language>.PDF RCS_ x.x_ Analist_ y.y_ <language>.PDF RCS_ x.x_ SysAdmin_ y.y_ <language>.PDF RCS_ x.x_ Technician_ y.y_ <language>.PDF	*RCS installation and user manuals. Each manual is addressed to a specific user role.* • *"x.x": RCS version.* • *"y.y": manual version.* • *<language>: manual language.*
x:\setup	AdoberAIRinstaller.exe	*Adobe AIR installation file*
x:\setup	RCS-<version>.exe	*RCS server(s) installation file*
x:\setup	RCSconsole-<version>.air	*RCS Console installation file*
x:\setup	RCS-ocr-<version>.exe	*OCR module installation file (optional)*

USB key with user license

The package contains a USB key with the user license for the supplied RCS version.

The file is required for installation and software updates. It can be copied from the USB key to any other support device.

USB hardware keys

Two hardware keys are included in the package: a main one, already linked to the license in the USB license key, and a backup, ready to be activated in the event the main key fails.

IMPORTANT: the hardware key must always be connected to the server (to Master Node in distributed architecture) to allow all RCS services to run. All services are immediately aborted when the key is disconnected!

Minimum system requirements

Hardware must be configured as instructed by support service in the contract phase. The computers on which RCS is installed require the following characteristics:

Machine	***Component***	***Requirement***
Front end and back end server	Operating system	*Microsoft Windows Server 2008 R2 Standard (English)*
Computer for RCS Console	Operating system	*Microsoft Windows or Apple Mac OS X.*
	Browser	*Firefox 11* *IE 9* *Chrome*
VPS for Anonymizer	Operating system	*Linux CentOS 6*
Network Injector (Appliance or Tactical)	Operating system	*Provided by HackingTeam*

Ports to be opened on the firewall

If a firewall is installed between RCS server components, the following TCP ports must be opened to allow services to communicate:

From...	***To...***	***Port to be opened***
Agent/Anonymizer	Collector	80
Collector	Master Node	443
Collector	remote	all
Master Node	Collector	80

From...	*To...*	*Port* *to be opened*
Network Controller	remote	443
Console	Master Node	443, 444

System administrator procedures

Introduction

Typical System administrator procedures are listed below with references to the pertinent chapters.

Procedures

Install RCS and setup components

The server, Console, Shard, additional Collector and optional Anonymizer and Network Injector component installation procedure is described below:

Step	*Action*
1	Prepare the installation environment. *See "**Installation introduction**" on page 12 .*
2	Install the RCS server (in All-In-One or distributed architecture). *See "**RCS installation**" on page 17 .*
3	Install the RCS Consoles. *See "**RCS Console installation** " on page 30 .*
4	(optional) Install an OCR module. *See "**OCR module installation**" on page 33* *Service call: to install other RCS modules, contact Hacking Team technicians.*
5	(optional) Install the Shard databases and additional Collectors. *See "**Additional component installation in distributed architecture**" on page 52 .*
6	(optional) Install and setup up Anonymizers. *See "**Anonymizer installation and settings**" on page 38*
7	(optional) Install Network Injectors. *See "**What you should know about Network Injector Appliance**" on page 40 .* *See "**What you should know about Tactical Network Injector**" on page 46 .*

Maintain and update the system

References to the chapters on how to maintain performance and update the system are listed below:

- *See "**Routine maintenance and software updates**" on page 60 .*
- *See "**Editing Master Node and Collector settings**" on page 67 .*
- *See "**Troubleshooting**" on page 72 .*

Monitoring the system

References to chapters on how to monitor the system are given below:

- *See "**RCS Console for the System administrator**" on page 82*

4

RCS installation

Presentation

Introduction

RCS installation requires intervention on various local and remote servers.

Content

This section includes the following topics:

What you should know about RCS installation

Login privileges

RCS was designed to guarantee maximum server and collected data security. To achieve this goal, four distinct roles were defined that usually refer to the professionals who can login to the system:

- ⚙ System administrator: exclusively in charge of hardware and software installation and backups
- ★ Administrator: in charge of all system login, investigations and investigation goals
- 🔧 Technician: in charge of setting up and installing tapping agents
- 🔍 Analyst: in charge of data analysis

Tip: several roles can be assigned to the same user, for example, an Administrator can also have Technician privileges.

Admin user and System administrator user

A special user is created during installation with the name "admin" and all privileges (system administrator, administrator, technician and analyst) to be used for all RCS Console settings and login functions.

This user must only be used for this purpose. After completing installation, we recommend you create one or more users with the required privileges according to your organization.

IMPORTANT: we usually refer to the admin user in this manual as the System Administrator, even if she/he has all privileges.

RCS server installation in All-in-One architecture

Introduction

RCS server installation in All-in-One architecture installs all server components on the same computer.

The RCS Console will be installed with a separate procedure.

See "RCS Console installation " on page 30

Installation requirements

The following is required before installing RCS server(s):

- the name or IP address of the server(s) where RCS is to be installed
- the license file, found on the USB key supplied in the delivered package or other support if downloaded from Internet.
- the USB hardware key, supplied in the package.

- for firewall, open the ports for correct service operations. *See "Ports to be opened on the firewall" on page 14* .

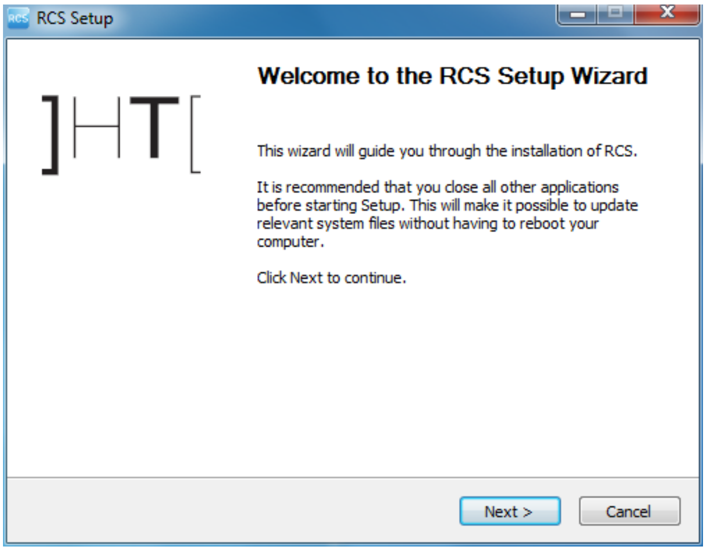
Installation sequence

The complete installation procedure for All-in-One architecture is described below:

Step	*Action*	*Machine*
1	Prepare that indicated in *installation requirements.*	-
2	Install RCS.	*server*
3	Make sure services have started.	*server*
4	Check the installation log.	*server*
5	Install RCS Console.	*server or other computer*
6	Setup the backup folder on the remote unit.	*server*

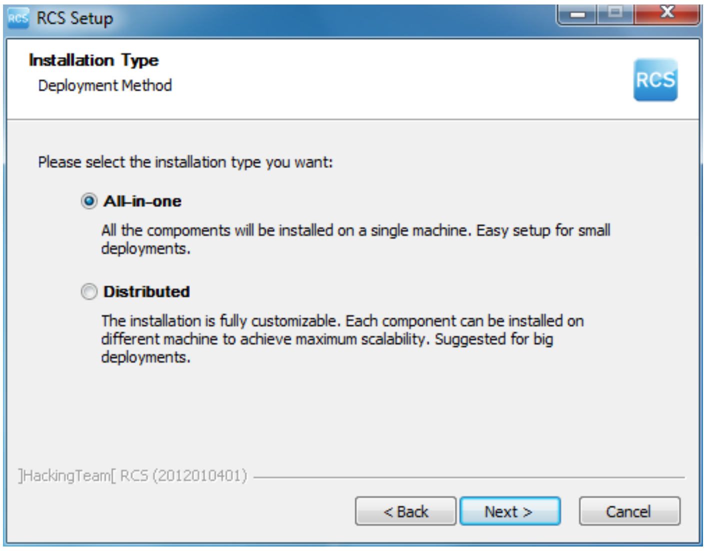
Installation

To install the server in All-in-One architecture:

Steps	*Result*
1. Insert the hardware key.	-
2. Insert the CD with the installation package. Run file RCS-<version>.exe in folder x:\setup the first wizard window appears. 3. 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.

Steps ***Result***

4. Select **All-in-One.**
5. Click **Next**.



Installation Type
Deployment Method

Please select the installation type you want:

● **All-in-one**

All the components will be installed on a single machine. Easy setup for small deployments.

○ **Distributed**

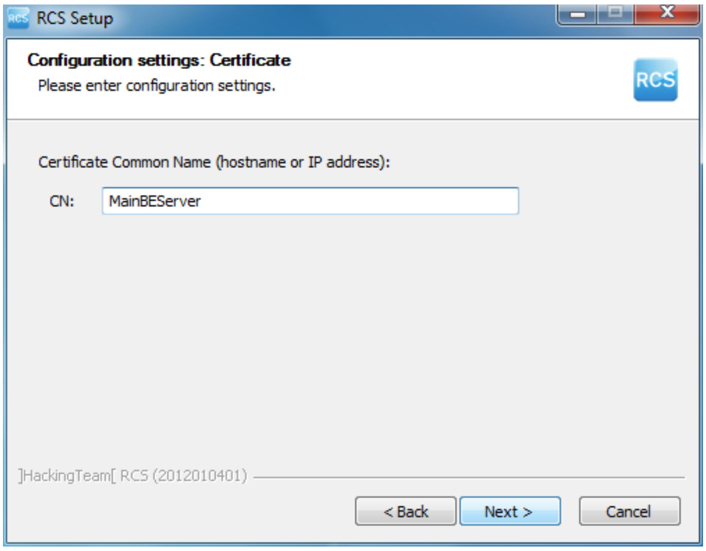
The installation is fully customizable. Each component can be installed on different machine to achieve maximum scalability. Suggested for big deployments.

]HackingTeam[RCS (2012010401)

6. Enter the server name or IP address where the software is being installed and that will be indicated at RCS Console login (i.e.: **RCSserver**).

IMPORTANT: the name and/or IP address must be univocal.

7. Click **Next**.

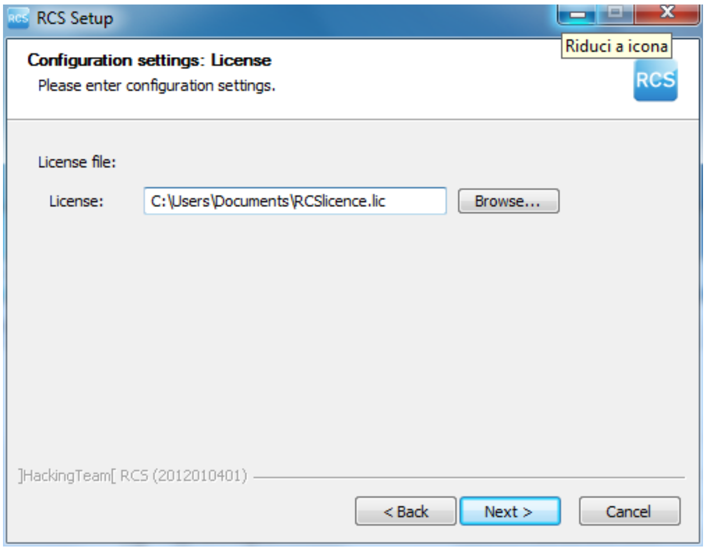


Configuration settings: Certificate
Please enter configuration settings.

Certificate Common Name (hostname or IP address):

CN: MainBEServer

]HackingTeam[RCS (2012010401)

Steps	***Result***
8. Select the license file. 9. Click **Next**.	 RCS Setup Configuration settings: License Please enter configuration settings. License file: License: C:\Users\Documents\RCSlicence.lic]HackingTeam[RCS (2012010401) Riduci a icona RCS Browse... < Back Next > Cancel
10. Enter the system administrator's password. 11. Click **Next**: installation is launched.	-

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 .*

Checking service start

Make sure all RCS services are up and running. If services are not running, manually start them. *See "List of started RCS services" on page 29*

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 addresses, open RCS Console, **System** section, **Frontend**: the server address appears on the screen (Collector).*See "Anonymizer installation and settings" on page 38*

Uninstall

RCS can be uninstalled from the Windows Control Panel.

CAUTION: All saved data is lost when the RCS server is uninstalled. For correct operations, backup data. See "Backup management" on page 94

RCS server installation in distributed architecture

Introduction

Installation in distributed architecture typically installs all components on two or more servers: one server for the front end environment to collect data and manage remote devices and one server for the back end environment to process and save data.

Service call: distributed architecture is scalable. Check with the HackingTeam support service.

NOTE: RCS Console will be installed with a separate procedure on either the same server or other remote computer.

Installation requirements

The following is required before installing RCS server(s):

- the name or IP address of the server(s) where RCS is to be installed
- the license file, found on the USB key supplied in the delivered package or other support if downloaded from Internet.
- the USB hardware key, supplied in the package.
- for firewall, open the ports for correct service operations. *See "**Ports to be opened on the firewall**" on page 14* .

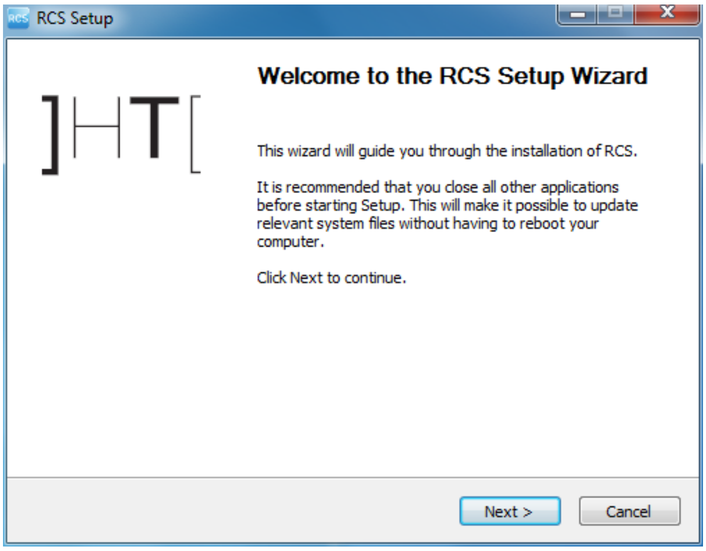
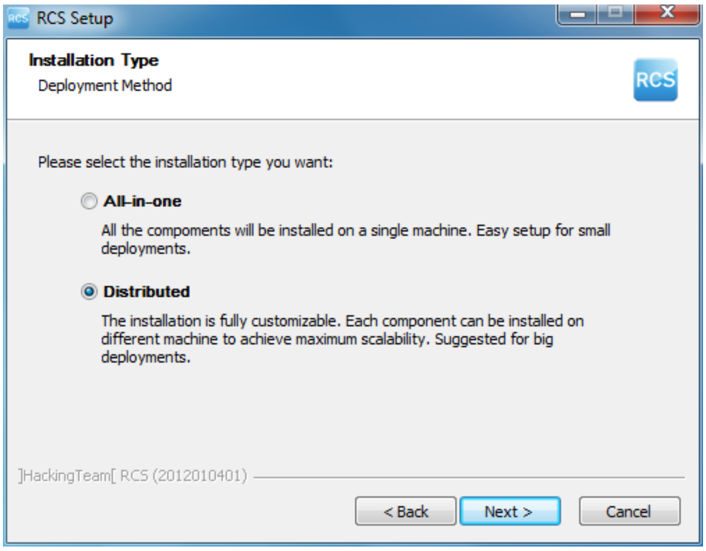
Installation sequence

The installation sequence in distributed architecture is described below:

Step	*Action*	*Machine*
1	Prepare that indicated in *installation requirements.*	-
2	Install Master Node.	*server in back end environment*
3	Check installation logs.	
4	Make sure Master Node services have started.	
5	Install Collector and Network Controller.	*server in front end environment*
6	Check installation logs.	
7	Check Collector redirecting	*same server or other computer*
8	Install RCS Console.	*server in back end environment or other computer*
9	Setup the backup folder on the remote unit.	*server in back end environment*

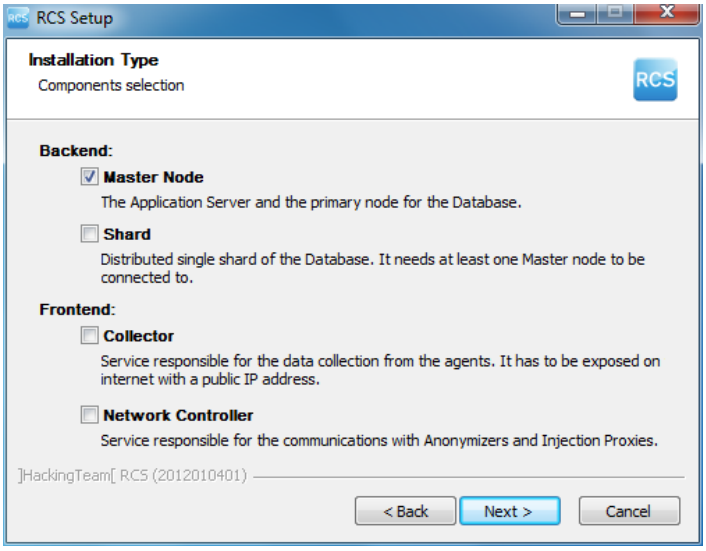
Master Node installation

To install Master Node on the server in back end environment:

Steps	***Result***
1. Insert the hardware key.	-
2. Insert the CD with the installation package. Run file RCS-<version>.exe in folder x:\setup: the first wizard window appears. 3. 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.
4. Select **Distributed.** 5. Click **Next**.	 **Installation Type** Deployment Method Please select the installation type you want: ○ **All-in-one** All the components will be installed on a single machine. Easy setup for small deployments. ● **Distributed** The installation is fully customizable. Each component can be installed on different machine to achieve maximum scalability. Suggested for big deployments.]HackingTeam[RCS (2012010401)

Steps ***Result***

6. Select **Master Node.**
7. 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. It has to be exposed on internet with a public IP address.

☐ **Network Controller**

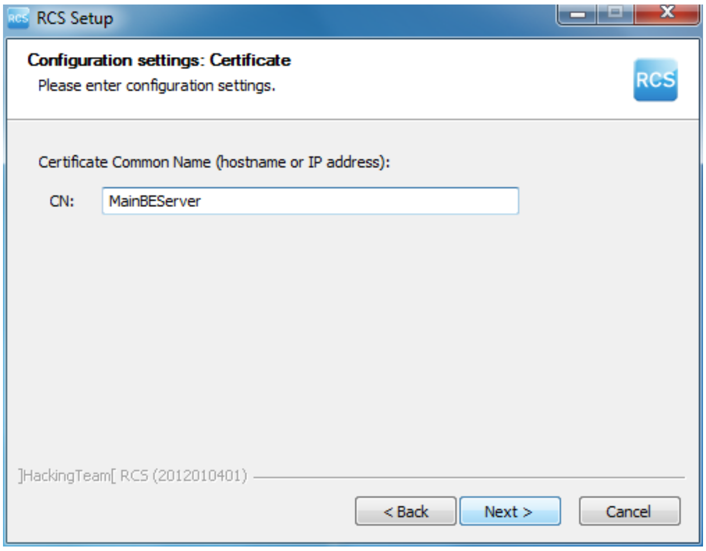
Service responsible for the communications with Anonymizers and Injection Proxies.

]HackingTeam[RCS (2012010401)

8. Enter the server name or IP address where the software is being installed and that will be indicated at RCS Console login (i.e.: RCSMasterNode).

IMPORTANT: the name and/or IP address must be univocal.

9. Click **Next**.



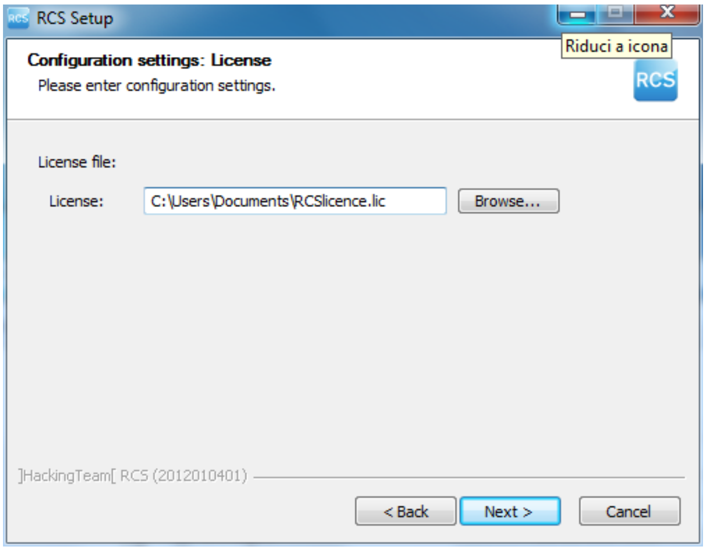
Configuration settings: Certificate

Please enter configuration settings.

Certificate Common Name (hostname or IP address):

CN: MainBEServer

]HackingTeam[RCS (2012010401)

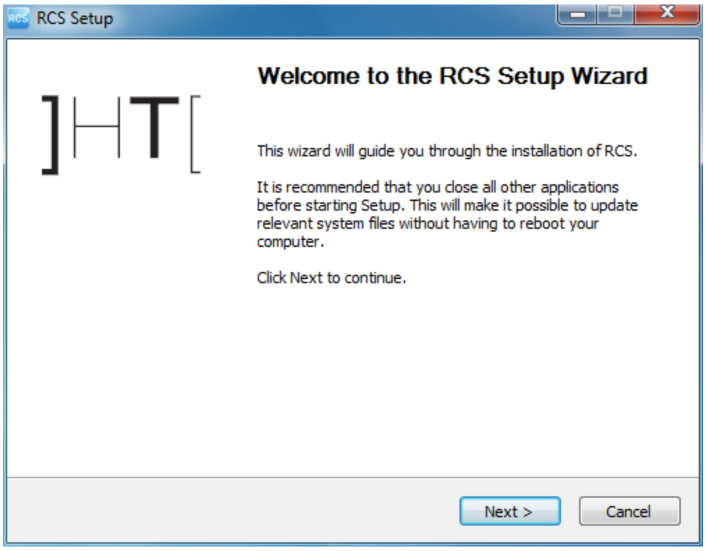
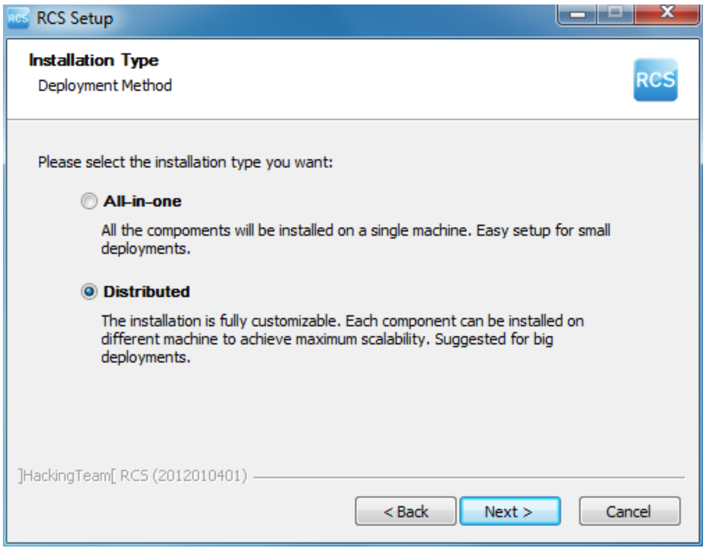
Steps	*Result*
10. Select the license file. 11. Click **Next**.	 RCS Setup Configuration settings: License Please enter configuration settings. License file: License: C:\Users\Documents\RCSlicence.lic]HackingTeam[RCS (2012010401)
12. Enter the system administrator's password. 13. Click **Next**: when installation has completed, services are started and are ready to receive data and communicate with the RCS Console.	-

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* .

Collector and Network Controller installation

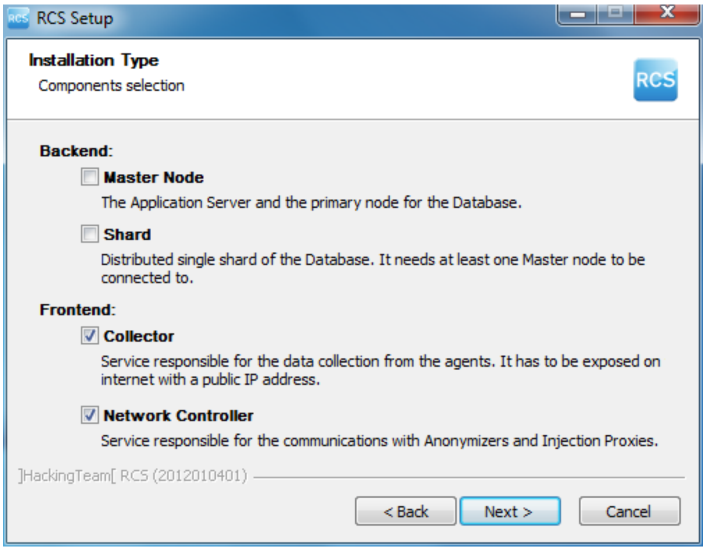
To install Collector(s) and Network Controller(s) in front end environment:

Steps	*Result*
1. Insert the hardware key.	-

Steps	***Result***
2. Insert the CD with the installation package. Run file RCS-<version>.exe in folder x:\setup: the first wizard window appears. 3. 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.
4. Select **Distributed.** 5. Click **Next**.	 RCS Setup **Installation Type** Deployment Method Please select the installation type you want: ○ **All-in-one** All the components will be installed on a single machine. Easy setup for small deployments. ● **Distributed** The installation is fully customizable. Each component can be installed on different machine to achieve maximum scalability. Suggested for big deployments.]HackingTeam[RCS (2012010401)

Steps ***Result***

6. Select **Collector** and **Network Controller.**
7. 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.

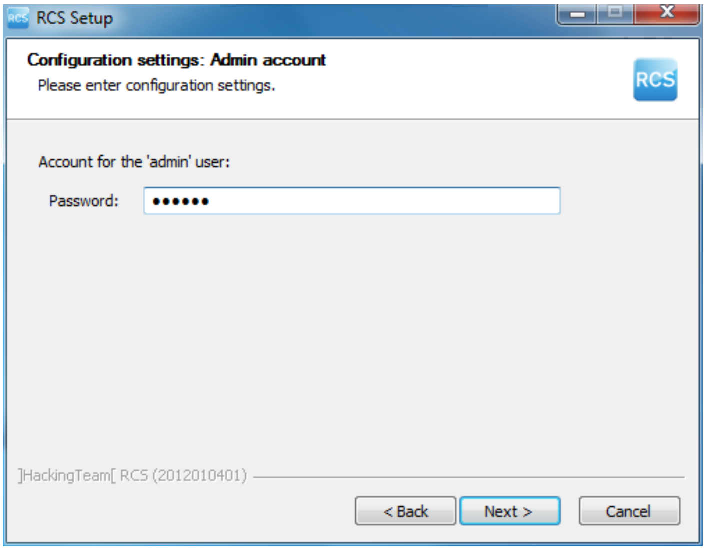
Frontend:

☑ **Collector**
Service responsible for the data collection from the agents. It has to be exposed on internet with a public IP address.

☑ **Network Controller**
Service responsible for the communications with Anonymizers and Injection Proxies.

]HackingTeam[RCS (2012010401)

8. Enter the system administrator password indicated in Master Node installation.
9. Click **Next**: installation is launched.

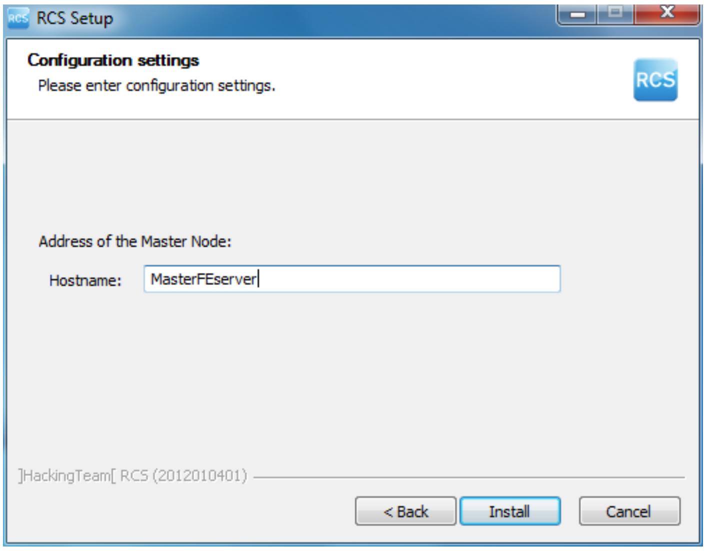


Configuration settings: Admin account
Please enter configuration settings.

Account for the 'admin' user:

Password: ••••••

]HackingTeam[RCS (2012010401)

Steps	*Result*
10. Enter the Master Node server name or IP address (i.e.: **RCSMasterNode**). 11. Click **Install**: 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: Hostname: MasterFEserver]HackingTeam[RCS (2012010401)

Checking service start

Make sure all RCS services are up and running. If services are not running, manually start them.

See "List of started RCS services" on the facing page

Checking Collector redirecting

To check whether Collector installation was successfully completed:

If	*Then*
on the server	• open a browser • enter `localhost` • **Result**: the browser must be redirected to Google.
on another computer	• open a browser • enter `http://<front end server name or IP address>`. • **Result**: the browser must be redirected to Google.

Tip: you can edit redirecting or create a custom page. To do this, edit page `decoy.html`.

See "Files installed at the end of installation" on page 35

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 38*

Uninstall

RCS can be uninstalled from the Windows Control Panel.

CAUTION: All saved data is lost when Master Node is uninstalled. For correct operations, backup data. See "Backup management" on page 94 .

NOTE: data will not be lost when other servers are uninstalled.

List of started RCS services

RCS services appear at the end of the various installation phases. Making sure they have correctly started is one of the procedures required to ensure installation is complete.

Services are listed below:

Architecture	*Services*	*Server in environment*
All-in-One	RCSMasterConfig RCSMasterRouter RCSMasterShard RCSMasterWorker RCSMasterDb RCSCollector RCSDB Mongodb	*back end*
Distributed	RCSCollector	*front end*
	RCSMasterConfig RCSMasterRouter RCSMasterShard RCSMasterWorker RCSMasterDb RCSDB Mongodb	*back end only with Master Node*
	RCSWorker RCSShard	*back end with additional Shards*

NOTE: Network Controller does not appear amongst services since it is a RCSCollector service setting.

To learn more

To restart any stopped services *see "**Service restart procedures** " on page 77* .

RCS Console installation

Introduction

RCS Console is a client designed to interact with Master Node. It is typically installed on control room computers (for inspectors and analysts) and used by all personnel involved in RCS installation.

NOTE: for All-in-One architecture you can also install an RCS Console on the RCS server.

Requirements

Before installing RCS Console you must:

If you are installing..	*Then you must...*
RCS All-in-One	• have the RCS server installed • prepare the server name or IP address • prepare the system administrator's password.
Distributed RCS	• have the RCS server(s) installed • prepare the Master Node name or IP address • prepare the Master Node System administrator's password

Installation sequence

The full RCS Console installation sequence is the following:

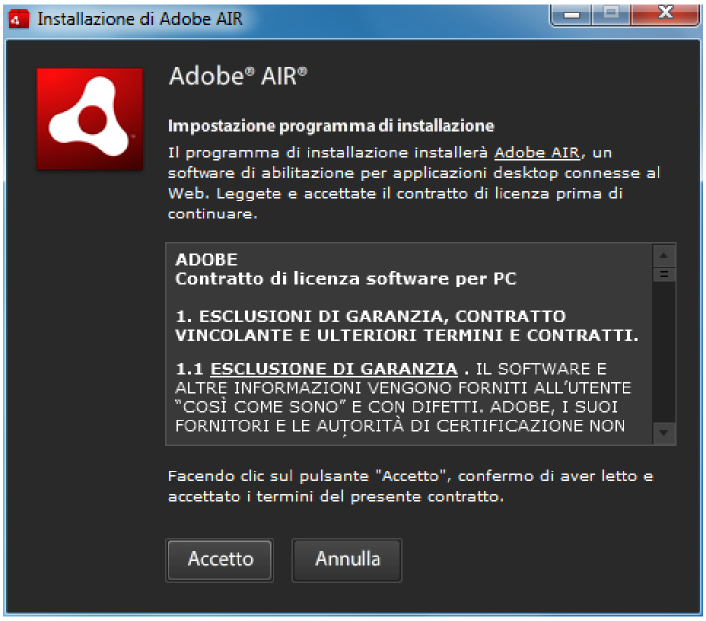
Step	*Action*
1	Install Adobe AIR.
2	Install RCS Console.

Adobe AIR installation

To install Adobe AIR:

Steps ***Result***

1. Install Adobe AIR: no icon appears on the desktop at the end of installation.



Installazione di Adobe AIR

Adobe® AIR®

Impostazione programma di installazione

Il programma di installazione installerà Adobe AIR, un software di abilitazione per applicazioni desktop connesse al Web. Leggete e accettate il contratto di licenza prima di continuare.

ADOBE
Contratto di licenza software per PC

1. ESCLUSIONI DI GARANZIA, CONTRATTO VINCOLANTE E ULTERIORI TERMINI E CONTRATTI.

1.1 ESCLUSIONE DI GARANZIA . IL SOFTWARE E ALTRE INFORMAZIONI VENGONO FORNITI ALL'UTENTE "COSÌ COME SONO" E CON DIFETTI. ADOBE, I SUOI FORNITORI E LE AUTORITÀ DI CERTIFICAZIONE NON

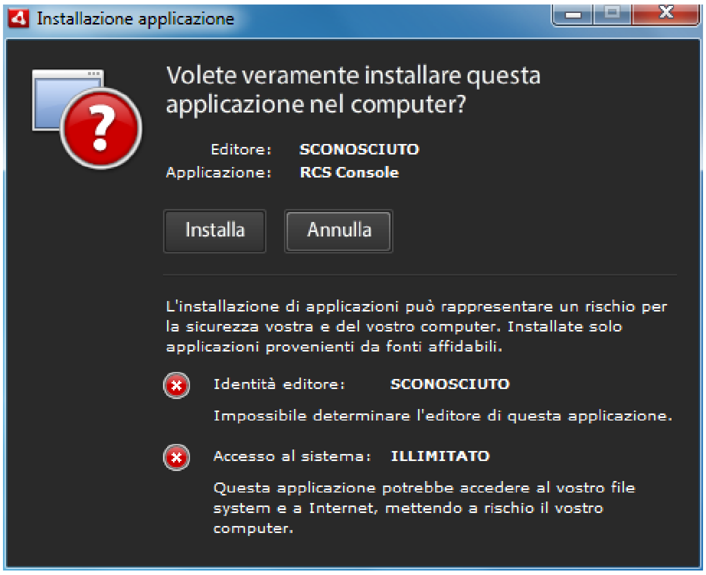
Facendo clic sul pulsante "Accetto", confermo di aver letto e accettato i termini del presente contratto.

RCS Console installation

To install RCS Console:

Steps ***Result***

1. Run the file RCSconsole-<version>.air
2. Click **Install**.



Installazione applicazione

Volete veramente installare questa applicazione nel computer?

Editore: SCONOSCIUTO
Applicazione: RCS Console

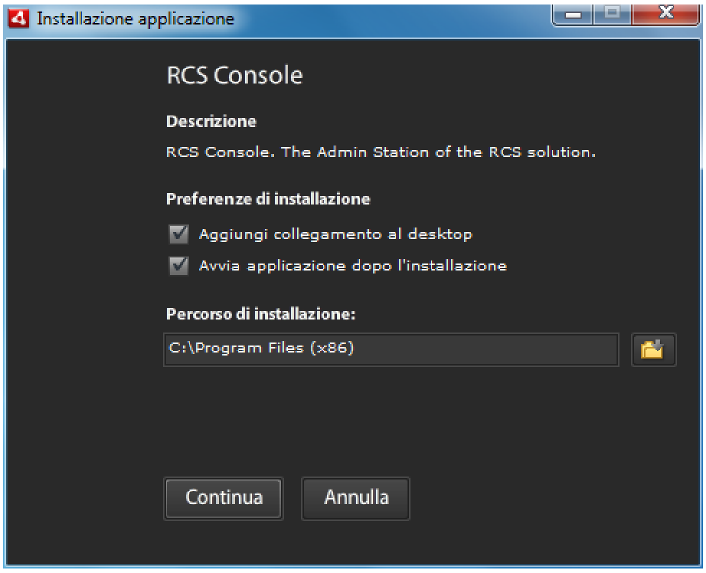
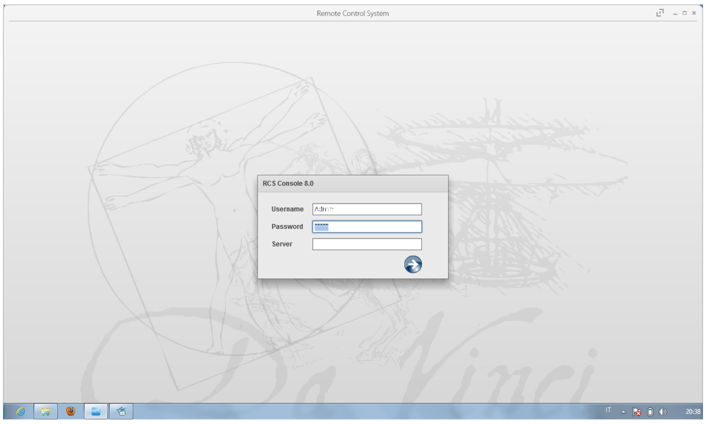
L'installazione di applicazioni può rappresentare un rischio per la sicurezza vostra e del vostro computer. Installate solo applicazioni provenienti da fonti affidabili.

Identità editore: SCONOSCIUTO

Impossibile determinare l'editore di questa applicazione.

Accesso al sistema: ILLIMITATO

Questa applicazione potrebbe accedere al vostro file system e a Internet, mettendo a rischio il vostro computer.

Steps	*Result*
3. Set any preferences. 4. Click **Continue**: RCS Console will be installed on the computer.	 Installazione applicazione RCS Console **Descrizione** RCS Console. The Admin Station of the RCS solution. **Preferenze di installazione** ☑ Aggiungi collegamento al desktop ☑ Avvia applicazione dopo l'installazione **Percorso di installazione:** C:\Program Files (x86) Continua Annulla
5. The RCS Console login window appears at the end of installation. 6. Enter your credentials and the server name/IP address. 7. Click ➔. NOTE: the System administrator logs in with name "admin" and the password selected during installation.	 Remote Control System RCS Console 8.0 Username Password Server

RCS Console uninstall

RCS Console can be uninstalled at any time, for example, to use the computer in another way or to remove RCS Console from the All-in-One server and install it on a separate computer. Database data and user preferences are not influenced in any way.

Creating the Administrator user

An RCS Console Administrator user must be created during RCS installation. The Administrator is in charge of creating all other users and managing operations and targets.*See "**Product and guide addressees**" on page 4* .

To create an Administrator user:

Step	*Action*
1	From **RCS Console,** in the **Accounting** section, click **New user** .
2	Enter the required data, selecting the **Administrator role** and click **Save**: the new user appears in the main work area with icon 👤. from now on the user with the indicated credential can log into RCS Console and run the foreseen functions.

OCR module installation

Introduction

The OCR module is an optional module that indexes all content (i.e.: in addition to traditional documents, also images, audio, video) for full-text search.

NOTE: it supports only ASCII characters and left to right reading.

Installation requirements

For all-in-one architecture, install the module on Master Node.

For distributed architecture, install the first OCR module on Shard to avoid increasing the Master Node work load.

OCR module operations

OCR module operations are described below:

Phase	*Description*
1	Screenshot evidence images, awaiting conversion, are saved in a separate queue from evidence awaiting analysis.
2	The OCR module read the image queue and converts it into text. This operation can last from one to 5-10 seconds according to the number of words to be acquired.
3	Each image text is saved in the database and tagged as full-text.
4	Storage times and tags for the single image are saved in the module log.
5	The text is made available to the Analyst in the page with the list of evidence for a search in the **Info** field and in the detailed evidence page.

Space occupied by tagged text in the database

Each piece of screenshot evidence occupies more space in the database because it is always accompanied by its tagged text. The increase in space cannot be predicted since it depends on both the number of screenshots acquired from the agent and the number of words in each screenshot.

OCR module work load

The OCR module occupies a lot of the CPU when converting a screenshot, but is run with a lower priority than other processes.

Thus the CPU load will only have an effect when the system shows the converted image text during evidence analysis.

For distributed architecture, it can be installed on Shard and not on the Master Node, already full of processes.

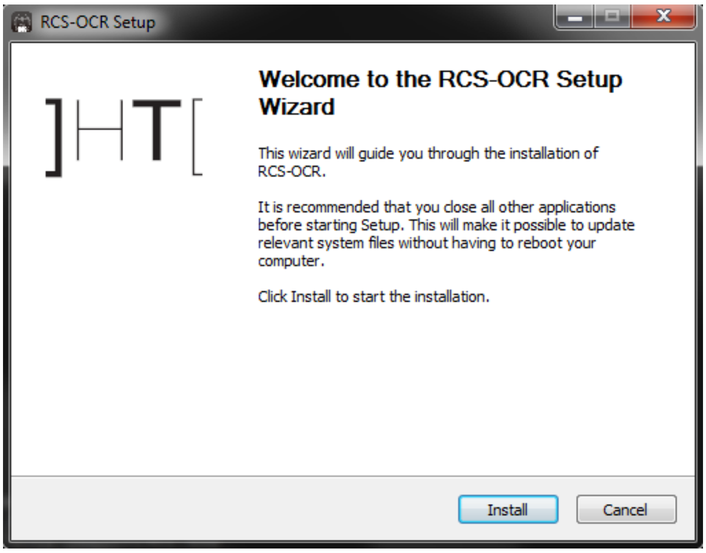
Symptoms of excessive load

Check how long it takes for the text to be displayed in the single evidence detail and check the times recorded in the log when acquiring images. If these are deemed excessive and another server is free (i.e.: that housing another shard database or Master Node) install another OCR module.

This way the work load will be divided amongst all installed modules.

OCR module installation

To install an OCR module in back end environment:

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

Welcome to the RCS-OCR Setup Wizard

This wizard will guide you through the installation of RCS-OCR.

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.

Steps	*Result*
3. Follow the steps below until installation has completed: the module will begin converting images the first time a screenshot type of evidence is received.	-

Checking correct OCR module operations

To check whether image conversion to text is too slow, check how long it takes for the ≡ button to appear in the evidence details page.

Uninstall

The OCR module can be uninstalled from the Windows Control Panel.

NOTE: uninstalling an OCR module does not compromise converted and tagged text.

Files installed at the end of installation

Various folders appear at the end of installation, organized according to the type of architecture and installed optional components:

Folder	*Included files*
backup	The folder contains files with data saved in the databases. *See "**Backup management**" on page 94* IMPORTANT: This folder's content should not be touched. To save backup data on remote disks, use the Windows **Disk Management** function and install the disk as a NTFS folder, selecting it as the target. **Path**: C:\RCS\DB\backup
bin	The folder contains the utilities (i.e.: rcs-db-config) used to set RCS utilities. *See "**Setup utilities**" on page 68* **Path**: C:\RCS\DB\bin C:\RCS\Collector\bin

Folder	*Included files*
certs	The folder contains the certificates used by the various services to access Master Node. They are updated when RCS settings are edited. *See "Editing Master Node settings" on page 69* **Path**: \RCS\DB\config\certs
config	The folder contains: • `decoy.htm` page to redirect or customize undesired remote login landing on the server. It can be customized. *See "Routine maintenance procedures" on page 61* • License file copied from the USB key. • Export.zip: file containing the style sheets to be customized for evidence export. **Path**: C:\RCS\DB\config C:\RCS\Collector\config
log	RCS component log file. *See "System logs" on page 74* **Path**: C:\RCS\DB\log C:\RCS\Collector\log

5

Optional and additional component installation

Presentation

Introduction

RCS installation may include the installation of other optional and additional components:

- Network Injector
- Anonymizer
- Shard database
- Collector

Content

This section includes the following topics:

Anonymizer installation and settings

Introduction

Installing Anonymizers in a chain is optional and is used to redirect data from a group of agents. The Anonymizer is installed on a server connected to Internet which cannot be reconnected to the rest of the infrastructure like, for example, a VPS (Virtual Private Server), rented for this purpose. Once installed and set up, the Anonymizer communicates its status to the Network Controller every 30 seconds.

Installation requirement

A VPS must be rented with the minimum system requirements defined in the contract phase to install anonymizers.

*See "**Minimum system requirements**" on page 14*

Installation

CAUTION: use SSH protocol for all installation, setup and data exchange operations to the remote unit.

To install the Anonymizer on a private server:

Step	*Action*
1	From **RCS Console,** in the **System** section, click **Frontend**, **New Anonymizer**.
2	Enter the required data and click **Save.** **Result**: the Anonymizer appears in the Anonymizer list with icon . In the **Monitor** section, a monitoring object appears for the added Anonymizer.
3	Select the Anonymizer and drag it to the Collector or another Anonymizer to create a chain. **Result**: the Anonymizer appears in the Anonymizer list with icon .
4	Click **Download installer**. **Result**: the `rcsanon_install.zip` installer file is generated and saved on the console desktop.
5	Connect to the server and copy file `rcsanon_install.zip` to a folder on the server.

Step	*Action*
6	Connect to the server, unzip the file and launch the installer by entering: `# sh rcsanon-install.sh` **Result**: the Anonymizer is installed in server folder /opt/rcsanon and listens on port 443.
7	From **RCS Console,** in the **System** section, **Frontend**, select the Anonymizer and click **Apply configuration**.

Anonymizer data

Selected Anonymizer data is described below:

Data	*Description*
Name Description	User's description
Version	Software version. To view software versions for all components see the **Monitor** section.
Address	IP address of the VPS where the Anonymizer was installed.
Port	443. To view the ports to be opened for firewall *see "**Ports to be opened on the firewall**" on page 14* .
Monitor via NC	If enabled, Network Controller acquires Anonymizer status every 30 seconds. If not enabled, the Anonymizer runs normally but Network Controller does not check status. To be used to avoid connections with Anonymizers in untrusted environments.
Log	Last messages logged. To view log file content *see "**System logs**" on page 74*

Boot check

The Anonymizer sends its logs to syslog that manages and saves them in a file. Files are normally saved in the following files (based on the operating system version and syslog service settings):

```
/var/log/messages
/var/log/syslog
```

IP address check

To check all Anonymizer addresses, start the **RCS Console** , **System** section, **Frontend** : the addresses appear on the screen. *See "**Anonymizer update**" on page 62*

Editing settings

To edit Anonymizer settings:

Step	*Action*
1	In the **System** section, **Frontend**, click on the Anonymizer icon.
2	Edit the required data and click **Save.** **Result**: the screen is updated.
3	Check Anonymizer status in the **Monitor** section.
4	Click **Apply settings**. **Result**: RCS connects to the Anonymizer and copies the new settings.

Uninstall

To uninstall the Anonymizer delete the private server folder /opt/rcsanon and delete the Anonymizer from the RCS Console. *See "**Anonymizer update**".*

What you should know about Network Injector Appliance

Introduction

Network Injector Appliance is a network server for installation in an intra-switch segment at an Internet service provider.

An RCS agent can be injected in visited web pages or downloaded files by monitoring target connections.

NOTE: Network Injector Appliance is supplied installed and ready for use, complete with all the foreseen applications.

Operations

Network Injector Appliance analyzes the target's traffic and, in the event set rules match, injects agents.

Network Controller queries Network Injector Appliance every 30 seconds to receive status and logs and send injection rules.

Network connections

Network Injector Appliance requires two network connections: one to tap the target's traffic and the other to inject agents and communicate with the RCS server.

Tip: after setup, Network Injector Appliance is independent. It can be left to run without further communication with the RCS server.

Service call: given special Network Injector Appliance features, this manual only provides essential connection indications, letting support service provide all those strategic aspects that are defined in the start-up and delivery phase.

Standard connection layout

Typical layout for an Access Switch that routes data to Network Injector Appliance:

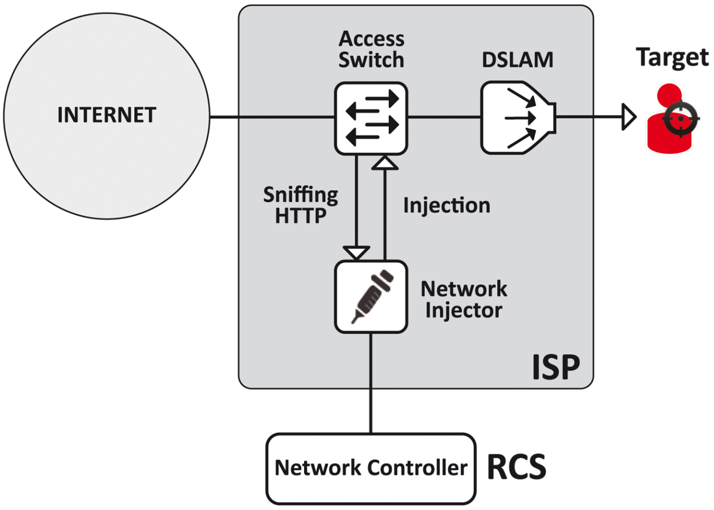


Figure 1: Network Injector Appliance: physical layout

Connection layout as an intra-switch segment

Typical layout with TAP device to boost Access Switch data routing:

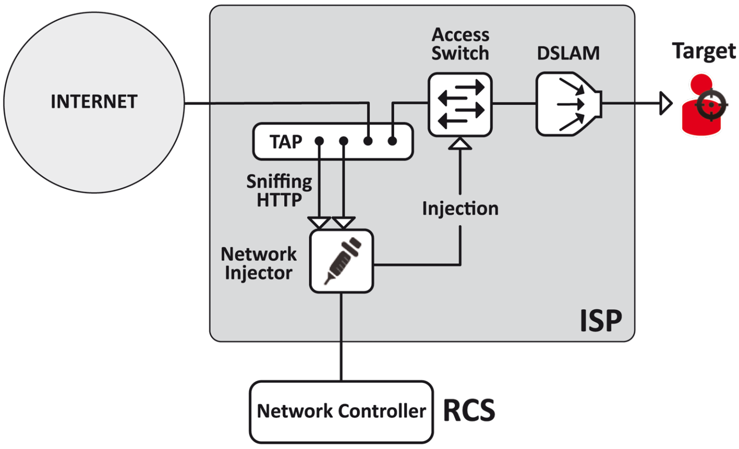


Figure 2: Network Injector Appliance with TAP: physical layout

Data sniffing via TAP, SPAN port

A TAP device is often installed at the Internet service provider and is the most appropriate solution for traffic monitoring.

Using a SPAN port has the following drawbacks:

- switch CPU use may significantly increase due to port use
- the SPAN port on the switch may already be in use.

Network Injector Appliance installation

Introduction

Network Injector Appliance is supplied already installed and set up. Its hardware must be installed at the Internet service provider.

Appliance Control Center lets you:

- enable synchronization with the operating center to receive injection rules and send logs.
- apply device identification rules to infect them
- update Network Appliance with the latest version sent by RCS Console.
- automatically identify connected devices using the rules and infect them

Package content

The package includes a series of GBIC connectors to monitor optic fiber and RJ45 connections.

Installation sequence

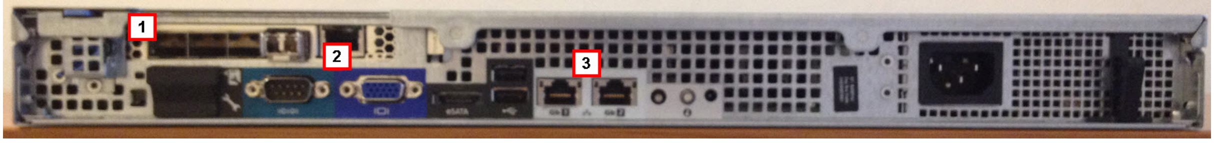
Tip: prepare Network Injector Appliance at your offices before installing it at the Internet provider.

The full installation sequence is provided below:

Step	***Action***	***Paragraph***
1	Connect Network Injector Appliance to the network.	*"**Network connections**" on the facing page*
2	Set up Network Injector.	*"" on page 44*
3	Run a test from RCS Console.	*"**Managing the Network Injector**" on page 100*
4	Transfer Network Injector Appliance to the Internet service provider and change the network addresses.	*"**Network Injector settings**" on page 51*

Rear panel description

The rear panel is described below:



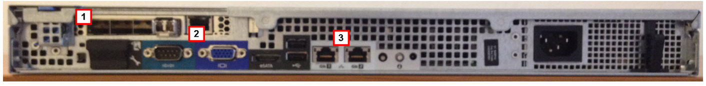
A list of visible components is provided below:

Area	*Component*	*Description*
1	**Sniffing ports**	*Up to four connections to the traffic switches on the targets to be monitored or up to two for redundant devices.* *NOTE: optic fiber or copper connections are admitted.*
2	**Mother board**	*Standard PC outputs for monitor and keyboard connections to launch* `sysconf` *utilities or complete updates from the installation CD.* *See "Routine maintenance procedures" on page 61*
3	**Management and injection ports**	***Port 1**: network connection with Network Controller to receive settings and send status. The address must be set with Network Manager.* ***Port 2**: network connection for traffic injection.*

Network connections

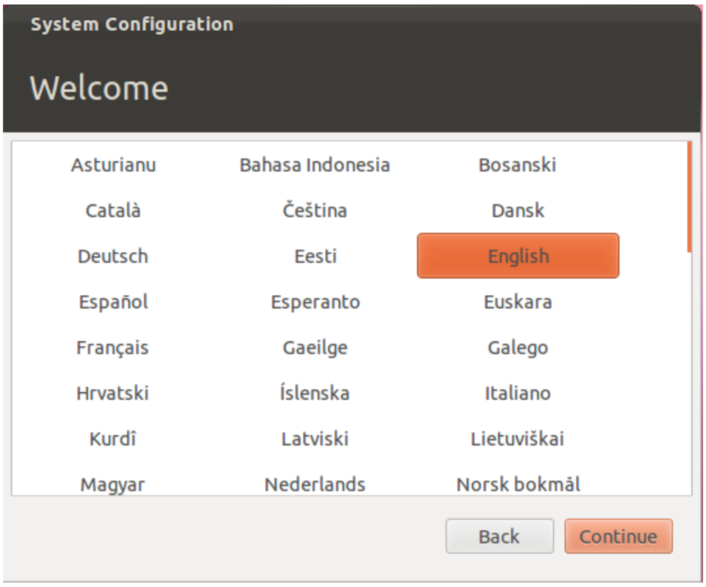
Tip: prepare Network Injector Appliance first connecting it to its network and setting parameters to then be transferred to the Internet provider.

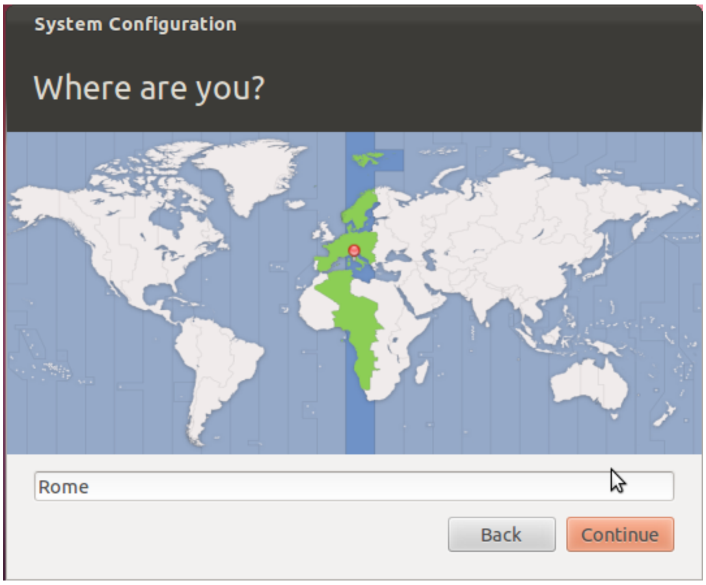
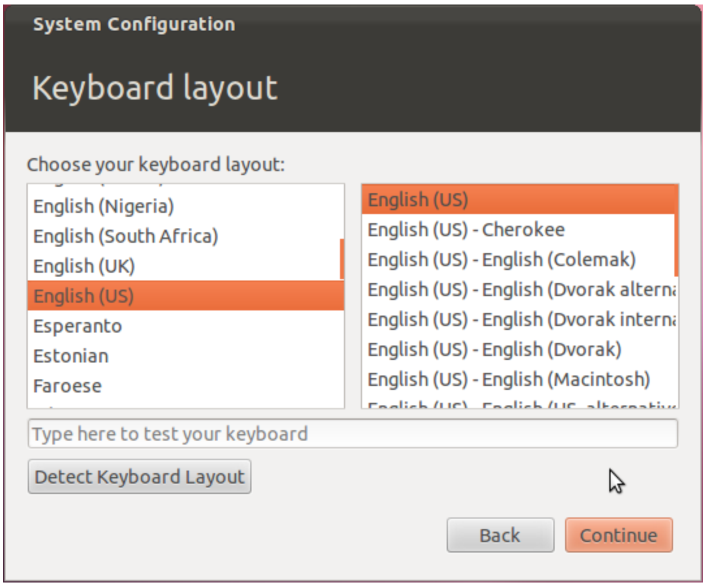
The network connection procedure is described below:

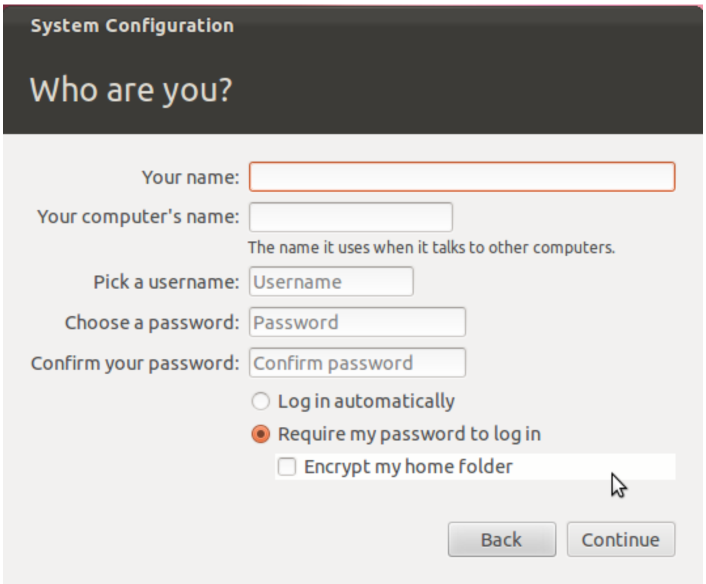
Steps	*Layout*
1. Connect the target's traffic switch to the sniffing ports**[1].** IMPORTANT: for redundant devices, connect both devices. 2. Connect management (port 1) and injection (port 2) ports **[3]** to the Internet. 3. Connect the monitor and keyboard **[2].**	

Operating system installation and settings

The procedure is described below:

Steps	***Result***
1. Connect the notebook to the network via Ethernet cable and insert the installation CD: the operating system is installed and the notebook turns off when completed. IMPORTANT: the computer must remain connected to the internet during the entire installation process.	-
2. Reboot the notebook.	-
3. The first setup window appears. 4. Select the language.	 System Configuration Welcome Asturianu Bahasa Indonesia Bosanski Català Čeština Dansk Deutsch Eesti English Español Esperanto Euskara Français Gaeilge Galego Hrvatski Íslenska Italiano Kurdî Latviski Lietuviškai Magyar Nederlands Norsk bokmål Back Continue

Steps	*Result*
5. Select the correct time zone.	 System Configuration Where are you? Rome Back Continue
6. 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

Steps	*Result*
7. Enter user data: operating system setup starts.	 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
8. The standard login page appears at the end of operating system installation.	-

IP address check

To check all addresses, open RCS Console, **System** section, **Network Injector** and view data for each Network Injector. *See "Managing the Network Injector" on page 100*

Uninstall

To uninstall a Network Injector Appliance, simply delete the object in RCS Console and turn off the device.

See "Managing the Network Injector" on page 100

What you should know about Tactical Network Injector

Introduction

Tactical Network Injector is a notebook for tactical installation on LAN or WiFi networks.

Tactical Control Center, installed on it, can be used to open protected WiFi networks or wired networks or emulate an Access Point already known to the target device.

NOTE: Tactical Network Injector is supplied installed and ready for use, complete with disk encryption and all the foreseen applications.

Network connections

Tactical Network Injector requires two network connections: one to tap the target's traffic and the other to inject agents and communicate with the RCS server.

Tip: after setup, Tactical Network Injector is independent. Internet connection is required to obtain updated rules from RCS and send logs (synchronization).

Access point emulation connection diagram

Typical layout in WiFi where Tactical Network Injector emulates the open WiFi network access point to attract target devices.

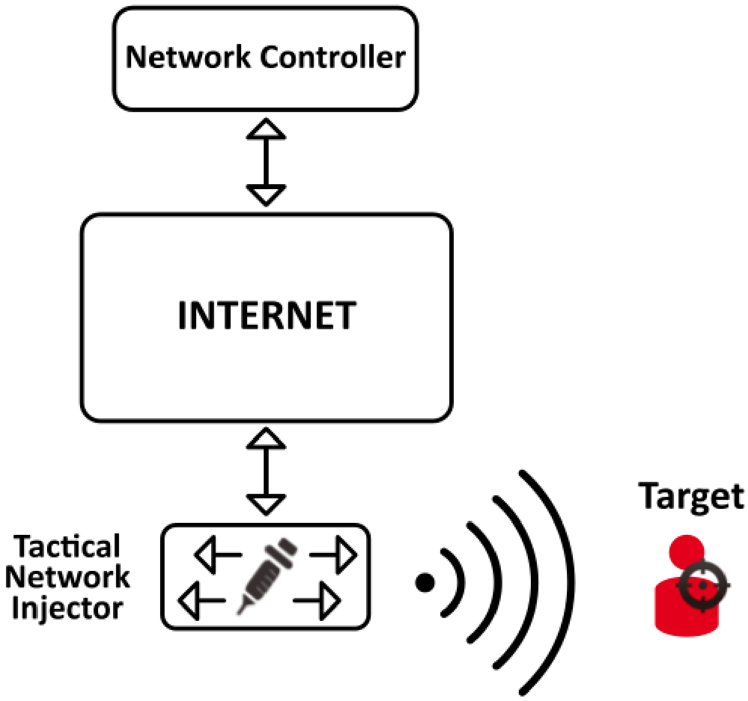


Figure 1: Tactical Network Injector: access point emulation diagram

Tactical Control Center installation

Introduction

Tactical Control Center is normally already installed and set on the Tactical Network Injector notebook.

It can be re-installed on a notebook using a restore disk.

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

Tactical Control Center features

Tactical Control Center lets you:

- crack protected WiFi network passwords
- simulate a WiFi network to attract target devices
- automatically identify connected devices using the rules and infect them
- manually identify connected devices using the rules and infect them

Package content

The package includes a notebook and installation CD.

The full installation sequence is provided below:

Step	*Action*	*Paragraph*
1	Install and set up the operating system and create the Tactical Control Center object from the RCS Console.	*"Operating system installation and settings" below*
2	Set Network Injector.	*"Network Injector settings" on page 51*

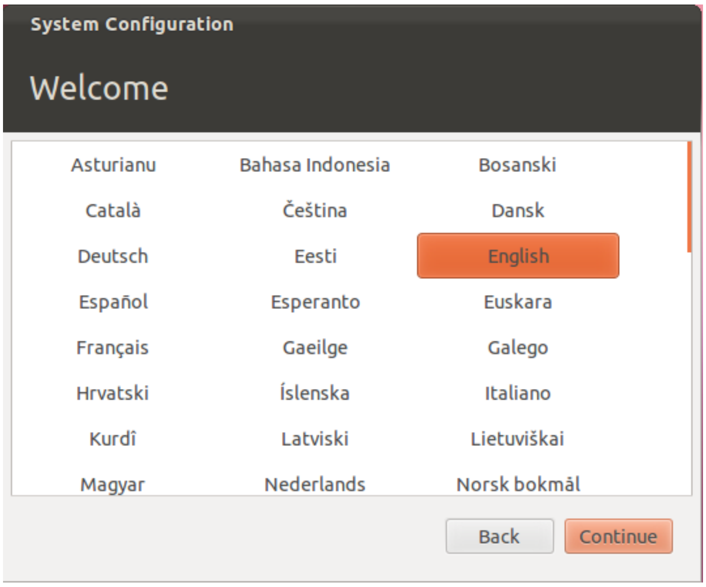
Operating system installation and settings

The procedure is described below:

Steps	*Result*
1. Connect the notebook to the network via Ethernet cable and insert the installation CD: the operating system is installed and the notebook turns off when completed. IMPORTANT: the computer must remain connected to the internet during the entire installation process.	-
2. Reboot the notebook; enter the *passphrase* to unlock the encrypted disk. The passphrase for first boot is "firstboot".	-

Steps ***Result***

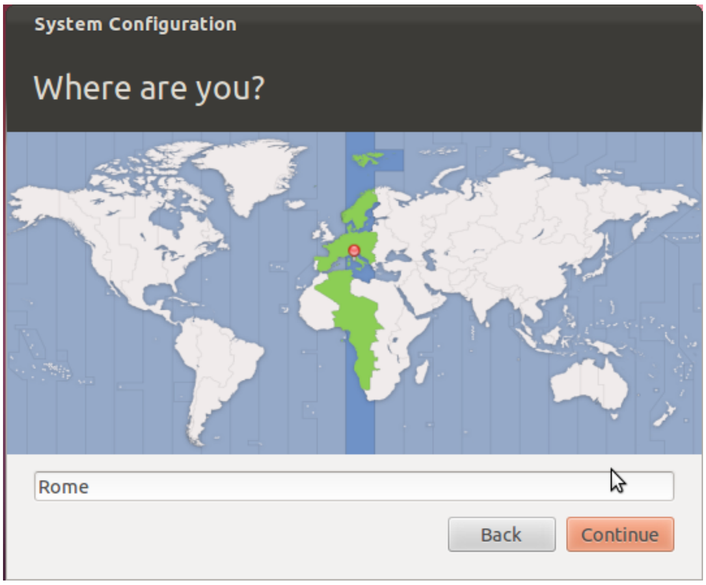
3. The first setup window appears.
4. Select the language.



System Configuration

Welcome

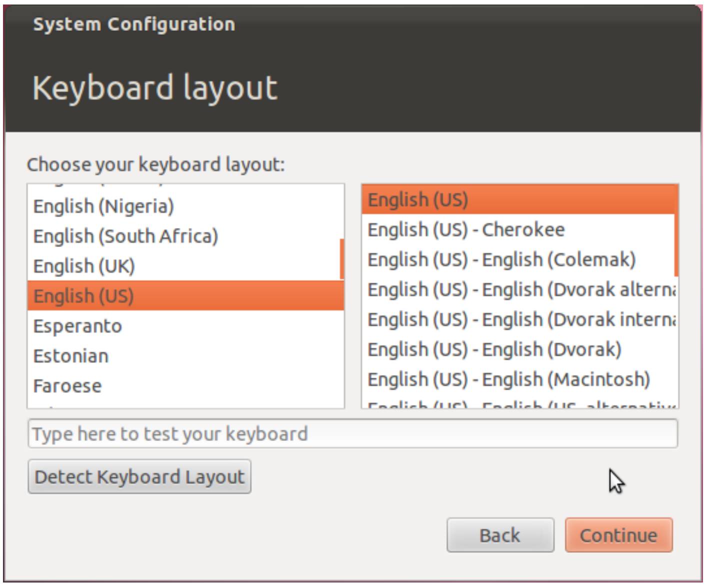
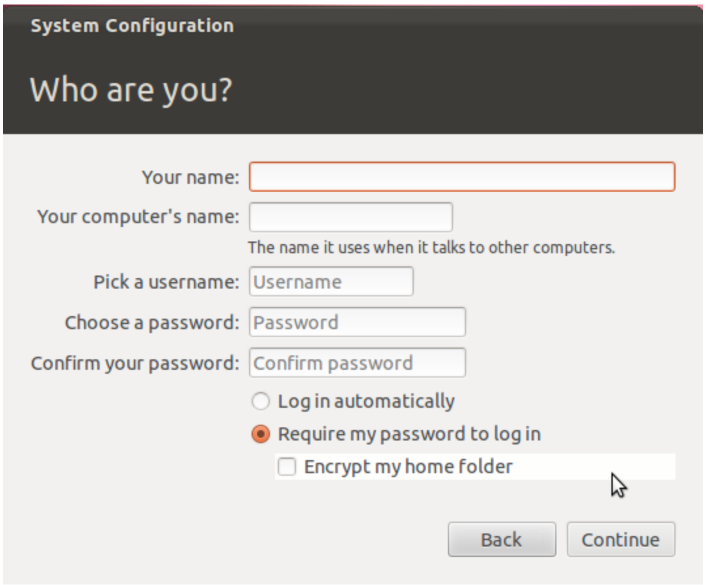
5. Select the correct time zone.



System Configuration

Where are you?

Rome

Steps	*Result*
6. 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 altern English (US) - English (Dvorak intern English (US) - English (Dvorak) English (US) - English (Macintosh) Type here to test your keyboard Detect Keyboard Layout Back Continue
7. 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
8. The standard login page appears at the end of operating system installation.	-

IP address check

To check all addresses, open RCS Console, **System** section, **Network Injector** and view data for each Network Injector. *See "**Managing the Network Injector**" on page 100*

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 100

Network Injector settings

Introduction

Network Injector must be set up to allow the technician to create sniffing and injection rules and to include the device in Network Controller polling. Once installed and set up, the Network Controller polls the Network Injector status every 30 seconds.

Adding a Network Injector

To complete Network Injector installation:

Step	*Action*
1	From **RCS Console,** in the **System** section, click **Frontend**, **New Injector**.
2	Enter the required data and click **Save.** **Result**: Network Injector appears in the list. RCS connects to Network Injector and checks operations. A monitoring object appears in the **Monitor** section for the added Network Injector.
3	Check Network Injector status in the **Monitor** section.

Network Injector data

Selected Network Injector data is described below:

Data	*Description*
Name **Description**	User's descriptions.
Version	Software version. To view the software versions of all the components *see "System monitoring (Monitor)" on page 103* .
Address	Device IP address.
Port	4444. To view all ports to be opened on the firewall *see "Ports to be opened on the firewall" on page 14*

Data	*Description*
Monitor via NC	If enabled, Network Controller acquires the Network Injector status every 30 seconds. If not enabled, Network Injector continues sniffing and injection operations, but the Network Controller does not check its status. Used when connections to Network Injector are down for any reason once installed at ISP, or for tactical use.
Log	Last messages logged. NOTE: Tactical Network Injector log updates depend on the frequency with which the operator enables synchronization. To view log file content *see "System logs" on page 74* . : update the list. : delete viewed logs.

Editing settings

The IP address already set on the device is simply indicated in RCS Console. If changed, Network Injector must be re-installed *see "Network Injector Appliance installation" on page 42* , and IP address changed in RCS Console.

Additional component installation in distributed architecture

Introduction

Installation in distributed architecture lets you add Shard databases (larger data volumes) and Collectors (one for each Anonymizer chain).

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 in distributed architecture" on page 22 .

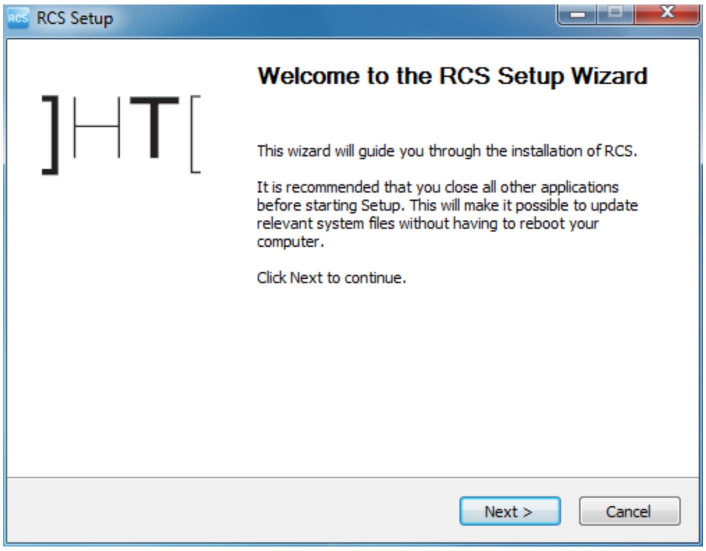
Installation sequence

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 redirecting on each Collector.	*same server or other computer*
7	Check for the installed objects in the **System**, **Backend** and **Frontend** sections.	*RCS Console*

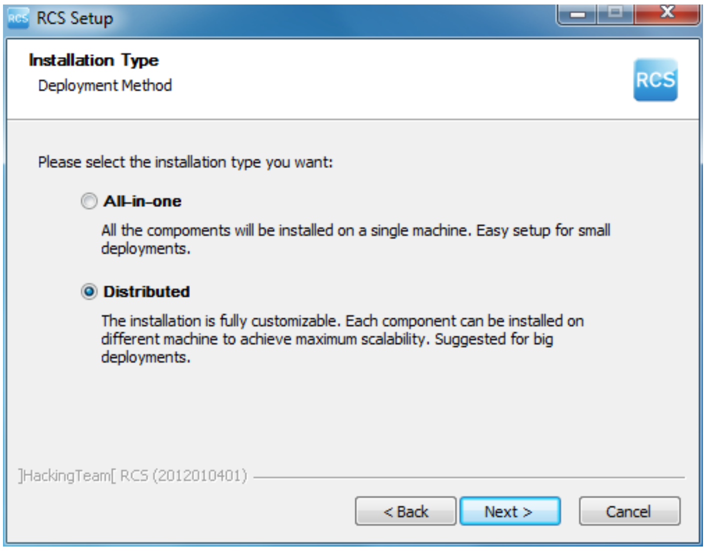
Additional Shard database installation

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.

Steps	*Result*

3. Select **Distributed.**
4. Click **Next**.



Installation Type

Deployment Method

Please select the installation type you want:

○ **All-in-one**

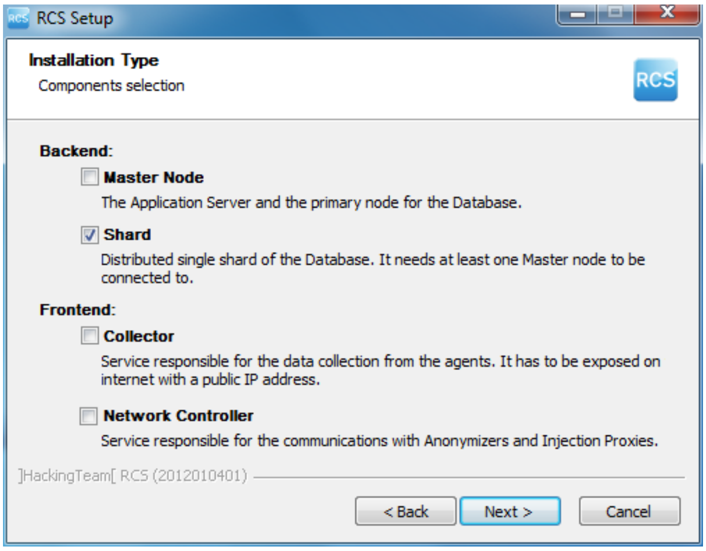
All the components will be installed on a single machine. Easy setup for small deployments.

● **Distributed**

The installation is fully customizable. Each component can be installed on different machine to achieve maximum scalability. Suggested for big deployments.

]HackingTeam[RCS (2012010401)

5. Select **Shard.**
6. 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. It has to be exposed on internet with a public IP address.

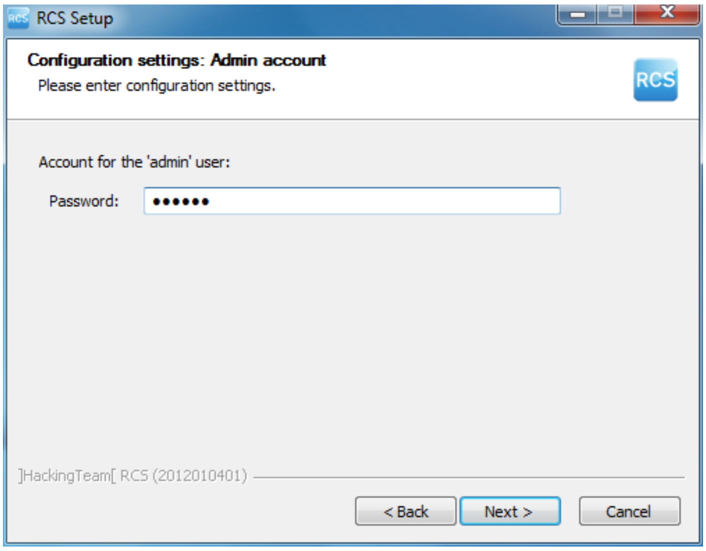
□ **Network Controller**

Service responsible for the communications with Anonymizers and Injection Proxies.

]HackingTeam[RCS (2012010401)

Steps ***Result***

7. Enter the system administrator's password.
8. Click **Next**: when installation has completed, services are started and are ready to receive data and communicate with the RCS Console.



Configuration settings: Admin account

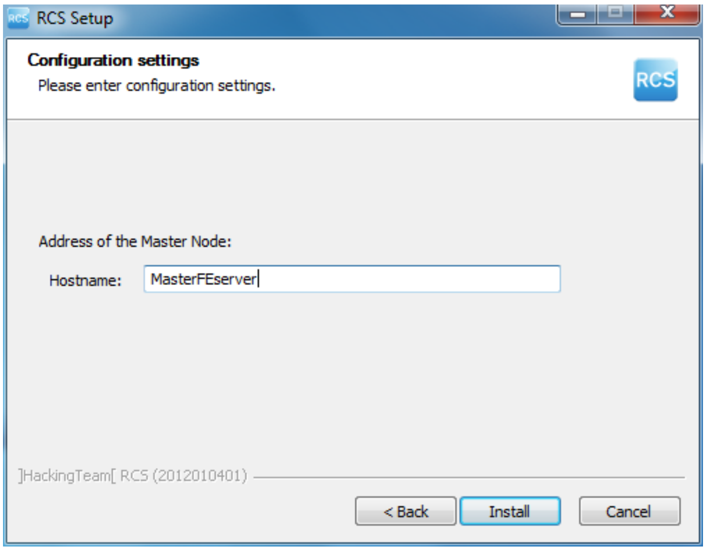
Please enter configuration settings.

Account for the 'admin' user:

Password: ••••••

]HackingTeam[RCS (2012010401)

9. Enter the Master Node server name or IP address (i.e.: **RCSMasterNode**).
10. Click **Install**: 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:

Hostname: MasterFEserver

]HackingTeam[RCS (2012010401)

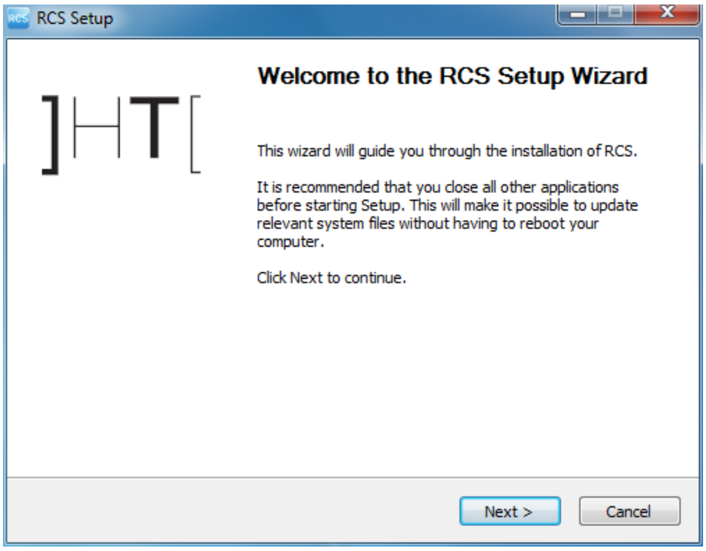
NOTE: if the server name or IP address needs to be changed after installation due to faults *see "**Editing Master Node settings**" on page 69 .*

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**.



RCS Setup

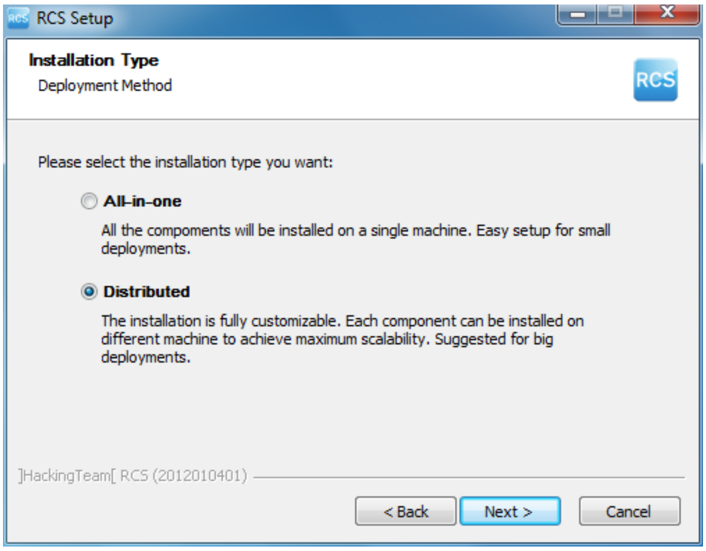
Welcome to the RCS Setup Wizard

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 **Distributed.**
4. Click **Next**.



RCS Setup

Installation Type

Deployment Method

Please select the installation type you want:

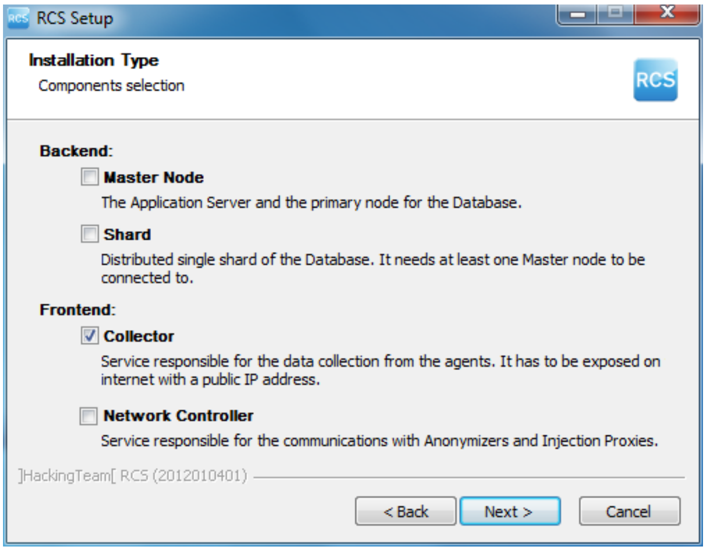
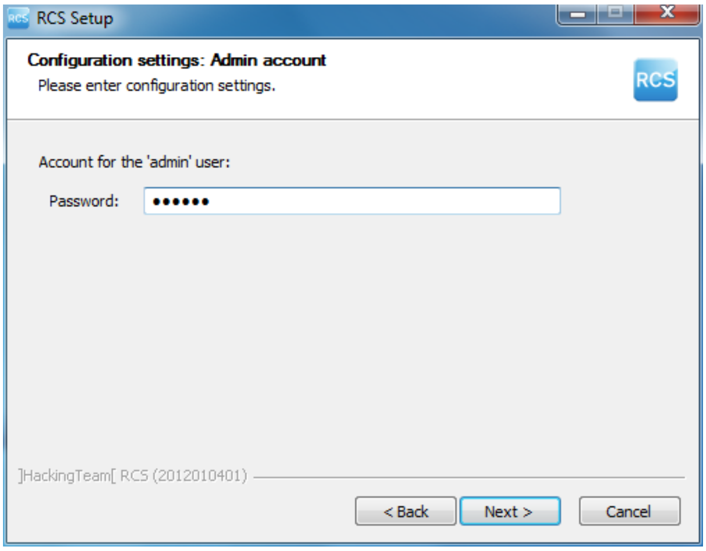
○ **All-in-one**

All the components will be installed on a single machine. Easy setup for small deployments.

● **Distributed**

The installation is fully customizable. Each component can be installed on different machine to achieve maximum scalability. Suggested for big deployments.

]HackingTeam[RCS (2012010401)

Steps	***Result***
5. Select **Collector.** 6. Click **Next**.	
7. Enter the system administrator password indicated in Master Node installation. 8. Click **Next**: installation is launched.	

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. It has to be exposed on internet with a public IP address.

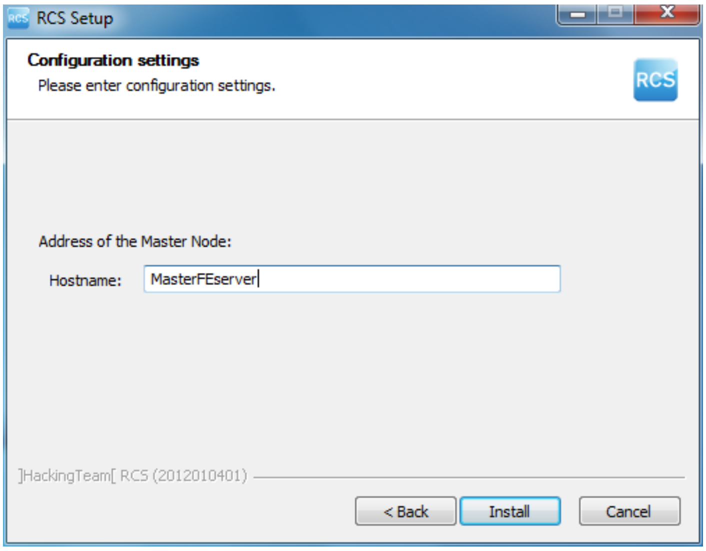
□ **Network Controller**
Service responsible for the communications with Anonymizers and Injection Proxies.

RCS Setup

Configuration settings: Admin account
Please enter configuration settings.

Account for the 'admin' user:

Password: ••••••

Steps	*Result*
9. Enter the Master Node server name or IP address (i.e.: **RCSMasterNode**). 10. Click **Install**: 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: Hostname: MasterFEserver]HackingTeam[RCS (2012010401)

Checking service start

Make sure all RCS services are up and running. If services are not running, manually start them.

*See "**List of started RCS services**" on page 29*

Checking Collector redirecting

To check whether Collector installation was successfully completed:

If	*Then*
on the server	• open a browser • enter `localhost` • **Result**: the browser must be redirected to Google.
on another computer	• open a browser • enter `http://<front end server name or IP address>`. • **Result**: the browser must be redirected to Google.

Tip: you can edit redirecting or create a custom page. To do this, edit page `decoy.html`.

*See "**Files installed at the end of installation**" on page 35*

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 38*

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 94 .

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

6

Routine maintenance and software updates

Presentation

Introduction

Routine maintenance includes RCS updates and operations scheduled or indicated by support service for system performance upkeep.

⚠ **WARNING: lack of maintenance may cause unforeseeable system behavior.**

Content

This section includes the following topics:

What you should know about RCS maintenance

Receiving updates

Support service publishes the update package on the support portal for every RCS software release. The package can be linked to a new license file that may be required during the update procedure.

Download the package and complete the update procedures.

Updating machine behavior

During updates, normal system service may not be guaranteed.

All data normally received and managed by the updating machine are kept for the required period of time and automatically retrieved as soon as the system resumes normal operations.

Routine maintenance procedures

Introduction

Procedure recommended to keep system performance high are provided below.

WARNING: lack of maintenance may cause unforeseeable system behavior.

Check and delete log files

Purpose: check the amount of log files and delete the older ones to avoid occupying excessive disk space.

Suggested frequency: depends on the amount of agents being monitored. Checking disk space once a month may be sufficient.

Checking available backup disk space

Purpose: routinely check the backup disk based on the quantity and frequency of backups set in the **RCS Console System** section.

Recommended frequency: depends on backup frequency and size.

Linux operating system updates

Purpose: keep Linux operating systems installed on the VPS that host Anonymizers and Network Injectors constantly updated.

RCS server update

Update requirements

CAUTION: fully backup before proceeding with an update.See "Backup management" on page 94

Update methods

Once the installer is launched, it identifies machine components and suggests automatic update. The procedure is thus identical in both All-in-One and distributed architecture.

RCS server(s) update

IMPORTANT: the hardware key must always be inserted in the server.

To update RCS, repeat the following steps for each server:

Step	*Action*
1	Run the `rcs-<version>.exe` installation file: the list of installed components that will be automatically updated appears. Click **Next**.
3	Select the new license file from the installation package. Click **Next**.

RCS Console update

Update requirements

No data is saved in RCS Console. The software can thus be updated without any special precaution.

RCS Console update

The console is automatically updated by the server, if necessary, after each login.

As an alternative, repeat the installation procedure using the files in the new installation package.

See "RCS Console installation " on page 30

Anonymizer update

Update requirements

No data is saved in Anonymizers. The software can thus be updated without any special precaution.

Anonymizer update

Repeat the installation procedure using the files in the new installation package.

IMPORTANT: keep the Linux operating system updated

See "Anonymizer installation and settings" on page 38

Network Injector Appliance update

Introduction

There are three ways to re-install Network Injector Appliance:

- fully, including the operating system, *see "Full Network Injector Appliance update" below* .
- partially, saving data, with a current infection and with the Appliance Control Center application closed,*see "Partial update with current infection and Appliance Control Center closed" on the facing page* .
- partially, saving data, without a current infection and with a closed Appliance Control Center update request,*see "Partial update without current infection and with Appliance Control Center open" on the facing page*

Full Network Injector Appliance update

CAUTION: updating deletes all data on the machine.

To fully re-install Network Injector Appliance:

Step	*Action*
1	Insert the installation CD and boot from CD: disk content will be deleted and both the operating system and Network Injector files will be re-installed. This procedures takes about 20 minutes.
2	Reboot the server: the procedure must be confirmed. ***CAUTION: the entire hard disk will be deleted.*** **Result**: Network Injector Appliance is installed.
4	From RCS Console, **System** section, **Network Injector** send rules to the updated Network Injector. *See "Managing the Network Injector" on page 100*
5	From RCS Console, **Monitor** section, check Network Injector status.

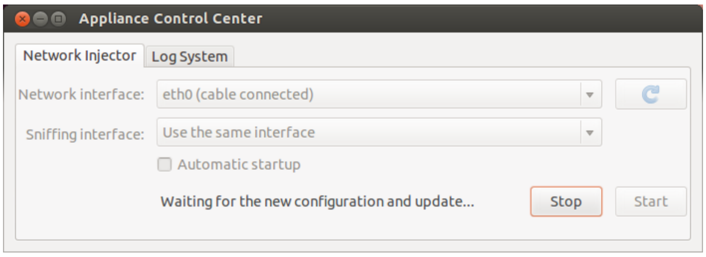
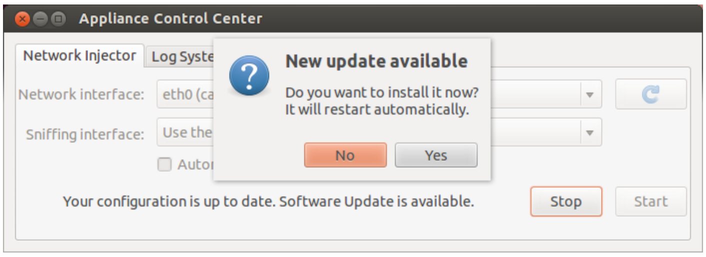
Partial update with current infection and Appliance Control Center closed

These are the updating steps with a current infection and the Appliance Control Center interface closed:

Phase	*Description*
1	The RCS console sends the update to network appliance
2	The current infection receives the update and automatically installs it. When the update is completed, the infection is restarted with the updated software.

Partial update without current infection and with Appliance Control Center open

These are the updating steps without a current infection and with an Appliance Control Center interface update request:

Step	*Action*
1. Open Appliance Control Center	-
2. Click **Config** and wait for the update to complete	 Appliance Control Center Network Injector | Log System Network interface: eth0 (cable connected) Sniffing interface: Use the same interface □ Automatic startup Waiting for the new configuration and update... Stop | Start
3. If an update was sent by the console, a message appears to request installation permission. NOTE: if the update is not installed, it will be automatically installed at the next infection start or an installation authorization request at next Appliance Control Center reboot will appear.	 Appliance Control Center Network Injector | Log Syste Network interface: eth0 (ca Sniffing interface: Use the □ Autor New update available Do you want to install it now? It will restart automatically. No | Yes Your configuration is up to date. Software Update is available. Stop | Start
4. Install the update.	
5. When the update is completed, Appliance Control Center reboots.	-

Tactical Network Injector update

Introduction

There are two ways to re-install Tactical Network Injector:

- fully, including the operating system, *see "Full Tactical Network Injector update " below* .
- partially, saving data, without a current infection and with a closed Appliance Control Center update request,*see "Partial update without current infection and with Appliance Control Center open" below*

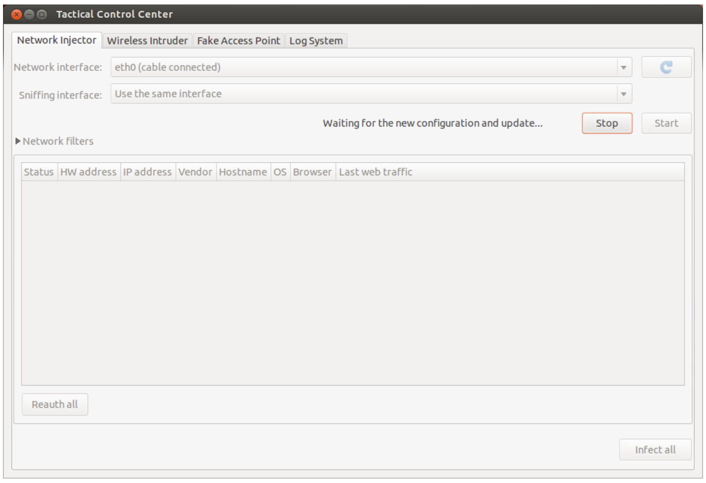
Full Tactical Network Injector update

CAUTION: updating deletes all data on the machine.

Tactical Network Injector is updated from a CD or installation file distributed by HackingTeam support service.

Partial update without current infection and with Appliance Control Center open

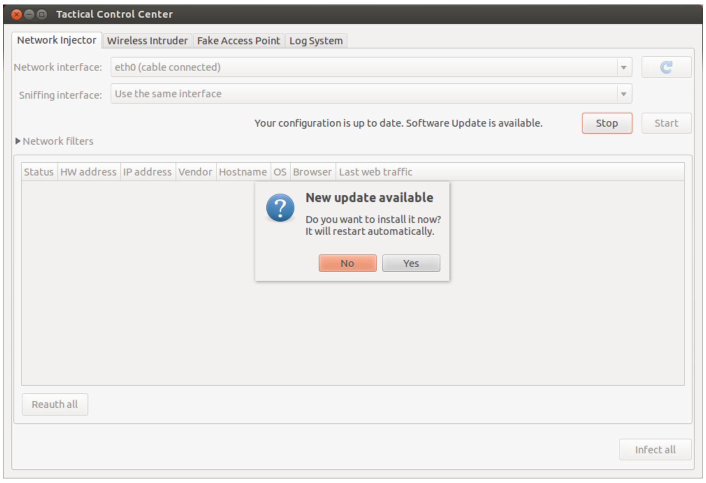
These are the updating steps without a current infection and with an Appliance Control Center interface update request:

Step	*Action*
1. Open Appliance Control Center	-
2. Click **Config** and wait for the update to complete	

Network interface: eth0 (cable connected)

Sniffing interface: Use the same interface

Waiting for the new configuration and update...

Step	***Action***
3. If an update was sent by the console, a message appears to request installation permission. NOTE: if the update is not installed, an installation authorization request will appear the next time Appliance Control Center is booted.	 Your configuration is up to date. Software Update is available. **New update available** Do you want to install it now? It will restart automatically. Tactical Control Center Network Injector Wireless Intruder Fake Access Point Log System Network interface: eth0 (cable connected) Sniffing interface: Use the same interface Stop Start Network filters Status HW address IP address Vendor Hostname OS Browser Last web traffic No Yes Reauth all Infect all
4. Install the update.	
5. When the update is completed, Appliance Control Center reboots.	-

7

Editing Master Node and Collector settings

Presentation

Introduction

Component settings can be edited after installation if needed.

Content

This section includes the following topics:

What you should know about settings

What you can edit

The following Master Node Collector installation data can be edited:

- the Master Node name/IP address
- System administrator's password
- backup folder
- The outgoing mail server to send alert e-mails

When to edit settings

The name/IP address or password may need to be changed when servers are replaced or simply due to incorrect data entry during installation.

IMPORTANT: specifying a different backup folder, for example on a remote device, is highly recommended to protect backup data.

Order used to edit settings

Since the server where Master Node is installed is the system "master", the following order must be followed to change the installation:

1. Change the Master Node name/IP address or password
2. Inform the Collector of the new Master Node name/IP address or password

Mail server settings

The RCS system can be set to send e-mail when the first pieces of evidence is received from a target. E-mail addressees must have Analyst privileges and belong to the alerting group set for that operation.

To do this, set the sender settings of the outgoing mail server and, especially, the required authentication level.

*See "**Setup utilities**" below*

Setup utilities

RCS utilities

Setup is run through some utilities in the Windows command prompt in folder C:\RCS\DB\bin or C:\RCS\Collector\bin (based on the type of installation).

Component setup utilities include:

- for Master Node: **rcs-db-config**
- for Collector: **rcs-collector-config**

NOTE: The RCS settings procedure in All-in-One architecture is identical to the RCS one in distributed architecture.

Utility command syntax

Utility command syntax is the following:

```
> rcs-db-config -x AAA
> rcs-collector-config -x AAA
```

Where:

- -x: selected option
- AAA: entered value

Other options

For prompt diagnostics, support service can request additional commands be launched. For the correct syntax, enter:

```
> rcs-db-config --help
> rcs-collector-config --help
```

Service call: only use the other options if indicated by support service.

Tip: syntax "-x" is the short version of syntax "--xxxxx": "`rcs-db-config -n`" is the same as "`rcs-db-config --CN`"

Editing Master Node settings

From folder C:\RCS\DB\bin or C:\RCS\Collector\bin (based on the type of installation) enter the following commands:

To edit...	*Enter...*

the Master Node name/IP address	`> rcs-db-config -n <name> -g`
	or
	`> rcs-db-config -n <IPaddress> -g`
	Result : certificates are updated and appear in folder \RCS\DB\config\certs. Collector settings must also be edited. *See "**Editing the Collector configuration**" on next page*

To edit...	***Enter...***
the System administrator's password (admin)	`> rcs-db-config -R <password>` **Result** : certificates are updated and appear in folder \RCS\DB\config\certs. Collector settings must also be edited. *See "**Editing the Collector configuration**" below*
backup folder	`> rcs-db-config -B <folder>` NOTE: "<folder>" can be a path for the `RCS\db` folder or absolute path. IMPORTANT: any backup files in the previously set folder will be copied to the new one. **Result**: all subsequent backup files are saved in the new folder. Tip: a remote device can be installed in an NTFS folder using Windows **Disk Manager**: this way, a remote disk can be used for backup.

outgoing mail server settings for alert e-mails	`> rcs-db-config -M -server <hostName>:<portNumber>`
	to set the outgoing main server name and port to be used.
	`> rcs-db-config -from <senderEmail>`
	to set the alert e-mail sender's e-mail (i.e.: "alert@myplace.com").
	`> rcs-db-config -user <userName>`
	To set the e-mail sender's user name.
	`> rcs-db-config -pass <password>`
	To set his password.
	`> rcs-db-config -auth <authenticationType>`
	To set the type of authentication to be used ("plain", "login" or "cram_md5").

Editing the Collector configuration

From folder C:\RCS\DB\bin or C:\RCS\Collector\bin (based on the type of installation) enter the following commands:

To...	*Enter...*

communicate the new Master Node name/IP address	`> rcs-collector-config -d <name> -u admin -p <password> -t`
	or
	`> rcs-collector-config -d <IPaddress> -u admin -p <password> -t`
	IMPORTANT: "<password>" must match the one used to login to Master Node.
	Result: certificates are restored in folder \RCS\DB\config\certs.

Settings check

Previous and current settings can be checked using RCS utilities.
To check previous and current settings, launch the relevant utilities without any option:

```
> rcs-db-config
> rcs-collector-config
```

Example of settings check output

An example of a check is given below:

```
Current configuration:
{"CA_PEM"=>"rcs.pem",
"DB_CERT"=>"rcs-db.crt",
"DB_KEY"=>"rcs-db.key",
"LISTENING_PORT"=>443,
"HB_INTERVAL"=>30,
"WORKER_PORT"=>5150,
"CN"=>"172.20.20.157",
"BACKUP_DIR"=>"backup",
"PERF"=>true,
"SMTP"=>"mail.abc.com:25",
"SMTP_FROM"=>"alert@abc.com",
"SHARD"=>"shard0000"}
```

8

Troubleshooting

Presentation

Introduction

RCS is a system where the greatest focus must be on collected data transmission, decoding and saving. RCS design focuses on preventing any data loss and quickly managing potential errors that may occur.

Content

This section includes the following topics:

Potential faults

Potential installation faults

Following is a list of potential faults that may occur during installation and references to recommended actions:

If...	*Then...*
installation does not progress	make sure the hardware key is correctly inserted.
RCS console cannot connect to the server	• Make sure you logged in with the System administrator's name, password and name of the server where Master Node was installed. or • connect from the browser with "https://<serverName>" or "https://<backendServerName>" • The browser inspects the HTTPS certificate and returns some addresses to find out what went wrong.

Possible server problems

Following is a list of potential faults that may occur during product use and references to recommended actions:

If	*And*	*Then*
cannot connect to Master Node	the hardware key is correctly inserted but Master Node service does not start	• *check Master Node service status* • *request hardware key replacement.*
data no longer arrives from agents	from RCS Console the Collector is running and correctly communicates	*check Collector status.*
The Master Node is not available	The Collector is running	• *check whether an update is in progress* • *check the Collector log file*
images are not converted into text	the OCR module is installed	*check how slow in the module log and install another OCR module (if in distributed architecture).*
The Collector is not available	-	*restart RCScollector service.*

If	*And*	*Then*
data is queued in the Master Node	the most recent data does not appear on RCS	*check Worker service status for Master Node and for the other Shards.*
Network Controller indicates an error		*Connect to the machine where Network Injector or Anonymizer is installed and check the log file.*

Potential backup problems

Following is a list of potential faults that may occur during backup and references to recommended actions:

If	*And*	*Then*
backup status is **error**	-	check available disk space and manually restart backup.

To learn more

To check component status *see "Component status check procedure" on page 76*

To restart services *See "Service restart procedures " on page 77*

System logs

Introduction

Each RCS component generates daily logs that help to analyze possible fault or error causes. Analyzing file content lets you review RCS operations step by step and understand any error cause (i.e.: service starts but immediately stops, service started but with incorrect deploy.htm page redirect).

Log analysis utility

The reasons that can lead to log analysis are provided below:

Component	*Analysis reason*
Master Node	Check problems with RCS Console.
Collector	Check data reception from agents.
OCR module	Check for any slowed indexing in exported content.
Translate module	Check for any slowed content translation.
Network Controller	In the event of doubts on Network Injector or Anonymizer status.

Component	*Analysis reason*
Network Injector	Check completed operations.
Anonymizer	Check incoming data flow from agents.

Log file example

The log file name has the following syntax: `<component> yyyy-mm-dd.log` (i.e.: `rcs-dbdb 2012-02-04.log`)

RCS log files

Log files generate by components in full installation are provided below:

Component	*Folder*
Master Node	C:\RCS\DB\log
Collector	C:\RCS\Collector\log
OCR module	C:\RCS\DB\log
Translate module	C:\RCS\DB\log
Network Controller	C:\RCS\Collector\log
Network Injector	/var/log/syslog
Anonymizer	/var/log

WARNING: the lack of log files indicates incomplete installation.

Quick log display

BareTail, an application that lets you immediately view the content of several log files, is included in the RCS installation.

To run BareTail, enter:

```
> rcs-db-log
```

Log file content

Each record is identified by one of the following levels of severity:

Severity level	*Description*
Fatal	RCS is not running and requires service (i.e.: no settings, no certificates).

Severity level	*Description*
Error	There is a component error but RCS can guarantee main service coverage (i.e.: Master Node not running).
Debug	(only appears if enabled upon support service indication, increases and provides more details on log records to resolve problems).
Info	information note.

Component status check procedure

Introduction

Typical procedures on how to check hardware and software status are provided below.

Installed license check

Check all licenses installed in RCS, including updates.

Command

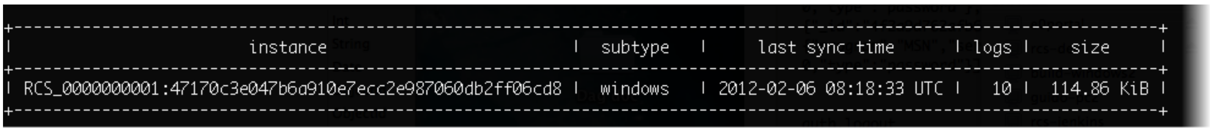
In folder C:\RCS\DB\bin enter **rcs-db-license**

Master Node status check

Make sure Master Node is routinely communicating data to databases via Worker services.

Command

In folder C:\RCS\DB\bin enter **rcs-db-evidence-queue.**
Result: an example is provided below .



```
+-------------------------------------------------------------------------------------------------------------------+
|                        instance                         | subtype   |     last sync time      | logs |    size    |
+-------------------------------------------------------------------------------------------------------------------+
| RCS_0000000001:47170c3e047b6a910e7ecc2e987060db2ff06cd8 | windows   | 2012-02-06 08:18:33 UTC |   10 | 114.86 KiB |
+-------------------------------------------------------------------------------------------------------------------+
```

What to check

If the *logs* and *size* values begin to significantly increase, this may be due to Worker service that is not running. Check status on each Worker service.

Checking Worker service status

Make sure that Worker service is correctly running to decode and save data in databases.

What to check

In folder C:\RCS\DB\log check log rcs-worker*.log logs

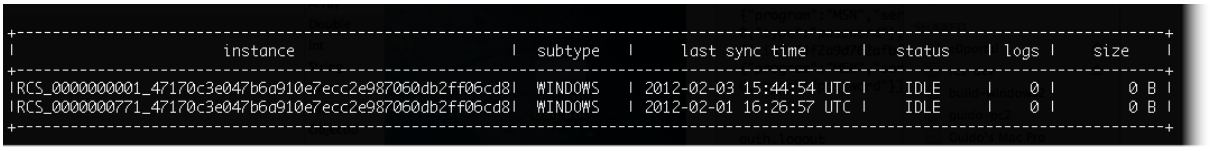
Check agent status via Collector

Make sure agents are routinely communicating their status to RCS via Network Controller and that they are sending their data to Collector. Agent data may be lost in the event of a persistent Collector fault.

Command

In folder C:\RCS\Collector\bin enter **rcs-collector-status**

Result: the Collector status report appears



```
+-----------------------------------------------------------------------------------------------------------+
|                        instance                        | subtype  |     last sync time      | status | logs |    size  |
+-----------------------------------------------------------------------------------------------------------+
|RCS_0000000001_47170c3e047b6a910e7ecc2e987060db2ff06cd8| WINDOWS  | 2012-02-03 15:44:54 UTC |  IDLE  |    0 |      0 B |
|RCS_0000000771_47170c3e047b6a910e7ecc2e987060db2ff06cd8| WINDOWS  | 2012-02-01 16:26:57 UTC |  IDLE  |    0 |      0 B |
+-----------------------------------------------------------------------------------------------------------+
```

What to check

The *Last sync time* must be as recent as possible, compatible with the set synchronization methods for each agent: a recent *Last sync time* indicates that agents correctly communication with Collector. If *Last sync time* is not recent, wait for any other synchronizations to check whether it is updated. Alternatively, check Collector logs to see whether there are synchronization attempts: in this case inform support service.

The logs value must be minimum since it is the data saved by the Collector awaiting to be sent to Master Node. If the value is high, this means that Master Node is not running or is not connected. Check Master Node service status.

The number of logs will decrease as soon as the connection is resumed.

Network Injector start check

Network Injector logs are normally saved in folder /var/log/syslog.

To learn more

To view logs *see "**System logs**" on page 74*

Service restart procedures

Introduction

Typical procedures on how to restart services are provided below.

Restarting RCSDB service

Purpose

In the event of faults, RCSDB service can be restarted using this utility instead of using the Windows Service Management function.

Command

The commands to start, stop and restart the service are given below in order:

- `> rcs-db-service start`
- `> rcs-db-service stop`
- `> rcs-db-service restart`

Restarting MongoDB service

Purpose

In the event of faults, MongoDB service can be restarted using this utility instead of using the Windows Service Management function.

Command

The commands to start, stop and restart the service are given below in order:

- `> rcs-mongo-service start`
- `> rcs-mongo-service stop`
- `> rcs-mongo-service restart`

Restarting Collector service

Purpose

In the event of faults, Collector service can be restarted using this utility instead of using the Windows Service Management function.

Command

The commands to start, stop and restart the service are given below in order:

- `> rcs-collector-service start`
- `> rcs-collector-service stop`
- `> rcs-collector-service restart`

Restarting Worker service

Purpose

In the event of faults, Worker service can be restarted using this utility instead of using the Windows Service Management function.

Command

The commands to start, stop and restart the service are given below in order:

- `> rcs-worker-service start`
- `> rcs-worker-service stop`
- `> rcs-worker-service restart`

Restarting Network Injector service

CAUTION: use SSH protocol for all installation, setup and data exchange operations to the remote unit.

Purpose

In the event of faults you can directly work on Network Injector and restart service.

Command

To restart the service with the same settings or new ones, open Appliance Control Center, reset if necessary and reboot the service by clicking **Restart**.

Restarting Anonymizer service

CAUTION: use SSH protocol for all installation, setup and data exchange operations to the remote unit.

Purpose

In the event of faults signaled on RCS Console you can directly work on the VPS server and restart service.

Command

To restart the service, enter the following command:

```
# /etc/init.d/rcsanon restart
```

To stop the service, enter the following command:

```
# /etc/init.d/rcsanon stop
```

IMPORTANT: command syntax refers to the Linux CentOS 6 operating system version.

Hardware component service procedures

Introduction

Typical hardware component service procedures to be used in the event of hardware faults are provided below.

Hardware key replacement

If the main hardware key stops working, it must be immediately replaced with the backup key, contained in the supplied package. Contact support service for a license file compatible with the backup key.

Instructions on how to replace and activate a new key are given below:

Phase	*Who*	*Does what*
1	the client	*Informs HackingTeam of the fault.*
2	HackingTeam	*sends a new license file linked to the backup hardware key.*
3	the client	*replace the main key with the backup key and start the procedure to assign the new license file.*
4	the client	*sends the faulty key to HackingTeam.*
5	HackingTeam	*replace the faulty key with a new backup key and send it to the customer.*

Master Node replacement

The recommended procedure is described below:

Step	*Action*
1	Restore a server, repeating all installation operations. *See "RCS server installation in All-in-One architecture" on page 18* or *"RCS server installation in distributed architecture" on page 22*
2	Select the most recent backup (full or metadata). If the most recent backup is metadata, full backup can be restored later. In fact, the backup is not destructive and supplements the information it has with that present, *See "What you should know about backup" on page 97*

Shard replacement

The recommended procedure is described below:

Step	*Action*
1	Repeat the entire installation procedure. *See "RCS server installation in distributed architecture" on page 22*
2	Restore the last full backup. *See "Backup management" on page 94*

Replacing the Collector/Network Controller

Repeat the entire installation procedure.

See "RCS server installation in distributed architecture" on page 22

Replacing an Anonymizer

Repeat the entire installation procedure.

See "Anonymizer installation and settings" on page 38

Replacing a Network Injector Appliance

Repeat the entire installation procedure.

See "Network Injector Appliance installation" on page 42

Replacing a Tactical Injector Appliance

Repeat the entire installation procedure.

See "Tactical Control Center installation" on page 47

9

RCS Console for the System administrator

Presentation

System administrator's role

The *System Administrator's* role is to:

- complete installation with Anonymizer, Network Injector and Backup settings
- check Shard database space
- check Collector, Anonymizer, Network Injector and other system component operations
- update system components
- manage backup
- resolve any problems

Enabled functions

To complete his/her assigned activities, the System administrator has access to the following functions:

- **System**
- **Monitor**

Content

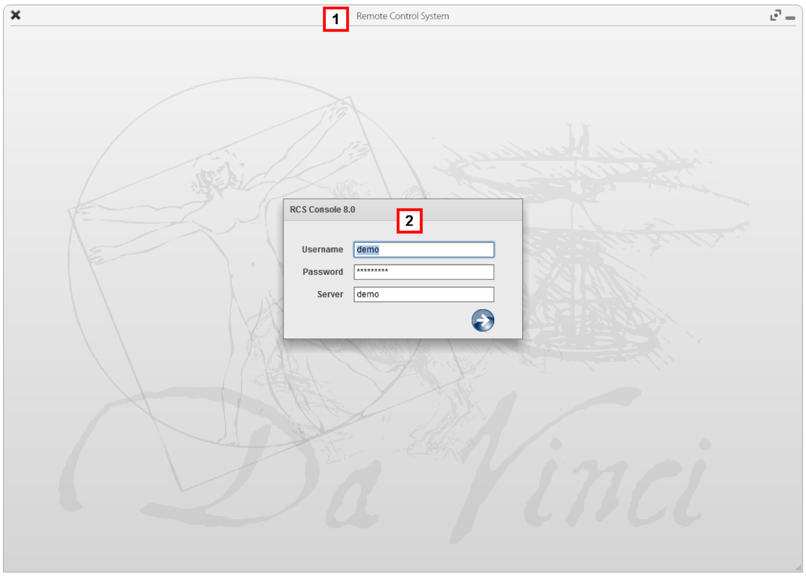
This section includes the following topics:

Starting the RCS Console

When started, RCS Console asks you to enter your credentials previously set by the Administrator.

What the login page looks like

This is what the login page looks like:



RCS Console 8.0

Username demo

Password *********

Server demo

Area	*Description*
1	Title bar with command buttons: ✖ Close RCS Console. ⧉ Expand window button. ▬ Shrink window button.
2	Login dialog window.

Open RCS Console

To open RCS Console functions:

Step	*Action*
1	In **Username** and **Password,** enter the credentials as assigned by the Administrator.
2	In **Server,** enter the name of the machine or server address to connect to.

Step	*Action*
3	Click : the homepage appears with the menus enabled according to your account privileges. *See "**Homepage description**" below* .

Homepage description

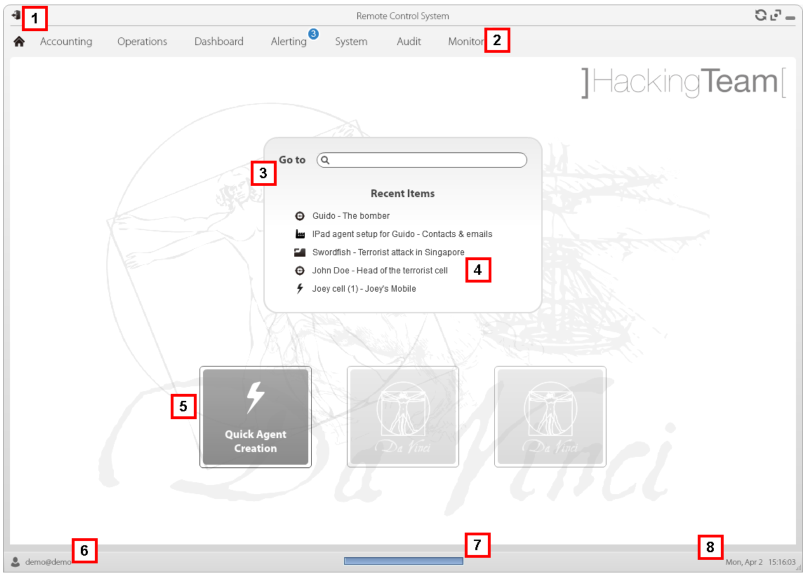
To view the homepage:	- click

Introduction

The homepage is displayed when the RCS Console is started, and is the same for all users. Enabled menus depend on the privileges assigned to the account.

What it looks like

This is what the homepage looks like, with recently opened items saved. For details on shared elements and actions:



Area	*Description*
1	Title bar with command buttons.
2	RCS menu with functions enabled for the user.
3	Search box to search operations, targets and agents, by name or description.

Area	*Description*
4	Links to last five opened elements (operation, target and agent).
5	Wizard buttons.
6	Logged in user with possibility of changing the language and password.
7	Download area with ability to view progress during export or compiling.
8	Current date and time with possibility of changing the time zone.

Wizards in the homepage

To view the homepage:

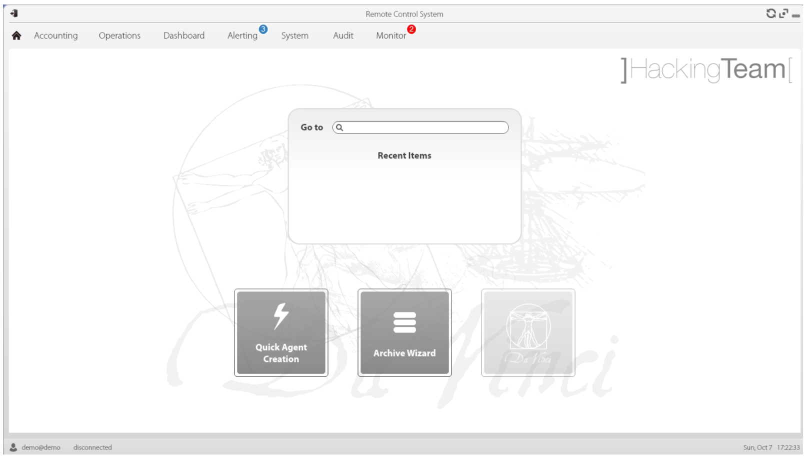
- click 🏠

Introduction

For users with certain privileges, RCS Console displays buttons that run wizards.

What it looks like

This is how the homepage is displayed with enabled wizards:



Button	*Function*
Investigation Wizard	Open the wizard to quickly create an agent. NOTE: the button is only enabled for users with Administrator and Technician privileges.

Button	***Function***
Archive Wizard	Open the wizard to quickly save operation and target data. NOTE: the button is only enabled for users with Administrator and System Administrator privileges.
	Button not used.

Archive Wizard

This wizard lets you quickly manage open operation or target data to save and delete them from the database.

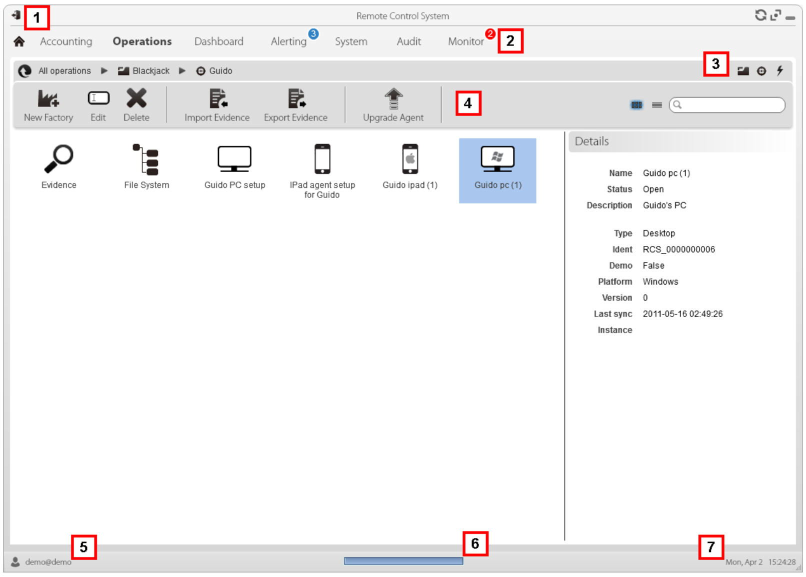
Shared interface elements and actions

Each program page uses shared elements and allows similar actions to be run.

For easier manual comprehension, elements and actions shared by some functions are described in this chapter.

What the RCS Console looks like

This is what a typical RCS Console page looks like. A target page is displayed in this example:



Name Guido pc (1)
Status Open
Description Guido's PC

Type Desktop
Ident RCS_0000000006
Demo False
Platform Windows
Version 0
Last sync 2011-05-16 02:49:26
Instance

Area	*Description*
1	Title bar with command buttons: ⇥ Logout from RCS. ↻ Page refresh button. ⤢ Expand window button. ▬ Shrink window button.
2	• ⌂ Return to homepage button • RCS menu with functions enabled for the user.
3	Operation scroll bar. Descriptions are provided below:

Icon	*Description*
◀	Back to higher level.
📁	Show the operation page.
⊕	Show the target page.
🏭	Show the factory page.
⚡	Show the agent page.

Area	*Description*
4	Buttons to display all elements regardless of their group membership. Descriptions are provided below:

Icon	*Description*
📁	Show all operations.
⊕	Show all targets.
⚡	Show all agents.

Area	*Description*
5	Window toolbar.
6	Search buttons and box:

Object	*Description*
John Doe	Search box. Enter part of the name to display a list of elements that contain the entered letters.
≡	Display elements in a table.
▦	Display elements as icons.

Area	*Description*
7	Logged in user with possibility of changing the language and password.

Area	*Description*
8	Download area with ability to view progress during export or compiling. Files are downloaded to the desktop in RCS Download folder. • top bar: percent generation on server • bottom bar: percent download from server to RCS Console.
9	Current date and time with possibility of changing the time zone.

Actions always available on the interface

Change interface language or password

To change the interface language or password:

Step	*Action*
1	Click **[6]** to display a dialog window with the user's data.
2	Change the language or password and click ✖ to confirm and exit.

Converting the RCS Console date-time to the actual time zone

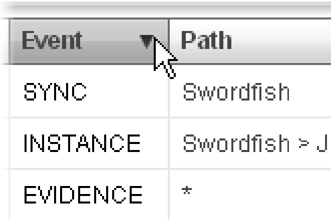
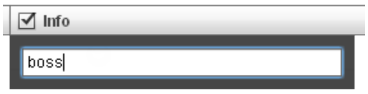
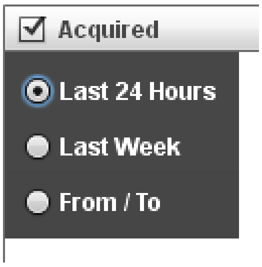
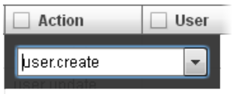
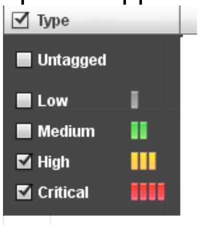
To convert all dates-times to the actual time zone:

Step	*Action*
1	Click **[8]** to display a dialog window with the current date-time: **UTC time**: Greenwich mean time (GMT) **Local time**: date-time where the RCS server is installed **Console time**: date-time of the console used that can be converted.
2	Change the time zone and click ✖ to confirm and exit: all displayed dates-times are converted as requested.

Table actions

The RCS Console displays various data in tables. Tables let you:

- sort data by column in increasing/decreasing order
- filter data by column

Action	***Description***
Sort by column	Click on the column heading to sort that column in increasing or decreasing order.  Event ▼ | Path SYNC | Swordfish INSTANCE | Swordfish > J EVIDENCE | *
Filter a text	Enter part of the text you are searching for: only elements that contain the entered text appear.  ☑ Info boss The example shows elements with descriptions like: - "my**boss**" - "**boss**anova"
Filter based on an option	Select an option: the elements that match the selected option appear.  ☑ Acquired ● Last 24 Hours ○ Last Week ○ From / To  □ Action | □ User user.create
Filter based on several options	Select one or more options: the elements that match all selected options appear.  ☑ Type □ Untagged □ Low □ Medium ☑ High ☑ Critical
Change the column size	Select the edge of the column and drag it.

Front end management

To manage the front end:
- System section, Frontend

Function scope

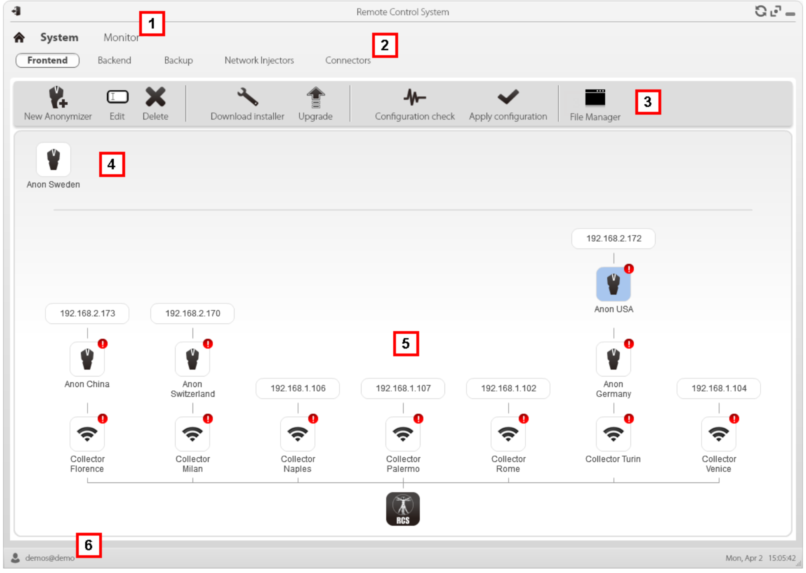
When RCS is running, this function lets you monitor the Anonymizers and Collectors, change the Anonymizer and chains settings and update the VPSes.

During installation, this function lets you create a new Anonymizer "object" that acts as the logical connection between the RCS Console and the software component to be installed on a VPS.

NOTE: the function is only enabled if the user has **Frontend management** authorization.

What the function looks like

This is what the page looks like:



Area	***Description***
1	RCS menu.
2	**System** menu.

<table>
<tr><th><em>Area</em></th><th><em>Description</em></th></tr>
<tr><td><strong>3</strong></td><td>Window toolbar.
Descriptions are provided below:
<table>
<tr><th><em>Icon</em></th><th><em>Description</em></th></tr>
<tr><td>+</td><td>Create a new Anonymizer.</td></tr>
<tr><td>▭</td><td>Edit Anonymizer data.
After editing, click <strong>Apply settings</strong>.
Show last logs.
Tip: double-click an Anonymizer to check/edit data.</td></tr>
<tr><td>✖</td><td>Delete an Anonymizer. This does not delete the Anonymizer installed on the VPS.</td></tr>
<tr><td>🔧</td><td>It generates the installer for the first Anonymizer installation and saves it on the desktop. Copy the file via SSH to the remote VPS and run it.</td></tr>
<tr><td>⬆</td><td>Update the Anonymizer software version from remote.</td></tr>
<tr><td>〰</td><td>Simulate agent behavior. It connects to each Anonymizer in the chain up to the gateway Collector, and returns connection results.</td></tr>
<tr><td>✓</td><td>Update settings on all Anonymizers. This command is used after adding, deleting or changing the Anonymizer chain in use.</td></tr>
<tr><td>▬</td><td>It shows packets automatically created on the Collector by <strong>Exploit, WAP Push and QR Code</strong> vectors made available for the target device. Files that are no longer used can be deleted.
⚠ <strong><em>CAUTION: deleting files too early could compromise infection by vectors.</em></strong>
ℹ NOTE: any files manually copied to the folder do not appear.</td></tr>
</table>
</td></tr>
<tr><td><strong>4</strong></td><td>Anonymizers set but not yet included in a chain.</td></tr>
</table>

Area	*Description*
5	Anonymizer chains on the system with the IP address of the last element. Possible conditions: : Anonymizer not in chain. : Anonymizer in chain and running. : Anonymizer not monitored by the Network Controller. : Anonymizer with faults. : Collector running. : Collector not running.
6	RCS status bar.

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 86* .
To install, edit or cancel an Anonymizer *see "**Anonymizer installation and settings**" on page 38* .

Adding an Anonymizer to the configuration

To add an Anonymizer *see "**Anonymizer installation and settings**" on page 38*

Editing Anonymizer settings

To edit Anonymizer settings *see "**Anonymizer installation and settings**" on page 38* .

File Manager data

Descriptions are provided below:

Field	*Description*
Time	Vector installation date-time on the device.
Name	File name created by the installer.
Factory	Factory that generated the installer.

Field	*Description*
User	User who created the installer.

Back end management

To manage back end:	• System section, Backend

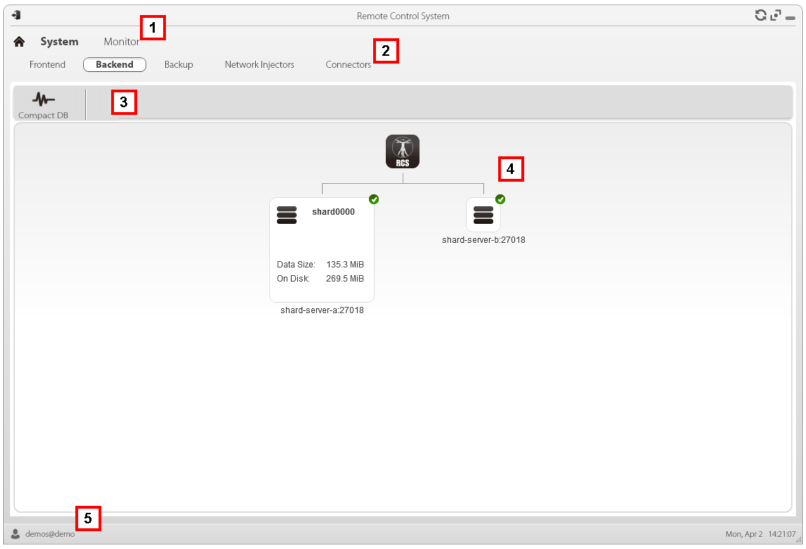
Function scope

When RCS is running, this function lets you check database status and available disk space.

NOTE: the function is only enabled if the user has **Backend management** authorization.

What the function looks like

This is what the page looks like:



Area	*Description*
1	RCS menu.
2	**System** menu.

<table>
<tr><th><em>Area</em></th><th><em>Description</em></th></tr>
<tr><td><strong>3</strong></td><td>Window toolbar. Descriptions are provided below:
<table>
<tr><th><em>Icon</em></th><th><em>Description</em></th></tr>
<tr><td></td><td>Zip the database.</td></tr>
</table>
</td></tr>
<tr><td><strong>4</strong></td><td>Shard database structures with their status, occupied and available disk space.
NOTE: database 0 is the one included in MasterNode.</td></tr>
<tr><td><strong>5</strong></td><td>RCS status bar.</td></tr>
</table>

To learn more

For interface element descriptions *See "**Shared interface elements and actions**" on page 86* .

For further information on backups *see "**What you should know about backup**" on page 97* .

Significant Shard database data

Selected Shard database data is described below:

Field	*Description*
Data Size	Occupied space.
On Disk	Total Shard device space.
<serverName>:<port>	Shard server port

Backup management

To manage backups:	• System section, Backup

Function scope

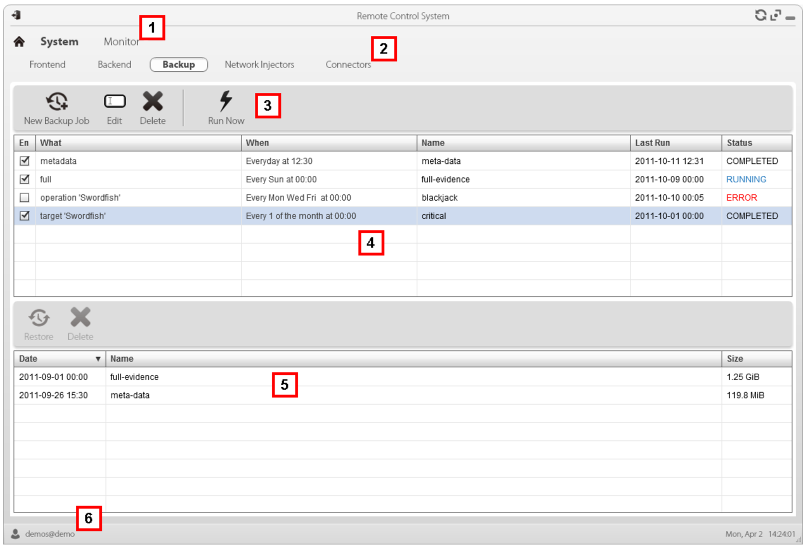
When RCS is running, this function lets you check the last backup status, create new backup processes or immediately run a backup process.

During RCS maintenance, this function lets you fix damaged data restoring them with a backup.

NOTE: the function is only enabled if the user has **System Backup&Restore** authorization.

What the function looks like

This is what the page looks like:



En	What	When	Name	Last Run	Status
☑	metadata	Everyday at 12:30	meta-data	2011-10-11 12:31	COMPLETED
☑	full	Every Sun at 00:00	full-evidence	2011-10-09 00:00	RUNNING
□	operation 'Swordfish'	Every Mon Wed Fri at 00:00	blackjack	2011-10-10 00:05	ERROR
☑	target 'Swordfish'	Every 1 of the month at 00:00	critical	2011-10-01 00:00	COMPLETED

Date	Name	Size
2011-09-01 00:00	full-evidence	1.25 GiB
2011-09-26 15:30	meta-data	119.8 MiB

Area	*Description*
1	RCS menu. See "Shared interface elements and actions"
2	**System** menu.
3	Backup process toolbar. Descriptions are provided below:

Icon	*Description*
	Add a backup process.
	Edit a backup process, for example, to disable it or change its frequency. **IMPORTANT: do not use this function to change the type of data processed. It is better to disable the process and create a new one with a matching name.**
✖	Delete a backup process. Does not delete the backup files generated by the process.
⚡	Run backup even if disabled.

Area	*Description*
4	List of programmed backup processes (enabled and non) with last backup status.

<table>
<tr><th><em>Area</em></th><th><em>Description</em></th></tr>
<tr><td><strong>5</strong></td><td>Backup toolbar. Descriptions are provided below:
<table>
<tr><th><em>Icon</em></th><th><em>Description</em></th></tr>
<tr><td>↻</td><td>Restore data from the selected backup file.
⚠ <strong><em>CAUTION: restoring data is a delicate operation. Make sure you have fully understood RCS' restore mechanisms.See "What you should know about backup" on next page</em></strong></td></tr>
<tr><td>✖</td><td>Deleting the backup file.</td></tr>
</table>
</td></tr>
<tr><td><strong>6</strong></td><td>List of completed backups.</td></tr>
<tr><td><strong>7</strong></td><td>RCS status bar.
<em>See "Homepage description" on page 84</em></td></tr>
</table>

Significant backup process data

The selected backup process data is described below:

Field	*Description*
Enabled	Enables/disables the backup process. Use to temporarily disable the process, for example, when replacing the backup device. Tip: to quickly enable/disable a process, flag the box in the **En** column in the list.
What	Data to be included in backup. **metadata**: the entire system configuration: database, Collector, Network Injector, Anonymizer, agent. This is the bare minimum required to restore the system in the event of disaster. All information required to collect agent information is contained in this type of backup. **full**: full backup of the system configuration and tapping data (operation and target). It may take a while to execute. **operation**: backup of the indicated operation, data included. **target**: backup of the indicated target, data included
When	Backup frequency. **UTC**: time zone.
Name	Name to be assigned to the backup.

What you should know about backup

Management responsibilities

The System administrator must protect logged data and set frequency for the various types of backups.

Backup methods

RCS saves all data in databases in the specified folder when editing RCS settings. *See "**Editing Master Node settings**" on page 69*

A backup can save one or more types of data. Backup types are:

- metadata
- full
- operation
- target

Metadata type backup

The metadata backup type is fast and saves the entire system configuration, allowing normal system operations to be quickly restored in the event of problems. This type of backup does not include collected evidence. Daily backup is recommended.

WARNING: agents installed on various devices may be lost without a recent metadata backup.

NOTE: the job that runs weekly metadata backup is set by default and enabled whenever the system is rebooted. The default job cannot be deleted.

Full type backup

Full backup contains all evidence, therefore this could take a long time. Since it can be restored after a metadata backup, it is recommended once a month.

Operation type backup

The **operation** backup saves all open and closed operations. Since it can be restored after a metadata backup, it is recommended once a month.

Target type backup

The **target** backup saves all opened and closed target data. Since it can be restored after a metadata backup, it is recommended once a month.

Incremental backup

Full, **operation** and **target** backups can also be incremental. This way the system saves data generated from the date-time of the last backup. The first incremental backup is always complete (full, operation or target). Only subsequent backups are incremental.

NOTE: if the incremental option is removed and reapplied to a job, the next backup of that job will be complete.

Tip: name the job so it is later recognized as an incremental backup (i.e.: "Increm_ lastWeek").

We suggest you run a complete backup (full, operation or target) once a month and an incremental backup once a week.

Backup restore for severe reasons

CAUTION: restoring a backup should only be considered in severe situations such as replacing a database.

A backup must be restored whenever a server is replaced.

Backup data restore

IMPORTANT: backup restore is never destructive. For this reason, restore should not be used to restore accidentally changed elements.

Some examples are provided below:

If after the last backup	*Then restore*
an element was deleted	restores the deleted element.
an element was edited	leaves the element changed.
a new element was added	leaves the element changed.

IMPORTANT: backup does not restore information on operations that were erroneously closed (deleted).

IMPORTANT: to restore an incremental backup, restore them all starting with the oldest.

Connector management

To manage connectors:	• System section, Connectors

Function scope

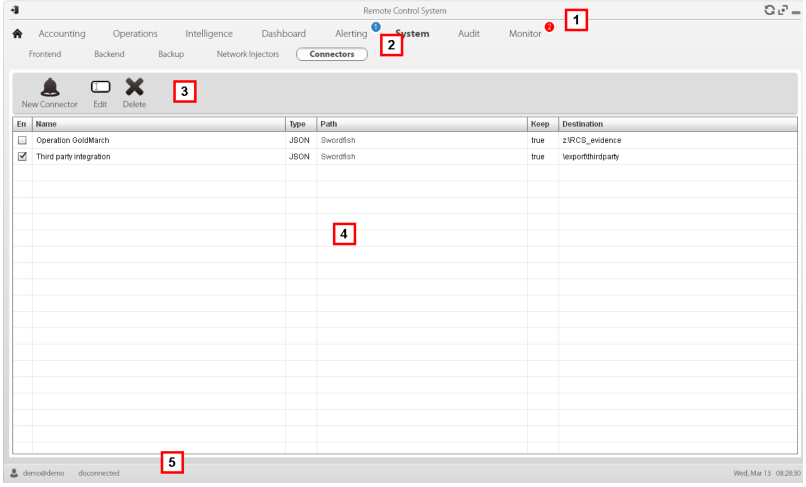
This function lets you create connection rules with third party software. The evidence received by RCS will be sent to the software according to these rules.

IMPORTANT: each connector is subject to a license.

NOTE: the function is only enabled if the user has **Connector management** authorization.

What the function looks like

This is what the page looks like:



En	Name	Type	Path	Keep	Destination
□	Operation GoldMarch	JSON	Swordfish	true	z:\RCS_evidence
☑	Third party integration	JSON	Swordfish	true	\export\thirdparty

Area	*Description*
1	RCS menu.
2	**System** menu.
3	Window toolbar. Descriptions are provided below:

Icon	*Description*
🔔	Add a connection rule.
▭	Edit the selected connection rule.
✖	Delete the selected connection rule.

Area	*Description*
4	List of connection rules.
5	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 86* .

Significant connection rule data

Selected rule data is described below:

Field	*Description*
Path	Name of the operation or target evidence is sent to. If not specified, all operations and evidence will be sent to third party software.
Type	Evidence format.
Keep the evidence	If selected, a copy of the evidence is kept in the RCS database. ⚠ CAUTION: if not selected, this evidence can no longer be viewed in RCS, nor can alerts be received.
Destination	Folder where evidence is sent (local or remote, i.e.: "c:\RCSevidence").

Managing the Network Injector

To manage Network Injectors:	• **System** section, **Network Injector**

Purpose

During installation, this function lets you create a new Network Injector "object" that creates the logical connection between the RCS Console and single hardware device.

NOTE: the function is only enabled if the user has **Injector management** authorization.

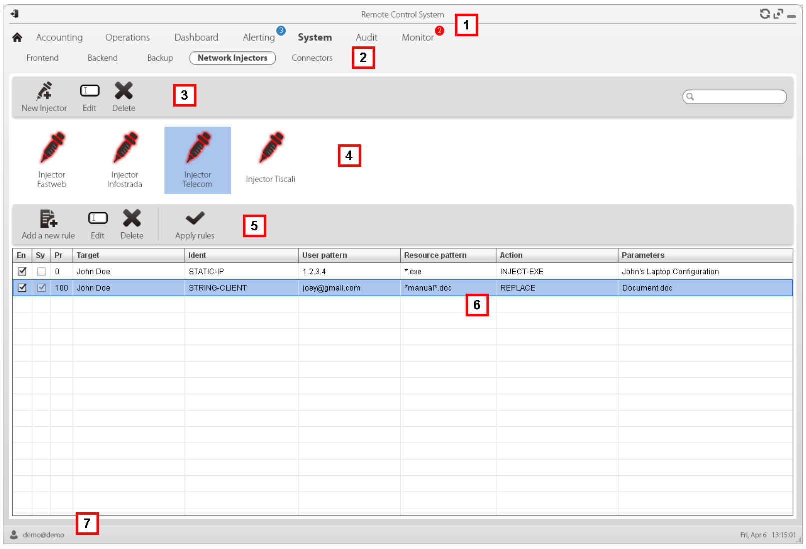
What you can do

With this function you can:

- create a new Network Injector

What the function looks like

This is what the page looks like:



En	Sy	Pr	Target	Ident	User pattern	Resource pattern	Action	Parameters
☑	□	0	John Doe	STATIC-IP	1.2.3.4	*.exe	INJECT-EXE	John's Laptop Configuration
☑	☑	100	John Doe	STRING-CLIENT	joey@gmail.com	*manual*.doc	REPLACE	Document.doc

Area	*Description*
1	RCS menu.
2	**System** menu.
3	Network Injector toolbar. Descriptions are provided below:

Action	*Function*
✚	Add a new Network Injector
▭	Edit Network Injector data.
✖	Delete the selected Network Injector.
⇧	Update Network Injector.

4	Network Injector list.

<table>
<tr><th><em>Area</em></th><th><em>Description</em></th></tr>
<tr><td><strong>5</strong></td><td>Injection rule toolbar.
NOTE: the functions are only enabled if the user has <strong>Injector rules management</strong> authorization.
Descriptions are provided below:
<table>
<tr><th><em>Action</em></th><th><em>Description</em></th></tr>
<tr><td>➕</td><td>Add a new rule.</td></tr>
<tr><td>▭</td><td>Open the window with rule data.</td></tr>
<tr><td>✖</td><td>Delete the selected rule.</td></tr>
<tr><td>✔</td><td>Update the selected Network Injector's settings.</td></tr>
</table>
</td></tr>
<tr><td><strong>6</strong></td><td>List of selected Network Injector rules
<strong>En</strong>: select to enable the rules to be applied.</td></tr>
<tr><td><strong>7</strong></td><td>RCS status bar. .</td></tr>
</table>

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 86* .

To learn more about Network Injector Appliance installation *see "Network Injector Appliance installation" on page 42*

To learn more about Tactical Network Injector installation *see "Tactical Control Center installation" on page 47 see "Network Injector Appliance installation" on page 42*

Updating Network Injector

To update Network Injector:

Step	*Action*
1	- Select the Network Injector - Click **Upgrade**: update data appears. - Click **OK**: Network Injector is updated.

Network Injector data

Selected Network Injector data is described below:

Data	*Description*
Name	User's descriptions.
Description	
Version	Software version. To view the software versions of all the components *see "System monitoring (Monitor)" below* .
Address	Device IP address.
Port	4444. To view all ports to be opened on the firewall *see "Ports to be opened on the firewall" on page 14*
Monitor via NC	If enabled, Network Controller acquires the Network Injector status every 30 seconds. If not enabled, Network Injector continues sniffing and injection operations, but the Network Controller does not check its status. Used when connections to Network Injector are down for any reason once installed at ISP, or for tactical use.
Log	Last messages logged. NOTE: Tactical Network Injector log updates depend on the frequency with which the operator enables synchronization. To view log file content *see "System logs" on page 74* . ⟳: update the list. ✖: delete viewed logs.

System monitoring (Monitor)

To monitor the system: | • **Monitor** section

Purpose

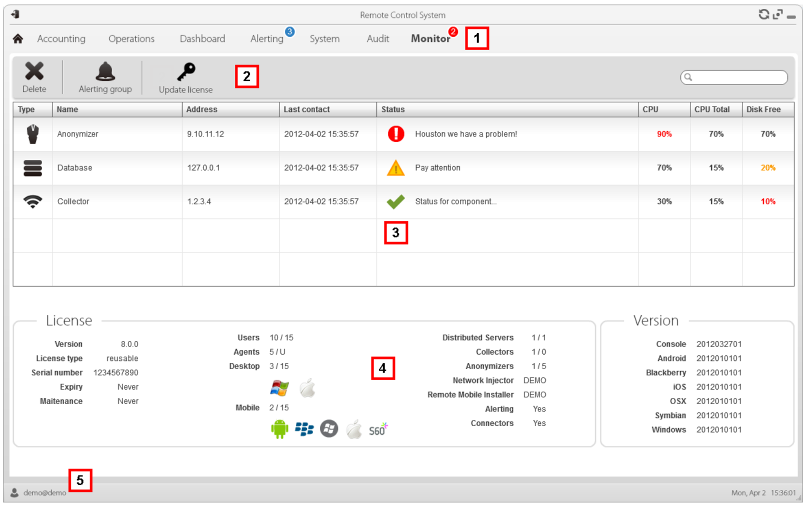
This function lets you:

- monitor system status in both hardware and software terms
- delete elements to be monitored since uninstalled
- monitor license used compared to those purchased
- define the alerting group and alert e-mail addressee in the event of system alarms

Service call: Contact your HackingTeam Account Manager if additional licenses are required.

What the function looks like

This is what the page looks like:



Type	Name	Address	Last contact	Status	CPU	CPU Total	Disk Free
	Anonymizer	9.10.11.12	2012-04-02 15:35:57	Houston we have a problem!	90%	70%	70%
	Database	127.0.0.1	2012-04-02 15:35:57	Pay attention	70%	15%	20%
	Collector	1.2.3.4	2012-04-02 15:35:57	Status for component...	30%	15%	10%

License

Version 8.0.0
License type reusable
Serial number 1234567890
Expiry Never
Maitenance Never

Users 10 / 15
Agents 5 / U
Desktop 3 / 15
Mobile 2 / 15

Distributed Servers 1 / 1
Collectors 1 / 0
Anonymizers 1 / 5
Network Injector DEMO
Remote Mobile Installer DEMO
Alerting Yes
Connectors Yes

Version

Console 2012032701
Android 2012010101
Blackberry 2012010101
iOS 2012010101
OSX 2012010101
Symbian 2012010101
Windows 2012010101

Area	*Description*
1	RCS menu. Monitor 1 : indicates the current number of system alarms triggered.

<table>
<tr><th><i>Area</i></th><th><i>Description</i></th></tr>
<tr><td>2</td><td>Window toolbar. Descriptions are provided below:
<table>
<tr><th><i>Icon</i></th><th><i>Description</i></th></tr>
<tr><td>✖</td><td>Deletes the component to be monitored.</td></tr>
<tr><td>🔔</td><td>Defines the alerting group.</td></tr>
<tr><td>🔑</td><td>Loads a new license file.</td></tr>
</table>
</td></tr>
<tr><td>3</td><td>List of RCS components and their status:
❗ Alarm (generates an e-mail sent to the alerting group)
⚠ Warning
✓ Component running</td></tr>
<tr><td>4</td><td>License status.</td></tr>
<tr><td>5</td><td>RCS status bar.</td></tr>
</table>

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 86* .
For a description of the data in this window *see "System monitoring data (Monitor)" on the facing page* .

Deleting a component to be monitored

To delete an uninstalled component:

Step	*Action*
1	Select the component.

Step	*Action*
2	Click **Delete**: RCS will no longer read the status of that component. Only subsequent installations of new components automatically updates the list. NOTE: erroneously deleting a component that is still installed is not destructive. Component status will reappear the next time the page is refreshed.

System monitoring data (Monitor)

System component monitoring data

System monitoring data is described below:

Data	*Description*
Type Name	Monitored component type and name: Network Controller Anonymizer Database Collector
Address	Component's IP address.
Last contact	Last synchronization date-time.
Status	Component status at last synchronization: ❗ Alarm: the component is not running, contact the alerting group for immediate service. ⚠ Warning: the component signals a risky situation, contact the system administrator for necessary checks. ✓ Component running.
CPU	% CPU use by the single process.
CPU Total	% CPU use by server.

Data	*Description*
Disk Free	% free disk space.

License monitoring data

License monitoring data is described below: For restricted licenses, the format is "x/y" where x is the amount of licenses currently used by the system and y the maximum amount of licenses.

CAUTION: if all the licenses are in use, any new agents will be put in queue until a license is freed or new ones purchased.

Data	*Description*
License type	Type of license currently in use for agents. **reusable**: an agent's license can be reused after it is uninstalled. **oneshot**: an agent's license is only valid for one installation. NOTE: the license can only be updated if the user has **License modification** authorization.
Users	Amount of users currently used by the system and maximum admitted quantity.
Agents	Amount of agents currently used by the system and maximum admitted quantity.
Desktop **Mobile**	Amount of desktop and mobile agents currently used by the system and maximum admitted quantities respectively.
Distributed server	Amount of database currently used by the system and maximum admitted quantity.
Collectors	Amount of Collectors currently used by the system and maximum admitted quantity.
Anonymizers	Amount of Anonymizers currently used by the system and maximum admitted quantity.

]HackingTeam[

HT S.r.l.
via della Moscova, 13
20121 Milano (MI)
Italy
tel.: + 39 02 29 060 603
fax:+ 39 02 63 118 946
www.hackingteam.com
e-mail:info@hackingteam.com

RCS 8.3 System Administrator's Guide
System Administrator's Guide 1.3 MAR-2013

info@hackingteam.com