

]HackingTeam[

RCS 8.2

The hacking suite for governmental interception

System Administrator's Guide



Information property

© COPYRIGHT 2012, HT S.r.l.

All rights reserved in all countries.

No part of this manual can be translated into other languages and/or adapted and/or reproduced in other formats and/or mechanically, electronically processed or photocopied, recorded or otherwise without prior written authorization from HackingTeam.

All corporations and product names may be legal or registered trademarks, property of their respective owners. Specifically Internet Explorer™ is a Microsoft Corporation registered trademark.

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

Glossary	x
Guide introduction	1
New guide features	2
Supplied documentation	2
Print concepts for notes	3
Print concepts for format	3
Product and guide addressees	4
Software author identification data	4
RCS (Remote Control System)	6
All-in-One architecture components	7
Introduction	7
All-In-One architecture layout	7
All-in-One RCS architecture components	7
Distributed architecture components	9
Introduction	9
Distributed architecture layout	9
Distributed architecture components	9
What you should know about RCS	10
Operations	10
Data flow and protection	10
Data logging continuity	10
Redirecting login to Collector	11
Digital certificates	11
Decoding data	11
Differences with previous versions	11
Glossary	11
Installation introduction	12
Package content	13
Package content	13
Installation package content (CD or web)	13
USB key with user license	13
USB hardware keys	14
Minimum system requirements	14
Ports to be opened on the firewall	14
System administrator procedures	15
Introduction	15
Procedures	15
Install RCS and setup components	15

Maintain and update the system	16
Monitoring the system	16
RCS installation	17
What you should know about RCS installation	18
Login privileges	18
Admin user and System administrator user	18
RCS server installation in All-in-One architecture	18
Introduction	18
Installation requirements	18
Installation sequence	19
Installation	19
Checking service start	21
Checking installation logs	21
Check IP addresses	21
Uninstall	21
RCS server installation in distributed architecture	22
Introduction	22
Installation requirements	22
Installation sequence	22
Master Node installation	23
Collector and Network Controller installation	25
Checking service start	28
Checking Collector redirecting	28
Checking installation logs	28
Check IP addresses	29
Uninstall	29
List of started RCS services	29
To learn more	30
RCS Console installation	30
Introduction	30
Requirements	30
Installation sequence	30
Adobe AIR installation	30
RCS Console installation	31
RCS Console uninstall	32
Creating the Administrator user	32
OCR module installation	33
Introduction	33
Installation requirements	33
OCR module operations	33

Space occupied by tagged text in the database	34
OCR module work load	34
Symptoms of excessive load	34
OCR module installation	34
Checking correct OCR module operations	35
Uninstall	35
Files installed at the end of installation	35
	36
Optional and additional component installation	37
Anonymizer installation and settings	38
Introduction	38
Installation requirement	38
Installation	38
Anonymizer data	39
Boot check	39
IP address check	39
Editing settings	40
Uninstall	40
What you should know about Network Injector Appliance	40
Introduction	40
Operations	40
Network connections	40
Standard connection layout	41
Connection layout as an intra-switch segment	41
Data sniffing via TAP, SPAN port	42
Network Injector Appliance installation	42
Introduction	42
Package content	42
Installation sequence	42
Rear panel description	42
Network connections	43
Network Injector Appliance settings	43
Network Injector Appliance start check	44
IP address check	45
Uninstall	45
What you should know about Tactical Network Injector	45
Introduction	45
Network connections	45
Access point emulation connection diagram	45
Tactical Control Center installation	46

Introduction	46
Tactical Control Center features	46
Package content	47
Requirements	47
Operating system installation and settings	47
IP address check	50
Uninstall	50
Network Injector settings	50
Introduction	50
Adding a Network Injector	50
Network Injector data	50
Editing settings	51
Additional component installation in distributed architecture	51
Introduction	51
Additional component installation requirements	51
Installation sequence	52
Additional Shard database installation	52
Additional Collector installation	54
Checking service start	57
Checking Collector redirecting	57
Checking installation logs	57
Check IP addresses	58
Uninstall	58
Routine maintenance and software updates	59
What you should know about RCS maintenance	60
Receiving updates	60
Updating machine behavior	60
Routine maintenance procedures	60
Introduction	60
Check and delete log files	60
Checking available backup disk space	60
Linux operating system updates	60
RCS server update	61
Update requirements	61
Update methods	61
RCS server(s) update	61
RCS Console update	61
Update requirements	61
RCS Console update	61
Anonymizer update	61

Update requirements	61
Anonymizer update	62
Network Injector Appliance update	62
Introduction	62
Network Injector Appliance update	62
Tactical Network Injector update	62
Introduction	62
Full Tactical Network Injector update	63
Partial Tactical Network Injector update	63
Editing Master Node and Collector settings	64
What you should know about settings	65
What you can edit	65
When to edit settings	65
Order used to edit settings	65
Mail server settings	65
Setup utilities	65
RCS utilities	65
Utility command syntax	66
Other options	66
Editing Master Node settings	66
Modifica alla configurazione di Collector	67
Settings check	68
Example of settings check output	68
Troubleshooting	69
Potential faults	70
Potential installation faults	70
Possible server problems	70
Potential backup problems	71
To learn more	71
System logs	71
Introduction	71
Log analysis utility	71
Log file example	72
RCS log files	72
Quick log display	72
Log file content	72
Component status check procedure	73
Introduction	73
Installed license check	73
Command	73

Master Node status check	73
Command	73
What to check	73
Checking Worker service status	73
What to check	73
Check agent status via Collector	73
Command	74
What to check	74
Network Injector start check	74
To learn more	74
Service restart procedures	74
Introduction	74
Restarting RCSDB service	74
Purpose	74
Command	75
Restarting MongoDB service	75
Purpose	75
Command	75
Restarting Collector service	75
Purpose	75
Command	75
Restarting Worker service	75
Purpose	75
Command	76
Restarting Network Injector service	76
Purpose	76
Command	76
Restarting Anonymizer service	76
Purpose	76
Command	76
Hardware component service procedures	77
Introduction	77
Hardware key replacement.	77
Master Node replacement	77
Shard replacement	77
Replacing the Collector/Network Controller	78
Replacing an Anonymizer	78
Replacing a Network Injector Appliance	78
Replacing a Tactical Injector Appliance	78
RCS Console for the System administrator	79

Starting the RCS Console	80
What the login page looks like	80
Open RCS Console	80
Homepage description	81
Introduction	81
What it looks like	81
Wizards in the homepage	82
Introduction	82
What it looks like	82
Archive Wizard	83
Shared interface elements and actions	83
What the RCS Console looks like	83
Actions always available on the interface	85
Change interface language or password	85
Converting the RCS Console date-time to the actual time zone	85
Table actions	85
Front end management	87
Function scope	87
What the function looks like	87
To learn more	89
Adding an Anonymizer to the configuration	89
Editing Anonymizer settings	89
File Manager data	89
Back end management	90
Function scope	90
What the function looks like	90
To learn more	91
Significant Shard database data	91
Backup management	91
Function scope	91
What the function looks like	91
Significant backup process data	93
What you should know about backup	94
Management responsibilities	94
Backup methods	94
Metadata type backup	94
Full type backup	94
Operation type backup	94
Target type backup	94
Incremental backup	95

Backup restore for severe reasons	95
Backup data restore	95
Managing the Network Injector	95
Purpose	96
What you can do	96
What the function looks like	96
To learn more	97
Network Injector data	97
System monitoring (Monitor)	98
Purpose	98
What the function looks like	99
To learn more	100
Deleting a component to be monitored	100
System monitoring data (Monitor)	100
System component monitoring data	100
License monitoring data	101

List of diagrams

Figura 1: All-In-One RCS architecture: logical layout	7
Figura 1: Distributed RCS architecture: logical layout	9
Figura 1: Network Injector Appliance: physical layout	41
Figura 2: Network Injector Appliance with TAP: physical layout	42
Figura 1: Tactical Network Injector: access point emulation diagram	46

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

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, where 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.

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	2
Supplied documentation	2
Print concepts for notes	3
Print concepts for format	3
Product and guide addressees	4
Software author identification data	4

New guide features

List of release notes and updates to this online help.

Release date	Code	Software version.	Description
15 October 2012	System Administrator's Guide 1.201 NOV-2012	8.2	<p>Added utility to restart Windows services, see "Service restart procedures" on page 74 .</p> <p>Added BareTail for Windows, log code viewer. See "System logs" on page 71 .</p> <p>Added incremental backup management and mandatory metadata backup job. See "What you should know about backup" on page 94 .</p> <p>E-mail delivery authentication support for alerts. See "Editing Master Node settings" on page 66 .</p> <p>Optional OCR module See "OCR module installation" on page 33</p> <p>Added fast database management wizard. See "Wizards in the homepage" on page 82</p> <p>Sole Tactical Control Center application on Tactical Network Injector.</p>
30 June 2012	System Administrator's Guide 1.1 JUN-2012	8.1	<p>File Manager to delete file packets in the folder C:\RCS\Collector\public. See "Front end management" on page 87 .</p>
16 April 2012	System Administrator's Guide 1.0 APR-2012	8.0	<p>First publication</p>

Supplied documentation

The following manuals are supplied with RCS software:

Manual	Addressees	Code	Distribution format
System Administrator's Guide (this manual)	System administrator	<i>System Administrator's Guide</i> 1.201 NOV-2012	PDF

<i>Manual</i>	<i>Addressees</i>	<i>Code</i>	<i>Distribution format</i>
Administrator's Guide	Administrators	<i>Administrator's Guide 1.2 OCT-2012</i>	PDF
Technician's Guide	Technicians	<i>Technician's Guide 1.201 OCT-2012</i>	PDF
Analyst's Guide	Analysts	<i>Analyst's Guide 1.2 OCT-2012</i>	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:

<i>Example</i>	<i>Style</i>	<i>Description</i>
See " <i>User data</i> "	<i>italic</i>	this indicates a chapter, section, sub-section, paragraph, table or illustration heading in this manual or other publication of reference.

<i>Example</i>	<i>Style</i>	<i>Description</i>
<ddmmyyy>	<aaa>	indicates text that must be specified by the user according to a certain syntax. In the example <ddmmyyy> 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.

<i>Addressee</i>	<i>Activity</i>	<i>Skills</i>
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.	<i>Expert network technician</i>
Administrator	Creates authorized accounts and groups. Creates operations and target. Monitors system and license status.	<i>Investigation manager</i>
Technician	Creates and sets up agents. Sets Network Injector rules	<i>Tapping specialist technician</i>
Analyst	Analyzes and exports evidence.	<i>Operative</i>

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

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	7
Distributed architecture components	9
What you should know about RCS	10
Differences with previous versions	11

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:

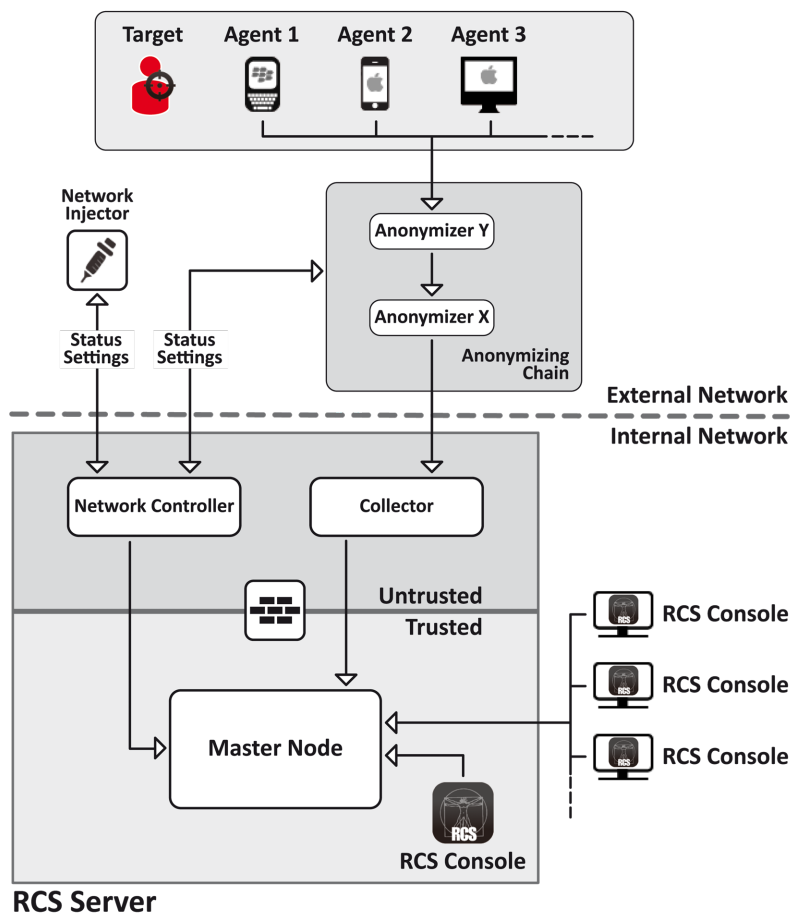


Figura 1: All-in-One RCS architecture: logical layout

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.	<ul style="list-style-type: none"> • <i>target devices</i> • <i>data sources</i>
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.	<i>VPS (Virtual Private Server)</i>
Collector	RCS server component that collects agent data either directly or through the Anonymizer chain.	<i>RCS server</i>
Firewall	Optional but highly recommended, it protects the <i>trusted</i> environment where data is processed and saved from the <i>untrusted</i> environment where data is collected.	<i>RCS server</i>
RCS console	Setup, monitoring and analysis console used by operating center workers.	<ul style="list-style-type: none"> • <i>RCS server</i> • <i>internal network</i>
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.	<i>RCS server</i>
Network Controller	(optional) RCS server component, sends settings to Network Injector, Anonymizer chains and constantly acquires their status.	<i>RCS server</i>
Network Injector	(optional) Fixed hardware component (Appliance) or notebook (Tactical), it runs sniffing and injection operations on the target's HTTP connections.	<ul style="list-style-type: none"> • <i>ISP</i> • <i>Wired or Wireless LAN (homes, hotel)</i>
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:

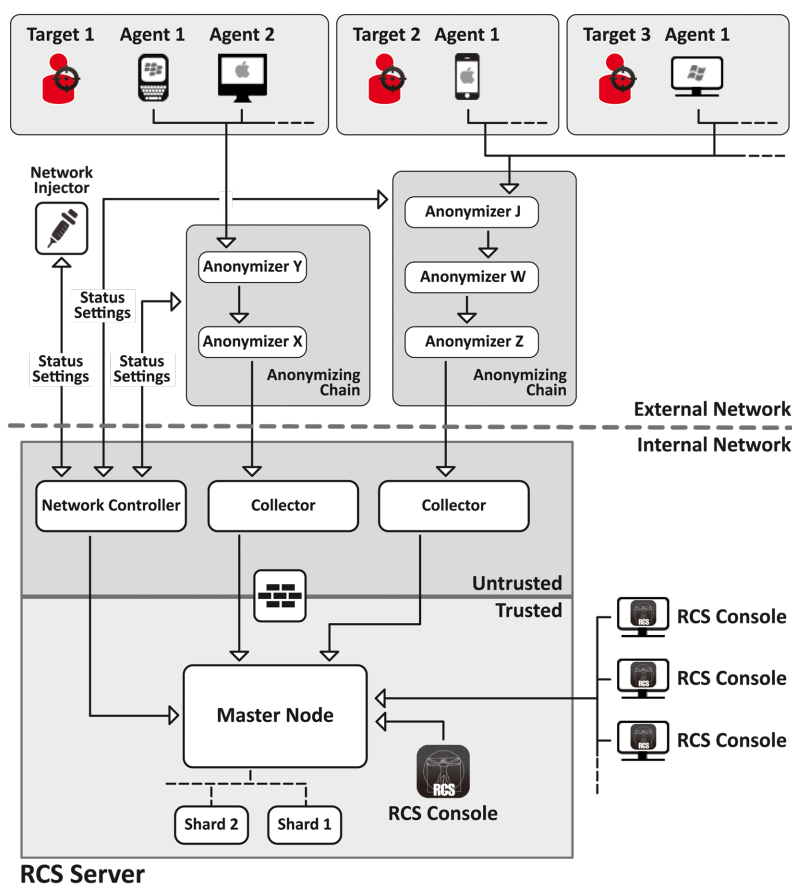


Figura 1: Distributed RCS architecture: logical layout

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.	<i>one or more servers in front end environment</i>
Network Controller	One per architecture, it is included in first Collector installation.	<i>one server in front end environment</i>
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.	<i>one or more servers in back end environment</i>

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 unsuspecting 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

<i>RCS v. 7.6</i>	<i>RCS 8.0 and higher</i>
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

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	13
Minimum system requirements	14
Ports to be opened on the firewall	14
System administrator procedures	15

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	<i>Release notes</i>
x:\doc	RCS_ x.x_ Admin_ y.y_ <language>.PDF RCS_ x.x_ Analyst_ y.y_ <language>.PDF RCS_ x.x_ SysAdmin_ y.y_ <language>.PDF RCS_ x.x_ Technician_ y.y_ <language>.PDF	<i>RCS installation and user manuals. Each manual is addressed to a specific user role.</i> <ul style="list-style-type: none"> • "x.x": RCS version. • "y.y": manual version. • <language>: manual language.
x:\setup	AdoberAIRinstaller.exe	<i>Adobe AIR installation file</i>
x:\setup	RCS-<version>.exe	<i>RCS server(s) installation file</i>
x:\setup	RCSconsole-<version>.air	<i>RCS Console installation file</i>
x:\setup	RCS-ocr-<version>.exe	<i>OCR module installation file (optional)</i>

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:

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

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:

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

<i>From...</i>	<i>To...</i>	<i>Port to be opened</i>
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:

<i>Step</i>	<i>Action</i>
-------------	---------------

- 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
- 5 (optional) Install the Shard databases and additional Collectors.
See "[Additional component installation in distributed architecture](#)" on page 51 .
- 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 45 .

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 59 .
- See "[Editing Master Node and Collector settings](#)" on page 64 .
- See "[Troubleshooting](#)" on page 69 .

Monitoring the system

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

- See "[RCS Console for the System administrator](#)" on page 79

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	18
RCS server installation in All-in-One architecture	18
RCS server installation in distributed architecture	22
List of started RCS services	29
To learn more	30
RCS Console installation	30
OCR module installation	33
Files installed at the end of installation	35
	36

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 .

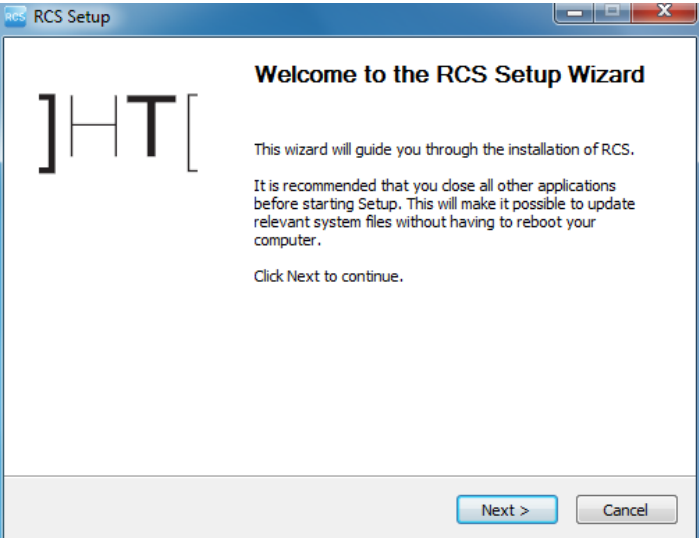
Installation sequence

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

Step	Action	Machine
1	Prepare that indicated in <i>installation requirements</i> .	-
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 .	

Steps

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

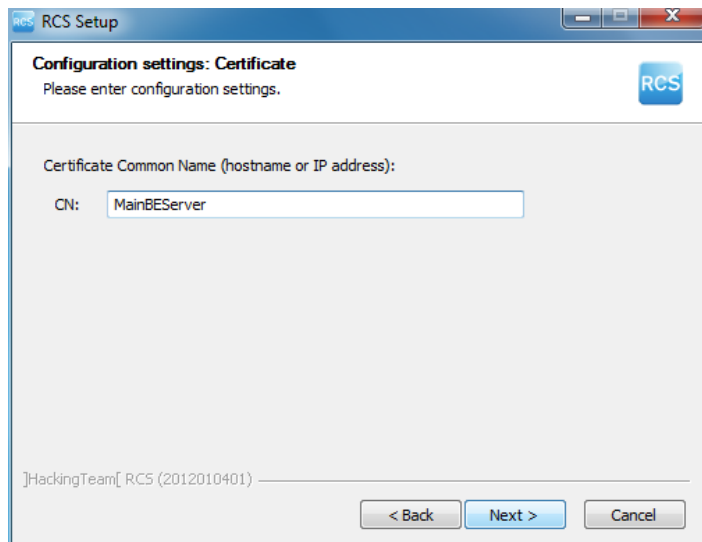
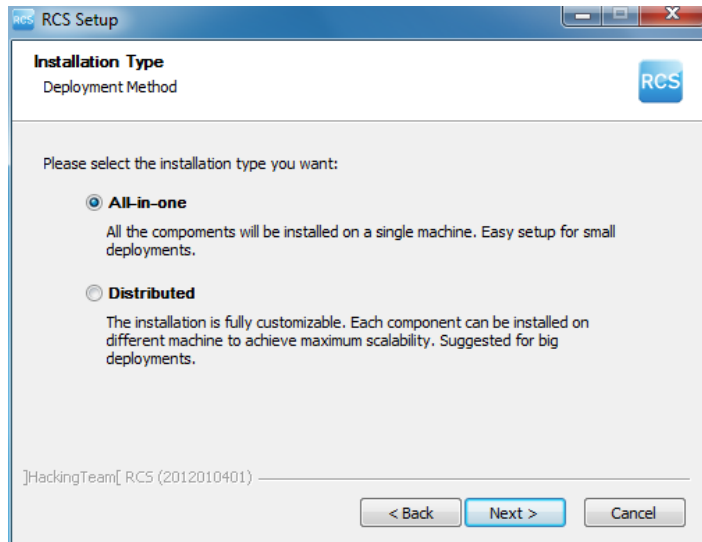
6. Enter the server name or IP address where the software is being installed and that will be indicated at RCS Console login (i.e.: **RCSserver**).



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

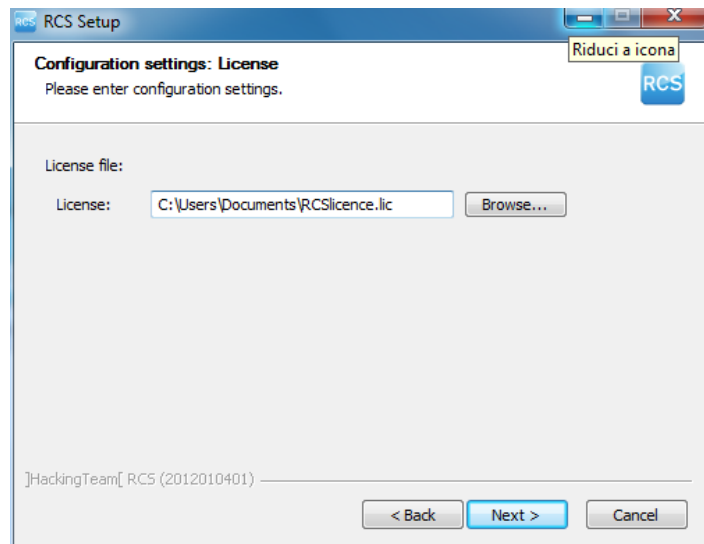
7. Click **Next**.

Result



Steps

8. Select the license file.
9. Click **Next**.

Result

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 66 .

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 71

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 91

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 <i>installation requirements</i> .	-
2	Install Master Node.	<i>server in back end environment</i>
3	Check installation logs.	
4	Make sure Master Node services have started.	
5	Install Collector and Network Controller.	<i>server in front end environment</i>
6	Check installation logs.	
7	Check Collector redirecting	<i>same server or other computer</i>
8	Install RCS Console.	<i>server in back end environment or other computer</i>
9	Setup the backup folder on the remote unit.	<i>server in back end environment</i>

Master Node installation

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

Steps

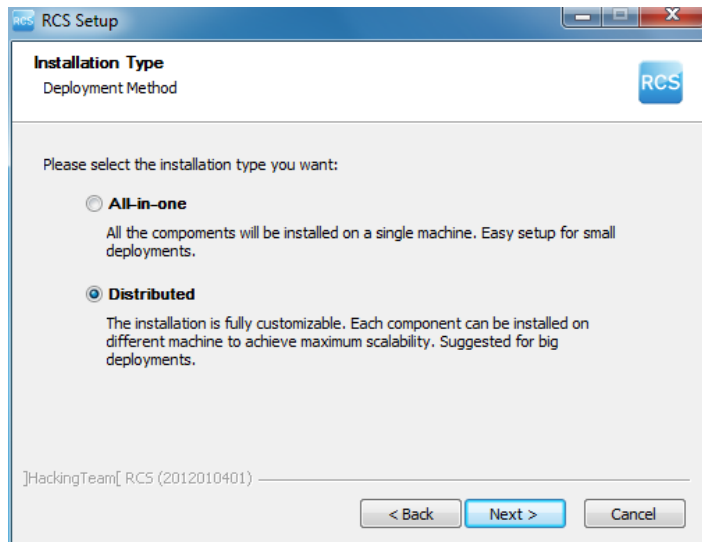
1. Insert the hardware key.
2. Insert the CD with the installation package.
Run file RCS-<version>.exe in folder
x:\setup: the first wizard window appears.
3. Click **Next**.

Result

-



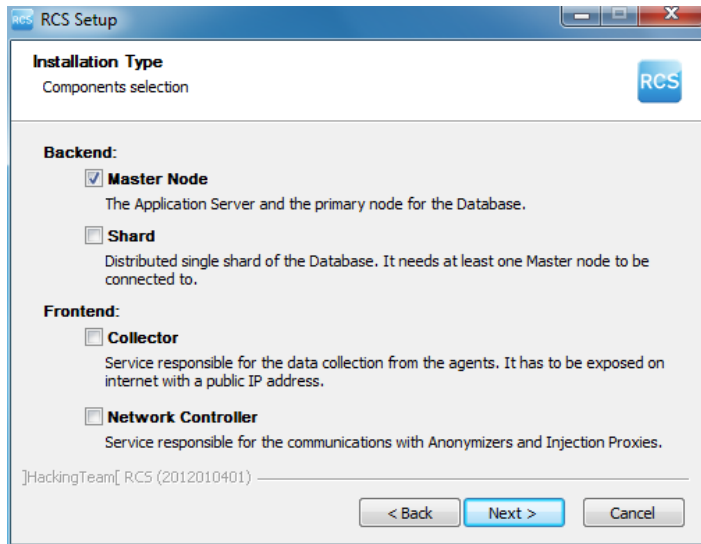
4. Select **Distributed**.
5. Click **Next**.



Steps

- 6. Select **Master Node**.
- 7. Click **Next**.

Result

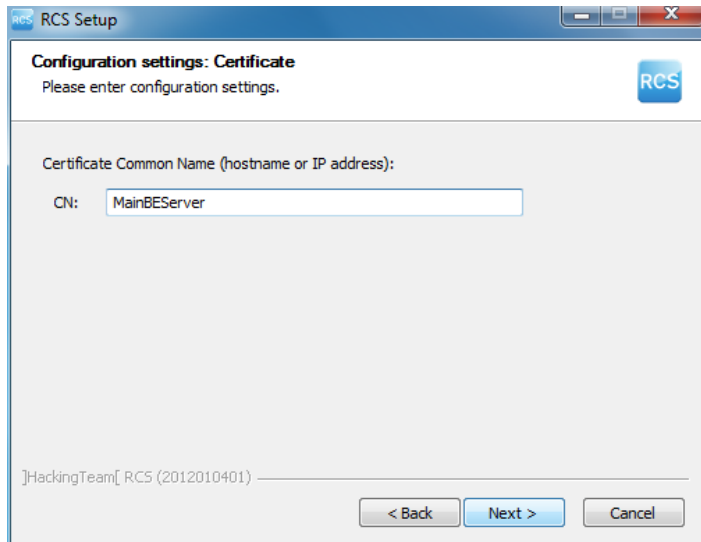


- 8. Enter the server name or IP address where the software is being installed and that will be indicated at RCS Console login (i.e.: RCSMasterNode).



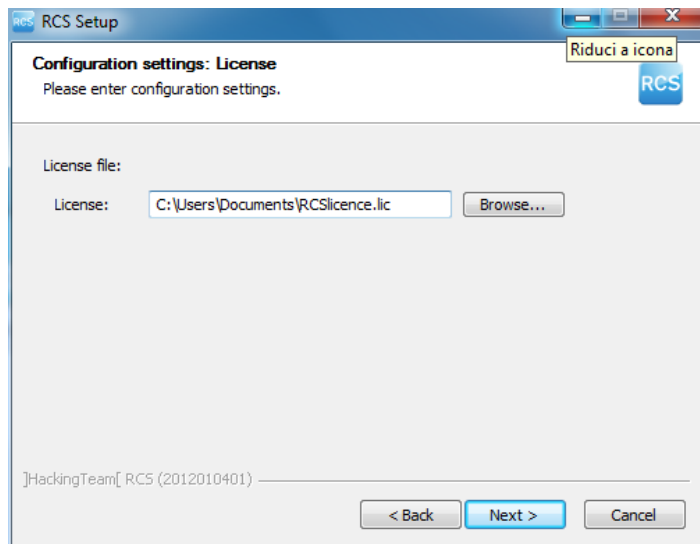
IMPORTANT: the name and/or IP address must be univocal.

- 9. Click **Next**.



Steps

10. Select the license file.
11. Click **Next**.

Result

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 66 .

Collector and Network Controller installation

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

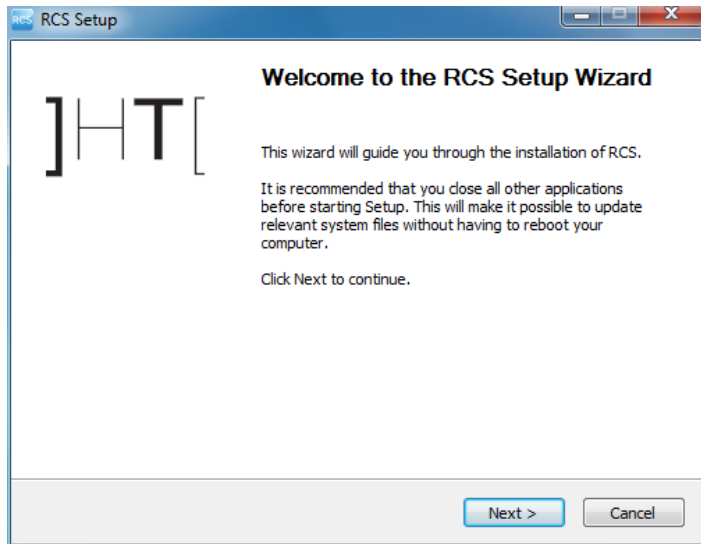
Steps**Result**

1. Insert the hardware key.

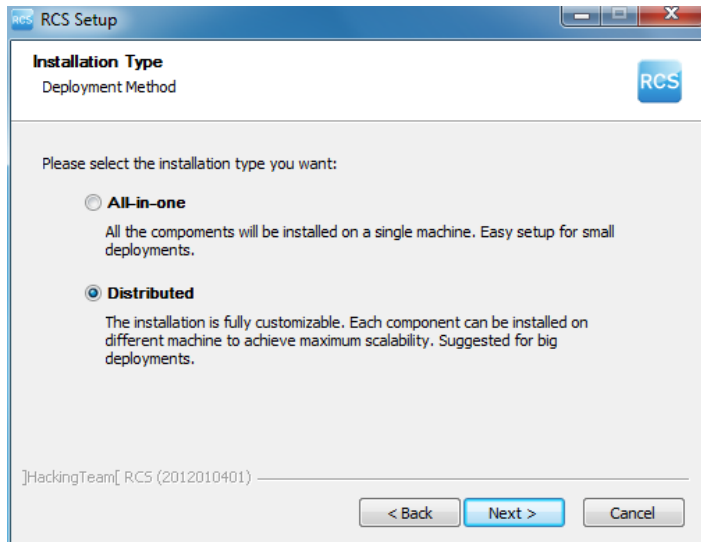
Steps

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**.

Result



4. Select **Distributed**.
5. Click **Next**.

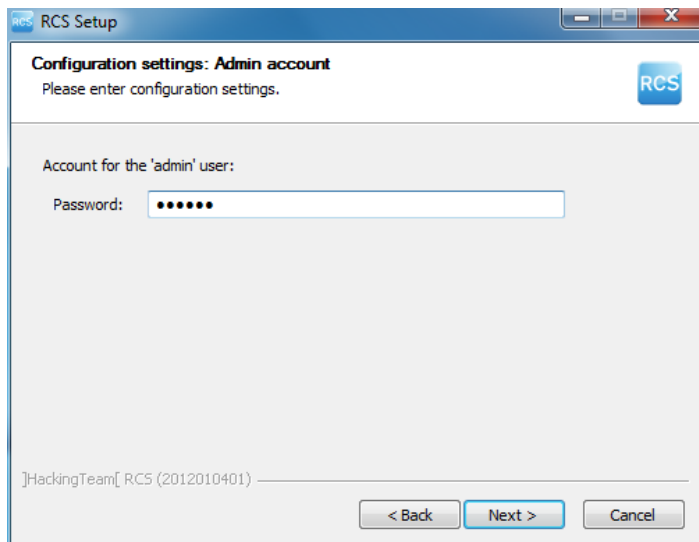
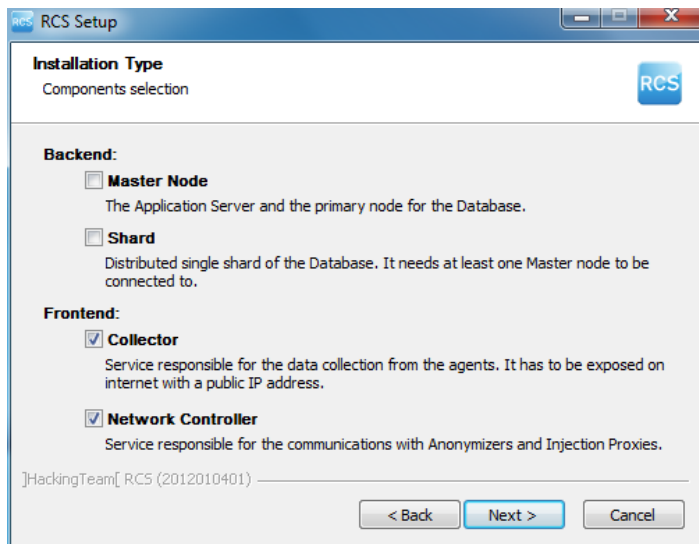


Steps

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

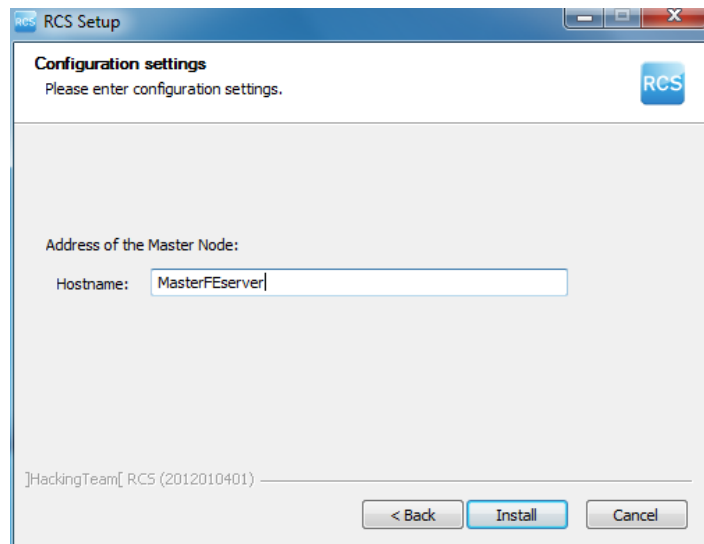
Result

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



Steps

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

Result**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:

<i>If</i>	<i>Then</i>
on the server	<ul style="list-style-type: none"> • open a browser • enter localhost • Result: the browser must be redirected to Google.
on another computer	<ul style="list-style-type: none"> • open a browser • enter <code>http://<front end server name or IP address></code>. • 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 71

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 91 .



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:

<i>Architecture</i>	<i>Services</i>	<i>Server in environment</i>
All-in-One	RCSMasterConfig	<i>back end</i>
	RCSMasterRouter	
	RCSMasterShard	
	RCSMasterWorker	
	RCSMasterDb	
	RCSCollector	
	RCSDb	
	Mongodb	
Distributed	RCSCollector	<i>front end</i>
	RCSMasterConfig	<i>back end only with Master Node</i>
	RCSMasterRouter	
	RCSMasterShard	
	RCSMasterWorker	
	RCSMasterDb	
	RCSDb	
	Mongodb	
	RCSWorker	<i>back end with additional Shards</i>
	RCSShard	



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 74 .

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	<ul style="list-style-type: none">• have the RCS server installed• prepare the server name or IP address• prepare the system administrator's password.
Distributed RCS	<ul style="list-style-type: none">• 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

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

Result



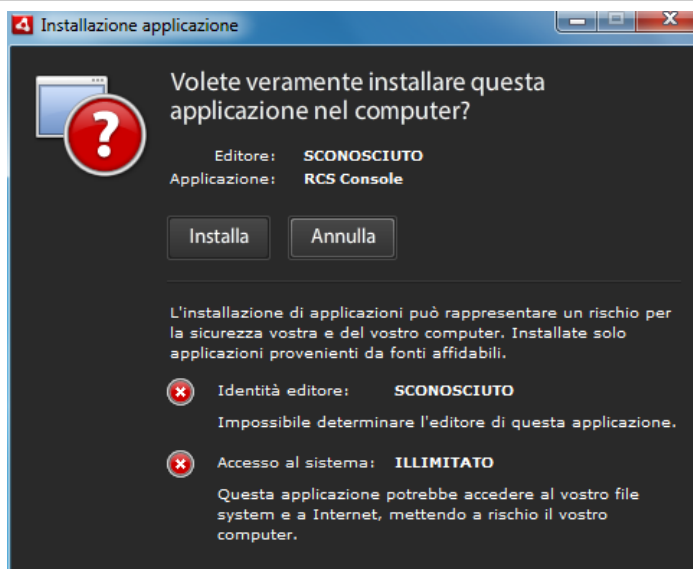
RCS Console installation

To install RCS Console:

Steps

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

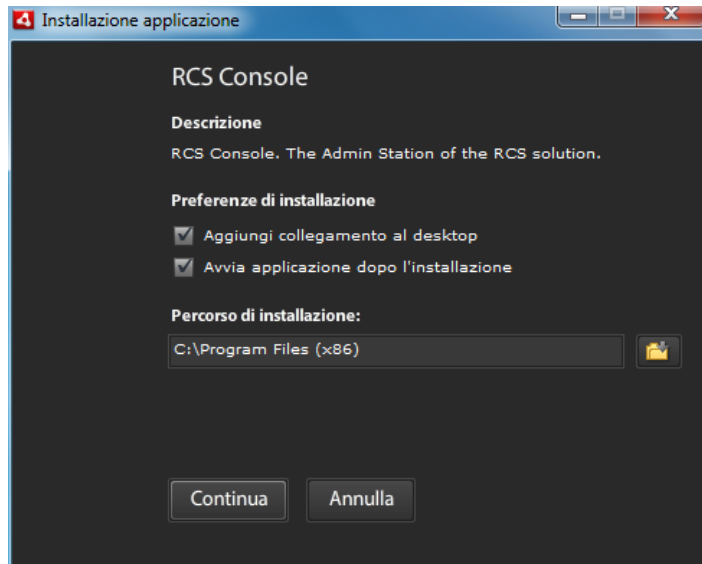
Result



Steps


3. Set any preferences.
4. Click **Continue**: RCS Console will be installed on the computer.

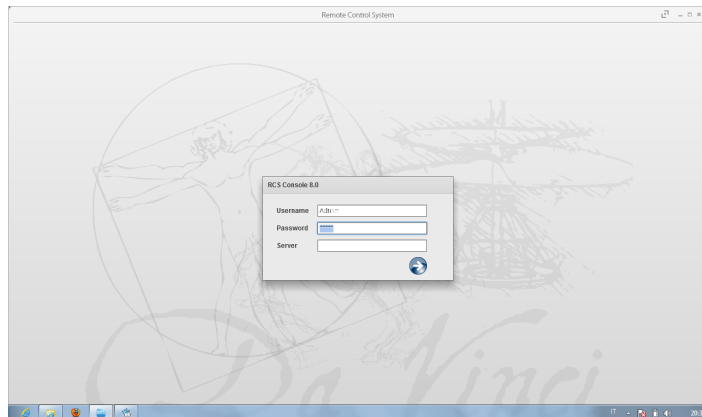
Result



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.




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:

<i>Step</i>	<i>Action</i>
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 converts all images acquired by the agent as screenshots into tagged text for full-text searches.



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:

<i>Phase</i>	<i>Description</i>
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.

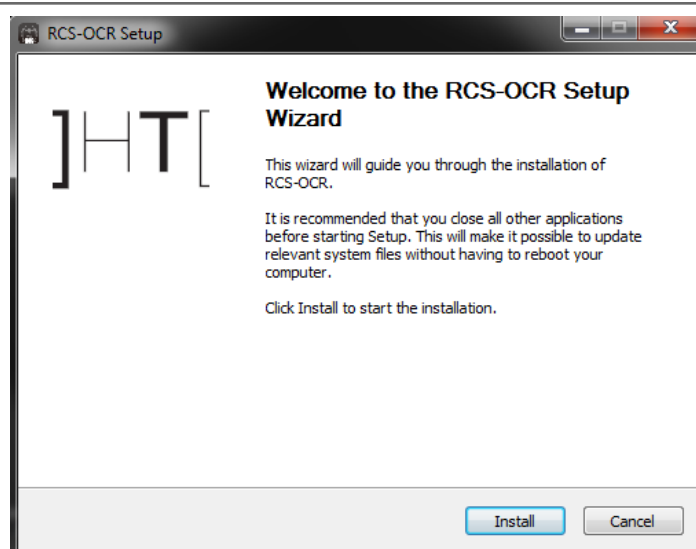
OCR module installation

To install an OCR module in back end environment:

Steps

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**.


Result



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 91



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 65

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 66

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 60
- 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 71

Path:

C:\RCS\DB\log

C:\RCS\Collector\log

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	38
What you should know about Network Injector Appliance	40
Network Injector Appliance installation	42
What you should know about Tactical Network Injector	45
Tactical Control Center installation	46
Network Injector settings	50
Additional component installation in distributed architecture	51

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 <code>rcsanon_install.zip</code> installer file is generated and saved on the console desktop.
5	Connect to the server and copy file <code>rcsanon_install.zip</code> 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:

<i>Data</i>	<i>Description</i>
Name	User's description
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 71

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 61

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 disk encryption and 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:

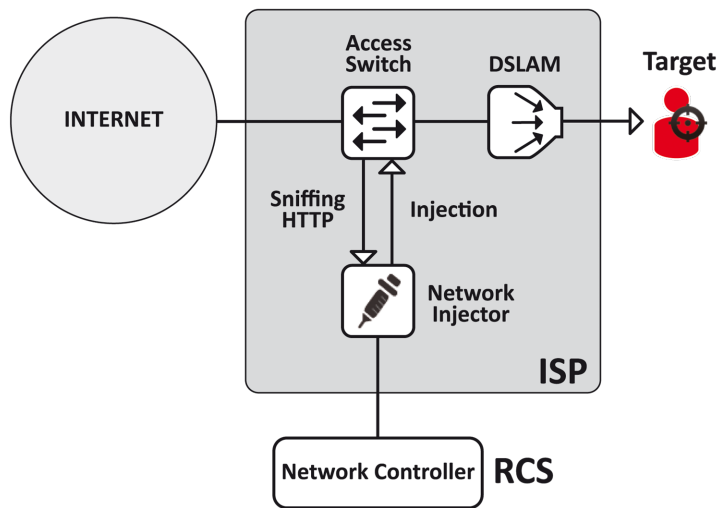


Figura 1: Network Injector Appliance: physical layout

Connection layout as an intra-switch segment

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

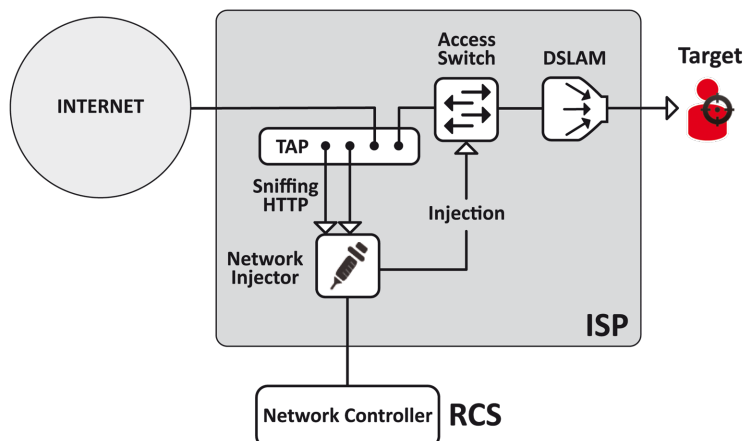


Figura 2: Network Injector Appliance with TAP: physical layout

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.

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.	<i>"Network connections" on the facing page</i>
2	Set up Network Injector.	<i>"Network Injector Appliance settings" on the facing page</i>
3	Run a test from RCS Console.	<i>"Managing the Network Injector" on page 95</i>
4	Transfer Network Injector Appliance to the Internet service provider and change the network addresses.	<i>"Network Injector settings" on page 50</i>

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 <i>sysconf</i> utilities or complete updates from the installation CD. See " Routine maintenance procedures " on page 60
3	Management and injection ports	Port 1: network connection with Network Controller to receive settings and send status. The address must be set with the <i>sysconf</i> utility. 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].	

Network Injector Appliance settings



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

The settings procedure is provided below:

Step Action

- 1 Turn on the device and login with your credentials:

- Username: **root**
- Password: **rcsnia**



CAUTION: immediately change the password

- 2 From the command prompt, run `sysconf` and use the Arrow and TAB keys to move between and open menus.

Select the **Network** menu and its sub-menus to enter all the data required for Network Controller connections:

- host name,
- IP address,
- Netmask,
- Gateway



CAUTION: leave DNS automatically read

Select **File menu, Save configuration**: the configuration is saved.

- 4 In Master Node, from folder `\RCS\DB\config\certs` copy the Network Injector `rcs.pem` and `rcs-network.sig` authentication files to Network Injector folder `rcsipa/etc`.

- 5 From the remote terminal, in Network Injector Appliance open file `/rcsipa/etc/rcsredirect.conf` and set management port 1 in variable `response_iface` and injection port 2 in variable `sniffing_iface`.

- `response_iface="eth0"`
- `sniffing_iface="eth1"`

or, if network accelerator cards are used:

- `response_iface="eth0"`
- `sniffing_iface="dag0"`

- 6 From the remote terminal, connect to Network Injector Appliance and start the service by entering command:

/etc/init.d/rcsipa start

- 7 From **RCS Console** create a Network Injector and send the configuration.

See "[Managing the Network Injector](#)" on page 95

Network Injector Appliance start check

Check the log file in folder `/rcsnia/log`.

See "[System logs](#)" on page 71

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 95

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 95

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.

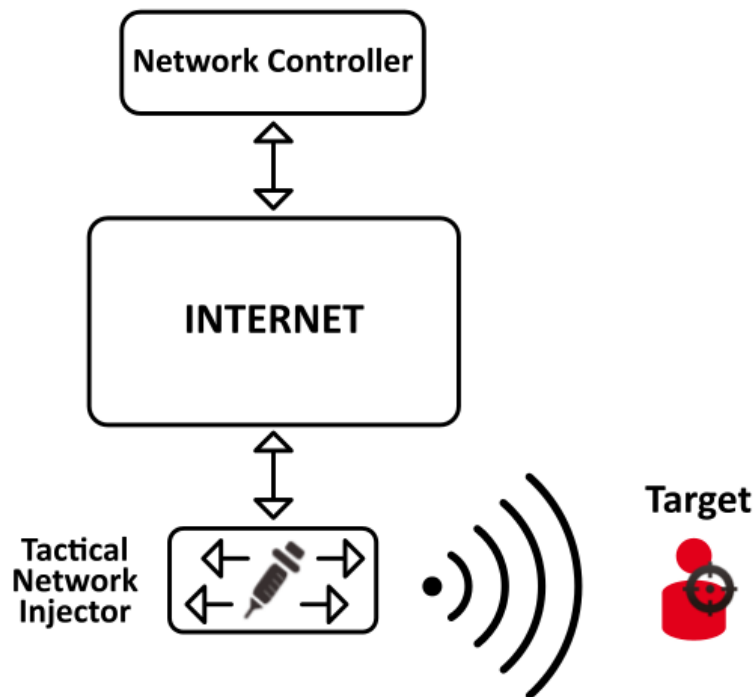


Figura 1: Tactical Network Injector: access point emulation diagram

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:


<i>Step</i>	<i>Action</i>	<i>Paragraph</i>
1	Install and set up the operating system and create the Tactical Control Center object from the RCS Console.	<i>"Operating system installation and settings" below</i>
2	Set Network Injector.	<i>"Network Injector settings" on page 50</i>

Requirements

In Master Node, copy the `rca.pem` and `rca-network.sig` authentication files from folder `\RCS\DB\config\certs`: they will be copied to Tactical Network Injector.

Operating system installation and settings

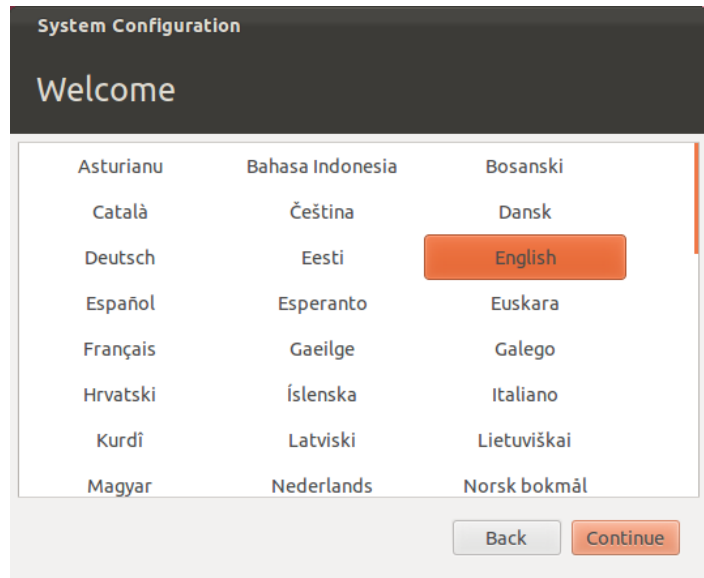
The procedure is described below:

<i>Steps</i>	<i>Result</i>
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 <i>passphrase</i> to unlock the encrypted disk. The passphrase for first boot is "firstboot".	-

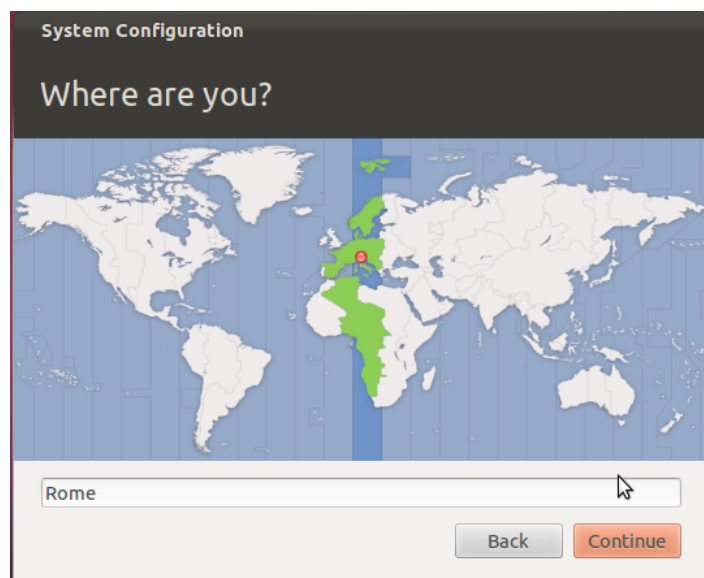
Steps

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

Result



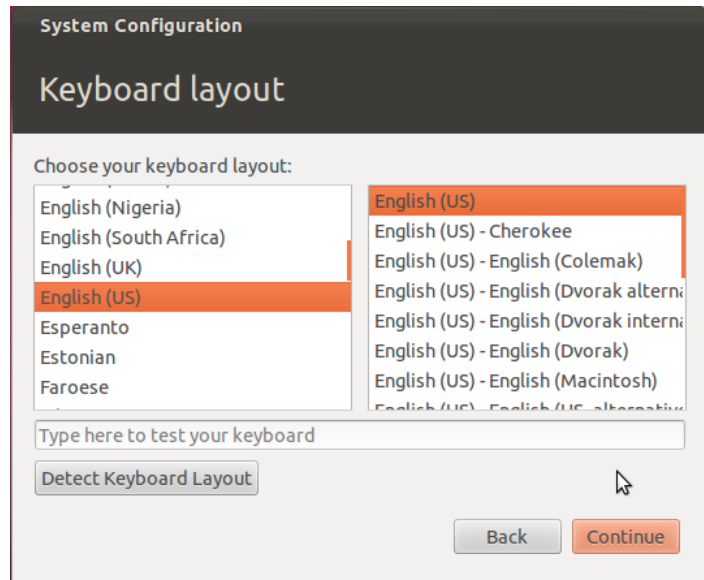
5. Select the correct time zone.



Steps

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

Result



7. Enter user data: operating system setup starts.



WARNING: if you lose your password you must re-install Tactical Control Center.



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.



8. The standard login page appears at the end of operating system installation.

9. Copy `rca.pem` and `rca-network.sig` Master Node authentication files to Tactical Network Injector folder `/opt/td-config/share`.

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 95

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 95

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:




<i>Step</i>	<i>Action</i>
-------------	---------------

- 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:

<i>Data</i>	<i>Description</i>
Name	User's descriptions.
Description	

<i>Data</i>	<i>Description</i>
Version	Software version. To view the software versions of all the components see " System monitoring (Monitor) " on page 98 .
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 71 .  : 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 .

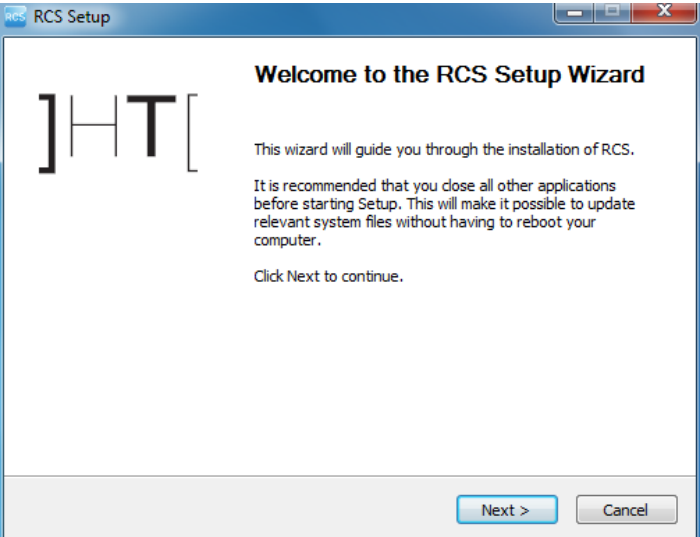
Installation sequence

The complete additional component installation sequence is described below:

Step	Action	Machine
1	Prepare that indicated in <i>installation requirements</i> .	-
2	Install additional Shard databases.	<i>server in back end environment</i>
3	Check installation logs.	
4	Install additional Collectors.	<i>server in front end environment</i>
5	Check installation logs.	
6	Check redirecting on each Collector.	<i>same server or other computer</i>
7	Check for the installed objects in the System, Backend and Frontend sections.	<i>RCS Console</i>

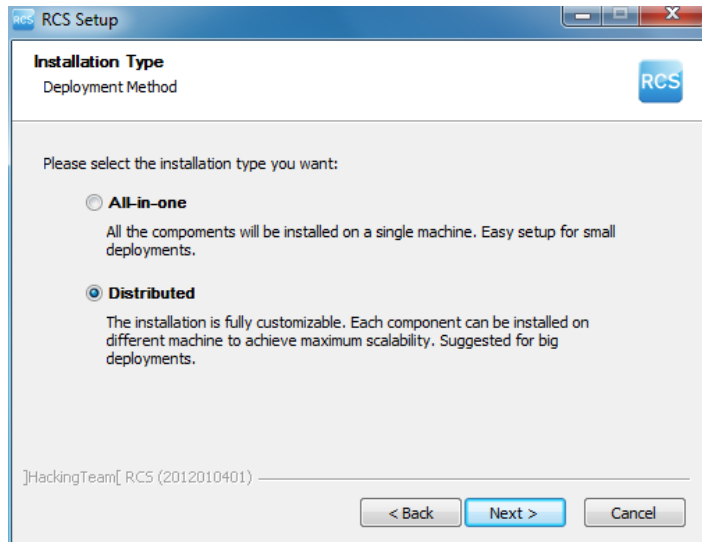
Additional Shard database installation

To install an additional Shard database in back end environment:

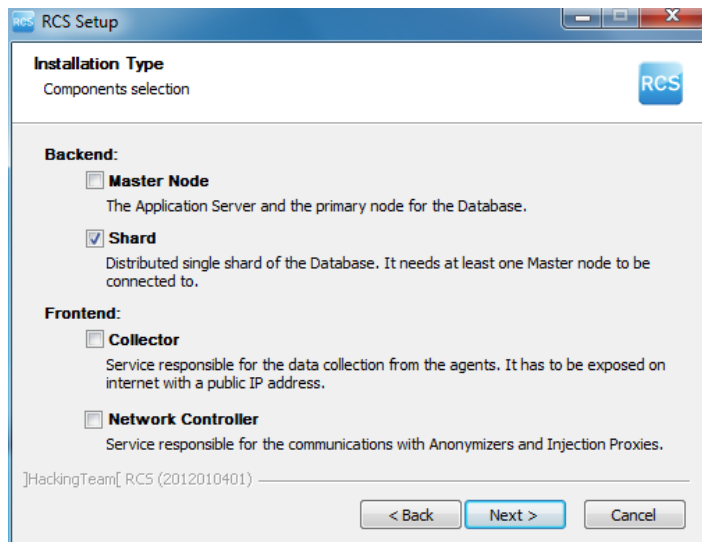
Steps	Result
<ol style="list-style-type: none"> 1. Insert the CD with the installation package. Run file RCS-<version>.exe in folder x:\setup: the first wizard window appears. 2. Click Next. 	

Steps

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

Result

5. Select **Shard**.
6. Click **Next**.

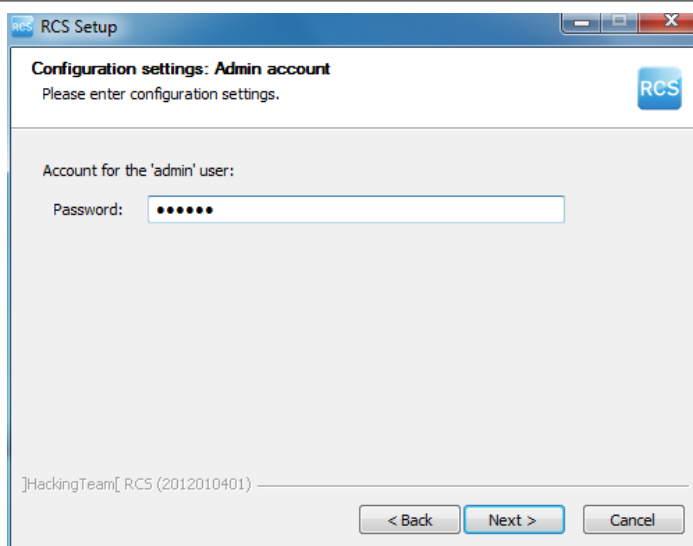


Steps

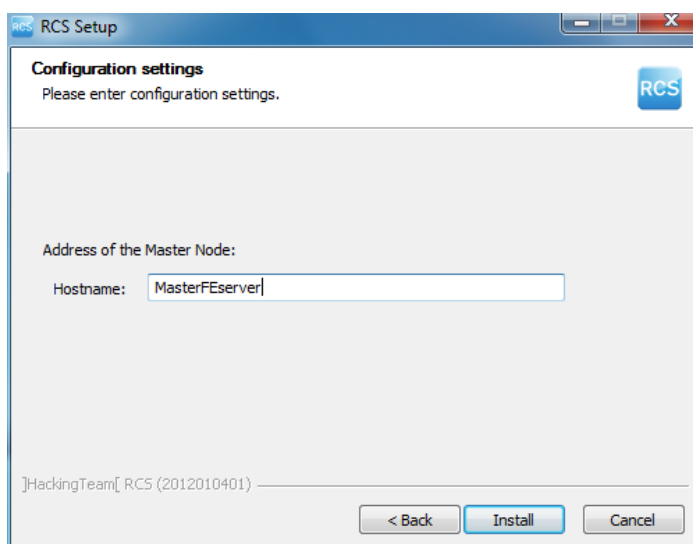
7. Enter the system administrator's password.
8. Click **Next**: when installation has completed, services are started and are ready to receive data and communicate with the RCS Console.

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



The screenshot shows the 'RCS Setup' window with the title 'Configuration settings: Admin account'. It prompts the user to 'Please enter configuration settings.' and shows a 'Password:' field with masked characters. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The footer text reads ']]HackingTeam[RCS (2012010401)'.



The screenshot shows the 'RCS Setup' window with the title 'Configuration settings'. It prompts the user to 'Please enter configuration settings.' and shows an 'Address of the Master Node:' section with a 'Hostname:' field containing 'MasterFEserver'. At the bottom, there are buttons for '< Back', 'Install', and 'Cancel'. The footer text reads ']]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 66 .

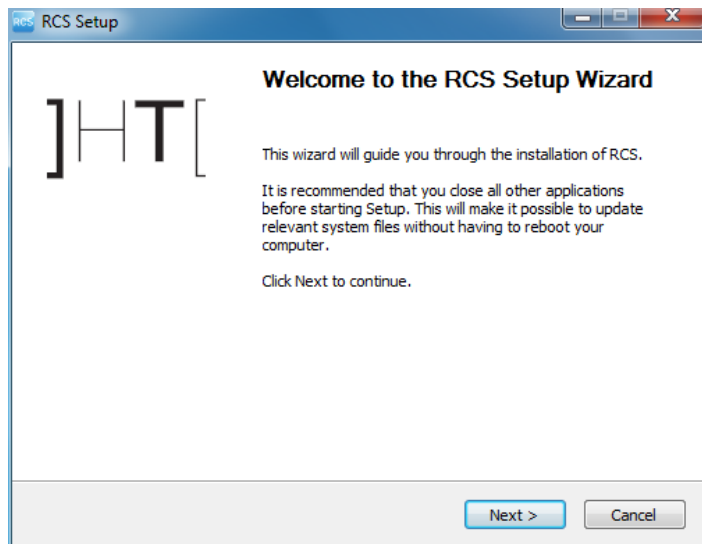
Additional Collector installation

To install several Collectors in front end environment:

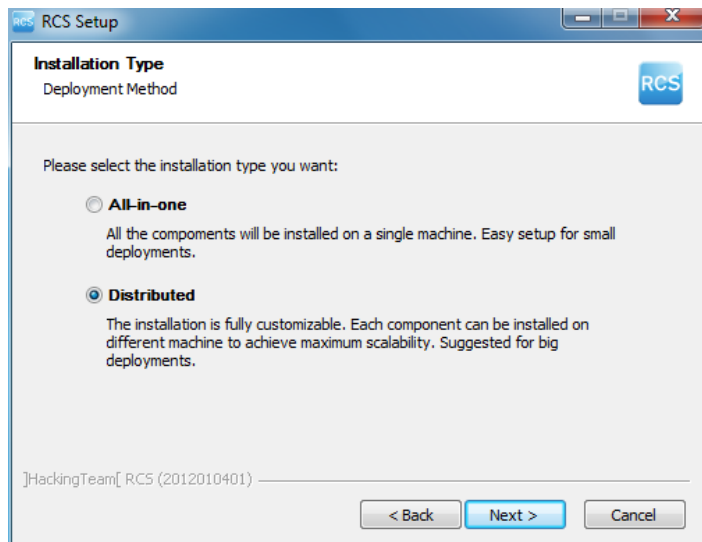
Steps

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**.

Result



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

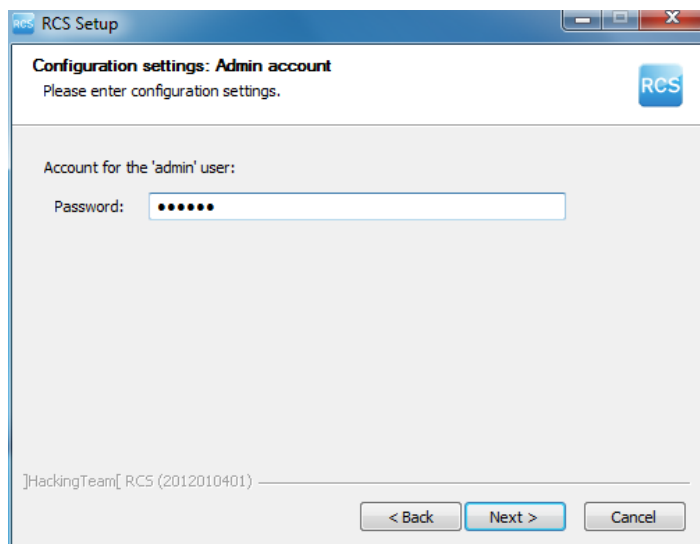
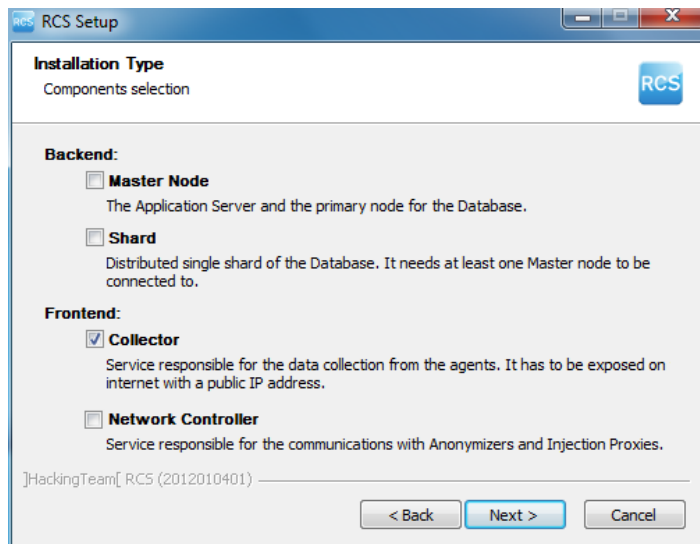


Steps

5. Select **Collector**.
6. Click **Next**.

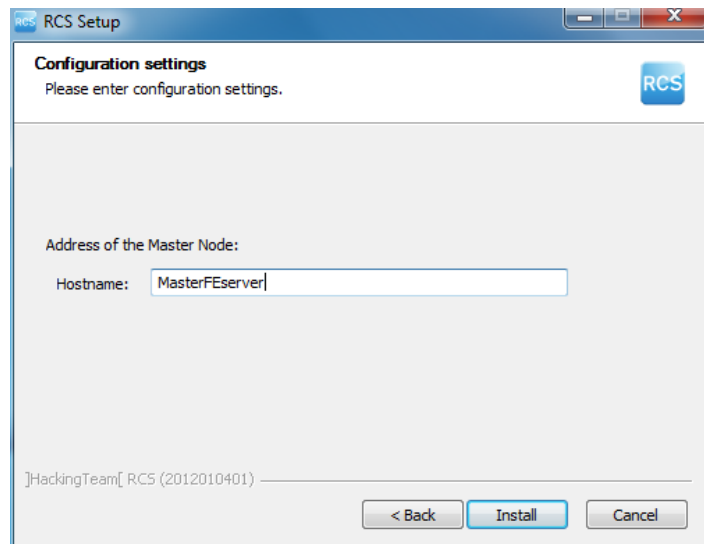
Result

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



Steps

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

Result**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:

<i>If</i>	<i>Then</i>
on the server	<ul style="list-style-type: none"> • open a browser • enter localhost • Result: the browser must be redirected to Google.
on another computer	<ul style="list-style-type: none"> • open a browser • enter <code>http://<front end server name or IP address></code>. • 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 71

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 91 .*



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

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	60
Routine maintenance procedures	60
RCS server update	61
RCS Console update	61
Anonymizer update	61
Network Injector Appliance update	62
Tactical Network Injector update	62

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 91*

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:

<i>Step</i>	<i>Action</i>
-------------	---------------

- | | |
|---|--|
| 1 | Run the <code>rsc-<version>.exe</code> 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

Network Injector Appliance can be fully re-installed, including the operating system.


Network Injector Appliance update



CAUTION: updating deletes all data on the machine.

To fully re-install Network Injector Appliance:

<i>Step</i>	<i>Action</i>
-------------	---------------

- 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 procedure 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 95
- 5 From RCS Console, **Monitor** section, check Network Injector status.

Tactical Network Injector update

Introduction

Tactical Network Injector can be fully installed, operating system included, or partially updated, excluding operating system re-installation.

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 Tactical Network Injector update

Tactical Network Injector is updated from an installation file distributed by HackingTeam support service.

Copy the installation file on the device and run it to complete updating without losing data.

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	65
Setup utilities	65
Editing Master Node settings	66
Modifica alla configurazione di Collector	67
Settings check	68

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 "--xxxx": "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:

<i>To edit...</i>	<i>Enter...</i>
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 "[Modifica alla configurazione di Collector](#)" on next page

<i>To edit...</i>	<i>Enter...</i>
the System administrator's password (admin)	<pre>> rcs-db-config -R <password></pre> <p>Result: certificates are updated and appear in folder \RCS\DB\config\certs. Collector settings must also be edited. See "Modifica alla configurazione di Collector" below</p>
backup folder	<pre>> rcs-db-config -B <folder></pre> <p> NOTE: "<folder>" can be a path for the RCS\db folder or absolute path.</p> <p> IMPORTANT: any backup files in the previously set folder will be copied to the new one.</p> <p>Result: all subsequent backup files are saved in the new folder.</p> <p> 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.</p>
outgoing mail server settings for alert e-mails	<pre>> rcs-db-config -M -server <hostName>:<portNumber></pre> <p>to set the outgoing main server name and port to be used.</p> <pre>> rcs-db-config -from <senderEmail></pre> <p>to set the alert e-mail sender's e-mail (i.e.: "alert@myplace.com").</p> <pre>> rcs-db-config -user <userName></pre> <p>To set the e-mail sender's user name.</p> <pre>> rcs-db-config -pass <password></pre> <p>To set his password.</p> <pre>> rcs-db-config -auth <authenticationType></pre> <p>To set the type of authentication to be used ("plain", "login" or "cram_md5").</p>

Modifica alla configurazione di Collector

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

To...

communicate the new Master
Node name/IP address

Enter...

```
> 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" }
```

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	70
System logs	71
Component status check procedure	73
Service restart procedures	74
Hardware component service procedures	77

Potential faults

Potential installation faults

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

<i>If...</i>	<i>Then...</i>
installation does not progress	make sure the hardware key is correctly inserted.
RCS console cannot connect to the server	<ul style="list-style-type: none"> Make sure you logged in with the System administrator's name, password and name of the server where Master Node was installed. <p>or</p> <ul style="list-style-type: none"> 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:

<i>If</i>	<i>And</i>	<i>Then</i>
cannot connect to Master Node	the hardware key is correctly inserted but Master Node service does not start	<ul style="list-style-type: none"> <i>check Master Node service status</i> <i>request hardware key replacement.</i>
data no longer arrives from agents	from RCS Console the Collector is running and correctly communicates	<i>check Collector status.</i>
The Master Node is not available	The Collector is running	<ul style="list-style-type: none"> <i>check whether an update is in progress</i> <i>check the Collector log file</i>
images are not converted into text	the OCR module is installed	<i>check how slow in the module log and install another OCR module (if in distributed architecture).</i>
The Collector is not available	-	<i>restart RCScollector service.</i>

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

Potential backup problems

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

<i>If</i>	<i>And</i>	<i>Then</i>
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 73

To restart services See "[Service restart procedures](#)" on page 74

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:

<i>Component</i>	<i>Analysis reason</i>
Master Node	Check problems with RCS Console.
Collector	Check data reception from agents.
OCR module	Check for any slow image conversions into text.
Network Controller	In the event of doubts on Network Injector or Anonymizer status.
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:

<i>Component</i>	<i>Folder</i>
Master Node	C:\RCS\DB\log
Collector	C:\RCS\Collector\log
OCR module	C:\RCS\DB\log
Network Controller	C:\RCS\Collector\log
Network Injector	/rcsnia/log
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:

<i>Severity level</i>	<i>Description</i>
Fatal	RCS is not running and requires service (i.e.: no settings, no certificates).
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_0000000001:47170c3e047b6d910e7ecc2e987060db2ff06cd8 | 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_000000001_47170c3e047b6a910e7ecc2e987060db2ff06cd8| WINDOWS | 2012-02-03 15:44:54 UTC | IDLE | 0 | 0 B |
|RCS_000000071_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 /rcsnia/log.

To learn more

To view logs see "[System logs](#)" on page 71

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, enter the following command:

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

To stop the service, enter the following command:

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

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:

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

Master Node replacement

The recommended procedure is described below:

<i>Step</i>	<i>Action</i>
1	Restore a server, repeating all installation operations. <i>See "RCS server installation in All-in-One architecture" on page 18 or "RCS server installation in distributed architecture" on page 22</i>
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, <i>See "What you should know about backup" on page 94</i>

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 91

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 46

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:

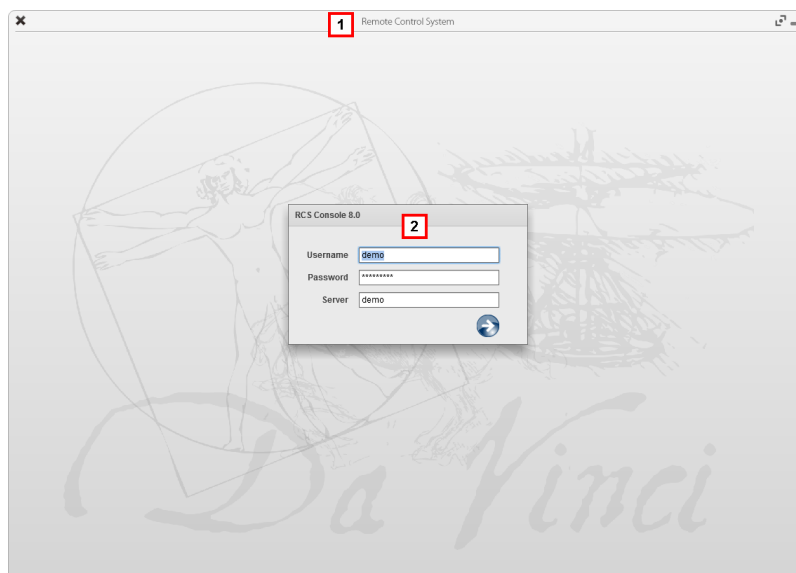
Starting the RCS Console	80
Homepage description	81
Wizards in the homepage	82
Shared interface elements and actions	83
Front end management	87
File Manager data	89
Back end management	90
Backup management	91
What you should know about backup	94
Managing the Network Injector	95
System monitoring (Monitor)	98
System monitoring data (Monitor)	100

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:



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

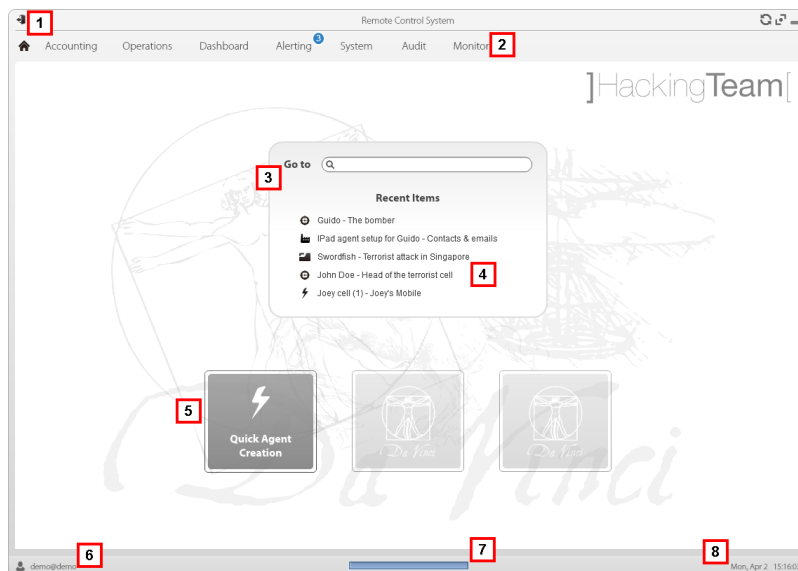
To view the homepage:  click 

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

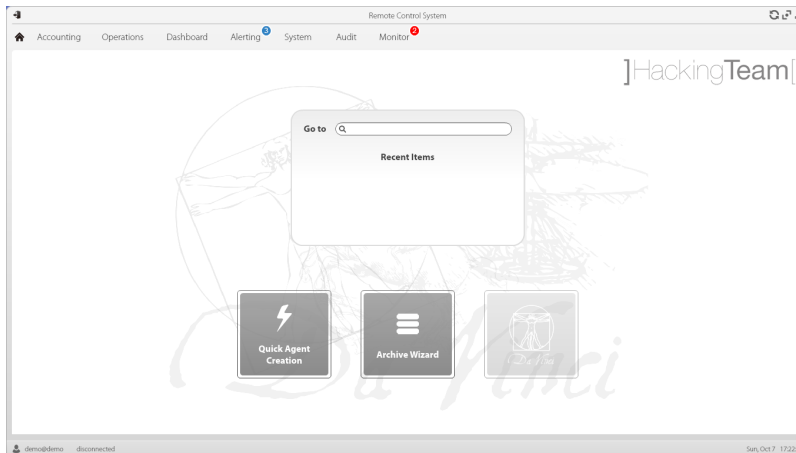
To view the homepage: • click 

Introduction

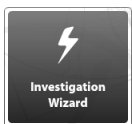
For users with certain privileges, RCS Console displays buttons that run wizards.

What it looks like

This is how the homepage is displayed with enabled wizards:



Button Function



Open the wizard to quickly create an agent.



NOTE: the button is only enabled for users with Administrator and Technician privileges.

Button Function



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.

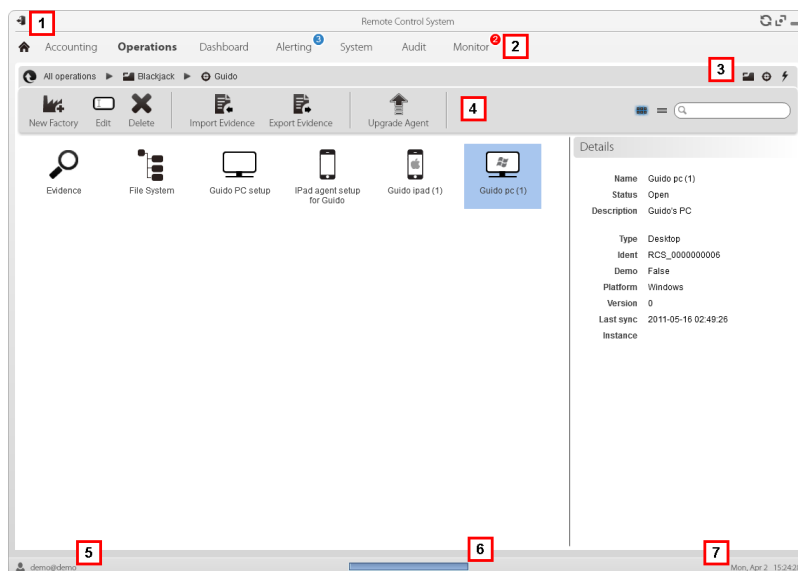
Shared interface elements and actions

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:






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.
- 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.

- 5 Window toolbar.
- 6 Search buttons and box:

Object	Description
	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.

- 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

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

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

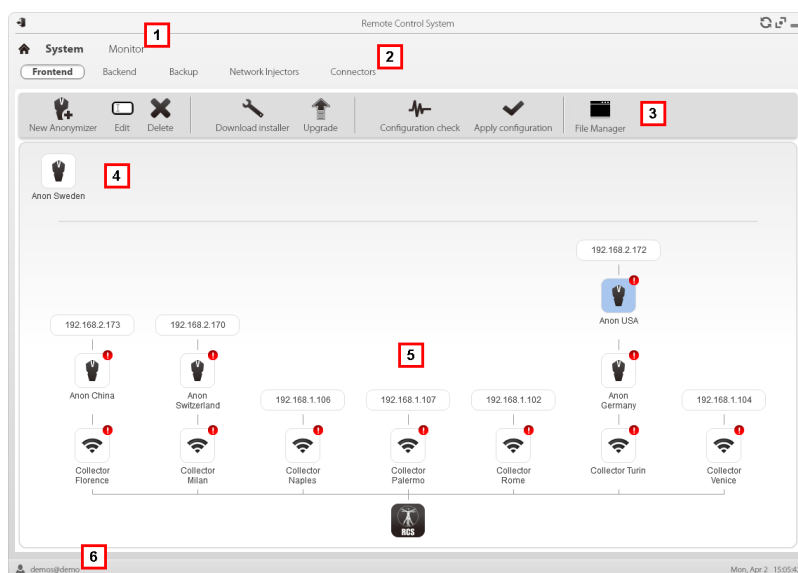
Function scope

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.

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 System menu.

Area Description

- 3** Window toolbar.
Descriptions are provided below:

Icon Description



Create a new Anonymizer.



Edit Anonymizer data.
After editing, click **Apply settings**.
Show last logs.



Tip: double-click an Anonymizer to check/edit data.



Delete an Anonymizer. This does not delete the Anonymizer installed on the VPS.



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.



Update the Anonymizer software version from remote.



Simulate agent behavior. It connects to each Anonymizer in the chain up to the gateway Collector, and returns connection results.



Update settings on all Anonymizers. This command is used after adding, deleting or changing the Anonymizer chain in use.



It shows packets automatically created on the Collector by **Exploit, WAP Push and QR Code** vectors made available for the target device. Files that are no longer used can be deleted.









CAUTION: deleting files too early could compromise infection by vectors.



NOTE: any files manually copied to the folder do not appear.

- 4** Anonymizers set but not yet included in a chain.

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 83 .

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.

<i>Field</i>	<i>Description</i>
--------------	--------------------

User	User who created the installer.
-------------	---------------------------------

Back end management

To manage back end:

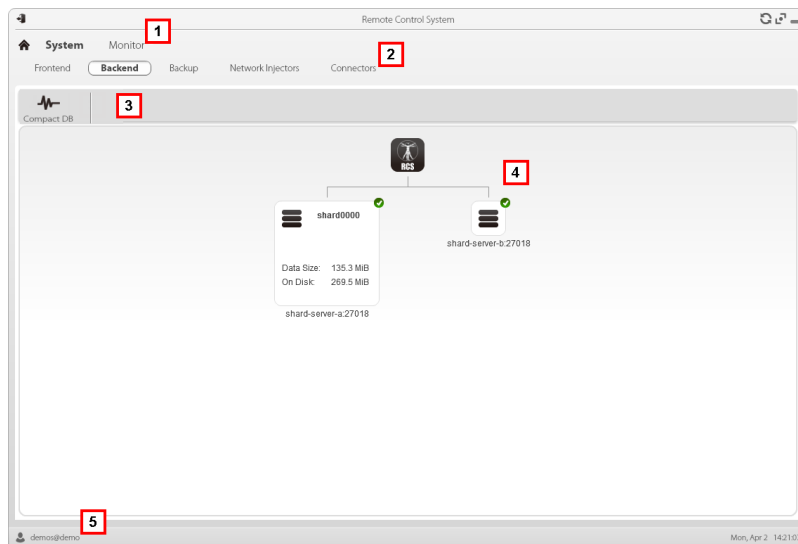
- System section, Backend

Function scope

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

What the function looks like

This is what the page looks like:



<i>Area</i>	<i>Description</i>
-------------	--------------------

- | | |
|----------|---------------------|
| 1 | RCS menu. |
| 2 | System menu. |

Area Description

- 3 Window toolbar. Descriptions are provided below:

Icon Description



Zip the database.

- 4 Shard database structures with their status, occupied and available disk space.



NOTE: database 0 is the one included in MasterNode.

- 5 RCS status bar.

To learn more

For interface element descriptions See "[Shared interface elements and actions](#)" on page 83 .
For further information on backups see "[What you should know about backup](#)" on page 94 .

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

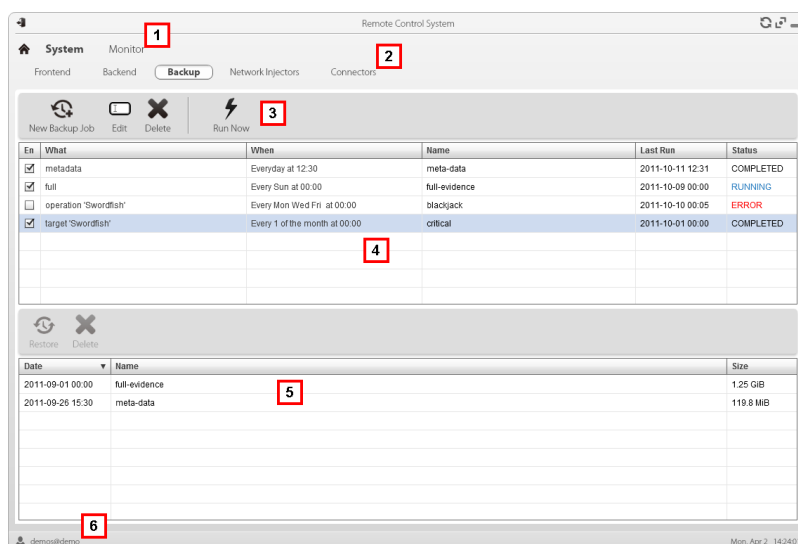
Function scope

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.

What the function looks like

This is what the page looks like:



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.

- 4 List of programmed backup processes (enabled and non) with last backup status.

Area Description

- 5 Backup toolbar. Descriptions are provided below:

Icon Description

Restore data from the selected backup file.



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



Deleting the backup file.

- 6 List of completed backups.
- 7 RCS status bar.
See "[Homepage description](#)" on page 81

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 66

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.

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.

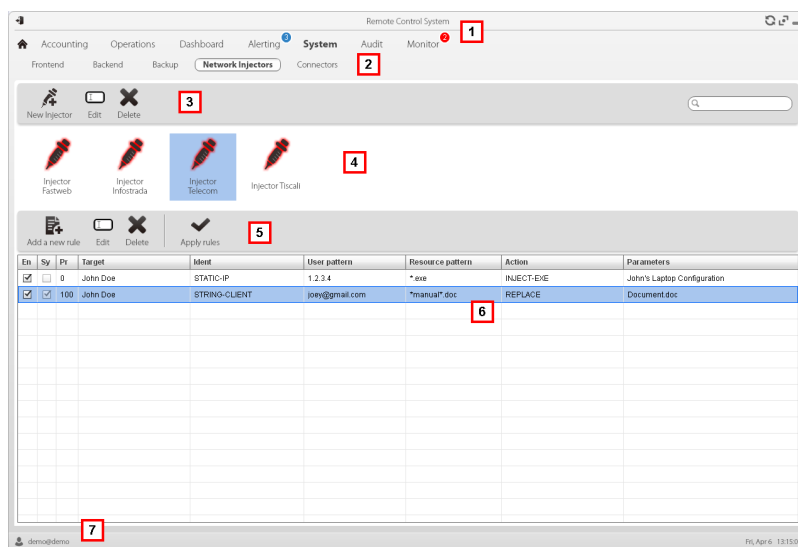
What you can do

With this function you can:

- create a new Network Injector

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 System menu.

Area Description

- 3 Network Injector toolbar. Descriptions are provided below:

Action Description


Add a new Network Injector



Edit Network Injector data.



Delete the selected Network Injector.

- 4 Network Injector list.

- 5 Injection rule toolbar. Descriptions are provided below:

Action Description


Add a new rule.



Open the window with rule data.



Delete the selected rule.



Update the selected Network Injector's settings.

- 6 List of selected Network Injector rules
En: select to enable the rules to be applied.
- 7 RCS status bar. .

To learn more




For interface element descriptions See "[Shared interface elements and actions](#)" on page 83 .

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 46 see "[Network Injector Appliance installation](#)" on page 42

Network Injector data

Selected Network Injector data is described below:

<i>Data</i>	<i>Description</i>
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 71 .  : update the list.  : delete viewed logs.

System monitoring (Monitor)

To monitor the system:

- Monitor section

Purpose

This function lets you:

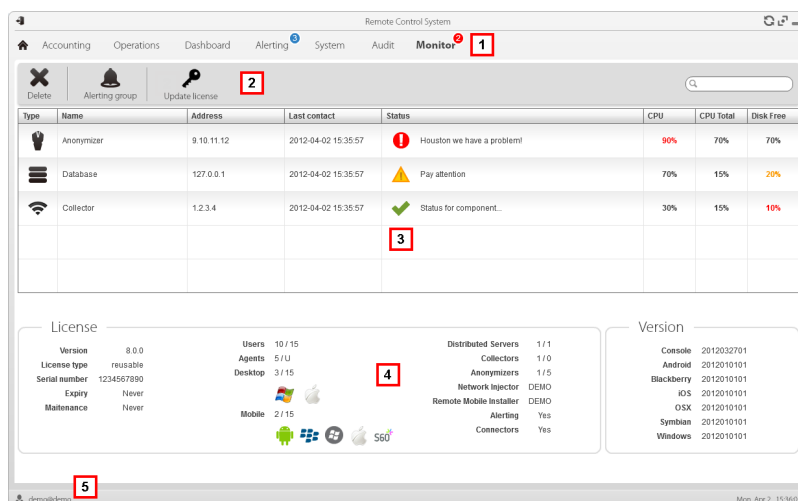
- monitor system status in both hardware and software terms
- delete elements to be monitored since uninstalled
- monitor license used compared to those purchased
- define the alerting group and alert e-mail addressee in the event of system alarms



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

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.

Monitor ¹: indicates the current number of system alarms triggered.

- 2 Window toolbar. Descriptions are provided below:

Icon Description

Deletes the component to be monitored.

Defines the alerting group.

Loads a new license file.

- 3 List of RCS components and their status:

Alarm (generates an e-mail sent to the alerting group)

Warning

Component running

- 4 License status.

Area Description

- 5 RCS status bar.

To learn more

For interface element descriptions See "[Shared interface elements and actions](#)" on page 83 .
For a description of the data in this window see "[System monitoring data \(Monitor\)](#)" below .

Deleting a component to be monitored

To delete an uninstalled component:

Step Action

- 1 Select the component.
- 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:

<i>Data</i>	<i>Description</i>
Type Name	Monitored component type and name:
	 Network Controller
	 Anonymizer
	 Database
	 Collector

<i>Data</i>	<i>Description</i>
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.
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.**

<i>Data</i>	<i>Description</i>
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.
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.

<i>Data</i>	<i>Description</i>
Anonymizers	Amount of Anonymizers currently used by the system and maximum admitted quantity.

]HackingTeam[

RCS 8.2 System Administrator's Guide
System Administrator's Guide 1.201 NOV-2012
© COPYRIGHT 2012
info@hackingteam.com

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
