

# ]HackingTeam[

## RCS 9.6

*The hacking suite for governmental interception*

---

### System administrator manual



## Information ownership

© COPYRIGHT 2015, 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.

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

HT S.r.l.

via della Moscova, 13

20121 Milan (MI)

Italy

**Tel.:** + 39 02 29 060 603

**Fax:** + 39 02 63 118 946

**e-mail:** [info@hackingteam.com](mailto:info@hackingteam.com)

# Contents

---

Guide introduction .....	1
Helpful information on the guide .....	1
Manual goals .....	1
New guide features .....	1
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) .....	5
RCS system architecture .....	6
Introduction .....	6
Architecture layout .....	6
Architecture components .....	6
What you should know about RCS .....	8
Operations .....	8
Data flow and protection .....	8
Data logging continuity .....	8
Digital certificates .....	8
Decoding data .....	9
Several RCS system architecture .....	9
Introduction .....	9
One-many architecture layout .....	9
Many-one architecture layout .....	10
Sender RCS systems .....	10
RCS receiver systems .....	10
Received data structure .....	11
RCS receiver system installation .....	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 .....	13
Minimum system requirements .....	14
Ports to be opened on the firewall .....	14
<b>System administrator procedures .....</b>	<b>15</b>
Introduction .....	15
Install RCS and setup components .....	15
Maintain and update the system .....	15
Monitoring the system .....	15
<b>RCS installation .....</b>	<b>16</b>
<b>What you should know about RCS installation .....</b>	<b>17</b>
Login privileges .....	17
Admin user and System administrator user .....	17
<b>RCS server installation .....</b>	<b>17</b>
Introduction .....	17
Installation requirements .....	17
Installation sequence .....	18
Master Node installation .....	18
Collector installation .....	21
Checking service start .....	23
Checking installation logs .....	23
Check IP addresses .....	23
Uninstall .....	23
<b>OCR module .....</b>	<b>23</b>
Introduction .....	23
Installation .....	23
OCR module operation .....	24
Space occupied by tagged text in the database .....	24
OCR module work load .....	24
Symptoms of excessive load .....	24
Checking correct OCR module operations .....	24
Disabling or re-enabling the OCR module .....	24
<b>List of RCS services .....</b>	<b>25</b>
Front end services .....	25

---

Backend services (Master Node) .....	25
Backend services (Shard) .....	25
To learn more .....	26
<b>RCS Console installation .....</b>	<b>26</b>
Introduction .....	26
Requirements .....	26
Installation sequence .....	26
Adobe AIR installation .....	26
RCS Console installation .....	27
RCS Console uninstall .....	28
Creating the Administrator user .....	28
<b>Files installed at the end of installation .....</b>	<b>29</b>
Installed files .....	29
<b>Additional component installation .....</b>	<b>31</b>
<b>What you should know about Anonymizer .....</b>	<b>32</b>
Introduction .....	32
Anonymizer status .....	32
Communications between Anonymizer and Collector .....	33
Faulty Anonymizer .....	34
<b>Anonymizer installation and settings .....</b>	<b>34</b>
Installation requirement .....	34
Installation .....	34
Anonymizer data .....	35
Boot check .....	35
IP address check .....	36
Editing settings .....	36
Uninstall .....	36
<b>What you should know about Network Injector Appliance .....</b>	<b>37</b>
Introduction .....	37
Main functions .....	37
Network connections .....	37
Authentication key .....	37
Standard connection layout .....	37
Connection layout as an intra-switch segment .....	38

---

Data sniffing via TAP, SPAN port .....	38
<b>Network Injector Appliance installation .....</b>	<b>39</b>
Introduction .....	39
Package content .....	39
Installation sequence .....	39
Rear panel description .....	39
Network connections .....	40
Operating system installation and settings .....	41
Verifying the IP address .....	43
Changing the IP address .....	43
Uninstall .....	43
<b>What you should know about Tactical Network Injector .....</b>	<b>44</b>
Introduction .....	44
Main functions .....	44
Network connections .....	44
Authentication key .....	44
Standard connection layout .....	44
Access point emulation connection diagram .....	45
<b>Tactical Network Injector installation .....</b>	<b>46</b>
Introduction .....	46
Package content .....	46
Installation sequence .....	46
Operating system installation and settings .....	46
Verifying the IP address .....	48
Changing the IP address .....	49
Uninstall .....	49
<b>Other applications installed on Network Injectors .....</b>	<b>49</b>
Introduction .....	49
Applications .....	49
<b>Tactical Control Center and Appliance Control Center commands .....</b>	<b>50</b>
Introduction .....	50
Commands .....	50
<b>First Network Injector synchronization with RCS server .....</b>	<b>51</b>
Introduction .....	51

---

Synchronizing a Network Injector with RCS server .....	51
Checking Network Injector status .....	52
Introduction .....	52
Identifying when Network Injector is synchronized .....	52
Viewing Network Injector logs .....	52
Additional component installation .....	53
Introduction .....	53
Additional component installation requirements .....	53
Installation sequence .....	53
Additional Shard database installation .....	53
Additional Collector installation .....	55
Checking service start .....	57
Checking installation logs .....	57
Check IP addresses .....	57
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 .....	60
Update requirements .....	60
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 .....	61

---

Network Injector Appliance update .....	62
Introduction .....	62
Full Network Injector Appliance update .....	62
Partial update with infection in progress .....	62
Partial update without infection in progress .....	63
Tactical Network Injector update .....	64
Introduction .....	64
Full Tactical Network Injector update .....	64
Partial update .....	65
Editing Master Node and Collector settings .....	67
What you should know about settings .....	68
What you can edit .....	68
When to edit settings .....	68
Order used to edit settings .....	68
Mail server settings .....	68
Setup utilities .....	68
RCS utilities .....	68
Utility command syntax .....	69
Other options .....	69
Editing Master Node settings .....	69
Editing the Collector configuration .....	70
Settings check .....	71
Introduction .....	71
Example of settings check output .....	71
Troubleshooting .....	72
Potential faults .....	73
Potential installation faults .....	73
Possible server problems .....	73
Potential backup problems .....	74
To learn more .....	74
System logs .....	74
Introduction .....	74
Log analysis utility .....	74
Log file example .....	75



---

RCS log files .....	75
Quick log display .....	75
Log file content .....	75
<b>Component status check procedure .....</b>	<b>76</b>
Introduction .....	76
Installed license check .....	76
Master Node status check .....	76
Checking Worker service status .....	76
Check agent status via Collector .....	76
Network Injector start check .....	77
Check system components .....	77
Support service file creation .....	77
To learn more .....	78
<b>Service restart procedures .....</b>	<b>78</b>
Introduction .....	78
<b>Hardware component service procedures .....</b>	<b>79</b>
Introduction .....	79
Hardware key replacement .....	79
Master Node replacement .....	79
Shard replacement .....	80
Replacing the Collector .....	80
Replacing an Anonymizer .....	80
Replacing a Network Injector Appliance .....	80
Replacing a Tactical Injector Appliance .....	80
<b>RCS Console for the System administrator .....</b>	<b>81</b>
<b>Starting the RCS Console .....</b>	<b>82</b>
Introduction .....	82
Restoring disabled users who entered incorrect passwords .....	82
What the login page looks like .....	82
Open RCS Console .....	83
<b>Homepage description .....</b>	<b>83</b>
Introduction .....	83
What it looks like .....	83
<b>Wizards in the homepage .....</b>	<b>84</b>

---

Introduction .....	84
What it looks like .....	85
Quick Save .....	85
<b>Shared interface elements and actions .....</b>	<b>86</b>
Introduction .....	86
What the RCS Console looks like .....	86
Change interface language or password .....	88
Converting the RCS Console date-time to the actual time zone .....	88
Table actions .....	89
<b>Front end management .....</b>	<b>91</b>
Function scope .....	91
What the function looks like .....	91
To learn more .....	92
Adding an Anonymizer to the configuration .....	93
Editing Anonymizer settings .....	93
File Manager data .....	93
<b>Back end management .....</b>	<b>93</b>
Function scope .....	93
What the function looks like .....	93
To learn more .....	94
Significant Shard database data .....	94
<b>What you should know about backup .....</b>	<b>96</b>
Management responsibilities .....	96
Backup methods .....	96
Metadata type backup .....	96
Full type backup .....	96
Operation type backup .....	96
Target type backup .....	96
Incremental backup .....	96
Backup restore for severe reasons .....	97
Backup data restore .....	97
<b>Full backup for serious reasons .....</b>	<b>97</b>
Introduction .....	97
Run backup .....	97

---

Restore backup .....	98
<b>Backup management .....</b>	<b>98</b>
Function scope .....	98
What the function looks like .....	98
Significant backup process data .....	100
<b>Connector management .....</b>	<b>100</b>
Function scope .....	100
What the function looks like .....	100
To learn more .....	101
Significant connection rule data .....	101
<b>Managing the Network Injector .....</b>	<b>102</b>
Purpose .....	102
What you can do .....	102
To learn more .....	104
Updating Network Injector control software .....	104
Network Injector data .....	104
<b>System monitoring (Monitor) .....</b>	<b>105</b>
Purpose .....	105
What the function looks like .....	105
To learn more .....	106
Deleting a component to be monitored .....	106
System monitoring data (Monitor) .....	106
<b>Glossary .....</b>	<b>109</b>

## Illustration list

---

<i>Figure 2.1: RCS architecture: logical layout</i> .....	6
<i>Figure 2.1: One to many RCS architecture layout: logical layout</i> .....	9
<i>Figure 2.2: Many to one RCS architecture: logical layout</i> .....	10
<i>Figure 4.1: Master Node services and dependencies</i> .....	25
<i>Figure 4.2: Shard services and dependencies</i> .....	26
<i>Figure 5.1: Anonymizer chain example</i> .....	32
<i>Figure 5.2: Information flow between Anonymizer and Collector</i> .....	33
<i>Figure 5.3: Information flow between Anonymizer and Collector with a faulty Anonymizer</i> .....	34
<i>Figure 5.1: Network Injector Appliance: physical layout</i> .....	38
<i>Figure 5.2: Network Injector Appliance with TAP: physical layout</i> .....	38
<i>Figure 5.1: Tactical Network Injector: standard connection layout</i> .....	45
<i>Figure 5.2: Tactical Network Injector: access point emulation diagram</i> .....	45

# Guide introduction

## Helpful information on the guide

### 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

### New guide features

List of release notes and updates to this online help.

<i>Release date</i>	<i>Code</i>	<i>Software version.</i>	<i>Description</i>
March 15, 2015	System administrator manual 1.9 MAR-2013	9.6	Updated RCS server, Collector and Shard installation procedures, see " <a href="#">RCS server installation</a> " on page 17 and " <a href="#">Additional component installation</a> " on page 53. Added automatic incorrect password entry disabling and restore procedures, see " <a href="#">Starting the RCS Console</a> " on page 82.
November 24, 2014	System administrator manual 1.9 MAR-2013	9.5	Updated communication procedure between Network Injector and RCS server, see " <a href="#">RCS system architecture</a> " on page 6. Updated first Network Injector and RCS server synchronization procedure see " <a href="#">First Network Injector synchronization with RCS server</a> " on page 51.
September 20, 2014	System administrator manual 1.7 SET-2014	9.4	Updated communication methods between Collector and Anonymizer, see " <a href="#">RCS system architecture</a> " on page 6 and " <a href="#">What you should know about Anonymizer</a> " on page 32. Added Master Node RCSMonitor service, see " <a href="#">RCS system architecture</a> " on page 6 and " <a href="#">List of RCS services</a> " on page 25.

<b>Release date</b>	<b>Code</b>	<b>Software version.</b>	<b>Description</b>
June 23, 2014	System administrator manual 1.6 JUN-2014	9.3	<p>Added list of third party applications installed on Network Injector, see "<a href="#">Other applications installed on Network Injectors</a>" on page 49.</p> <p>Removed All-in-one architecture type.</p> <p>Added several RCS system architectures, see "<a href="#">Several RCS system architecture</a>" on page 9.</p> <p>Added utilities for RCS component troubleshooting, see "<a href="#">Component status check procedure</a>" on page 76</p> <p>Added dependencies between RCS services, see "<a href="#">List of RCS services</a>" on page 25 see "<a href="#">List of RCS services</a>" on page 25</p> <p>"<a href="#">RCS server update</a>" on page 60</p>
February 19, 2014	System administrator manual 1.5 FEB-2014	9.2	<p>Updated Anonymizer installation and update management, see "<a href="#">Anonymizer installation and settings</a>" on page 34 , "<a href="#">Anonymizer update</a>" on page 61.</p> <p>Added Collector Carrier service, see "<a href="#">What you should know about RCS</a>" on page 8</p> <p>Edited commands to check component status, see "<a href="#">Component status check procedure</a>" on page 76.</p> <p>Added description of terminal commands for Tactical Control center and Appliance Control Center applications, see "<a href="#">Tactical Control Center and Appliance Control Center commands</a>" on page 50</p>
September 30, 2013	System administrator manual 1.4 SET - 2013	9	<p>Updated Network Injector installation, update and management documentation, see "<a href="#">Additional component installation</a>" on page 31, "<a href="#">Routine maintenance and software updates</a>" on page 59, "<a href="#">Managing the Network Injector</a>" on page 102.</p> <p>Updated connector documentation, see "<a href="#">Connector management</a>" on page 100.</p> <p>Updated documentation due to improvements to the user interface.</p>

## Supplied documentation

The following manuals are supplied with RCS software:

## 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 " <b>User data</b> "	<i>italic</i>	this indicates a chapter, section, sub-section, paragraph, table or illustration heading in this manual or other publication of reference.
<ddmmyyyy>	<aaa>	indicates text that must be specified by the user according to a certain syntax. In the example <ddmmyyyy> is a date and could be "14072011".
Select one of the listed servers <b>[2]</b> .	<b>[x]</b>	indicates the object specified in the text that appears in the adjacent image.
Click <b>Add</b> . Select the <b>File menu, Save data</b> .	<b>bold</b>	indicates text on the operator interface, a graphic element (i.e.: table, tab) or screen button (i.e.: display).

<i>Example</i>	<i>Style</i>	<i>Description</i>
Press Enter	capital first letter	indicates a keyboard key name.
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>
<b>System administrator</b>	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.	Expert network technician
	 <b>WARNING: the system administrator must have the required necessary skills. The HackingTeam is not liable for equipment malfunctions or damages due to unprofessional installation.</b>	
<b>Administrator</b>	Creates authorized accounts and groups. Creates operations and target. Monitors system and license status.	Investigation manager
<b>Technician</b>	Creates and sets up agents. Sets Network Injector rules	Tapping specialist technician
<b>Analyst</b>	Analyzes and exports evidence.	Operative

## Software author identification data

HT S.r.l.

via della Moscova, 13

20121 Milan (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:

---

<b>RCS system architecture</b> .....	<b>6</b>
<b>What you should know about RCS</b> .....	<b>8</b>
<b>Several RCS system architecture</b> .....	<b>9</b>

## RCS system architecture

### 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.

### Architecture layout

Software components are installed on several server. The architecture layout is provided below:

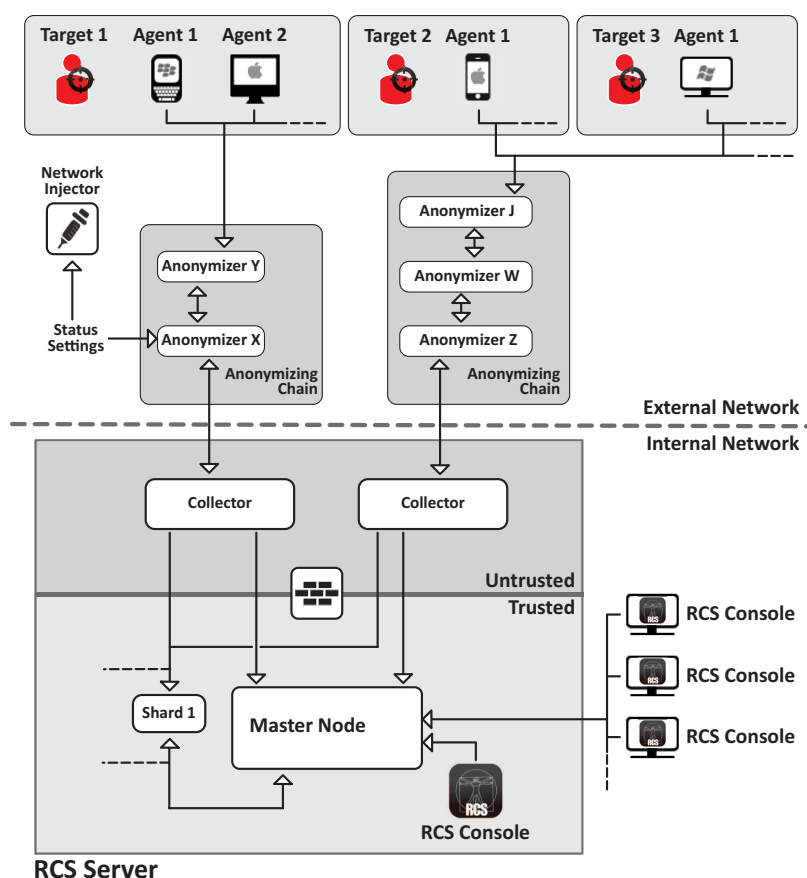


Figure 2.1: RCS architecture: logical layout

### Architecture components

Architecture components are provided below:

<b>Component</b>	<b>Function</b>	<b>Installation</b>
<b>Agent</b>	Software bugs tap and communicate the investigation target's data and information to an Anonymizer.	<ul style="list-style-type: none"> <li>target devices</li> <li>data sources</li> </ul>
<b>Anonymizing chain Anonymizer</b>	Geographically distributed Anonymizer groups that guarantee Collector anonymity and redirect collected data to protect servers from remote attacks. Transfers agent and Network Injector data to servers. Several Anonymizers can be set up in a chain to increase the level of protection. Each chain leads to one Collector.	VPS (Virtual Private Server)
<b>Collector</b>	<p>One per Anonymizing Chain. Three services are installed in each:</p> <ul style="list-style-type: none"> <li>Collector: collects agent data sent to the last Anonymizer in the chain and Network Injectors sent to the set Anonymizer.</li> <li>Carrier: sends data to Shards and Master Node</li> <li>Network Controller: receives Anonymizer status and logs and sends them updates and new settings.</li> </ul> <p>It requires a single license.</p>	one or more servers in front end environment
<b>Firewall</b>	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).	RCS server
<b>RCS console</b>	Setup, monitoring and analysis console used by operating center workers.	<ul style="list-style-type: none"> <li>RCS server</li> <li>internal network</li> </ul>
<b>Master Node</b>	Heart of the RCS server, it manages data flows, component status and includes the first Shard database. It includes Worker service to decode data before it is saved to the database and Monitor service to monitor all architecture components, including Master Node and sends e-mail in the event of alarms.	RCS server
<b>Network Injector</b>	(optional) Fixed hardware component (Appliance) or notebook (Tactical), it runs sniffing and injection operations on the target's HTTP connections. Communicates with the Collector via an Anonymizer (and its chain) to send data and receive rules and settings.	<ul style="list-style-type: none"> <li>ISP</li> <li>Wired or Wireless LAN (homes, hotel)</li> </ul>

<b>Component</b>	<b>Function</b>	<b>Installation</b>
<b>Shard x</b>	Additional RCS distributed database partitions. Shard 0 is included in Master Node. It includes Worker service to decode data and enter it in the database.	one or more servers in back end environment
<b>Target</b>	Investigation targets. Each device owned by the target is a data source and can be monitored by an agent.	-

## 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) and sent to the trusted environment via a specific service (Carrier). Remote entity status and settings are checked by a specific Collector machine 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 "[RCS system architecture](#)" on page 6.

### 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 Carrier 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.

### Digital certificates

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

Some agents 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 29

## 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.

## Several RCS system architecture

### Introduction

RCS can be set to communicate with other RCS systems to send or receive evidence received from agents.

There are two possible communication scenarios:

- one to many: an RCS system receives all evidence from agents and distributes them to several RCS systems that only display and process evidence of their interest. For example, if evidence is collected from a single central agency but investigations are conducted by several local courts.
- many to one: various RCS systems receive evidence from agents and send them to a single RCS system that displays and processes all of them. For example, if evidence is collected and processed by a local agency but there is a central agency that monitors the various local agencies and conducts global investigations.

### One-many architecture layout

The one-many architecture layout is provided below:

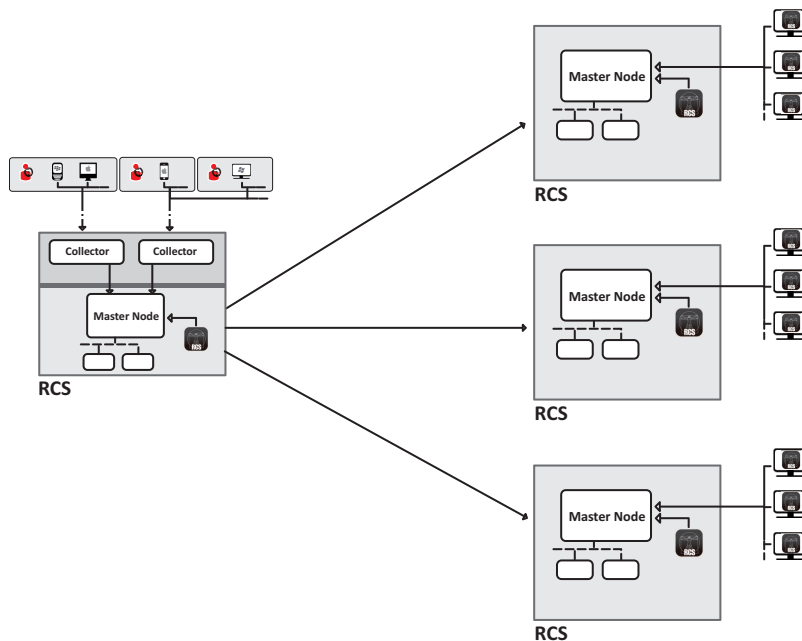


Figure 2.1: One to many RCS architecture layout: logical layout

## Many-one architecture layout

The many-one architecture layout is provided below:

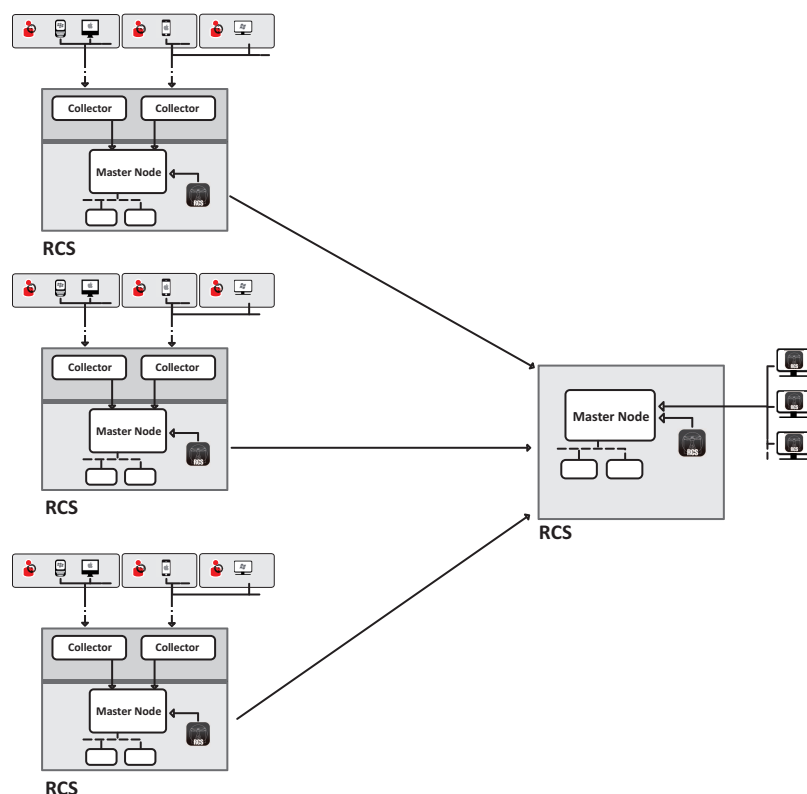


Figure 2.2: Many to one RCS architecture: logical layout

## Sender RCS systems

An RCS sender system (both in one-many and many-one architecture) is a complete RCS system. It includes the installation of a Collector and any other additional and optional components that allow for evidence to be received from agents installed on target devices. See "[RCS system architecture](#)" on page 6

Data transfer to one or more receiver RCS is set with RCS Console using connection rules, see "[Connector management](#)" on page 100.

## RCS receiver systems

The main purpose of an RCS receiver system (in both many-one and one-many architecture) is to display and process evidence. The evidence it has is only received from one or more RCS sender systems, never directly from agents.

The main operations enabled in RCS Console are those that concern evidence management and processing. On the other hand, agents are fully managed and set by the RCS sender system. The main components are Master Node, RCS Console and any additional shards.



NOTE: if data is received from a single RCS system, the only evidence that is displayed and can be processed are those from its own investigations. If data is received from several RCS systems, all evidence is displayed and can be cross-processed by several investigations.

## Received data structure

Data is received organized and named as set in the sender system's RCS Console. However, names can be changed to be better interpreted without creating communication problems between systems.

If data is received from several RCS systems, data arrive linked to the RCS sender system identifier.

## RCS receiver system installation



NOTE: RCS receiver systems require a specific user license.

The full installation sequence is provided below:

<b>Step</b>	<b>Action</b>	<b>See</b>
1	Install Master Node.	<a href="#">"RCS server installation" on page 17</a>
2	Check installation logs.	
3	Make sure Master Node services have started.	
4	Install RCS Console.	<a href="#">"RCS Console installation" on page 26</a>
5	Install any additional shards.	<a href="#">"Additional component installation" on page 53</a>

---

# 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 installation is optional and will be documented in the following chapters.

### Content

This section includes the following topics:

---

<b>Package content</b> .....	<b>13</b>
<b>System administrator procedures</b> .....	<b>15</b>



## 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:

<i>Folder</i>	<i>Included files</i>	<i>Description</i>
x:	ChangeLog.pdf	Release notes
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	RCS installation and user manuals. Each manual is addressed to a specific user role. <ul style="list-style-type: none"> <li>• x.x: RCS version.</li> <li>• y.y: manual version.</li> <li>• Language: manual language.</li> </ul>
x:\setup	AdoberAIRinstaller.exe	Adobe AIR installation file.
x:\setup	RCS-version.exe	RCS server(s) installation file.
x:\setup	RCSconsole-version.air	RCS Console installation file.

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

## Ports to be opened on the firewall

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

<i>From...</i>	<i>To...</i>	<i>Port to open</i>
Anonymizer	Collector	80
Collector	Master Node	443
Collector	remote	all
Carrier	Master Node/Shard	442
Master Node	Collector	80
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.

### Install RCS and setup components

Following is the RCS architecture component installation procedure:

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

---

- 1 Prepare the installation environment.  
See "[Installation introduction](#)" on page 12.
- 2 Install the RCS server.  
See "[RCS installation](#)" on page 16.
- 3 Install the RCS Consoles.  
See "[RCS Console installation](#)" on page 26.
- 4 Install and setup up Anonymizers.  
See "[Anonymizer installation and settings](#)" on page 34
- 5 (optional) Install the Shard databases and additional Collectors.  
See "[Additional component installation](#)" on page 53.
- 6 (optional) Install Network Injectors.  
See "[What you should know about Network Injector Appliance](#)" on page 37.  
See "[What you should know about Tactical Network Injector](#)" on page 44.

### 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 67.
- See "[Troubleshooting](#)" on page 72.

### Monitoring the system

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

- See "[RCS Console for the System administrator](#)" on page 81

---

# RCS installation

## Presentation

### Introduction

RCS installation requires intervention on various local and remote servers.

### Content

This section includes the following topics:





---

<b>What you should know about RCS installation .....</b>	<b>17</b>
<b>RCS server installation .....</b>	<b>17</b>
<b>OCR module .....</b>	<b>23</b>
<b>List of RCS services .....</b>	<b>25</b>
<b>RCS Console installation .....</b>	<b>26</b>
<b>Files installed at the end of installation .....</b>	<b>29</b>

## 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

### 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. See "[RCS Console installation](#)" on page 26

### 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 full installation sequence is provided below:

<b>Step</b>	<b>Action</b>	<b>Machine</b>
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	Installing the first Collector.	<i>server in front end environment</i>
6	Check installation logs.	
7	Install RCS Console.	<i>server in back end environment or other computer</i>
8	Setup the backup folder on the remote unit.	<i>server in back end environment</i>

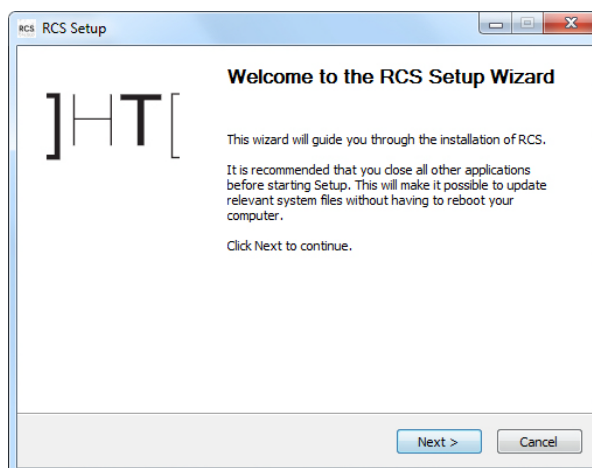
## Master Node installation

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

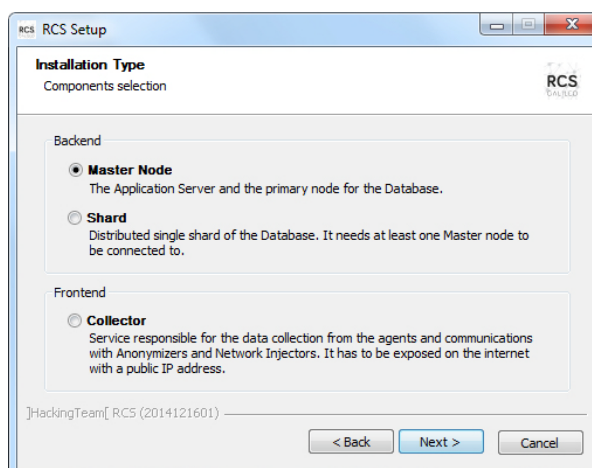
<b>Steps</b>	<b>Result</b>
1. Insert the hardware key.	-

**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 **Master Node**.
5. Click **Next**.

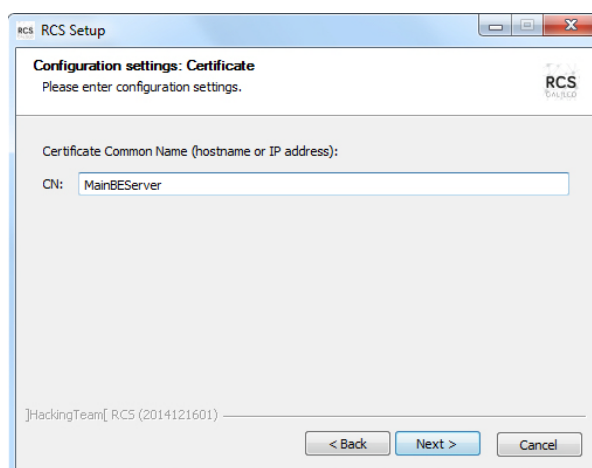


6. Enter the server name or IP address where the software is being installed and that will be indicated at RCS Console login (i.e.: MainBEServer).



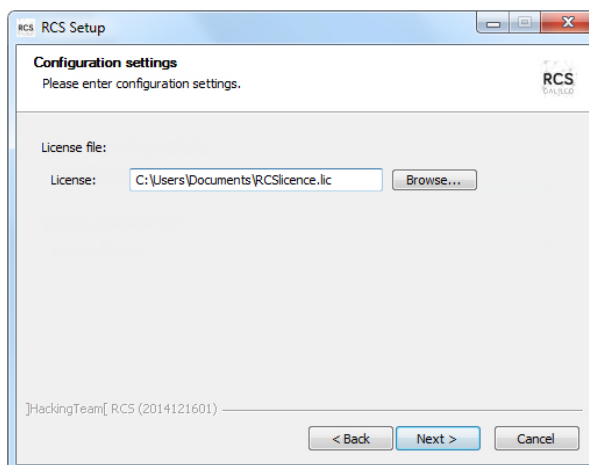
**IMPORTANT: the name and IP address must be univocal.**

7. Click **Next**.

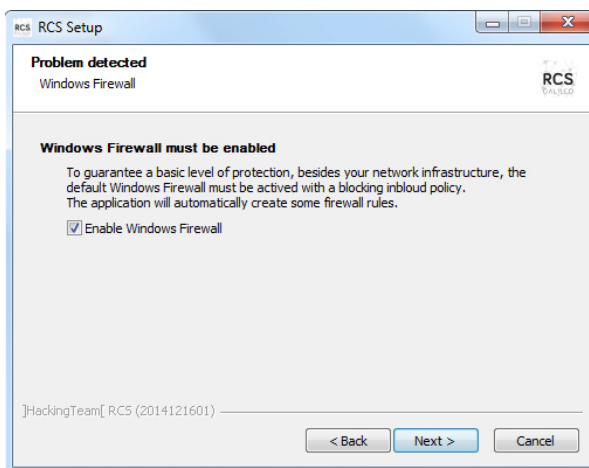


**Steps**

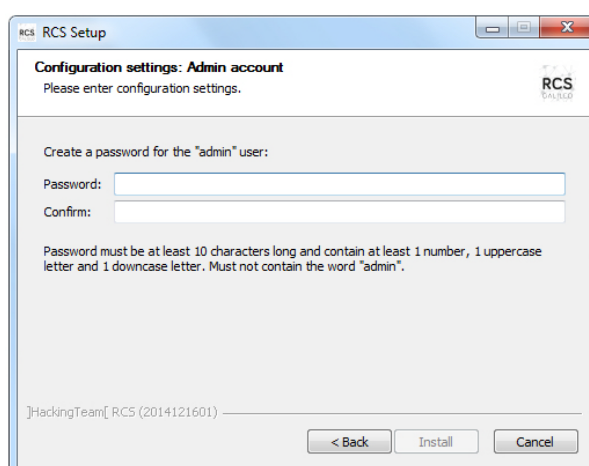
8. Select the license file.
9. Click **Next**.

**Result**

10. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.



11. Enter the System administrator's password.
12. Click **Install**: when installation has completed, services are started and are ready to receive data and communicate with the RCS Console.







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

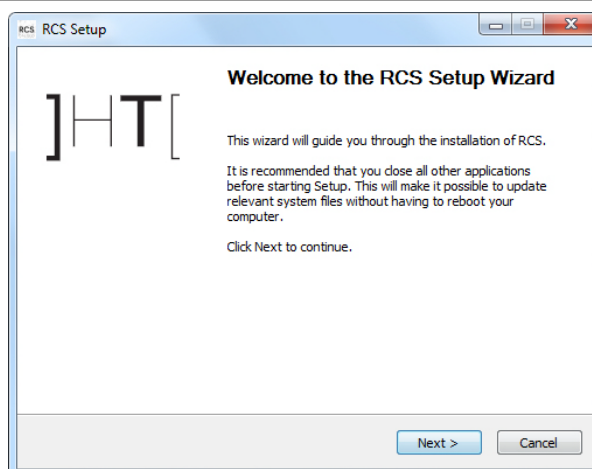
## Collector installation

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

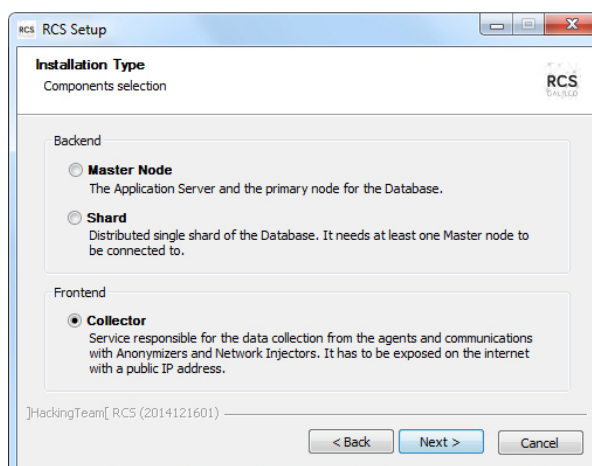


3. Select **Collector**.



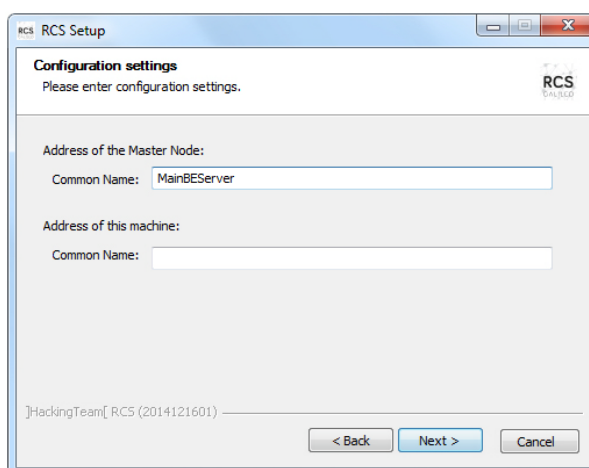
NOTE: all Collector services are automatically installed.

4. Click **Next**.

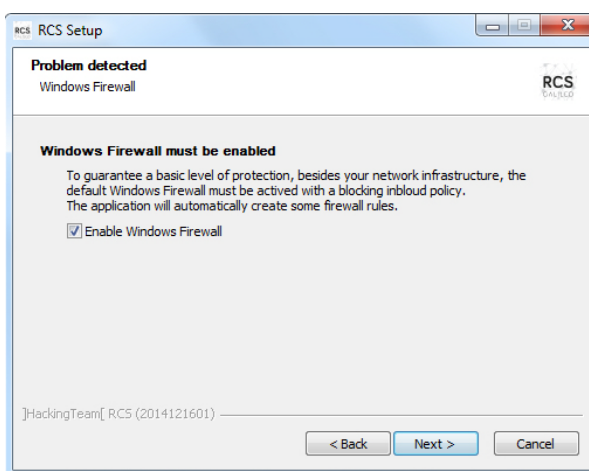


**Steps**

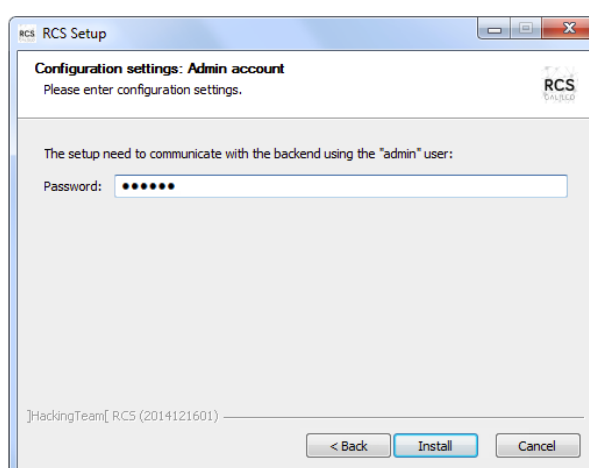
5. Enter the name or IP address of the Master Node server (i.e.: MainBEServer) and machine where Collector is being installed (i.e.: ServerB).
6. Click **Next**: when installation has completed, services start and attempt to communicate with Master Node. The server in back end environment is protected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

**Result**

7. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.



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



## Checking service start

Make sure all RCS services are up and running. If services are not running, manually start them. See "[List of RCS services](#)" on page 25.



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

## Checking installation logs

If errors occur during installation, check logs and send them to support service if necessary. See "[System logs](#)" on page 74

## Check IP addresses

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

## Uninstall

RCS can be uninstalled from the Windows Control Panel.



**CAUTION: All saved data is lost when Master Node is uninstalled. For correct operations, backup data. See "[Backup management](#)" on page 98.**



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

# OCR module

## Introduction

The OCR module is an optional module that indexes all content (i.e.: in addition to traditional documents, also images, audio, video) for full-text search. Furthermore, it runs "face detection" in images to help intelligence create target profiles.



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

## Installation

The OCR module is automatically installed and enabled when Master node and any additional shards are installed.



NOTE: the module is only enabled if included in the license.

## OCR module operation

OCR module operation are described below:

<i>Phase</i>	<i>Description</i>
1	Screenshot evidence images and all types of documents, awaiting conversion, are saved in a separate queue from evidence awaiting analysis.
2	The OCR module reads the image or document from the queue and converts them into text. This operation can last from one to 5-10 seconds according to the number of words to be acquired.
3	Each image or document text is saved in the database and tagged as full-text.
4	Conversion 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 <b>Info</b> 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.

## 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 deemed excessive, add a shard to the current installation.

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

## 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.

## Disabling or re-enabling the OCR module

To disable or re-enable the OCR module, from the Master node Windows command prompt, run the following commands:

- > `rds-db-config --disable-ocr`
- > `rds-db-config --enable-ocr`

**Result:** the OCR module is disabled/re-enabled along with all shards.



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

## List of 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.

### Front end services

Front end server services are:

- RCSCollector
- RCSCarrier
- RCSController

### Backend services (Master Node)

Master Node services and their dependencies are illustrated in the diagram below. For example **RCSDB** service depends on **RCSMasterRouter** service and **RCSMonitor** service.

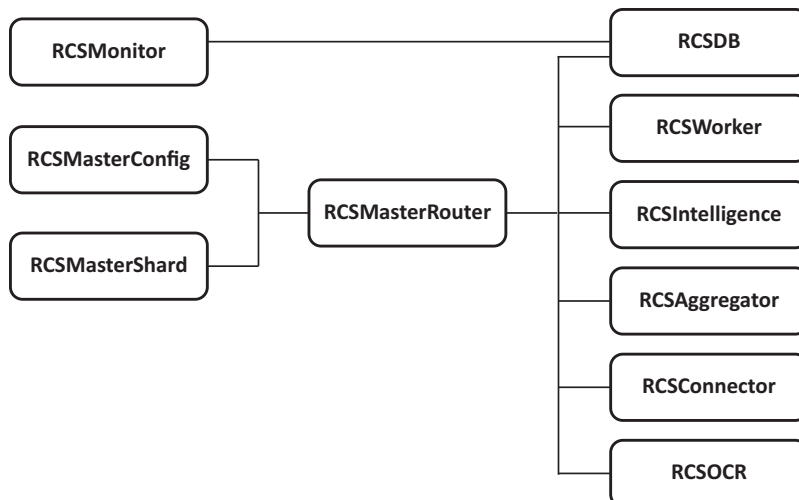


Figure 4.1: Master Node services and dependencies

### Backend services (Shard)

Shard services and their dependencies are illustrated in the diagram below.

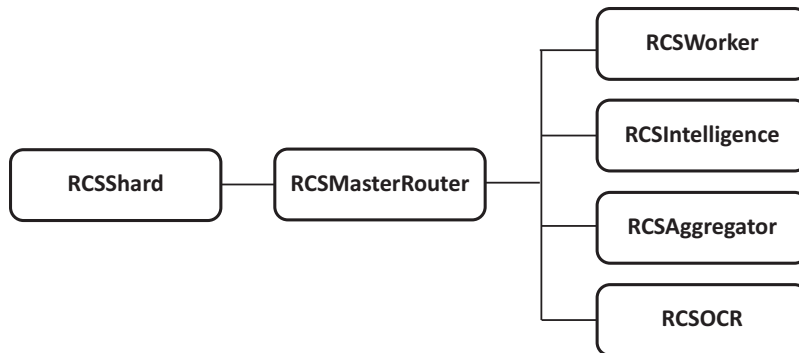


Figure 4.2: Shard services and dependencies

## To learn more

To restart any stopped services see "[Service restart procedures](#)" on page 78.

# 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.

## Requirements

Before installing RCS Console you must:

- 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:

<i>Step</i>	<i>Action</i>
1	Install Adobe AIR.
2	Install RCS Console.

## Adobe AIR installation

To install Adobe AIR:

**Steps**

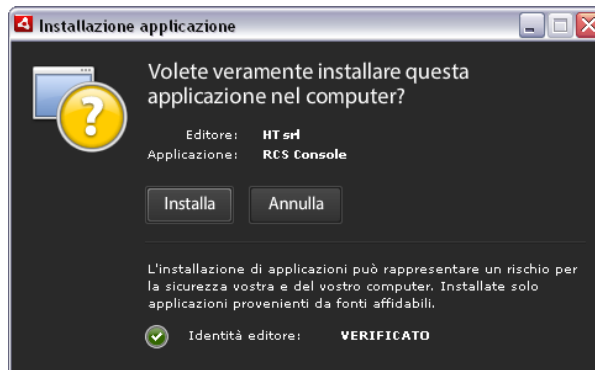
1. Install Adobe AIR: no icon appears on the desktop at the end of installation.

**Result****RCS Console installation**

To install RCS Console:

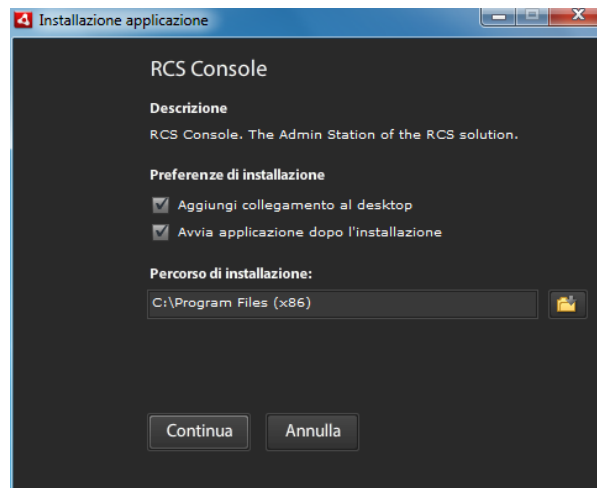
**Steps**

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

**Result**

**Steps**

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

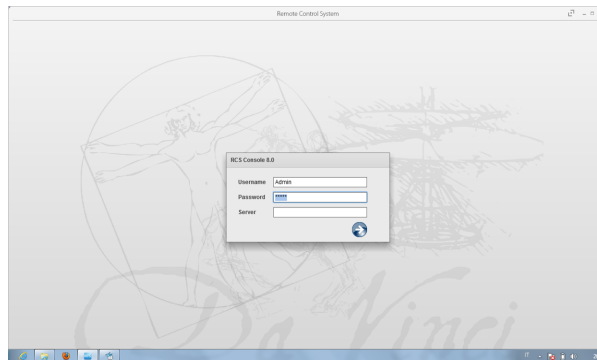
**Result**

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**

You can decide to uninstall RCS Console at any time to, for example, use the computer for something else. Database data and user preferences are not influenced in any way.

**Creating the Administrator user**


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

To create an Administrator user:

Step	Action
------	--------

- |   |   |
|---|---|
| 1 | From <b>RCS Console</b> , in the <b>Accounting</b> section, click <b>New user</b> . |
|---|---|




<i>Step</i>	<i>Action</i>
2	Enter the required data, selecting the <b>Administrator role</b> and click <b>Save</b> : 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.

## Files installed at the end of installation

### Installed files

Various folders appear at the end of installation, organized according to the installed optional component.

<i>Folder</i>	<i>Included files</i>
<b>backup</b>	<p>The folder contains files with data saved in the databases. See "<a href="#">Backup management</a>" on page 98</p> <p> <b>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.</b></p> <p><b>Path:</b> C:\RCS\DB\backup</p>
<b>bin</b>	<p>The folder contains the utilities (i.e.: rcs-db-config) used to set RCS utilities. See "<a href="#">Setup utilities</a>" on page 68</p> <p><b>Path:</b> C:\RCS\DB\bin C:\RCS\Collector\bin</p>
<b>certs</b>	<p>The folder contains the certificates used by the various services to access Master Node. They are updated when RCS settings are edited. See "<a href="#">Editing Master Node settings</a>" on page 69</p> <p><b>Path:</b> \RCS\DB\config\certs</p>
<b>config</b>	<p>The folder contains number system configuration files.</p> <p><b>Path:</b> C:\RCS\DB\config C:\RCS\Collector\config</p>

**Folder**    **Included files**

---

**log**        RCS component log file.  
              See "[System logs](#)" on page 74  
**Path:**  
              C:\RCS\DB\log  
              C:\RCS\Collector\log

---

# Additional component installation

## Presentation

### Introduction

RCS installation may include the installation of other additional components:

- Anonymizer
- Network Injector
- Shard database
- Collector

### Content

This section includes the following topics:

---

<b>What you should know about Anonymizer</b> .....	<b>32</b>
<b>Anonymizer installation and settings</b> .....	<b>34</b>
<b>What you should know about Network Injector Appliance</b> .....	<b>37</b>
<b>Network Injector Appliance installation</b> .....	<b>39</b>
<b>What you should know about Tactical Network Injector</b> .....	<b>44</b>
<b>Tactical Network Injector installation</b> .....	<b>46</b>
<b>Other applications installed on Network Injectors</b> .....	<b>49</b>
<b>Tactical Control Center and Appliance Control Center commands</b> .....	<b>50</b>
<b>First Network Injector synchronization with RCS server</b> .....	<b>51</b>
<b>Checking Network Injector status</b> .....	<b>52</b>
<b>Additional component installation</b> .....	<b>53</b>

## What you should know about Anonymizer

### Introduction

An Anonymizer is used to redirect data from a group of agents and Network Injectors. 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.

Several Anonymizers can be set up in a chain to increase the level of protection. Each chain leads to one Collector.

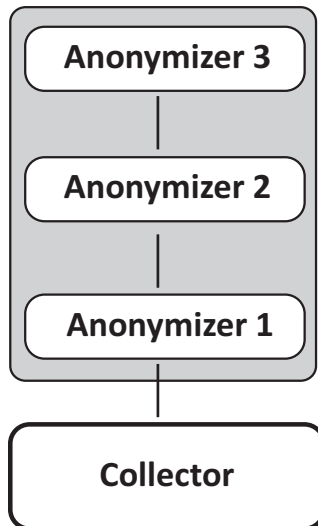




Figure 5.1: Anonymizer chain example

### Anonymizer status

An Anonymizer can have different status:

<b>Status</b>	<b>Symbol in RCS Console, System, Frontend</b>
In operating chain	
Not in chain	
Disabled	

Status	Symbol in RCS Console, System, Frontend
Anonymizer not recognized since it has not yet come into contact with the Collector	
Anonymizer with faults	

### Communications between Anonymizer and Collector

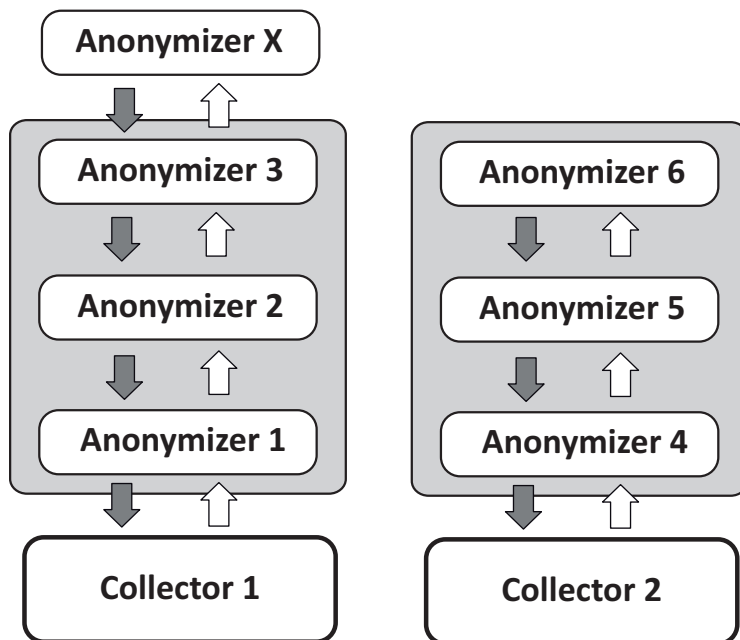


Figure 5.2: Information flow between Anonymizer and Collector

Once installed and set up, the Anonymizer sends status and logs to the Collector and receives settings and updates from the Collector via the Anonymizer chain. For example, **Anonymizer 2** sends its status to **Anonymizer 1** that sends it to **Collector 1**.



NOTE: if an Anonymizer does not belong to any chain (i.e.: **Anonymizer X** in the diagram), it uses the first Anonymizer chain in the configuration to communicate with the Collector.



NOTE: to exclude an Anonymizer from all communications, simply disable it.

## Faulty Anonymizer

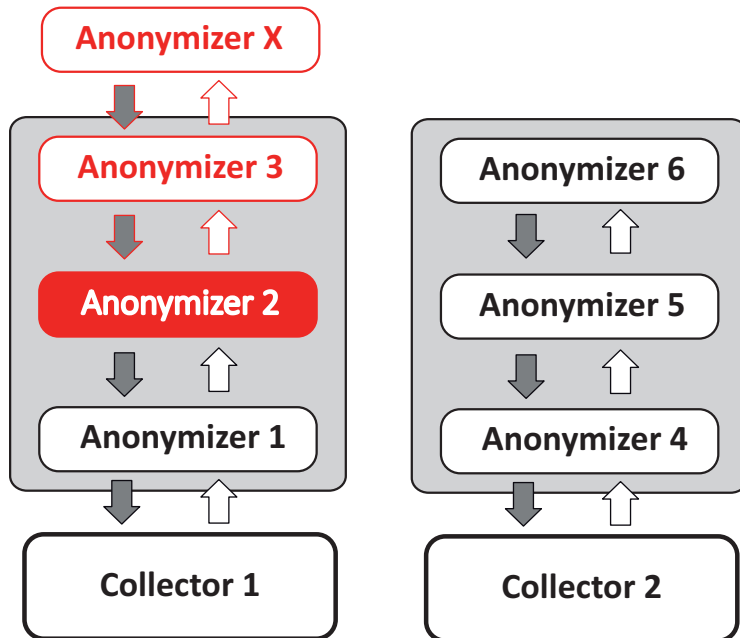


Figure 5.3: Information flow between Anonymizer and Collector with a faulty Anonymizer

A faulty Anonymizer (i.e.: **Anonymizer 2** in the diagram) interrupts communications between the Collector and Anonymizers in this chain and is thus faulty. To continue working with the other Anonymizers in the chain, move the faulty Anonymizer out of the chain and update the configuration.

## Anonymizer installation and settings

### 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**.

---

## Step Action

---

- 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.

- 4 Click **Download installer**.

**Result:** the `anon_install.zip` installer file is generated and saved on the console desktop.

- 5 Connect to the server and copy file `anon_install.zip` to a folder on the server.

- 6 Connect to the server, unzip the file and launch the installer by entering:  
`# sh install`

**Result:** the Anonymizer is installed in server folder `/opt/bbproxy`.

- 7 From **RCS Console**, in the **System, Frontend** section, select the Anonymizer and click **Apply configuration**: the new configuration is sent to the Anonymizer by the Collector via the Anonymizer chain.

## Anonymizer data

Selected Anonymizer data is described below:

<i>Data</i>	<i>Description</i>
<b>Name</b>	Anonymizer name.
<b>Description</b>	User's description
<b>Release</b>	Software version. To view software versions for all components see the <b>Monitor</b> section.
<b>Address</b>	IP address of the VPS where the Anonymizer was installed.
<b>Enabled</b>	If enabled, the Anonymizer is contacted for updates and new settings. Disable the function to avoid connections with Anonymizers in untrusted environments or with Anonymizers out of order.
<b>Log</b>	Last messages logged. To view log file content see " <a href="#">System logs</a> " on <a href="#">page 74</a>

## 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:

<i>Step</i>	<i>Action</i>
1	In the <b>System</b> section, <b>Frontend</b> , click on the Anonymizer icon.
2	Edit the required data and click <b>Save</b> . <b>Result:</b> the screen is updated.
3	Check Anonymizer status in the <b>Monitor</b> section.
4	Click <b>Apply settings</b> . <b>Result:</b> RCS connects to the Anonymizer and transfers the new configuration via the Anonymizer chain.



## Uninstall

To uninstall the Anonymizer delete private server folder /opt/bbproxy 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.

Network Injector Appliance uses Network Injector - Network Appliance as an operating system and Appliance Control Center for control software.



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

## Main functions

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

Network Injector Appliance communicates with RCS via an Anonymizer (and its chain, see "[What you should know about Anonymizer](#)" on page 32). Communications are run every 30 seconds to receive identification and infection rules and send status and logs.

Its Appliance Control Center control software can be set for remote access.

## 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.*

## Authentication key

An authentication key must be installed on Network Injector to securely communicate with the RCS server. The key must be generated when the Network Injector object is created on RCS Console and installed via Appliance Control Center at the first Network Injector synchronization with RCS, see "[First Network Injector synchronization with RCS server](#)" on page 51.

## Standard connection layout

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

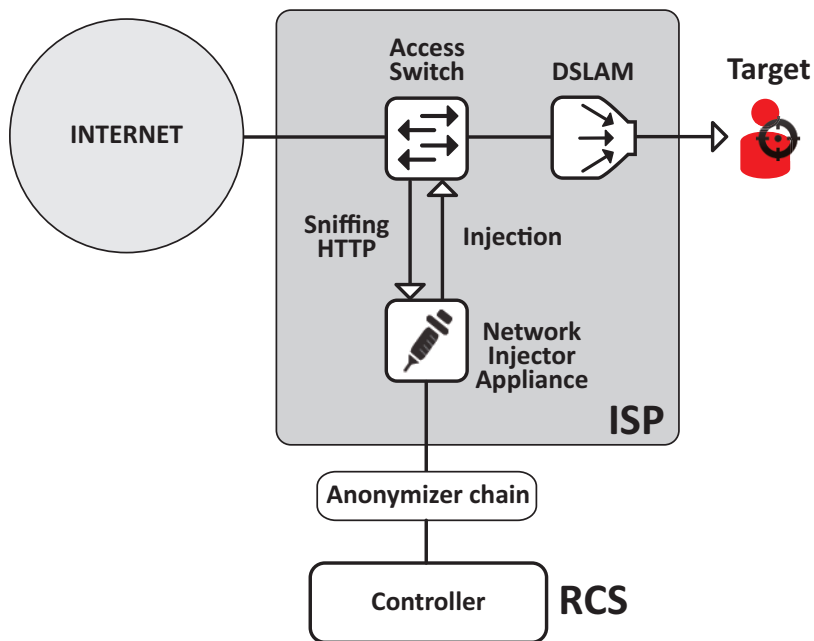


Figure 5.1: Network Injector Appliance: physical layout

### Connection layout as an intra-switch segment

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

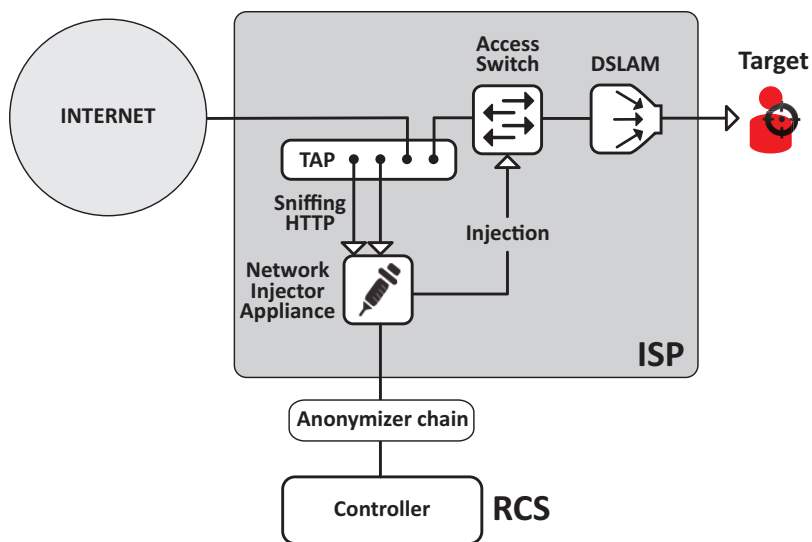


Figure 5.2: Network Injector Appliance with TAP: physical layout

### 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 with pre-installed and set Network Appliance operating system and Appliance Control Center control software. Hardware must be installed with the Internet service provider and synchronized with RCS server.

### Package content


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

### Installation sequence



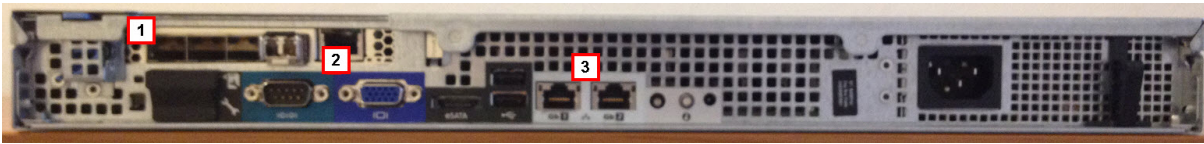
Tip: prepare Network Injector Appliance at your offices before installing it at the Internet provider.

The full installation sequence is provided below:


<b>Step</b>	<b>Action</b>	<b>Paragraph</b>
1	Connect Network Injector Appliance to the network.	<a href="#">"Network connections"</a> on the next page
2	Installing Network Appliance operating system  NOTE: the operating system is already installed at purchase.	<a href="#">"Operating system installation and settings"</a> on page 41
3	Synchronizing Network Injector with RCS server	<a href="#">"First Network Injector synchronization with RCS server"</a> on page 51
4	Checking Network Injector status	<a href="#">"Checking Network Injector status"</a> on page 52
5	Transfer Network Injector Appliance to the Internet service provider and change the network addresses to enable Internet access	-

### Rear panel description

The rear panel is described below:



A list of visible components is provided below:



<i>Area</i>	<i>Component</i>	<i>Description</i>
<b>1</b>	<b>Sniffing ports</b>	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.
<b>2</b>	<b>Mother board</b>	Standard PC outputs for monitor and keyboard connections to launch <code>sysconf</code> utilities or complete updates from the installation CD. See " <a href="#">Routine maintenance procedures</a> " on page 60
<b>3</b>	<b>Management and injection ports</b>	<b>Port 1:</b> network connection with Network Controller to receive settings and send status. The address must be set with Network Manager. <b>Port 2:</b> network connection for traffic injection.

## Network connections



Tip: prepare Network Injector Appliance by connecting it to your network and setting parameters before transferring it to the Internet provider.


The network connection procedure is described below:

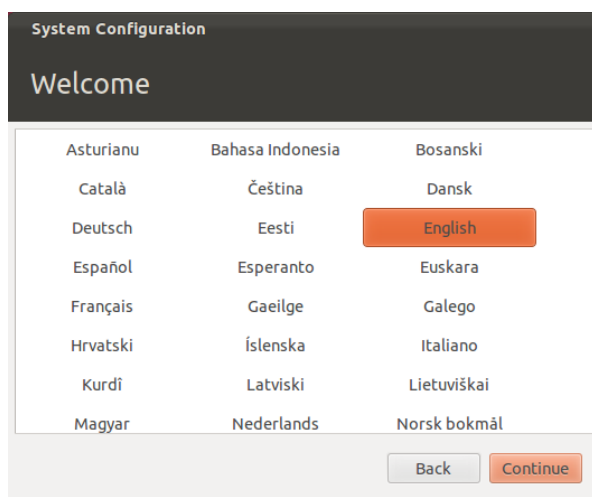
<i>Steps</i>	<i>Layout</i>
1. Connect the target's traffic switch to the sniffing ports[ <b>1</b> ].  <b>IMPORTANT: for redundant devices, connect both devices.</b>	
2. Connect management (port 1) and injection (port 2) ports [ <b>3</b> ] to the Internet.	
3. Connect the monitor and keyboard [ <b>2</b>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

## Operating system installation and settings

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

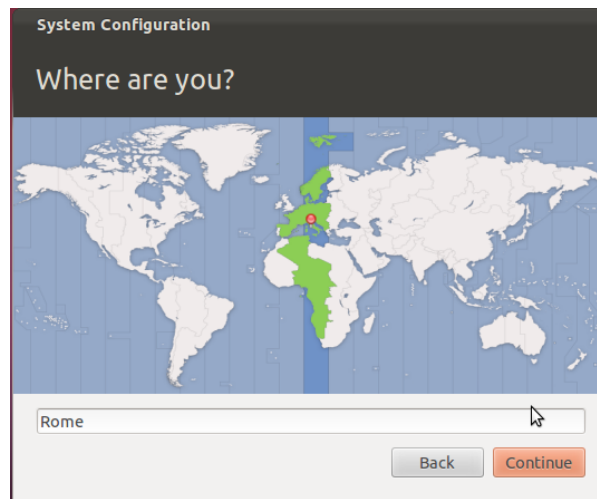
The procedure is described below:

<i>Steps</i>	<i>Result</i>
1. Connect the computer to the network using an Ethernet cable and insert the installation CD.	-
2. Select Network Appliance for server version installation: operating system installation is launched and the computer shuts down when finished.	-
 <b>IMPORTANT: the computer must remain connected to the internet during the entire installation process.</b>	-
3. Reboot the notebook.	-
4. The first setup window appears.	
5. Select the language.	

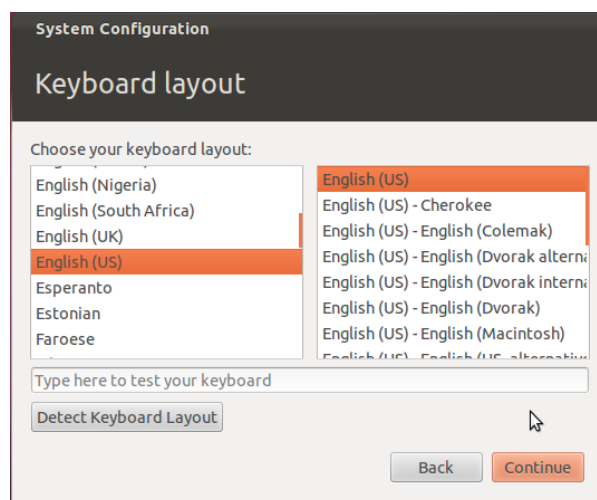


**Steps**

6. Select the correct time zone.

**Result**

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



## Steps

8. Enter user data: operating system setup starts.

## Result



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

## Verifying the IP address

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

## Changing the IP address

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

## Uninstall

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

See "[Managing the Network Injector](#)" on page 102

## What you should know about Tactical Network Injector

### Introduction

Tactical Network Injector is a notebook for tactical installation on LAN or WiFi networks. Furthermore, it can be used to unlock the target computer's operating system password to permit physical infections (i.e.: via Silent Installer).

Tactical Network Injector uses Network Injector - Tactical Device as an operating system and Tactical Control Center for control software.



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

### Main functions

Tactical Network Injector identifies devices in a WiFi or wired network and injects agents. It works based on identification (automatic or manual) or injection rules set in RCS Console. It can also connect to protected WiFi networks, emulate WiFi network Access Points and unlock the operating system password.

Tactical Network Injector communicates with RCS via an Anonymizer (and its chain, see "[What you should know about Anonymizer](#)" on page 32). Communications are run every 30 seconds to receive identification and infection rules and send status and logs.

Its Tactical Control Center control software can be set for remote access.

### 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).

### Authentication key

An authentication key must be installed on Network Injector to securely communicate with the RCS server. The key must be generated when the Network Injector object is created on RCS Console and installed via Tactical Control Center at the first Network Injector synchronization with RCS, see "[First Network Injector synchronization with RCS server](#)" on page 51.

### Standard connection layout

Typical WiFi layout where Tactical Network Injector is connected to the same WiFi network as target devices.



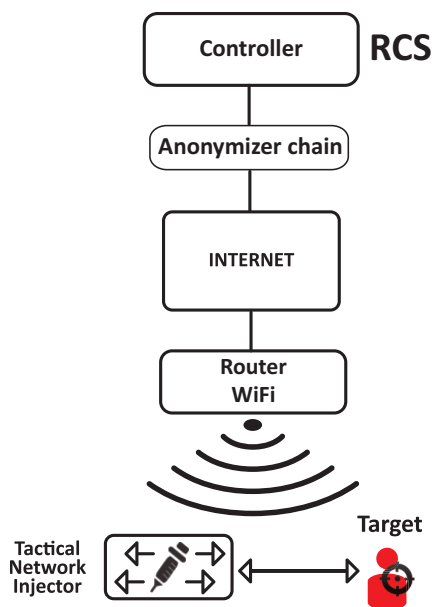


Figure 5.1: Tactical Network Injector: standard connection layout

### Access point emulation connection diagram

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

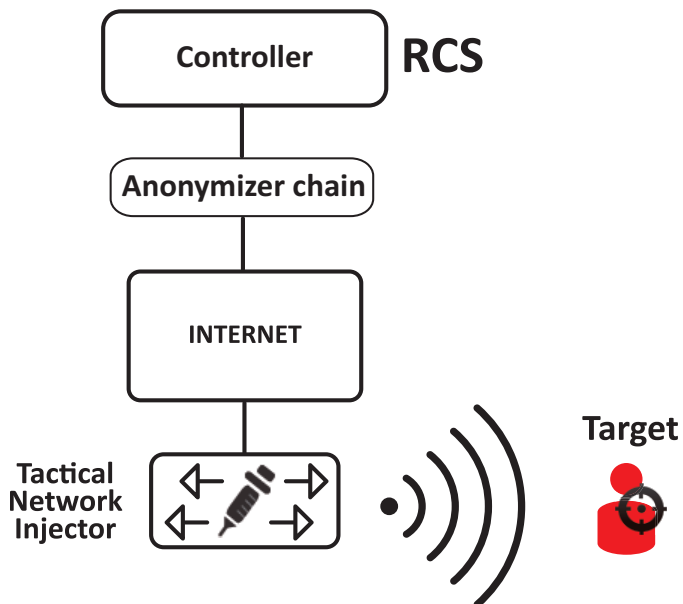


Figure 5.2: Tactical Network Injector: access point emulation diagram

# Tactical Network Injector installation

## Introduction

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




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

## Package content

The package includes a notebook and installation CD.

## Installation sequence

The full installation sequence is provided below:

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

## Operating system installation and settings

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

The procedure is described below:

<i>Steps</i>	<i>Result</i>
1. Connect the computer to the network using an Ethernet cable and insert the installation CD.	-

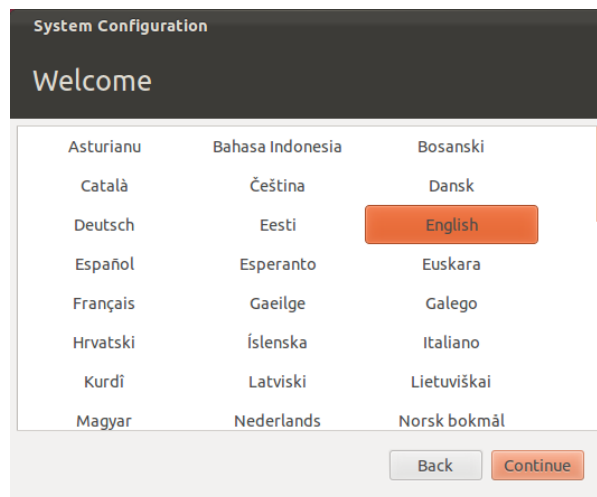
**Steps****Result**

2. Select Tactical Device for notebook version installation: operating system installation is launched and the computer shuts down when finished.

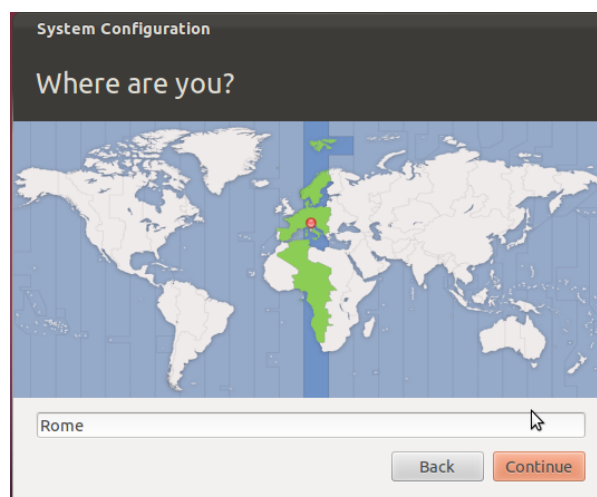


**IMPORTANT: the computer must remain connected to the internet during the entire installation process.**

3. Reboot the notebook; enter the *passphrase* to unlock the encrypted disk. The passphrase for first boot is "firstboot".
4. The first setup window appears.
5. Select the language.

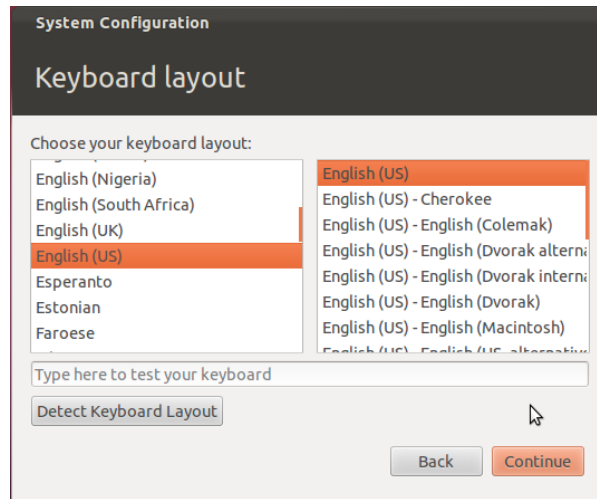


6. Select the correct time zone.



**Steps**

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

**Result**

8. Enter user data: operating system setup starts.



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



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



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

**Verifying the IP address**

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

## Changing the IP address

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

## Uninstall

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

See "[Managing the Network Injector](#)" on page 102

## Other applications installed on Network Injectors

### Introduction

Network Injectors come with some helpful third party applications installed.

### Applications

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



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

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

<i>Application name</i>	<i>Description</i>
<b>Tcpdump</b>	Network traffic analyzer from command prompt
<b>Wireshark</b>	Network traffic analyzer
<b>Xprobe</b>	Remote OS identifier tool

## Tactical Control Center and Appliance Control Center commands

### Introduction

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



NOTE: Administrator privileges are required to run commands.

### Commands

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

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

<b>Tactical Control Center command</b>	<b>Appliance Control Center command</b>	<b>Function</b>
tactical - v or Tactical --ver- sion	appliance - v or appliance --ver- sion	Displays the application version.
tactical -h or tactical --help	appliance -h or appliance --help	Displays available commands.

## First Network Injector synchronization with RCS server

### Introduction

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

### Synchronizing a Network Injector with RCS server

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



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

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

#### Step Action

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



NOTE: the default communications port is 80.

**Step Action**

---

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

## Checking Network Injector status

### Introduction

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

Network Injector status can be monitored from RCS Console.

Specifically:

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

### Identifying when Network Injector is synchronized

The procedure is described below:

**Step Action**

---

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



**IMPORTANT: applied rules and updates can only be received from RCS when Network Injector is synchronized.**

### Viewing Network Injector logs

The procedure is described below:



---

### Step Action

- 1 In the **System** section, **Network Injectors**, select the Network Injector to be analyzed, double-click or click **Edit**.

**Result** : a window opens with Network Injector data and saved logs. See "[Network Injector data](#)" on page 104



NOTE: logs are only received and displayed if Network Injector is synchronized.

## Additional component installation

### Introduction

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



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

### Additional component installation requirements

Before installing additional components, complete Master Node and Collector installation. See "[RCS server installation](#)" on page 17.

### Installation sequence

The complete additional component installation sequence is described below:

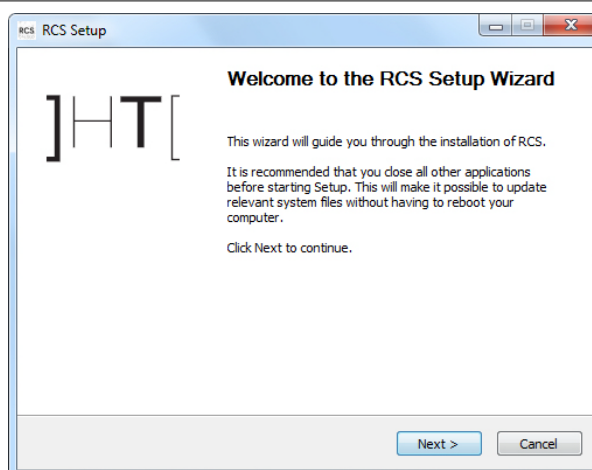
Step	Action	Machine
1	Prepare that indicated in <i>installation requirements</i> .	-
2	Install additional Shard databases.	<i>server in back end environment</i>
3	Check installation logs.	
4	Install additional Collectors.	<i>server in front end environment</i>
5	Check installation logs.	
6	Check for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

### Additional Shard database installation

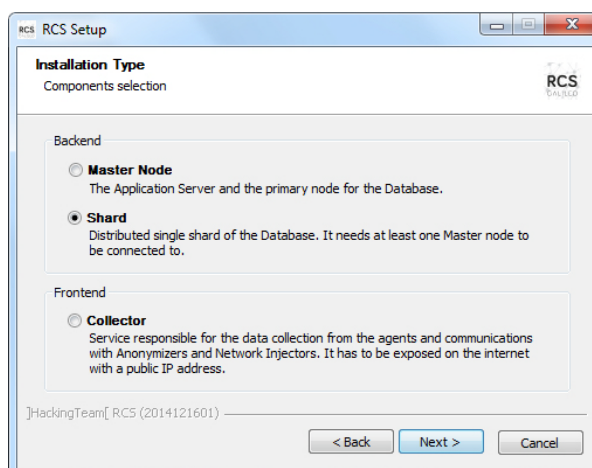
To install an additional Shard database in back end environment:

**Steps**

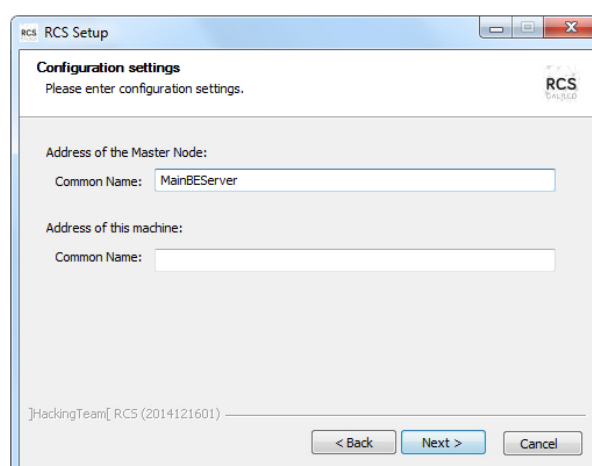
1. Insert the CD with the installation package. Run file RCS-version.exe in folder x:\setup: the first wizard window appears.
2. Click **Next**.

**Result**

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

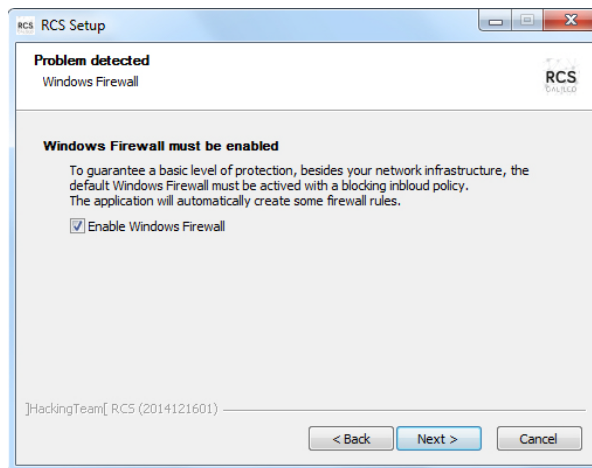


5. Enter the name of IP address of the Master Node server (i.e.: MainBEServer) and machine where Shard is being installed.
6. Click **Next**: when installation has completed, services start and attempt to communicate with Master Node. The server in back end environment is protected and any remote login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

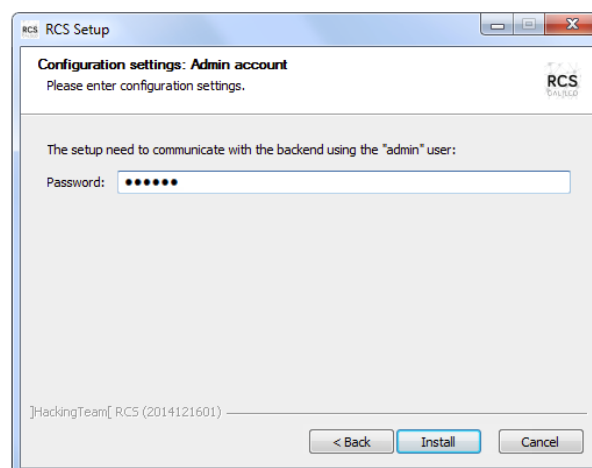


**Steps**

7. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.

**Result**

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



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

**Additional Collector installation**

To install several Collectors in front end environment:

**Steps**

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**.

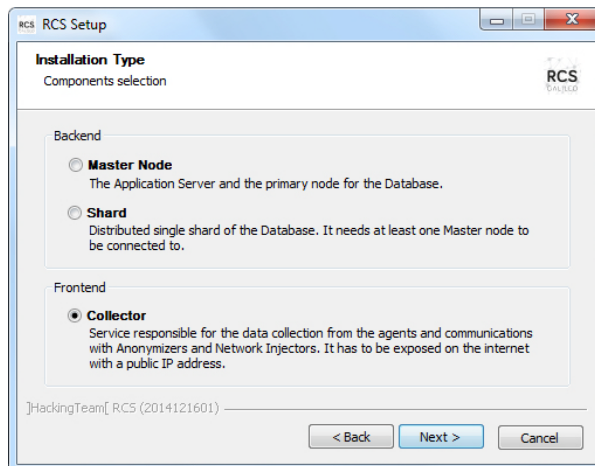
**Result**

3. Select **Collector**.

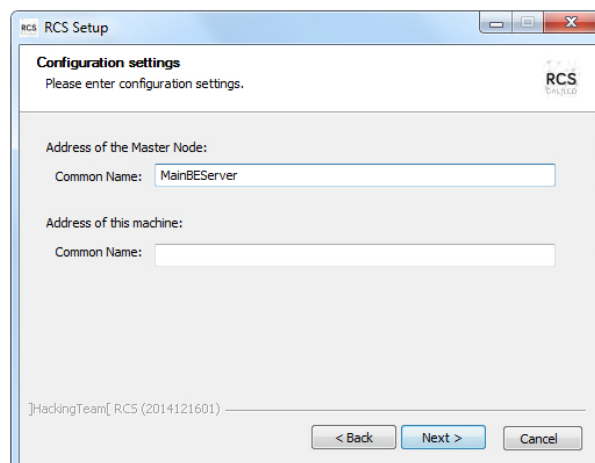


NOTE: all Collector services are automatically installed.

4. Click **Next**.

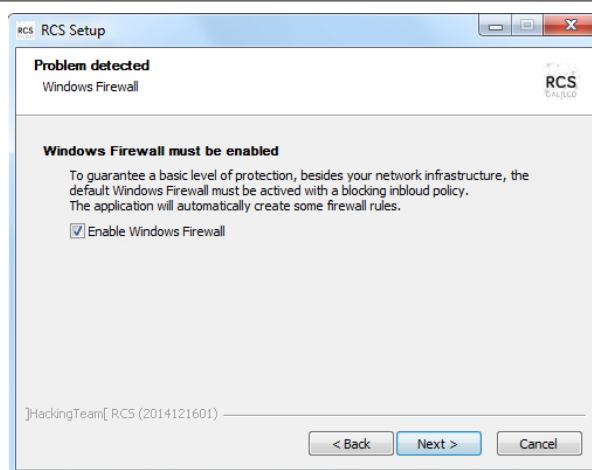


5. Enter the name or IP address of the Master Node server (i.e.: MainBEServer) and machine where Collector is being installed.
6. Click **Next**: when installation has completed, services start and attempt to communicate with Master Node. The server in back end environment is protected and any remote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

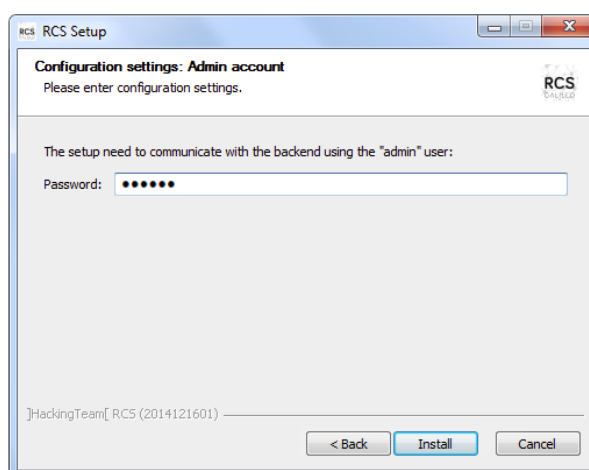


**Steps**

7. If the system finds the Windows firewalls disabled, it requests they be enabled. Select **Enable Windows Firewall** and click **Next**.

**Result**

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

**Checking service start**

Make sure all RCS services are up and running. If services are not running, manually start them. See "[List of RCS services](#)" on page 25.



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

**Checking installation logs**

If errors occur during installation, check logs and send them to support service if necessary. See "[System logs](#)" on page 74

**Check IP addresses**

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

## Uninstall

RCS can be uninstalled from the Windows Control Panel.



**CAUTION:** *data is lost when a Shard database is uninstalled. For correct operations, backup data. See "[Backup management](#)" on page 98.*



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

---

# 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:

---

<b>What you should know about RCS maintenance</b> .....	<b>60</b>
<b>Routine maintenance procedures</b> .....	<b>60</b>
<b>RCS server update</b> .....	<b>60</b>
<b>RCS Console update</b> .....	<b>61</b>
<b>Anonymizer update</b> .....	<b>61</b>
<b>Network Injector Appliance update</b> .....	<b>62</b>
<b>Tactical Network Injector update</b> .....	<b>64</b>

## 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

As a precaution, follow the steps below before updating RCS server:



**Step Action**

---

- 1 Stop all RCS services. See "[List of RCS services](#)" on page 25.
- 2 Create a copy of the entire folder content, C:\RCS\ the Master Node and any additional Shards.
- 3 When copied, restart RCS services.

**Update methods**

Once the installer is launched, it identifies machine components and suggests automatic update.

**RCS server(s) update**

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

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

**Step Action**

---

- 1 Run the `rsc-Version.exe` installation file: the list of installed components that will be automatically updated appears. Click **Next**.
- 2 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 26

**Anonymizer update****Update requirements**

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

**Anonymizer update**

In **RCS Console**, in section **System, Frontend** select the Anonymizer to be updated and click **Update**.

**IMPORTANT: keep the Linux operating system updated**

If the update fails, repeat the installation procedure using the files found in the new installation packet.

See "[Anonymizer installation and settings](#)" on page 34

## Network Injector Appliance update

### Introduction

There are three ways to update Network Injector Appliance:

- fully, including the operating system, see "[Full Network Injector Appliance update](#)" below.
- partially, saving data, with an infection in progress, see "[Partial update with infection in progress](#)" below.
- partially, saving data, without an infection in progress, see "[Partial update without infection in progress](#)" on the facing page

### Full Network Injector Appliance update



**CAUTION: updating deletes all data on the machine.**

If you have the updated .iso file, run the following procedure to install the operating system update:

#### **Step Action**

---

- 1 Insert the installation CD with the new operating system version 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.



**IMPORTANT: select Network Appliance for server version installation.**

- 2 Reboot the server: the procedure must be confirmed.



**CAUTION: the entire hard disk will be deleted.**

**Result:** Network Injector Appliance is installed.

### Partial update with infection in progress

These are the phases in updating Appliance Control Center software when an infection is in progress:


 **IMPORTANT:** to update, first synchronize Network Injector and RCS server. See "[First Network Injector synchronization with RCS server](#)" on page 51


 **IMPORTANT:** make sure the device to be updated is connected to Internet to download and additional packets required for the update.

#### *Phase Description*

---

- 1 From **RCS Console**, in the **System, Network Injector** section, select the Network Injector to be updated and click **Update**
- 2 At the next Network Injector communication request, the assigned Anonymizer will send the update that will be automatically installed.

 NOTE: the wait time for the Network Injector communication will be one minute at most. You can check operation progress in the RCS Console download area.

 NOTE: the installation phase only starts if the Appliance Control Center application window is closed.

When the update is completed, the infection is restarted with the updated software.

### **Partial update without infection in progress**

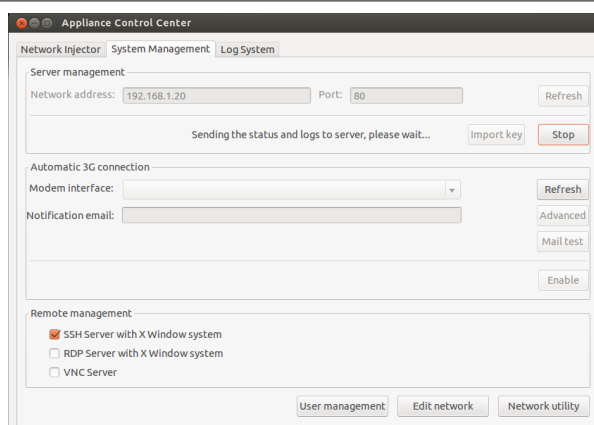
These are the phases in updating Appliance Control Center software when an infection is not in progress:

 **IMPORTANT:** make sure the device to be updated is connected to Internet to download and additional packets required for the update.

<i>Step</i>	<i>Action</i>
1. From RCS Console, in the <b>System, Network Injector</b> section, select the Network Injector to be updated and click <b>Update</b> .	
2. Open <b>Appliance Control Center</b>	-

**Step****Action**

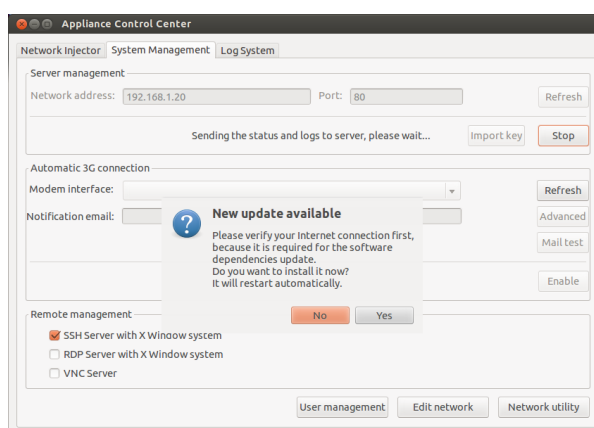
3. In the **System Management** tab, click **Configure**: synchronization is enabled.



4. During synchronization, Network Injector queries RCS every 30 seconds. A message appears at the end of the first interval requesting consent to install.



**NOTE:** if the update is not installed, it will be automatically installed at the next infection start or an installation authorization request at next Appliance Control Center reboot will appear.



5. Install the update.  
6. When the update is completed, Appliance Control Center reboots.

## Tactical Network Injector update

### Introduction

There are two ways to update Tactical Network Injector:

- fully, including the operating system, see "[Full Tactical Network Injector update](#)" below.
- partially see "[Partial update](#)" on the facing page

### Full Tactical Network Injector update



**CAUTION:** updating deletes all data on the machine.

If you have the updated .iso file, run the following procedure to install the operating system update:

### Step Action

- 1 Insert the installation CD with the new operating system version 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.



**IMPORTANT: select Tactical Device notebook version installation.**

- 2 Reboot the server: the procedure must be confirmed.



**CAUTION: the entire hard disk will be deleted.**

**Result:** Network Injector Appliance is installed.

### Partial update

These are the Tactical Control Center update phases:

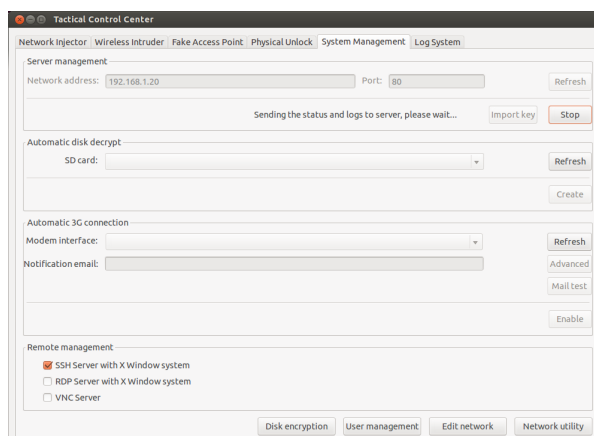


**IMPORTANT: make sure the device to be updated is connected to Internet to download and additional packets required for the update.**

### Step

### Action

1. From **RCS Console**, in the **System, Network Injector** section, select the Network Injector to be updated and click **Update**
2. Open **Tactical Control Center**
3. In the **System Management** tab, click **Configure**: synchronization is enabled.

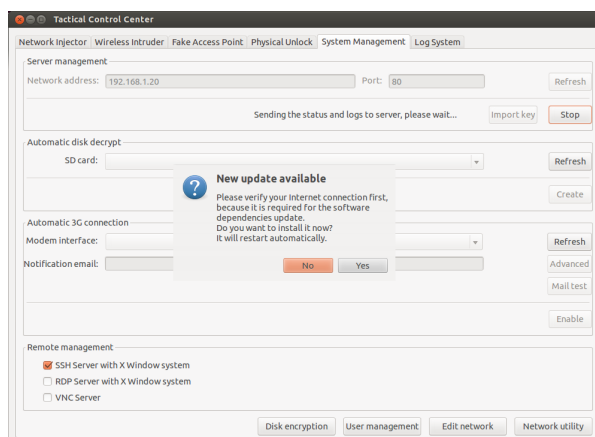


**Step**

4. During synchronization, Network Injector queries RCS every 30 seconds. A message appears at the end of the first interval requesting consent to install.



**NOTE:** if the update is not installed, an installation authorization request will appear the next time Tactical Control Center is booted.

**Action**

5. Install the update.
6. When the update is completed, Tactical Control Center reboots.

---

# Editing Master Node and Collector settings

## Presentation

### Introduction

Component settings can be edited after installation if needed.

### Content

This section includes the following topics:

---

<b>What you should know about settings</b> .....	<b>68</b>
<b>Setup utilities</b> .....	<b>68</b>
<b>Editing Master Node settings</b> .....	<b>69</b>
<b>Editing the Collector configuration</b> .....	<b>70</b>
<b>Settings check</b> .....	<b>71</b>

## What you should know about settings

### What you can edit

The following Master Node and 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: **rds-db-config**
- for Collector: **rds-collector-config**



## Utility command syntax

Utility command syntax is the following:

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

Where:

- -x: selected option
- AAA: entered value

## Other options

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

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



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






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

## Editing Master Node settings


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

<i>To edit...</i>	<i>Enter...</i>
the Master Node name/IP address	<pre>&gt; rcs-db-config -n <i>Name</i> -g</pre> or <pre>&gt; rcs-db-config -n <i>IPaddress</i> -g</pre> <p><b>Result :</b> certificates are updated and appear in folder \RCS\DB\config\certs. Collector settings must also be edited. See <a href="#">"Editing the Collector configuration"</a> on the next page</p>
the system user password	<pre>&gt; rcs-db-config -R <i>Username</i></pre> <p><b>Result:</b> the new password is requested that will be saved in the database. This operation automatically renews the password expiration date.</p>

<i>To edit...</i>	<i>Enter...</i>
backup folder	<pre>&gt; rcs-db-config -B <i>Folder</i></pre> <p> NOTE: "<i>Folder</i>" can be a path for the RCS\db folder or an absolute path.</p> <p> <b>IMPORTANT: any backup files in the previously set folder will be copied to the new one.</b></p> <p><b>Result:</b> 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 <b>Disk Manager</b>: this way, a remote disk can be used for backup.</p>
outgoing mail server settings for alert e-mails	<pre>&gt; rcs-db-config -M -server <i>HostName:PortNumber</i></pre> <p>to set the outgoing main server name and port to be used.</p> <pre>&gt; rcs-db-config -from <i>senderEmail</i></pre> <p>to set the alert e-mail sender's e-mail (i.e.: "alert@myplace.com").</p> <pre>&gt; rcs-db-config -user <i>UserName</i></pre> <p>To set the e-mail sender's user name.</p> <pre>&gt; rcs-db-config -pass <i>Password</i></pre> <p>To set his password.</p> <pre>&gt; rcs-db-config -auth <i>AuthenticationType</i></pre> <p>To set the type of authentication to be used ("plain", "login" or "cram_md5").</p>

## Editing the Collector configuration

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

<i>To...</i>	<i>Enter...</i>
communicate the new Master Node name/IP address	<pre>&gt; rcs-collector-config -d <i>Name</i> -u admin -p <i>Password</i> -t</pre> <p>or</p> <pre>&gt; rcs-collector-config -d <i>IPaddress</i> -u admin -p <i>Password</i> -t</pre> <p> <b>IMPORTANT: "<i>Password</i>" must match the one used to login to Master Node.</b></p> <p><b>Result:</b> certificates are restored in folder \RCS\DB\config\certs.</p>

## Settings check

### Introduction

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:

---

<b>Potential faults</b> .....	<b>73</b>
<b>System logs</b> .....	<b>74</b>
<b>Component status check procedure</b> .....	<b>76</b>
<b>Service restart procedures</b> .....	<b>78</b>
<b>Hardware component service procedures</b> .....	<b>79</b>

## Potential faults

### Potential installation faults

Following is a list of potential faults that may occur during installation and 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"> <li>• Make sure you logged in with the System administrator's name, password and name of the server where Master Node was installed.</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>• check the Master Node log file to check for any errors.</li> </ul>

### Possible server problems

Following is a list of potential faults that may occur during product use and 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"> <li>• check Master Node service status.</li> <li>• request a substitute protection key.</li> </ul>
data no longer arrives from agents	from RCS Console the Collector is running and correctly communicates	check Collector status.
The Master Node is not available	The Collector is running	<ul style="list-style-type: none"> <li>• check whether an update is in progress</li> <li>• check the Collector log file</li> </ul>
images are not converted into text	the OCR module is enabled	check slowing in the module log and install another OCR module.
The Collector is not available	-	restart RCS Collector service.

<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	check Worker service status, for Master Node and other Shards, and the services it depends on.
Network Controller indicates an error	-	login to the concerned Collector machine and check the log file.

## Potential backup problems

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

<i>If...</i>	<i>Then...</i>
backup status is <b>error</b>	check available disk space and manually restart backup.

## To learn more

To check component status see "[Component status check procedure](#)" on page 76

To restart services See "[Service restart procedures](#)" on page 78.

## System logs

### Introduction

Each RCS component generates daily logs that help to analyze possible fault or error causes. File content analysis lets you follow RCS operations step by step to find the causes of any errors (i.e.: service started but immediately stopped).

### Log analysis utility

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

<i>Component</i>	<i>Analysis reason</i>
<b>Master Node</b>	Check problems with RCS Console.
<b>Collector</b>	Check data reception from agents.
<b>Carrier</b>	Checks data delivery to shards and the Master Node.
<b>OCR module</b>	Check for any slowed indexing in exported content.
<b>Translate module</b>	Check for any slowed content translation.
<b>Network Controller</b>	Check Network Injector or Anonymizer status.
<b>Network Injector</b>	Check completed operations.

<i>Component</i>	<i>Analysis reason</i>
<b>Anonymizer</b>	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>
<b>Master Node</b>	C:\RCS\DB\log
<b>Collector</b>	C:\RCS\Collector\log
<b>Carrier</b>	C:\RCS\Collector\log
<b>OCR module</b>	C:\RCS\DB\log
<b>Translate module</b>	C:\RCS\DB\log
<b>Network Controller</b>	C:\RCS\Collector\log
<b>Network Injector</b>	/var/log/syslog
<b>Anonymizer</b>	/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>
<b>Fatal</b>	RCS is not running and requires service (i.e.: no settings, no certificates).
<b>Error</b>	There is a component error but RCS can guarantee main service coverage (i.e.: Master Node not running).

<i>Severity level</i>	<i>Description</i>
<b>Debug</b>	It only appears if enabled upon support service indication, increases and provides more details on log records to resolve problems.
<b>Info</b>	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 **racs-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 **racs-db-queue**.

**Result:** an example is provided below.

```

-----+-----
| instance | platform | last sync time | logs | size | shard |
| RCS_0000000001:20110602007b6d910e7ecc2e987060db2ff06cd8 | osx | 2014-02-11 07:51:17 UTC | 1 | 200 B | The-One.local |
-----+-----

```

### 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.

#### Command

In folder C:\RCS\DB\bin enter **racs-db-queue**.

### Check agent status via Collector

Make sure agents are routinely communicating their status to RCS 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 **rsc-collector-queue**

**Result:** the Collector status report appears

```

-----+-----
| instance | subtype | last sync time | status | logs | size |
-----+-----
|RCS_0000000001_47170c3e047b6a910e7ecc2e987060db2ff06cd8| WINDOWS | 2012-02-03 15:44:54 UTC | IDLE | 0 | 0 B |
|RCS_00000000771_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 other synchronizations to see if 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 via the Carrier. If the value is high, this means that Master Node is not running or is not connected or the Carrier malfunctioned. Check Master Node status and Carrier logs.

If the problem is the connection with Master Node, the number of logs will decrease as soon as the connection is restored.

**Network Injector start check**

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

**Check system components**

Check system component status and view front end and back end component topology.

**Command**

In folder C:\RCS\DB\bin enter **rsc-db-status** Use the following command to view the correct syntax and description of all options:

```
> rsc-db-status --help
```

**Support service file creation**

Create a .zip file with all the information required for technical support.

**Command**

In folder C:\RCS\DB\bin or C:\RCS\Collector\bin enter **rsc-db-diagnostic** or **rsc-collector-diagnostic** respectively. Use the following command to view the correct syntax and description of all options:

```
> rsc-db-diagnostic --help
```

```
> rsc-collector-diagnostic --help
```

For example, the **--hide-addresses** option lets you delete all references to IP addresses or domain names in files.

## To learn more

To view logs see "[System logs](#)" on page 74

# Service restart procedures


## Introduction

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





**IMPORTANT:** to restart services and identify fault causes, take service interdependencies into account. See "[List of RCS services](#)" on page 25.

Typical ways to start, stop and restart services are provided below.

<i>Service</i>	<i>Commands</i>
<b>RCSDB</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-db-service start</code></li> <li>• &gt; <code>rcs-db-service stop</code></li> <li>• &gt; <code>rcs-db-service restart</code></li> </ul>
<b>MongoDB</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-db-mongo-service start</code></li> <li>• &gt; <code>rcs-db-mongo-service stop</code></li> <li>• &gt; <code>rcs-db-mongo-service restart</code></li> </ul>
<b>Collector</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-collector-service start</code></li> <li>• &gt; <code>rcs-collector-service stop</code></li> <li>• &gt; <code>rcs-collector-service restart</code></li> </ul>
<b>Carrier</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-carrier-service start</code></li> <li>• &gt; <code>rcs-carrier-service stop</code></li> <li>• &gt; <code>rcs-carrier-service restart</code></li> </ul>
<b>Network Controller</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-controller-service start</code></li> <li>• &gt; <code>rcs-controller-service stop</code></li> <li>• &gt; <code>rcs-controller-service restart</code></li> </ul>
<b>Worker</b>	<ul style="list-style-type: none"> <li>• &gt; <code>rcs-worker-service start</code></li> <li>• &gt; <code>rcs-worker-service stop</code></li> <li>• &gt; <code>rcs-worker-service restart</code></li> </ul>
<b>Network Injector</b>	 <p><b>CAUTION:</b> use SSH protocol for all installation, setup and data exchange operations to the remote unit.</p>

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

<i>Service</i>	<i>Commands</i>
<b>Anonymizer</b>	 <b>CAUTION: use SSH protocol for all installation, setup and data exchange operations to the remote unit.</b>  To restart the service, enter the following command: <pre># /etc/init.d/bbproxy restart</pre> To stop the service, enter the following command: <pre># /etc/init.d/bbproxy stop</pre>  <b>IMPORTANT: command syntax refers to the Linux CentOS 6 operating system version.</b>

## 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. See " <a href="#">RCS server installation</a> " on page 17

**Step Action**

---

- 2 Select the most recent backup (full or metadata). If the most recent backup is metadata, full backup can be restored later. In fact, the backup is not destructive and supplements the information it has with that present,  
See "[What you should know about backup](#)" on page 96

## Shard replacement

The recommended procedure is described below:

**Step Action**

---

- 1 Repeat the entire installation procedure.  
See "[RCS server installation](#)" on page 17
- 2 Restore the last full backup.  
See "[Backup management](#)" on page 98

## Replacing the Collector

Repeat the entire installation procedure.

See "[RCS server installation](#)" on page 17

## Replacing an Anonymizer

Repeat the entire installation procedure.

See "[Anonymizer installation and settings](#)" on page 34

## Replacing a Network Injector Appliance

Repeat the entire installation procedure.

See "[Network Injector Appliance installation](#)" on page 39

## Replacing a Tactical Injector Appliance

Repeat the entire installation procedure.

See "[Tactical Network Injector 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 and fix any problems.
- update system components
- manage backup

### 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:

---

<b>Starting the RCS Console</b> .....	<b>82</b>
<b>Homepage description</b> .....	<b>83</b>
<b>Wizards in the homepage</b> .....	<b>84</b>
<b>Shared interface elements and actions</b> .....	<b>86</b>
<b>Front end management</b> .....	<b>91</b>
<b>Back end management</b> .....	<b>93</b>
<b>What you should know about backup</b> .....	<b>96</b>
<b>Full backup for serious reasons</b> .....	<b>97</b>
<b>Backup management</b> .....	<b>98</b>
<b>Connector management</b> .....	<b>100</b>
<b>Managing the Network Injector</b> .....	<b>102</b>
<b>System monitoring (Monitor)</b> .....	<b>105</b>

## Starting the RCS Console

### Introduction

When started, RCS Console asks you to enter your credentials (user name and password) previously set by the Administrator.



**IMPORTANT:** if the wrong password is entered five times in a row, the user is automatically disabled by the system and can no longer login to RCS Console. Contact the Administrator.

### Restoring disabled users who entered incorrect passwords

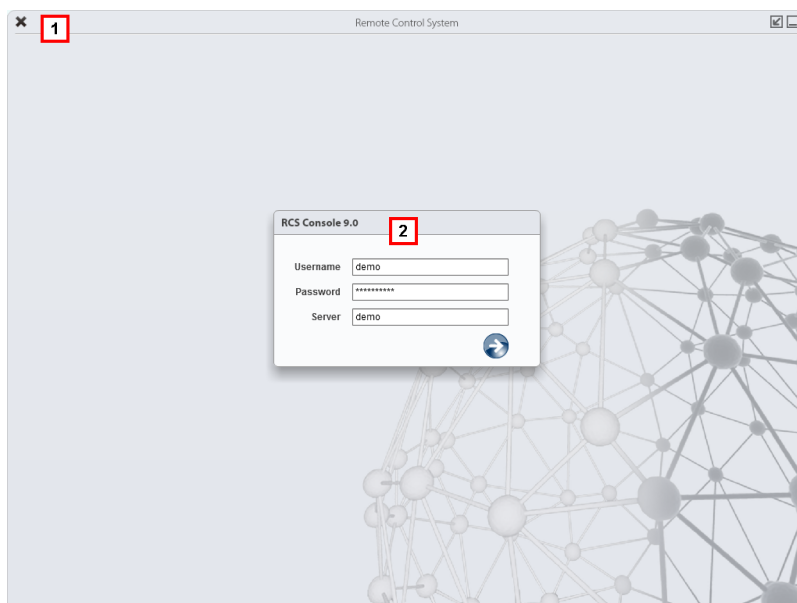
To restore a user, enter the following command in the Windows command prompt on the server:

```
> rcs-db-config -R Username
```

**Result:** the new password is requested that will be saved in the database. This operation automatically restores the user.




### 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.
- 3 Click : the homepage appears with the menus enabled according to your account privileges. See "[Homepage description](#)" below.

**Homepage description**

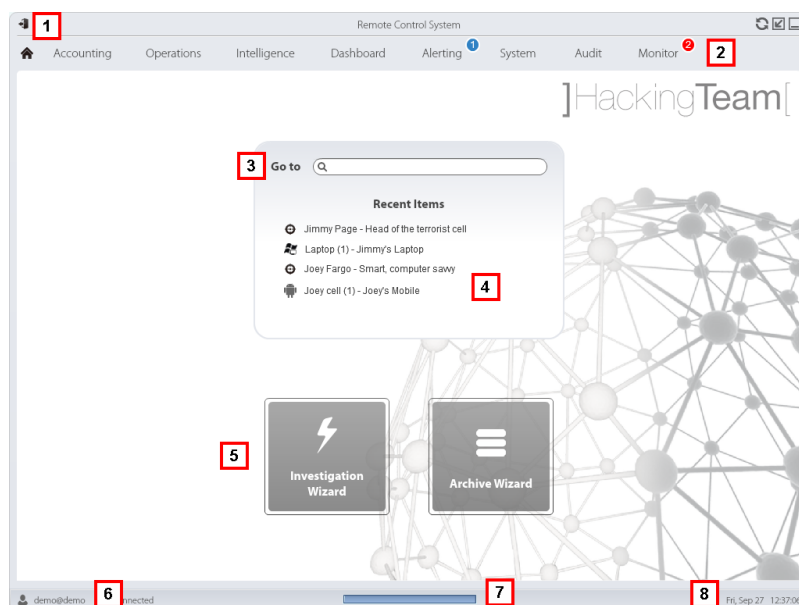
To view the homepage: | • click 

**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, agents and entities, by name or description.
- 4 Links to the last five elements opened (operation in the **Operations** section, operation in the **Intelligence** section, target, agent and entity).
- 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

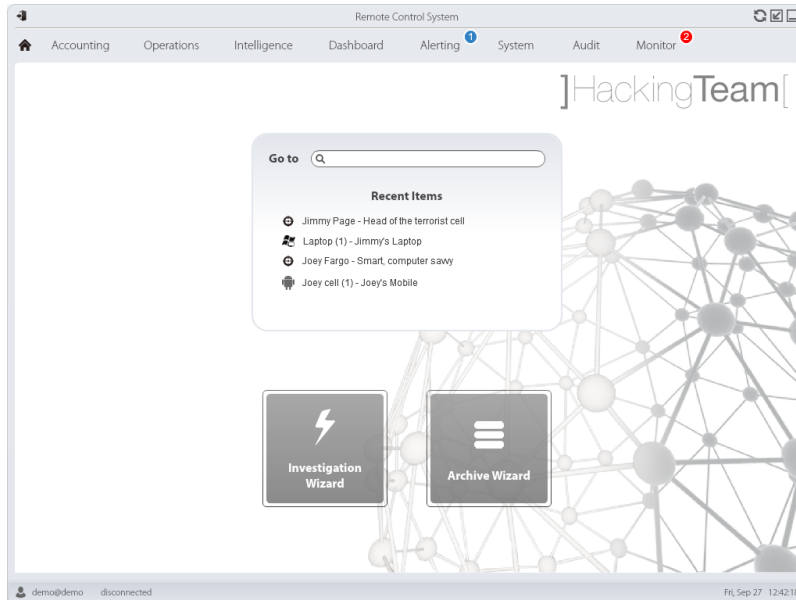
### Introduction

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

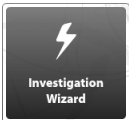


## What it looks like

This is how the homepage is displayed with enabled wizards:



Button	Function
	Open the wizard to quickly create an agent.
	Open the wizard to quickly save operation and target data.



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



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




## Quick Save

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

Data is saved in a backup and can be restored at any time.

Following are explanations of the various options:

Option	Description
<b>Backup all data</b>	Saves all selected operation or target data in a full type backup file. The backup appears in a programmed backup list and can be restored at any time.

<i>Option</i>	<i>Description</i>
<b>Delete all data from the system</b>	<p>Deletes all selected operation or target evidence from the database. The operation or target remain open and running Only the database is reduced in size.</p> <p> <b>CAUTION: if this option is combined with immediate backup, give the backup a name that clearly indicates that the corresponding evidence was deleted from the system.</b></p>
<b>Close the object</b>	<p>Close the selected operation or target.</p> <p> <b>CAUTION: the operation or target is closed and cannot be reopened. Agents no longer send data but evidence already received can still be viewed.</b></p>
<b>Delete the object from the system</b>	<p>Deletes all selected operation or target data. Operation data, targets, agents and all evidence is deleted from databases.</p> <p> <b>CAUTION: deleting an operation/target is irreversible and all data linked to that operation/target is lost.</b></p>

## Shared interface elements and actions

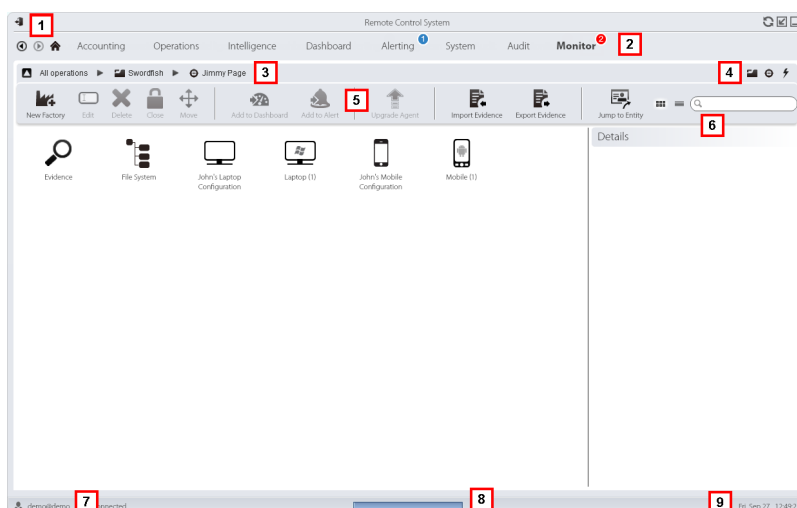
### Introduction

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

-  Back to navigation history button
-  Next navigation history button
-  Return to homepage button








RCS menu with functions enabled for the user.

### 3 Operation navigation bar. Descriptions are provided below:

-  Back to higher level.
-  Show the operation page (**Operations** section).
-  Show the target page.
-  Show the factory page.
-  Show the agent page.
-  Show the operation page (**Intelligence** section).
-  Show the entity page.

---

## Area Description

- 4** Buttons to display all elements regardless of their group membership. Descriptions are provided below:
-  Show all operations.
  -  Show all targets.
  -  Show all agents.
  -  Show all entities.
- 5** Window toolbar.
- 6** Search buttons and box:
-  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.
- 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.

## Change interface language or password

To change the interface language or password:

### Step Action

---

- 1** Click **[7]** to display a dialog window with the user's data.
- 2** Change the language or password and click **Save** 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 **[9]** 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.

**Step Action**

- 2 Change the time zone and click **Save** 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  

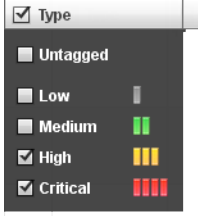

The example shows elements with descriptions like:

- "my**boss**"
- "**boss**anova"

**Sort 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

<i>Action</i>	<i>Description</i>
<b>Filter based on several options</b>	Select one or more options: the elements that match all selected options appear. 
<b>Change the column size</b>	Select the edge of the column and drag it.

## Front end management

To manage the front end: 

- System section, Frontend

### Function scope

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

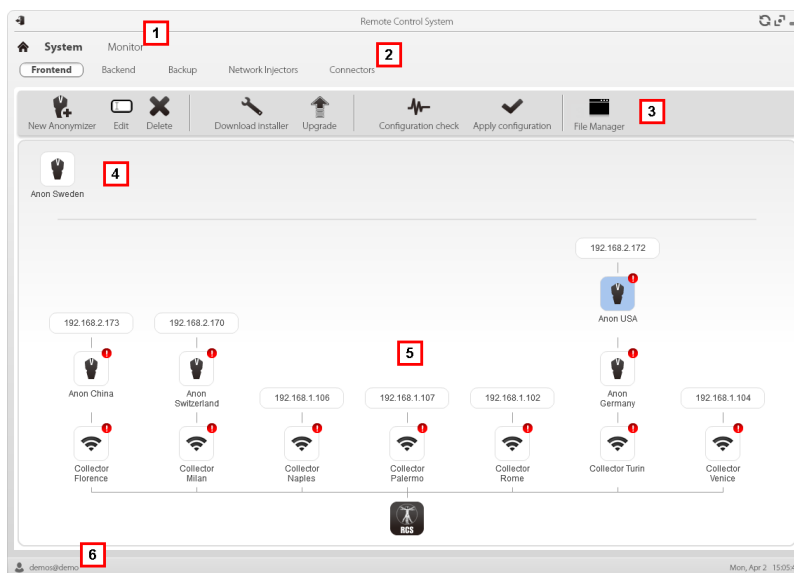
During installation, this function lets you create a new Anonymizer "object" that acts as the logical connection between the RCS Console and the software component to be installed on a VPS.



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

### 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:
-  Creates a new Anonymizer.
  -  Edits Anonymizer data. After editing, click **Reload Log**. Show last logs.  
 Tip: double-click an Anonymizer to check/edit data.
  -  Deletes 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.
  -  Updates the Anonymizer software version from remote.
  -  Simulates agent behavior. It connects to each Anonymizer in the chain up to the gateway Collector, and returns connection results.
  -  Updates 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.
- 5** Anonymizer chains on the system with the IP address of the last element.
-  Anonymizer (for the meanings of the various symbols, see "[What you should know about Anonymizer](#)" on page 32)
  -  Collector running.
  -  Collector not running.
- 6** RCS status bar.

## To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 86.  
To install, edit or cancel an Anonymizer see "[Anonymizer installation and settings](#)" on page 34.



## Adding an Anonymizer to the configuration

To add an Anonymizer see "[Anonymizer installation and settings](#)" on page 34.

## Editing Anonymizer settings

To edit Anonymizer settings see "[Anonymizer installation and settings](#)" on page 34.

## File Manager data

Descriptions are provided below:

<i>Field</i>	<i>Description</i>
<b>Time</b>	Vector installation date-time on the device.
<b>Name</b>	File name created by the installer.
<b>Factory</b>	Factory that generated the installer.
<b>User</b>	User who created the installer.

## Back end management

To manage back end: | • System section, Backend

### Function scope

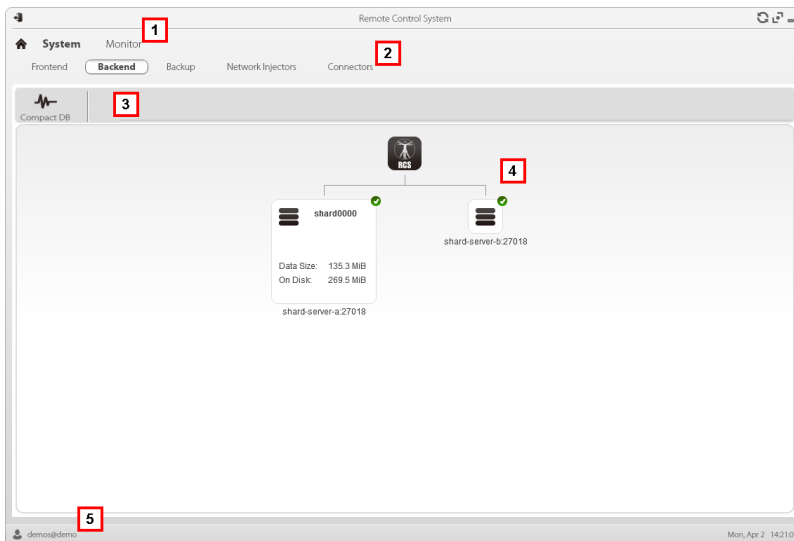
When RCS is running, this function lets you check database status and available disk space.





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

### What the function looks like

This is what the page looks like:



### Area Description

- 1 RCS menu.
- 2 **System** menu.
- 3 Window toolbar. Descriptions are provided below:
  -  Zips the database.
- 4 Shard database structure with status, occupied and free 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 86.

For further information on backups see "[What you should know about backup](#)" on page 96.

### Significant Shard database data

Selected Shard database data is described below:

<i>Field</i>	<i>Description</i>
<b>Occupied space.</b>	Occupied space.
<b>Total space</b>	Total Shard device space.
<b><i>serverName.port</i></b>	Shard server port

## What you should know about backup

### Management responsibilities

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

### Backup methods

RCS saves all data in databases in the specified folder when editing RCS settings. See "[Editing Master Node settings](#)" on page 69

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

- metadata
- full
- operation
- target

### Metadata type backup

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



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



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

### Full type backup

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

### Operation type backup

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

### Target type backup

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

### Incremental backup

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

<i>If after the last backup</i>	<i>Then restore</i>
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.

## Full backup for serious reasons

### Introduction

In extreme cases (i.e.: server migration to different hardware, corrupted data restore), run full backup.

### Run backup

How to run backup:

**Step Action**

---

- 1 Stop all RCS services.
- 2 Create a full copy of folder C:\RCS\.

**Restore backup**

How to run restore:

**Step Action**

---

- 1 Install an RCS system as if it were new.
- 2 Stop all RCS services.
- 3 Replace the new folder C:\RCS\ with the previously copied one.
- 4 Restart services.

**Backup management**

*To manage backups:* | • System section, Backup

**Function scope**

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

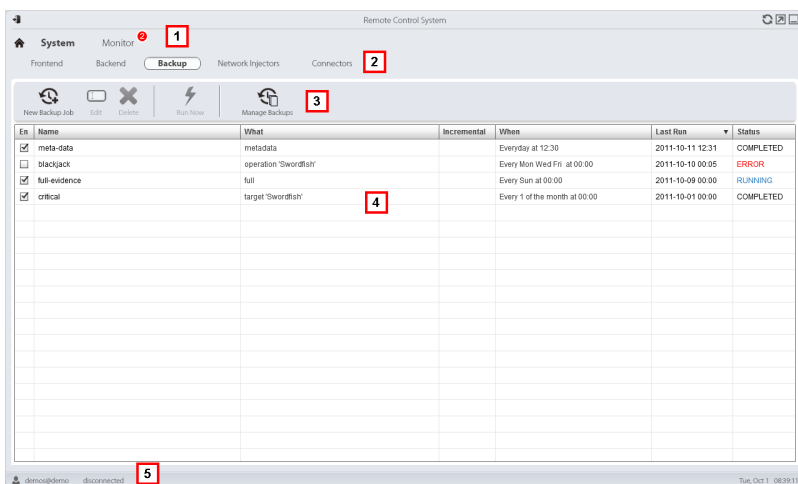
During RCS maintenance, this function lets you fix damaged data restoring them with a backup.












NOTE: the function is only enabled with **System backup and restore** permissions.

**What the function looks like**

This is what the page looks like:




## Area Description

- 1 RCS menu.
- 2 **System** menu.
- 3 Backup process toolbar. Descriptions are provided below:
  -  Adds a backup process.
  -  Edits 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.**
  -  Deletes a backup process. Does not delete the backup files generated by the process.
  -  Runs backup even if disabled.
  -  View the list of completed backups. Buttons are described below:
  -  Restores selected backup data.
    -  **CAUTION: restoring data is a delicate operation. Make sure you have fully understood RCS restore mechanisms. See "What you should know about backup" on page 96**
  -  Deletes the selected backup.
- 4 List of programmed backup processes (enabled and non) with last backup status.
- 5 RCS status bar.

## Significant backup process data

The selected backup process data is described below:

<i>Field</i>	<i>Description</i>
<b>Enabled</b>	<p>Enables/disables the backup process. Use to temporarily disable the process, for example, when replacing the backup device.</p> <p> Tip: to quickly enable/disable a process, flag the check box in the <b>En</b> column in the list.</p>
<b>What</b>	<p>Data to be included in backup.</p> <p><b>Metadata:</b> 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.</p> <p><b>Full:</b> full backup of the system configuration and tapping data (operation and target). It may take a while to execute.</p> <p><b>Operation:</b> backup of the indicated operation, data included.</p> <p><b>Target:</b> backup of the indicated target, data included</p>
<b>When</b>	<p>Backup frequency.</p> <p><b>UTC:</b> time zone.</p>
<b>Name</b>	Name to be assigned to the backup.

## Connector management

To manage connectors: | • System section, Connectors

### Function scope

This function lets you create connection rules with other installed RCS servers with specific licenses or third party software. The evidence received by RCS will be sorted according to these rules.



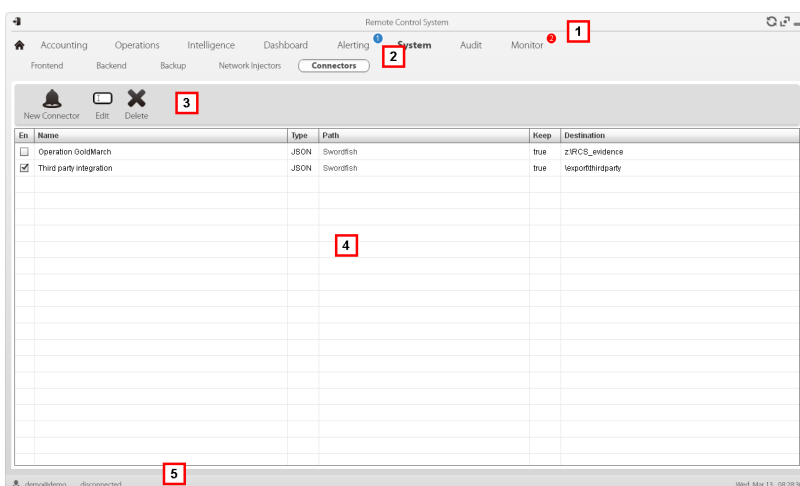
**IMPORTANT:** this function requires a user license.






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

### What the function looks like

This is what the page looks like:



### Area Description

- 1 RCS menu.
- 2 **System** menu.
- 3 Window toolbar. Descriptions are provided below:
  -  Adds a connection rule.
  -  Edits the selected connection rule.
  -  Deletes the selected connection rule.
- 4 List of connection rules.
- 5 RCS status bar.

### To learn more



For interface element descriptions See "[Shared interface elements and actions](#)" on page 86.

### Significant connection rule data

Selected rule data is described below:

<b>Field</b>	<b>Description</b>
<b>Path</b>	Name of the operation or target evidence is sent to. If not specified, all operations and evidence will be sent to third party software.
<b>Type</b>	Evidence storage type: <ul style="list-style-type: none"> <li>• <b>Local:</b> evidence is sent to a local folder</li> <li>• <b>Remote:</b> evidence is sent to RCS system.</li> </ul>



<i>Field</i>	<i>Description</i>
<b>Format</b>	Evidence format. <ul style="list-style-type: none"> <li>• <b>JSON, XML</b> for <b>Local</b> type</li> <li>• <b>RCS</b> for <b>Remote</b> type</li> </ul>
<b>Saves evidence</b>	If selected, a copy of the evidence is kept in the RCS database. <p> <b>CAUTION: if not selected, this evidence can no longer be viewed in RCS, nor can alerts be received.</b></p>
<b>Target</b>	Local folder path where evidence is sent (i.e.: "C:\RCSevidence") or RCS server IP address. <p> <b>NOTE:</b> evidence can only be sent to an RCS server with a specific user license. The ID that will be linked to the sent evidence can be set in the system configuration file.</p>


## Managing the Network Injector

To manage Network Injectors: | • System section, Network Injectors

### 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.
- export the authentication key to be installed on Network Injector to enable communications with RCS Console.

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

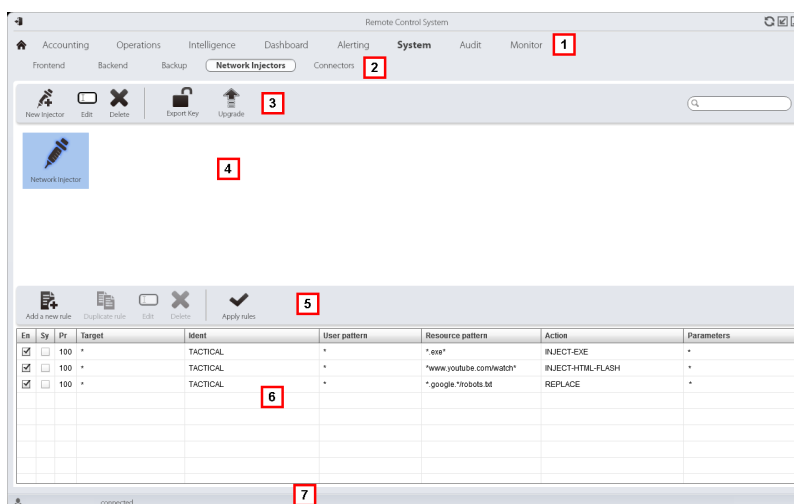
### What you can do

With this function you can:







- create a new Network Injector
- export the Network Injector authentication key
- update Appliance Control Center or Tactical Control Center software
- view logs and check Network Injector status

What the function looks like

This is what the page looks like:



## Area Description

- 1 RCS menu.
- 2 **System** menu.
- 3 Network Injector toolbar. Descriptions are provided below:
  -  Adds a new Network Injector
  -  Edits Network Injector data and views logs.
  -  Deletes the selected Network Injector.
  -  Generates a .zip file with the selected Network Injector authentication key.
  -  Updates Appliance Control Center or Tactical Control Center software. If Network Injector is Appliance type, it will be automatically updated at the next synchronization provided an infection process is running. If, instead, it is Tactical type, the operator must select whether the application is to be updated. See "[Network Injector Appliance update](#)" on page 62, "[Tactical Network Injector update](#)" on page 64
- 4 Network Injector list.
- 5 Injection rule toolbar.
  -  Opens the window with rule data.
- 6 List of selected Network Injector rules
- 7 RCS status bar.

## To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 86.

To learn more about Network Injector Appliance installation see "[Network Injector Appliance installation](#)" on page 39

To learn more about Tactical Network Injector installation see "[Tactical Network Injector installation](#)" on page 46.

To learn more on Network Injector data see "[Network Injector data](#)" below

## Updating Network Injector control software

To update Network Injector:

### Step Action




- 1
  - Select the Network Injector
  - Click **Upgrade**: update data appears.
  - Click **OK**: RCS receives the request to send the update to Network Injector.



**IMPORTANT: Network Injector only receives the software update when it is synchronized with the RCS server. See "[Checking Network Injector status](#)" on page 52**

## Network Injector data

Network Injector data is described below:

<i>Data</i>	<i>Description</i>
<b>Name</b>	Network Injector name
<b>Description</b>	Free description.
<b>Release</b>	Software version. To view the software versions of all the components see " <a href="#">System monitoring (Monitor)</a> " on the facing page.
<b>Log</b>	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 " <a href="#">System logs</a> " on page 74.
	 Updates the list.
	 Deletes 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



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

### What the function looks like

This is what the page looks like:

Type	Name	Address	Last contact	Status	CPU Proc	CPU Host	Disk Free
Satellite		127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%
Master		127.0.0.1	2014-05-30 11:57:21	✓	70%	15%	20%
Intelligence		172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
Money		172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
Dir		172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
Anonymizer		172.20.20.1	2014-05-30 11:57:21	✓	90%	70%	70%
Anonymizer		172.20.20.2	2014-05-30 11:57:21	✓	90%	70%	70%
Anonymizer		172.20.20.3	2014-05-30 11:57:21	✓	90%	70%	70%
Anonymizer		172.20.20.4	2014-05-30 11:57:21	✓	90%	70%	70%
Anonymizer		172.20.20.5	2014-05-30 11:57:21	✓	90%	70%	70%

### Area Description

1 RCS menu.

**Monitor** <sup>1</sup>: indicates the current number of system alarms triggered.

2 Window toolbar.




Descriptions are provided below:



Deletes the component to be monitored.

---

### Area Description

- 3 List of RCS components and their status:
  -  Alarm (generates an e-mail sent to the alerting group)
  -  Warning
  -  Component running
- 4 RCS status bar.

### To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 86.

For a description of the data in this window see "[System monitoring data \(Monitor\)](#)" 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>
<b>Type</b>	Monitored component type and name.
<b>Name</b>	Some examples are provided below:
	Anonymizer
	Carrier
	Collector
	Database
	Network Controller




<i>Data</i>	<i>Description</i>
<b>Address</b>	Component's IP address.
<b>Last contact</b>	Last synchronization date-time.
<b>Status</b>	Component status at last synchronization: <ul style="list-style-type: none"> <li> Alarm: the component is not running, contact the alerting group for immediate service.</li> <li> Warning: the component signals a risky situation, contact the system administrator for necessary checks.</li> <li> Component running.</li> </ul>
<b>CPU Proc</b>	% CPU use by the single process.
<b>CPU Host</b>	% CPU use by server.
<b>Free disk</b>	% 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>
<b>License type</b>	Type of license currently in use for agents. <ul style="list-style-type: none"> <li><b>reusable:</b> an agent's license can be reused after it is uninstalled.</li> <li><b>oneshot:</b> an agent's license is only valid for one installation.</li> </ul> <p> NOTE: the license can only be updated if the user has <b>License modification</b> authorization.</p>
<b>Users</b>	Amount of users currently used by the system and maximum admitted quantity.
<b>Agent</b>	Amount of agents currently used by the system and maximum admitted quantity.
<b>Desktop Mobile</b>	Amount of desktop and mobile agents currently used by the system and maximum admitted quantities respectively.

<i>Data</i>	<i>Description</i>
<b>Distributed servers</b>	Amount of databases currently used by the system and maximum admitted quantity.
<b>Collectors</b>	Amount of Collectors currently used by the system and maximum admitted quantity.
<b>Anonymizers</b>	Amount of Anonymizers currently used by the system and maximum admitted quantity.

# 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. 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.

**BSSID**

(Basic Service Set Identifier) Access Point and its client identifier.

**C**

---

**Carrier**

Collector Service: sends data received from Anonymizers to shards or the Master Node.

**Collector**

Collector Service: receives data sent by agents, via 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**

---

### **Elite agent**

Agent installed on secure devices. Lets you collect all types of available evidence.

### **entity**

Group of intelligence information linked to the target and people and places involved in the investigation.

### **ESSID**

(Extended Service Set Identifier) Known as SSID, identifies the WiFi network.

### **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.

### **Exploit**

Code which, exploiting a bug or vulnerability, runs an unforeseen code. Used to infect target devices.

## **F**

---

### **factory**

A template for agent configuration and compiling.

### **front end**

Environment designed to communicate with agents to collect information and set their configurations. It includes Collectors.

## **G**

---

### **Group**

Intelligence entity that groups several entities.

## **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**

Collector Service: 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.

## **P**

---

### **Person**

Intelligence entity that represents a person involved in the investigation.

### **Position**

Intelligence entity that represents a place involved in the investigation.

## **R**

---

### **RCS**

(Remote Control System) the product documented hereto.

### **RCS Console**

Software designed to interact with the RCS Server.

### **RCS receiver**

RCS system that receives evidence from other RCS sender systems (see) and never directly from agents. Compared to a complete RCS, RCS receiver provides functions only to process evidence.

### **RCS sender**

RCS system that receives evidence from agents and transfer them to other RCS receiver systems (see) via connection rules. It is a complete RCS system.

### **RCS Server**

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

## **S**

---

### **Scout agent**

Replaced the agent sent to the device to check the security level before installing actual agents (elite or soldier).

### **Soldier agent**

Agent installed on not fully secure devices. Only lets you collect some types of evidence.

## **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. It is represented by the Target entity in the intelligence section.

## **Technician**

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

## **V**

---

### **Virtual**

Intelligence entity that represents a virtual location (i.e.: website) involved in the investigation.

## **VPS**

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

## **W**

---

### **WPA**

(WiFi Protected Access) WiFi network protection.

### **WPA 2**

(WiFi Protected Access) WiFi network protection.

# ]HackingTeam[

RCS 9.6 System administrator manual  
System administrator manual 1.9 MAR-2013  
© COPYRIGHT 2015  
info@hackingteam.com

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

---