

]HackingTeam[

RCS 8.0

The hacking suite for governmental interception

Analyst's Guide



Information property

© COPYRIGHT 2012, HT S.r.l.

All rights reserved in all countries.

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

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

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

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

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

HT S.r.l.

via della Moscova, 13

20121 Milano (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

Contents

Glossary	iv
Guide introduction	1
New guide features.....	2
Supplied documentation.....	2
Print concepts for notes.....	2
Print concepts for format.....	3
Product and guide addressees.....	3
Software author identification data.....	4
RCS (Remote Control System)	5
Differences with previous versions.....	6
Glossary.....	6
RCS Console for the Analyst	7
Starting the RCS Console.....	8
What the login page looks like.....	8
Open RCS Console.....	8
Homepage description.....	9
Introduction.....	9
What it looks like.....	9
Shared interface elements and actions.....	10
What the RCS Console looks like.....	10
Actions always available on the interface.....	12
Change interface language or password.....	12
Converting the RCS Console date-time to the actual time zone.....	12
Table actions.....	12
Analyst's procedures.....	14
Introduction.....	14
Procedures.....	14
To retrieve important evidence and be alerted.....	14
Analyzing, selecting and exporting evidence.....	14
Alert on new evidence	16
What you should know about target alerts.....	17
What are alerts.....	17
Alert rule utilities.....	17
Alert rule application field.....	17
Alert process.....	17
Target alert (Alerting).....	18
Purpose.....	18
What the function looks like.....	18

To learn more.....	20
Adding a rule to be alerted.....	20
Editing an alert rule.....	20
Adding a rule to automatically tag certain evidence.....	20
Viewing evidence matching the logged alert.....	21
Target alert data (Alert).....	21
Alert rule data.....	21
Log data.....	22
Monitoring the target's activities from the Dashboard.....	24
What you should know about the Dashboard.....	25
Dashboard Components.....	25
Evidence alert process.....	25
Monitoring evidence (Dashboard).....	26
Purpose.....	26
What the function looks like.....	26
To learn more.....	27
Adding an element to the Dashboard.....	27
Viewing evidence indicated in the Dashboard.....	28
Evidence analysis.....	29
What you should know about evidence.....	30
Analysis process.....	30
Filtering evidence.....	30
.tgz file description with exported evidence.....	30
Evidence analysis (Evidence).....	31
Purpose.....	31
What the function looks like.....	31
To learn more.....	32
Preparing evidence for analysis and export, tagging by relevance.....	32
Preparing evidence for analysis and export, tagging for the report.....	33
Preparing evidence for analysis and export adding personal notes.....	33
Analyzing evidence.....	34
Viewing counters divided by type.....	34
Exporting displayed evidence.....	34
Evidence data.....	34
Evidence details.....	36
Purpose.....	36
What the function looks like.....	36
To learn more.....	37
Image type evidence actions.....	37
Audio type evidence actions.....	38

Evidence export data.....	38
List of types of evidence.....	39
Exploring and retrieving evidence from online devices.....	41
What you should know about retrieving evidence.....	42
Description.....	42
File System components.....	42
Retrieve evidence from devices (File System).....	42
Purpose.....	42
What the function looks like.....	43
To learn more.....	43
Exploring file system content and downloading files.....	44
Targets.....	45
Target page.....	46
Purpose.....	46
What the function looks like.....	46
To learn more.....	47
Exporting target evidence.....	47
Target page data.....	47
Icon view.....	48
Table view.....	48
Agents.....	50
Agent page.....	51
Purpose.....	51
What the function looks like.....	51
To learn more.....	52
Agent event log data.....	52

Glossary

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

A

Accounting

Console section that manages RCS access.

acquisition sequence

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

Administrator

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

Agent

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

alert rules

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

Alerting

Console section that manages new evidence alerts.

alerting group

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

Analyst

Person in charge of analyzing the data collected during operations.

Anonymizer

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

Audit

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

B

back end

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

BRAS

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

C

Collector

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

console

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

D

Dashboard

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

DSLAM

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

E

evidence

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

evidence alerts

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

F

factory

A template for agent configuration and compiling.

front end

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

I

injection rules

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

M

Monitor

Console section that monitors components and license status.

N

Network Controller

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

Network Injector

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

Network Injector Appliance

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

O

operation

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

R

RCS

(Remote Control System) the product documented hereto.

RCS Console

Software designed to interact with the RCS Server.

RCS Server

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

S

SSH

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

System

Console section that manages the system.

System administrator

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

T

Tactical Network Injector

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

TAP

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

target

The physical person under investigation.

Technician

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

V

VPS

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

Guide introduction

Presentation

Manual goals

This manual is a guide for the *Analyst* on how to use the RCS Console to:

- monitor the target
- explore target devices
- analyze and export evidence

Information on how to consult the manual is provided below.

Content

This section includes the following topics:

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

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>
16 April 2012	Analyst's Guide 1.0 APR-2012	8.0	First publication

Supplied documentation

The following manuals are supplied with RCS software:

<i>Manual</i>	<i>Addressees</i>	<i>Code</i>	<i>Distribution format</i>
System Administrator's Guide	System administrator	<i>System Administrator's Guide - 1.0 APR-2012</i>	PDF
Administrator's Guide	Administrators	<i>Administrator's Guide - 1.0 APR-2012</i>	PDF
Technician's Guide	Technicians	<i>Technician's Guide - 1.0 APR-2012</i>	PDF
Analyst's Guide (this manual)	Analysts	<i>Analyst's Guide - 1.0 APR-2012</i>	PDF

Print concepts for notes

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



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



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



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



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



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



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


Print concepts for format

A key to print concepts is provided below:

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

Product and guide addressees

Following is the list of professionals that interact with RCS.

Addressee	Activity	Skills
System administrator	Follows the HackingTeam's instructions provided during the contract phase. Installs and updates RCS servers, Network Injectors and RCS Consoles. Schedules and manages backups. Restores backups if servers are replaced.  WARNING: the system administrator must have the required necessary skills. The HackingTeam is not liable for equipment malfunctions or damages due to unprofessional installation.	<i>Expert network technician</i>
Administrator	Creates authorized accounts and groups. Creates operations and target. Monitors system and license status.	<i>Investigation manager</i>
Technician	Creates and sets up agents. Sets Network Injector rules	<i>Tapping specialist technician</i>
Analyst	Analyzes and exports evidence.	<i>Operative</i>

Software author identification data

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

RCS (Remote Control System)

Presentation

Introduction

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

Content

This section includes the following topics:

Differences with previous versions	6
---	----------

Differences with previous versions

Differences with the RCS 7.6 version are described below

Glossary

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

RCS Console for the Analyst

Presentation

The Analyst's role

The role of the Analyst is to:

- select and analyze evidence
- retrieve evidence from a device
- export evidence for the authorities

Analyst enabled functions

To complete his/her activities, the Analyst has access to the following functions:

- **Operation**
- **Dashboard**
- **Alerting**

Content

This section includes the following topics:

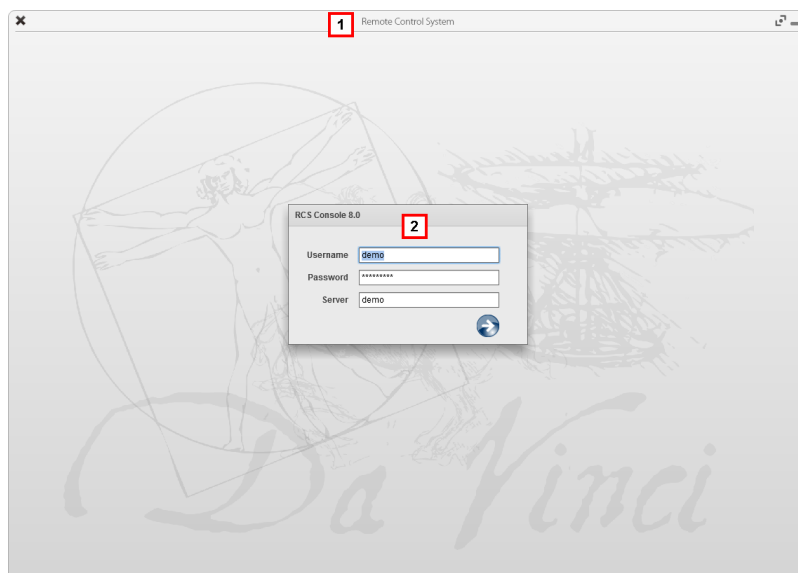
Starting the RCS Console	8
Homepage description	9
Shared interface elements and actions	10
Analyst's procedures	14

Starting the RCS Console

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

What the login page looks like

This is what the login page looks like:



Area Description

- 1 Title bar with command buttons:
 - ✕ Close RCS Console.
 - 🗑️ Expand window button.
 - ▭ Shrink window button.
- 2 Login dialog window.


Open RCS Console

To open RCS Console functions:

Step Action

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

Step Action

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

Homepage description

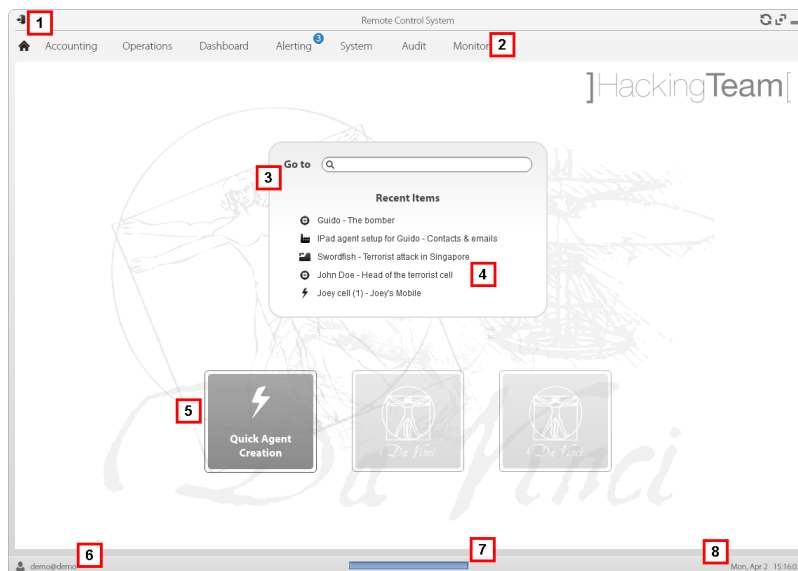
To view the homepage:  click 

Introduction

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

What it looks like

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



Area Description

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

Area Description

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

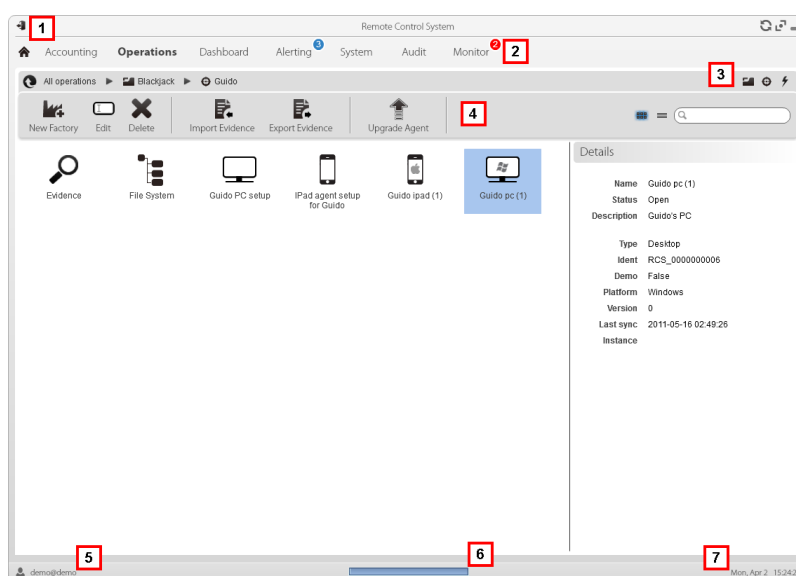
Shared interface elements and actions

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






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

What the RCS Console looks like






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






Area Description

- 1 Title bar with command buttons:
 -  Logout from RCS.
 -  Page refresh button.
 -  Expand window button.
 -  Shrink window button.
- 2
 -  Return to homepage button
 - RCS menu with functions enabled for the user.
- 3 Operation scroll bar. Descriptions are provided below:

Icon Description




-  Back to higher level.
 -  Show the operation page.
 -  Show the target page.
 -  Show the factory page.
 -  Show the agent page.
- 4 Buttons to display all elements regardless of their group membership. Descriptions are provided below:

Icon Description

-  Show all operations.
-  Show all targets.
-  Show all agents.

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

Object	Description
---------------	--------------------

	Search box. Enter part of the name to display a list of elements that contain the entered letters.
	Display elements in a table.
	Display elements as icons.

- 7 Logged in user with possibility of changing the language and password.

Area Description

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

Actions always available on the interface

Change interface language or password

To change the interface language or password:

Step Action

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

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

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

Step Action

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

Table actions

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

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

Action**Description****Sort by column**

Click on the column heading to sort that column in increasing or decreasing order.

Event	Path
SYNC	Swordfish
INSTANCE	Swordfish > J
EVIDENCE	*

Filter a text

Enter part of the text you are searching for: only elements that contain the entered text appear.

 Info

The example shows elements with descriptions like:

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

Filter based on an option

Select an option: the elements that match the selected option appear.

 Acquired
 Last 24 Hours
 Last Week
 From / To
 Action
 User

Filter based on several options

Select one or more options: the elements that match all selected options appear.

 Type
 Untagged
 Low
 Medium
 High
 Critical
Change the column size

Select the edge of the column and drag it.

Analyst's procedures

Introduction

The goal of the Analyst is to provide valid evidence for the investigation in progress. Evidence is:

- directly retrieved from the device through physical access,
- received from the installed agent,

To do this, the Analyst can perform the following procedures:

Procedures

To retrieve important evidence and be alerted

To select and retrieve important evidence:

<i>Step</i>	<i>Action</i>
1	In the File System section, during remote tapping, explore the device hard disks searching for files to be downloaded. See " Retrieve evidence from devices (File System) "
2	In the Dashboard section, add the operation, targets and agents to be monitored to the dashboard. See " Monitoring evidence (Dashboard) "
3	In the Alerting section, set rules to be alerted when evidence of special interest arrives and to tag evidence according to relevance. See " Target alert (Alerting) "

Analyzing, selecting and exporting evidence

To analyze, select and export evidence:

<i>Step</i>	<i>Action</i>
1	In the Evidence section, analyze evidence and tag them according to relevance and whether or not they are to be exported. See " Evidence analysis (Evidence) ".
2	For evidence of special interest, move on to detailed analysis. See " Evidence details ".

Step Action

- 3** In the **Evidence** section, export useful evidence.
See "[Evidence analysis \(Evidence\)](#)".
- 4** In the File System section, export the hard disk structure
See "[Retrieve evidence from devices \(File System\)](#)"

Alert on new evidence

Presentation

Introduction

Alerts signal the receipt of evidence and automatically tags evidence (for analysis and export) when received.

Content

This section includes the following topics:

What you should know about target alerts	17
Target alert (Alerting)	18
Target alert data (Alert)	21

What you should know about target alerts

What are alerts

During the investigation phase, various evidence is collected from the target device. In addition to collecting evidence to be analyzed, it can be useful receive "alerts" in real time on special events that concern the target via email or a notification on the RCS Console.

For example, if awaiting evidence from a target for a long time, an alert rule can be created to send an email and record a log for each piece of evidence received. This way, users are immediately notified when the target resumes activities. The rule can be disabled later and evidence can simply be viewed as it arrives.

Alert rule utilities

Alert rules inform the system when alerts must be sent for evidence or synchronizations. Furthermore, they can be used to automatically assign certain evidence levels of relevance that can be used in the analysis phase to select evidence.

Alert rule application field

Rules can be created to alert the arrival of evidence in the system at the following levels:

- **Operation:** all evidence for all operation targets
- **Target:** all evidence for all target agents
- **Agent:** all agent evidence



NOTE: each user will be alerted according to their set rules.

Alert process

The alert process is described below:



NOTE: sending an email is optional.

Phase **Description**

- 1 The Analyst creates the rules to be alerted when special evidence arrives or when the target device is synchronized. Rules log the alerts, notify them on the RCS Console and send them via email (optional).

Phase Description

- | | | |
|----------|--|---|
| 2 | The system taps incoming evidence and compares them with the alert rules. | |
| | <i>If the evidence...</i> | <i>Then...</i> |
| | corresponds to an alert rule | The system logs information as <i>evidence</i> and generates an alert that automatically applies the selected level of relevance. An email notification can be sent by the system as an option. |
| | does not correspond to an alert rule | the system logs the information as <i>evidence</i> without generating an alert. |
| 3 | The Analyst receives an alert email (if set by the alert rule) and checks the alert log. The evidence that generated an alert can be directly viewed from the alert. | |
| 4 | After checking, the Analyst deletes the alert logs. | |

Target alert (Alerting)

To receive alerts from the target: | • Alerting section

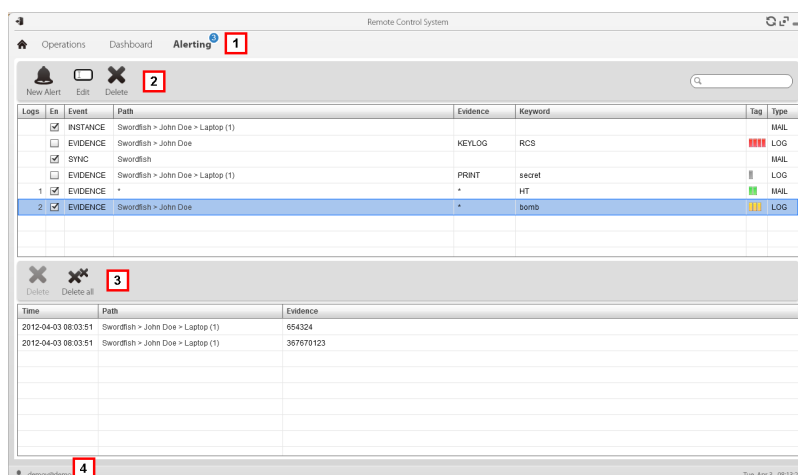
Purpose

This function lets you:

- receive alerts when a certain type of evidence is tapped or when the target device synchronizes with RCS.
- automatically tag evidence by relevance to facilitate later analysis.
- monitor all logged alerts and list the evidence that generated them.

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.

Alerting ³: indicates the amount of alerts received. The counter is automatically reset after two weeks or when notifications are deleted.

- 2 Alert rule toolbar. Descriptions are provided below:

Icon	Description
------	-------------



Create a new alert rule.



Edit the selected alert rule.



Delete the selected alert rule.



CAUTION: all generated notifications are deleted.

- 3 Alert log toolbar. Descriptions are provided below:

Icon	Description
------	-------------



Delete the selected alert log.



Delete all alert logs.

- 4 RCS menu.

To learn more

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

For a description of the data in this window see "[Target alert data \(Alert\)](#)".

For more information on alerts see "[What you should know about target alerts](#)".

Adding a rule to be alerted

A rule must be set in order for you to be alerted:

Step Action

- 1 Click **New Alert**: data entry fields appear.
- 2
 - Enter the required data indicating the alert method in **Type**.
 - Select the **Enabled** box to apply the rule.
- 3 Click **Save**: the new alert rule appears in the main work area. An alert is sent as soon as the system receives evidence that matches the rule.

Editing an alert rule

To edit an alert rule

Step Action

- 1 Select the alert rule to be edited
Click **Edit**: the data to be edited appears.
- 2
 - Edit data.
 - Select the **Enabled** box to immediately apply the rule.
- 3 Click **Save**: the new alert rule appears in the main work area. An alert is sent as soon as the system receives evidence that matches the rule.

Adding a rule to automatically tag certain evidence

To automatically tag certain evidence without logging or sending alerts:

Step Action

- 1 Click **New Alert**: data entry fields appear.

Step Action

-
- 2
 - Set evidence selection criteria
 - In **Type** select **None**.
 - In **Tag** set the relevance tag
 - Select the **Enabled** box to apply the rule.
 - 3 Click **Save**: the new alert rule appears in the main work area. As soon as the system receives evidence matching this rule, the evidence is tagged.

Viewing evidence matching the logged alert

To view evidence matching an alert:















Step Action

-
- 1 Select the alert rule with at least one log (**Logs** column): all logged alerts appear in the list.
 - 2 In the logged alert list, double-click the **Evidence** column: the list of evidence that triggered the alert appears.

Target alert data (Alert)**Alert rule data**

Alert rule data is described below:

<i>Data</i>	<i>Description</i>
Logs	(only in a table) Amount of notifications received matching the rule.
Enabled	Enables or disables the alert rule.
Event	Type of event that triggers the alert: <ul style="list-style-type: none"> • Evidence: triggers the rule when evidence that meets the criteria below arrives. • Sync: triggers the rule when the agent indicated below runs synchronization. • Instance: triggers the rule when the agent created (instanced) by the factory indicated below runs the first synchronization.
Path	operation, target, agent and factory whose evidence and synchronizations are to be monitored. Thus it indicates the rule application field. For example, if an operation is selected, all operation evidence is monitored. If an agent is selected, that agent's evidence is monitored.

<i>Data</i>	<i>Description</i>												
Evidence	<p>(only Evidence type events) Type of evidence that generates alerts.</p> <p> Tip: '*' indicates all types of evidence.</p> <p>For a description of all types see "List of types of evidence"</p>												
Keyword	<p>(only Evidence type events) Keyword that the evidence must contain to trigger the alert.</p> <p>For example, keyword "password" creates an alert when the evidence (audio, document) contains the word "password".</p>												
Tag	<p>(only Evidence type events) Automatically tags evidence with different levels of relevance to make it easier to search for the most important evidence in the analysis phase:</p> <table border="1"> <thead> <tr> <th>Icon</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td></td> <td>Maximum relevance.</td> </tr> <tr> <td></td> <td>Intermediate relevance.</td> </tr> <tr> <td></td> <td>Normal relevance.</td> </tr> <tr> <td></td> <td>Minimum relevance.</td> </tr> <tr> <td>-</td> <td>No relevance.</td> </tr> </tbody> </table>	Icon	Description		Maximum relevance.		Intermediate relevance.		Normal relevance.		Minimum relevance.	-	No relevance.
Icon	Description												
	Maximum relevance.												
	Intermediate relevance.												
	Normal relevance.												
	Minimum relevance.												
-	No relevance.												
Type	<p>Type of alert to be received when evidence arrives:</p> <ul style="list-style-type: none"> • Log: alert logged and notified on the RCS Console. • Mail: email and logged alert • None: no logged alert nor email. Useful to automatically tag evidence by importance (Tag) 												
Suppression Time	<p>(only Mail type alerts) Latency time for sending identical alert emails. Used to avoid identical emails after the first. For example, if the target has not communicated its evidence for a while and email alert was selected, you may be bombarded with emails when the first evidence arrives. Set a 30- minute Suppression time to receive one email every 30 minutes.</p> <p> NOTE: this setting only limits email delivery. Evidence is always logged.</p>												

Log data

Alert logs are described below:

<i>Data</i>	<i>Description</i>
Time	alert time-date.

<i>Data</i>	<i>Description</i>
Path	Range of action from which the alert was generated. For example, if a target was selected in the rule Path , the name of the target and the name of the operation it belongs to will appear here.
Evidence	Amount of evidence that generated the alert.

Monitoring the target's activities from the Dashboard

Presentation

Introduction

The Dashboard helps you to monitor connected agent activities and the incoming evidence flow.

Content

This section includes the following topics:

What you should know about the Dashboard	25
Monitoring evidence (Dashboard)	26

What you should know about the Dashboard




Dashboard Components

The Dashboard is made up of one or more elements selected by the user from:

- operation
- target
- agent

Each element shows the total amount of evidence collected. Values are updated at each synchronization:

- **Red number:** amount of evidence received at last synchronization.
- **Black number:** amount of evidence received since login.

Example	Description
<p>Operation evidence:</p> 	<p>Operation targets and the amount of evidence per target appear.</p>
<p>Target evidence:</p> 	<p>The target's evidence and the amount of evidence per type appear.</p>
<p>Agent evidence:</p> 	<p>The agent's evidence and the amount of evidence per type appear.</p>



NOTE: the lack of numbers indicates that evidence has not yet arrived since login.

To view the complete list of evidence types see "[List of types of evidence](#)".

Evidence alert process

The evidence alert process is described below:

Phase Description

- 1 The Analyst adds the operation, target or agent elements whose evidence is to be monitored to the Dashboard.
- 2 The system updates counters the next time agents are synchronized if evidence is received.
- 3 The Analyst checks the most recent evidence, those indicated by the red number. To view details, click on the corresponding icon.
- 4 The system resets numbers when the user exits the current session.

Monitoring evidence (Dashboard)

To monitor received evidence:

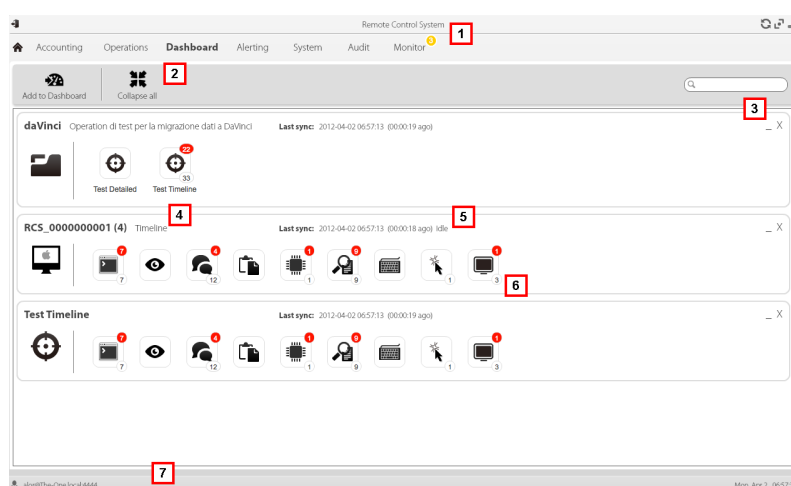
- Dashboard section

Purpose

The Dashboard lets you monitor certain operations, targets or agents and view incoming evidence. Settings are fully customizable. For example, a Dashboard can be set to only monitor some target devices.

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 Window toolbar. Descriptions are provided below:

Icon Description



Add a new element to be monitored.



Shrink or expand all Dashboard element windows.



- 3 Keys used to shrink or delete elements from the dashboard.
- 4 Dashboard element name and description.
- 5 Last element synchronization date.
In progress: synchronization in progress.
Idle: synchronization not in progress
- 6 Evidence recently acquired in an operation, target or agent.
- 7 RCS status bar.

To learn more

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

For more information on the Dashboard see "[What you should know about the Dashboard](#)".

Adding an element to the Dashboard

To add a new element to the Dashboard:

Step Action

- 1 Click **Add to Dashboard**: a window opens to search for elements to be added.
- 2 Enter part of the element name or description to be added: the list of elements that match the search appears.
- 3
 - Select the element from the list: the element is automatically added to the Dashboard and the search window is left open for a new search.
 - Repeat steps 2 and 3 until all required elements are added.
- 5 After adding elements, click ***** to close the search window and return to the Dashboard.

Viewing evidence indicated in the Dashboard

To view Dashboard evidence



NOTE: click a target or operation to open the selected object's work area where the Analyst can view the required agents.

Step **Action**

- 1 For the operation element:
 - double-click the target to open the target page. See "[Target page](#)".
- For the target element:
- double-click the agent: the agent page opens. See "[Agent page](#)".
- For the agent element:
- double-click the evidence type: the evidence page appears. See "[Evidence analysis \(Evidence\)](#)".

Evidence analysis

Presentation

Introduction

Evidence analysis on the list or detailed level, select evidence to be exported to the authorities.

Content

This section includes the following topics:

What you should know about evidence	30
Evidence analysis (Evidence)	31
Evidence data	34
Evidence details	36
Evidence export data	38
List of types of evidence	39

What you should know about evidence

Analysis process

The analysis process is described below:

<i>Phase</i>	<i>Description</i>
--------------	--------------------

- | | |
|---|--|
| 1 | As the system collects evidence from the agent, it displays and updates the total counter. |
| 2 | The Analyst views all evidence and tags it for easy table consultation and subsequent export. |
| 3 | The Analyst analyzes incoming evidence details. |
| 4 | At the end of the investigation or upon request, the Analyst exports evidence to a file that can be viewed in a browser. |

Filtering evidence

Column heading filters can be used to limit the amount of evidence viewed.

See "[Shared interface elements and actions](#)"



IMPORTANT: if no evidence is displayed, check the counter at the bottom right. If a value like "0/1270" is displayed, this means that there is a filter set that prevents evidence from being displayed.

.tgz file description with exported evidence

The exported .tgz file is a compressed file that can be opened with most compression programs (i.e.: WinZip, WinRar). Once unzipped, it looks like a folder with an HTML file.

To view the file:

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

- | | |
|---|--|
| 1 | Open index.html with a browser: the homepage displays the list of days with collected evidence statistics per hour. |
| 2 | Click on a day: the list of evidence appears, similar to the one displayed in the Evidence function. |
| 3 | The following actions can be performed from this list: <ul style="list-style-type: none">• on images: click to view the full image• on audio: click to run the mini player• on downloadable files: click ↓↓ to download the file |



Tip: there are style sheets in the Style folder for customizations (i.e.: logos, etc.). These style sheets can be copied to the server to be used on all reports generated by the RCS Console.

Evidence analysis (Evidence)

To analyze evidence:

- **Operations** section, double-click an operation, double-click a target, click **Evidence**
- **Operations** section, double-click an operation, double-click a target, double-click an agent, click **Evidence**

Purpose

This function lets you:

- prepare evidence for analysis, tag it by level of relevance, send it to a report or add personal notes
- view evidence of interest by filtering the list
- superficially analyze evidence from the list or entering in detail for more thorough analysis
- export evidence







What the function looks like

This is what the page looks like:

Area Description

- 1 RCS menu.
- 2 Scroll bar
- 3 Window toolbar. Descriptions are provided below:

Icon Description

- | | |
|---|--|
|  | Export evidence viewed in a .tgz file. |
|  | Apply a level of relevance to the selected evidence. |
|  | Apply a bookmark to the selected evidence. |
|  | Edit selected evidence notes. |
|  | Show the total quantities by evidence type. |
|  | Show selected evidence details. See " Evidence details " |
- 4 Evidence list based on set filters.
 - 5 RCS status bar.

To learn more

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

For a description of the data in this window see "[Evidence data](#)"

For a description of exportable data see "[Evidence export data](#)".

For more information on evidencesee "[What you should know about evidence](#)"

To view a list of evidence types see "[List of types of evidence](#)"

Preparing evidence for analysis and export, tagging by relevance

To assign levels of relevance to evidence, helpful for display and export:

Step Action

- 1 Select one or more pieces of evidence.

Step Action

- 2
 - Drag **Relevance** to the required positionor
 - Press the corresponding key combination.
- 3 **Result:** the single pieces of evidence are tagged with a symbol according to their level of relevance. Evidence can be filtered by this symbol and included/excluded from export.

Preparing evidence for analysis and export, tagging for the report

To include/exclude evidence in a report and filter for viewing:

Step Action

- 1 Select one or more pieces of evidence.
- 2
 - Click **Add Report**or
 - press ALT+R
- 3 **Result:** single pieces of evidence are bookmarked. Evidence can be filtered by this symbol and included/excluded from export.

Preparing evidence for analysis and export adding personal notes

To add personal notes to one or more pieces of evidence:

Step Action

- 1 Select one or more pieces of evidence.
- 2
 - Click **Edit Note**or
 - press ALT+N
- 3 **Result:** the **Notes** field can be edited. If several pieces of evidence are selected, the entered text will be copied to all other **Note** fields.

Analyzing evidence

To quickly or thoroughly analyze evidence:

Step Action

- 1 Analyze the evidence preview. For example, a mini player can be run for audio files to understand whether the evidence is of interest.
- 2 Double-click evidence: evidence details appear. See "[Evidence details](#)"

Viewing counters divided by type

To view the total amount of evidence divided by type:

Step Action

- 1 Click **Show Summary**: the evidence type symbols appear, each with its own counter.
- 2 Click **Hide Summary** to hide counters.

Exporting displayed evidence














To select some pieces of evidence and export them:

Step Action

- 1 First tag evidence by level of relevance and by whether they should be included in the report (**Add report** key).
- 2 Continue selections using the column heading filters on homogeneous groups of evidence (**Included in report** column).
- 3 Click **Export Evidence**: indicate which evidence to be included/excluded. Evidence that meets the selected criteria and has the **Included report** field flagged is exported. See "[Evidence export data](#)".
- 4 Click **Save**: a .tgz file is created and downloaded in folder RCS Download.

Evidence data

Evidence data is described below for both the agent and target:

<i>Data</i>	<i>Description</i>																		
Acquired	Date-time evidence was acquired. It can be filtered. Last 24 hours is set by default.																		
Received	Date-time evidence was logged in RCS. It can be filtered. Last 24 hours is set by default.  Tip: this data is helpful when you suspect that the target device's data-time is not updated and thus the Acquired is not valid.																		
Relevance	Level of evidence relevance, automatically assigned by alert rules or manually assigned in this list. The level of relevance is set using: <ul style="list-style-type: none"> the Relevance command in the menu short-cut keys <p>Short-cut key list.</p> <table border="1"> <thead> <tr> <th><i>Icon</i></th> <th><i>Short-cut keys</i></th> <th><i>Description</i></th> </tr> </thead> <tbody> <tr> <td></td> <td>ALT+4</td> <td><i>Maximum relevance</i></td> </tr> <tr> <td></td> <td>ALT+3</td> <td><i>Intermediate relevance</i></td> </tr> <tr> <td></td> <td>ALT+2</td> <td><i>Normal relevance</i></td> </tr> <tr> <td></td> <td>ALT+1</td> <td><i>Minimum relevance</i></td> </tr> <tr> <td>-</td> <td>ALT+0</td> <td><i>No relevance</i></td> </tr> </tbody> </table>	<i>Icon</i>	<i>Short-cut keys</i>	<i>Description</i>		ALT+4	<i>Maximum relevance</i>		ALT+3	<i>Intermediate relevance</i>		ALT+2	<i>Normal relevance</i>		ALT+1	<i>Minimum relevance</i>	-	ALT+0	<i>No relevance</i>
<i>Icon</i>	<i>Short-cut keys</i>	<i>Description</i>																	
	ALT+4	<i>Maximum relevance</i>																	
	ALT+3	<i>Intermediate relevance</i>																	
	ALT+2	<i>Normal relevance</i>																	
	ALT+1	<i>Minimum relevance</i>																	
-	ALT+0	<i>No relevance</i>																	
Type	Type of evidence to be selected. See " List of types of evidence "																		
Info	Evidence information: text, images, video, audio and so on. It can be filtered by indicating the full field name and part of the text to be searched. For example: <ul style="list-style-type: none"> "content:boss" "program:word" and so on 																		
Notes	Notes entered by the Analyst using: <ul style="list-style-type: none"> Edit Note menu short-cut key ALT+N 																		

<i>Data</i>	<i>Description</i>
Report	Bookmark, that indicates that evidence may be included/excluded during export. The bookmark is set using: <ul style="list-style-type: none"> • Add Report menu • short-cut key ALT+R
Agent	(only for target evidence) Name of the agent that logged the evidence.

Evidence details

To view evidence details:

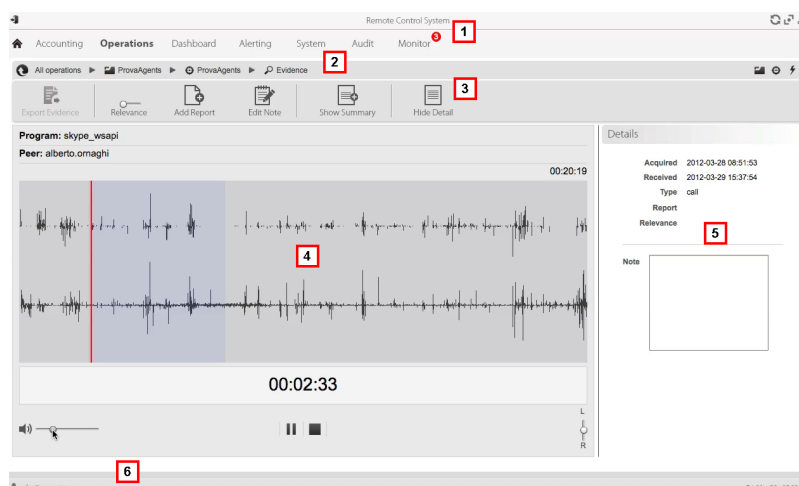
- **Operations** section, double-click an operation, double-click a target, click **Evidence**, double-click a piece of evidence
- **Operations** section, double-click an operation, double-click a target, double-click an agent, click **Evidence**, double-click a piece of evidence

Purpose

This function lets you analyze single evidence details. The interface changes according to the type of evidence - text, audio, image or map.

What the function looks like

This is what audio evidence details looks like:








Area Description

- 1 RCS menu.

Area Description

- 2 Scroll bar
- 3 Evidence action keys.

Icon Description



-  Apply a level of relevance to the selected evidence.
-  Apply a bookmark to the selected evidence.
-  Edit selected evidence notes.
-  Show the total quantities by evidence type.
-  Hide selected evidence details.
- 4 Evidence details. Analysis keys appear according to the type of evidence (audio, image, video).
- 5 Evidence detail data.
- 6 RCS status bar.


To learn more

For interface element descriptions See "[Shared interface elements and actions](#)".
 For more information on evidence see "[What you should know about evidence](#)".
 For a description of the data in this window see "[Evidence data](#)".

Image type evidence actions

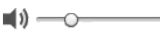


Actions that can be run on image evidence are described below:

Icon	Description
	Full screen view.
1:1	Actual image size view.
	Expand and shrink image.

<i>Icon</i>	<i>Description</i>
	Rotate image.
Anti alias	Reduces the image scaling effect.

Audio type evidence actions

Actions that can be run on audio evidence are described below:


<i>Icon</i>	<i>Description</i>
	Volume adjustment.
	Start, pause and stop audio.
	Balance left and right speaker volume.

Evidence export data

Data required to export evidence is described below.



IMPORTANT: only evidence that meets the specified criteria will be exported!

<i>Data</i>	<i>Description</i>
From To	Time range for the evidence to be exported.
Relevance	Level of relevance for the evidence to be exported.
Type	Types of evidence to be exported.  NOTE: when no type of evidence is selected, RCS automatically exports all types.
Report	If selected, only evidence with the Report field selected will be exported.

<i>Data</i>	<i>Description</i>						
Report Name	Exported file name. By default, RCS names the file as follows:						
	<table border="1"> <thead> <tr> <th><i>Evidence exported from page</i></th> <th><i>File name</i></th> </tr> </thead> <tbody> <tr> <td>Target</td> <td><target name - agent name> - Evidence Export.tgz</td> </tr> <tr> <td>Agent</td> <td><agent name> - Evidence Export.tgz</td> </tr> </tbody> </table>	<i>Evidence exported from page</i>	<i>File name</i>	Target	<target name - agent name> - Evidence Export.tgz	Agent	<agent name> - Evidence Export.tgz
<i>Evidence exported from page</i>	<i>File name</i>						
Target	<target name - agent name> - Evidence Export.tgz						
Agent	<agent name> - Evidence Export.tgz						

List of types of evidence

Available types of evidence are described below:

<i>Module</i>	<i>File type</i>	<i>Recording...</i>
Accessed files	text	<i>(desktop only) documents or images opened by the target.</i>
Addressbook	text	<i>contacts.</i>
Application	text	<i>applications used.</i>
Calendar	text	<i>calendar.</i>
Call	audio	<i>calls (phone, Skype, MSN).</i>
Camera	image	<i>Webcam images.</i>
Chat	text	<i>chat.</i>
Clipboard	text	<i>information copied to the clipboard.</i>
Device	text	<i>system information.</i>
File	text	<i>files opened by target.</i>
File System	text	<i>hard disk structure that can be explored in the File System function. See "Retrieve evidence from devices (File System)"</i>
Info	text	<i>information provided by the agent and defined in settings.</i>
Keylog	text	<i>keys pressed on the keyboard.</i>
Messages	text	<i>email.</i>
Mic	audio	<i>audio.</i>
Mouse	image	<i>mouse click.</i>
Password	text	<i>password.</i>
Position	image	<i>target's geographic position.</i>

Module	File type	Recording...
Print	image	<i>printed pages.</i>
Screenshots	image	<i>images on the target's screen.</i>
URL	text	<i>visited websites.</i>

Exploring and retrieving evidence from online devices

Presentation

Introduction

Gradual device exploration lets you find and download evidence of interest.

Content

This section includes the following topics:

What you should know about retrieving evidence	42
Retrieve evidence from devices (File System)	42

What you should know about retrieving evidence

Description

The function shows the FileSystem tree structure of the device where the agent is installed (or several devices if exploring a target FileSystem).

When opened, the tree structure will only contain a part of the files and directories in the system; specifically:

- all local roots (i.e.: "c:\", "d:\")
- the Documents folder for the currently logged in user

The **Retrieve** command lets you explicitly read (or re-read) certain folder content.

The **Download** command downloads a file or saves it as **File** type evidence.



NOTE: a folder is read or a file is downloaded after synchronization.

File System components

The structure of each device shows the folders to be explored and those explored:

<i>Example</i>	<i>Description</i>
Agents	Device root.
ProgramData	Folder not yet explored.
Users	Explored folder.

Retrieve evidence from devices (File System)

*To manage the device
File System:*

- **Operations** section, double-click an operation, double-click a target, click **File System**
- **Operations** section, double-click an operation, double-click a target, double-click an agent, click **File System**

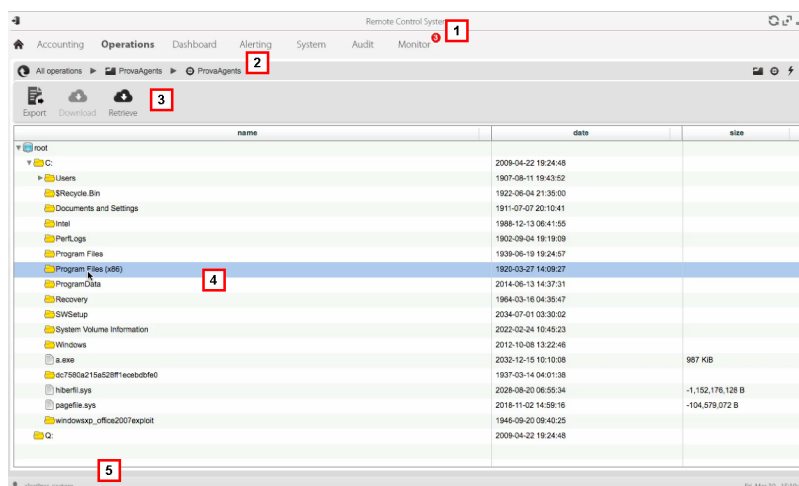
Purpose

This function lets you:

- explore the FileSystem tree structure of the device where the agent is installed (or several devices if exploring a target FileSystem).
- Select the file to be added to the agent's download queue
- export the explored structure (file system)

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 Scroll bar
- 3 Window toolbar. Descriptions are provided below:

Icon Description



Export the complete structure to a .tgz file.



Download: download the selected file to File type evidence.



Retrieve: request the selected folder content be explored.

- 4 Device hard disk structure.
- 5 RCS status bar.

To learn more


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

For more information on exploring the file-system see "[What you should know about retrieving evidence](#)".

Exploring file system content and downloading files

To explore content and download content of interest:

Step Action

- 1** Select a folder.
 - 2**
 - Click **Retrieve** and set the level of depth of sub-folders
 - Click **Save**: the structure of the sub-folders up to the required level will be returned at the next synchronization.
-  Tip: request a few levels at a time, proceed gradually.
- 3** Repeat steps 1-2 on the sub-folders to be explored.
 - 4** After identifying the file of interest, select it and click **Download**: the file will be downloaded as **File** type evidence at the next synchronization.

Targets

Presentation

Introduction

A target is a physical person to be monitored. Several agents can be used, one for each device owned by the target.

Content

This section includes the following topics:

Target page	46
Target page data	47

Target page

To open a target

- **Operations** section, double-click an operation, double-click a target

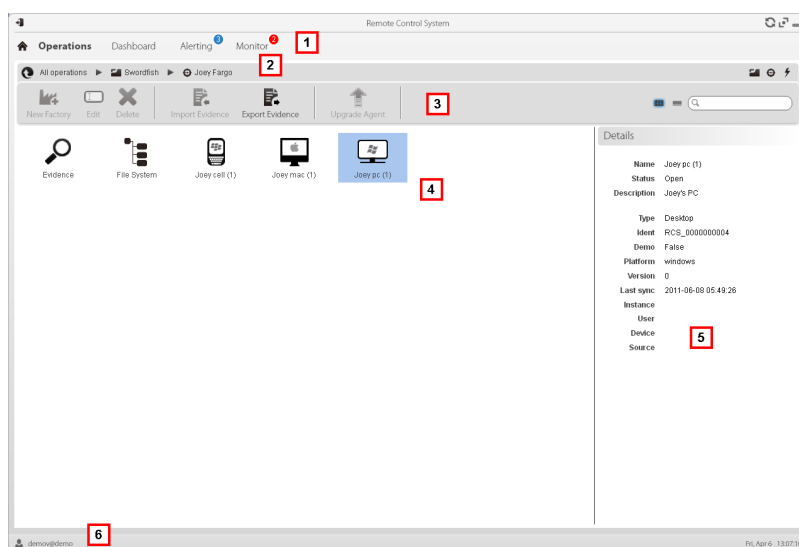
Purpose

This function lets you:

- export target evidence
- open an installed agent
- open agent evidence
- explore the agent device

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 Scroll bar

Area Description

- 3 Window toolbar. Descriptions are provided below:



NOTE: the key displays elements in a list with their data.

Icon Description



Export target evidence in .tgz format.

- 4 Icons/list of created factories and installed agents.



: agent in demo mode.

- 5 Selected factory or agent data.
6 RCS status bar.

To learn more

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

For a description of the data in this window see "[Target page data](#)".

For a description of evidence export data see "[Evidence export data](#)".

Exporting target evidence

To export evidence:

Step Action

- 1 Click **Export Evidence**: the export window opens.
- 2 Click **Ok**: evidence is saved in the specified folder.

Target page data

To view page data:

- **Operations** section, double-click an operation, double-click a target, click **Icon view** or **Table view**

Page elements can be viewed as icons or a table.

Icon view

Icons are described below:

Data *Description*



Desktop agent types, in Open status, for operating systems:

- OS X
- Windows



Mobile agent types, in Open status, for operating systems:

- Android,
- BlackBerry,
- iOS,
- Symbian
- Windows Mobile




NOTE: icons are light grey for **CLOSED** agents. This is the icon for a mobile agent for Android in Closed status: .

Table view

Data is described below:

Data *Description*

Name Factory or agent name.

Description Factory or agent description

Status **Open:** the agent is still active on the device and can continue to send data.
Closed: the agent is no longer active.



NOTE: a closed agent cannot be reopened. Data in RCS can still be viewed.

Type Desktop or mobile type.

Platform (agent only) Operating system on which the agent is installed.

Version (agent only) Agent version. A new version is created when a new configuration is created.

<i>Data</i>	<i>Description</i>
Last sync	(agent only) Date and time of the last agent synchronization.
Ident	(agent only) Univocal agent identification.
Instance	(agent only) Univocal identification of the device where the agent is installed.

Agents

Presentation

Introduction

Agents acquire data from the device on which they are installed and send it to the RCS Collectors. Their configuration and software can be updated and they can transfer files unnoticed to the target.

Content

This section includes the following topics:

Agent page	51
Agent event log data	52

Agent page

To manage agents:

- **Operations** section, double-click an operation, double-click a target, double-click an agent

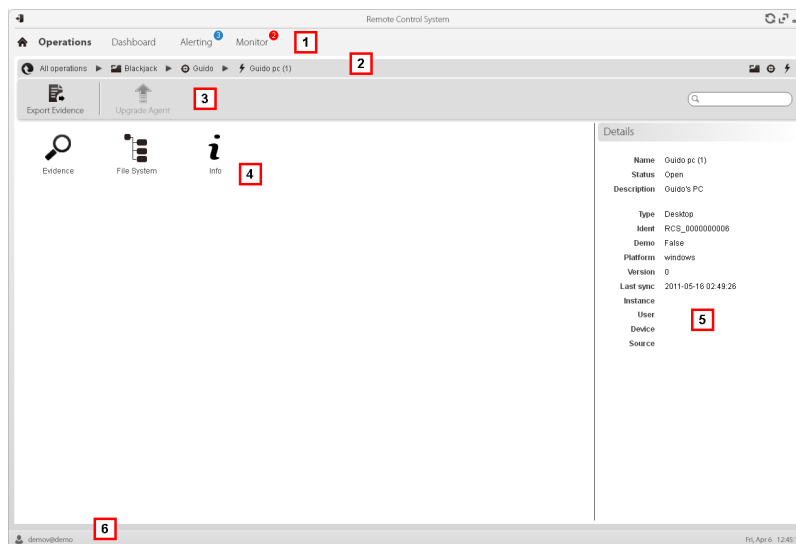
Purpose

This function lets you:

- check agent activities via the event log.
- export agent evidence
- view evidence collected by the agent
- explore the file system and transfer files from the device where the agent is installed

What the function looks like

This is what the page looks like:






Area Description

- 1 RCS menu.
- 2 Scroll bar
- 3 Window toolbar.

Area Description

- 4 Possible actions on the agent. Descriptions are provided below:

Icon Description

-  Show the list of evidence collected by the agent. See "[Evidence analysis \(Evidence\)](#)".
-  Show the device file system. See "[Retrieve evidence from devices \(File System\)](#)".
-  Show the agent event log. See "[Agent event log data](#)".

- 5 Agent details.

- 6 RCS status bar.

To learn more

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

Agent event log data

Descriptions are provided below:

Field Description

- Acquired** Date-time of the event acquired on the device.
It can be filtered. **Last 24 hours** is set by default.
- Received** Date-time of the event logged in RCS.
It can be filtered. **Last 24 hours** is set by default.
- Content** Status information sent by the agent.

]HackingTeam[

RCS 8.0 Analyst's Guide
Analyst's Guide 1.0 APR-2012
© COPYRIGHT 2012
info@hackingteam.com

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