]HackingTeam[

RCS 9
The hacking suite for governmental interception

Analyst's Guide

Information ownership

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

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.

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 cus-

tomer digital subscriber line (DSL) interfaces to a high-speed digital com-
munications 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. In distributed architecture, it includes the Collector and Network
Controller.

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 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.

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

List of release notes and updates to this online help.

Release date	Code	Software version.	Description
19 February 2014	Analyst's Guide 1.5 FEB-2014	9.2	Added group management and new filters in Intelligence, see *"Intelligence" on page 52* . Added possibility of transforming a Person entity into a Target entity, *see "What you should know about entities" on page 53* . Added **Money** type evidence *see "List of types of evidence" on page 46* . Added new type of evidence export to a connector, *see "Evidence export data" on page 45*
30 September 2013	Analyst's Guide 1.4 SEP - 2013	9	Updated documentation in the Intelligence section, *see "Intelligence" on page 52* . Updated the Analyst's procedures, *see "Analyst's procedures" on page 15* . Updated alert rule documentation, *see "Alert" on page 90* . Updated documentation due to improvements to the user interface. Improved the contents.
8 July 2013	Analyst's Guide -	8.4	No documentation update.
15 March 2013	Analyst's Guide 1.3 MAR-2013	8.3	Added the Intelligence section *see "Intelligence" on page 52* . Added content export from all file type evidence formats. *See "Evidence details" on page 42* A user license can be purchased to view evidence content in the interface language.*See "Evidence analysis (Evidence)" on page 36* and *see "Evidence details" on page 42* .

Release date	Code	Software version.	Description
15 October 2012	Analyst's Guide 1.2 OCT-2012	8.2	Added filter settings savings on evidence and simplified the **Info** filter on evidence. Added delete evidence.*See "Evidence analysis (Evidence)" on page 36* . If installed, the texts extracted from a screenshot type evidence can be viewed. *See "Evidence details" on page 42* .
30 June 2012	Analyst's Guide 1.1 JUN 2012	8.1	Different folder retrieve from disk. *See "Retrieve evidence from devices (File System)" on page 49* .
16 April 2012	Analyst's Guide 1.0 APR-2012	8.0	First publication

Supplied documentation

The following manuals are supplied with RCS software:

Manual	Addressees	Code	Distribution format
System Administrator's Guide	System administrator	*System Administrator's Guide 1.5 FEB-2014*	PDF
Administrator's Guide	Administrators	*Administrator's Guide 1.5 FEB-2014*	PDF
Technician's Guide	Technicians	*Technician's Guide 1.6 FEB-2014*	PDF
Analyst's Guide (this manual)	Analysts	*Analyst's Guide 1.5 FEB-2014*	PDF

Print concepts for notes

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

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

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

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

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

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

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

Print concepts for format

A key to print concepts is provided below:

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

Product and guide addressees

Following is the list of professionals that interact with RCS.

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

Software author identification data

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

2

RCS (Remote Control System)

Presentation

Introduction

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

Content

This section includes the following topics:

Differences between RCS 8.0 and RCS 7.6 versions

Differences with the RCS 7.6 version are described below

Glossary

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

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
- organize device and other evidence in your possession to formulate solutions for the investigation

Analyst enabled functions

To complete his/her activities, the Analyst has access to the following functions:
- **Operation**
- **Intelligence**
- **Dashboard**
- **Alerting**

Content

This section includes the following topics:

Starting the RCS Console

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

What the login page looks like

This is what the login page looks like:
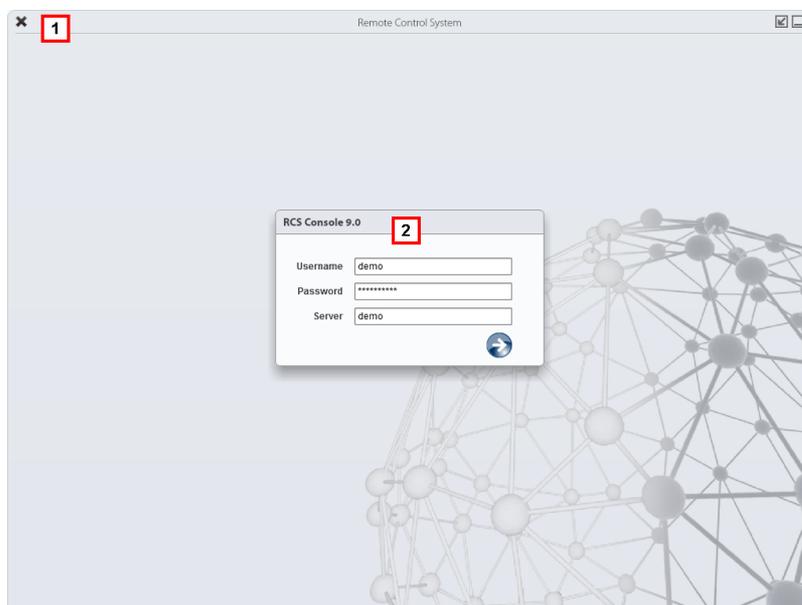
Area	Description
1	Title bar with command buttons: ✖ Close RCS Console. ↗ Expand window button. ▭ Shrink window button.
2	Login dialog window.

Open RCS Console

To open RCS Console functions:

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

Step	Action

3

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

Homepage description

To view the homepage:

- click 🏠

Introduction

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

What it looks like

This is what the homepage looks like, with recently opened items saved. For details on shared elements and actions:
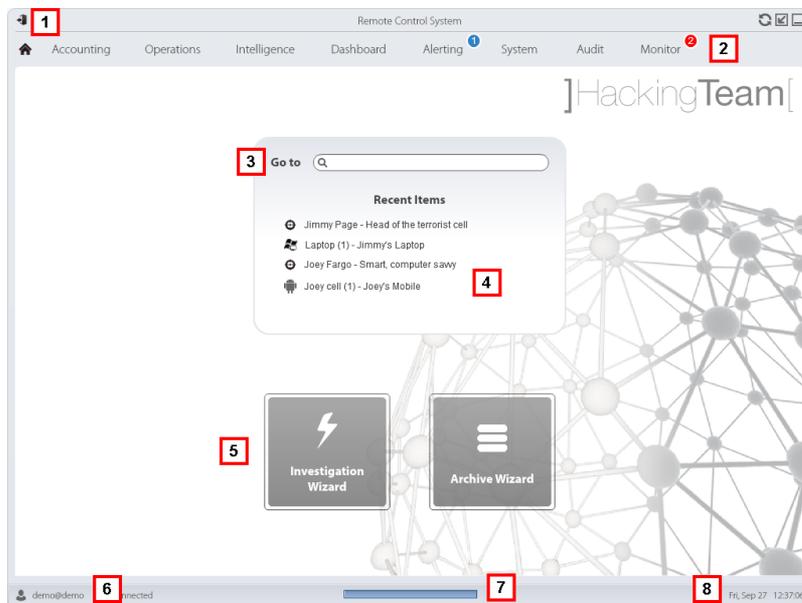
Area	Description
1	Title bar with command buttons.
2	RCS menu with functions enabled for the user.
3	Search box to search operations, targets, agents and entities, by name or description.

Area	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.

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:
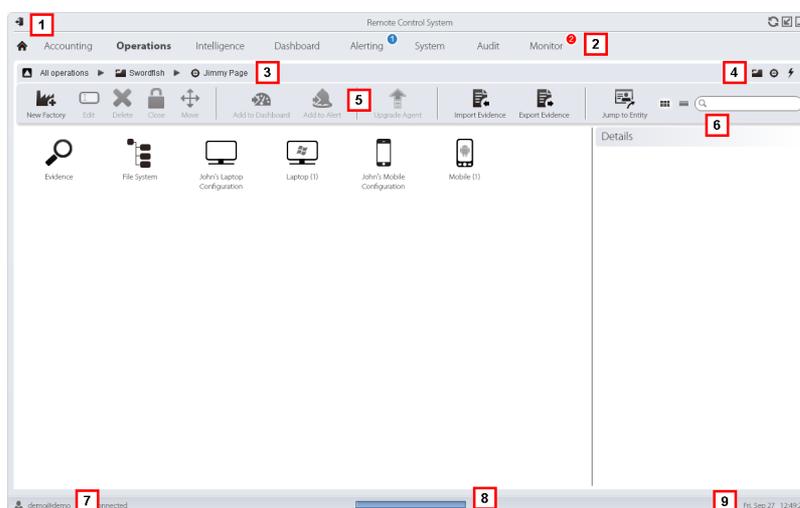
Area	Description

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 (Operations section).
⊕	Show the target page.
▥	Show the factory page.
⚡	Show the agent page.
◰	Show the operation page (Intelligence section).
★	Show the entity 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.
★	Show all entities.

5   Window toolbar.

Area	Description

6 Search buttons and box:

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

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.

Actions always available on the interface

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 and which can be converted.
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.
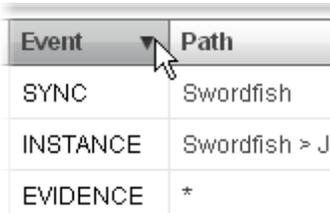
Filter a text	Enter part of the text you are searching for: only elements that contain the entered text appear.
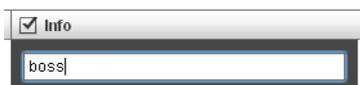
The example shows elements with descriptions like:

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

Filter based on an option	Select an option: the elements that match the selected option appear.

Action	Description
Filter based on several options	Select one or more options: the elements that match all selected options appear.
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:

Step	Action
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)" on page 49*
2	In the **Dashboard** section, add the operation, targets and agents to be monitored to the dashboard. *See "Monitoring evidence (Dashboard)" on page 87*
3	In the **Alerting** section, set rules to be alerted when evidence of special interest arrives and to tag evidence according to relevance. *See "Alert" on page 90* .

Analyzing, selecting and exporting evidence

To analyze, select and export evidence:

Step	Action
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)*" on page 36 .
2	For evidence of special interest, move on to detailed analysis. See "*Evidence details*" on page 42
3	In the **Evidence** section, export useful evidence. See "*Evidence analysis (Evidence)*" on page 36 .
4	In the **File System** section, export the hard disk structure See "*Retrieve evidence from devices (File System)*" on page 49

To process information obtained on people and places involved in the investigation

To process information obtained on people and places involved in the investigation:

Step	Action
1	In the **Intelligence** section, view and manage entities in an operation. See "*Entity management: icon and table views*" on page 62 , "*Entity management: link view*" on page 64 , "*Entity management: Position view*" on page 69 .
2	Viewing or editing entity details.*See "Target entity details*" on page 73 , "*Person entity details*" on page 78 "*Position entity details*" on page 80 "*Virtual entity details*" on page 82 See "*Evidence details*" on page 42
3	In the **Alerting** section, build rules to be alerted when the system automatically creates new entities and new links and to tag links according to their relevance. See "*Alerting* " on page 92

Operation and target

Presentation

Introduction

Managing operations sets the targets to be tapped.

Content

This section includes the following topics:

What you should know about operations

What is an operation

An operation is an investigation to be conducted. An operation contains one or more targets meaning the physical individuals to be tapped. The Technician assigns one or more agents, *desktop* or *mobile,* to the target. Thus the agent can be installed on a computer or mobile phone.

What you should know about targets

What is a target

A target is the physical person to be investigated. The Technician assigns one or more agents, desktop or mobile, to the target. Thus the agent can be installed on a computer or mobile phone.

Operation management

To manage operations:	● **Operations** section

Purpose

This function lets you:

- add the operation to the elements to be monitored

NOTE: the function is only enabled if the user has **Operation management** authorization.
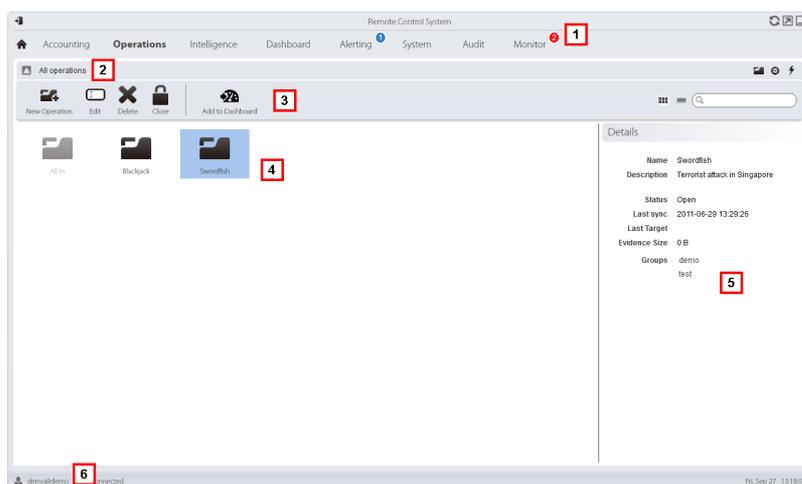
What the function looks like

This is what the page looks like:

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

Icon	Description
	Add the operation to the dashboard.

Area	Description
4	List of created operations: Open operation. If targets were set and agents correctly installed, collected evidence is received. Closed operation. All targets are closed and agents uninstalled. All its targets and evidence can still be viewed.
5	Selected operation data.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For a description of the data in this window *see "Operation data" on the facing page* .

For more information on operations *see "What you should know about operations" on the previous page* .

Viewing operation targets

To view operation targets:

Step	Action
1	Double-click an operation: the target management page opens. *See "Operation page" below*

Operation data

Selected operation data is described below:

Data	Description
Name	Operation name.
Description	User's description
Contact	Descriptive field used to define, for example, the name of a contact person (Judge, Attorney, etc.).
Status	Operation status and close command: **OPEN**: the operation is open. If targets were set and agents correctly installed, the RCS receives the collected evidence. **CLOSED**: the operation is closed and can not be re-opened. Agents no longer send data but evidence already received can still be viewed.
Groups	Groups that can see the operation.

Operation page

To view an operation:	● **Operation** section, double-click an operation

Purpose

This function lets you:

- add the target to the elements to be monitored

What the function looks like
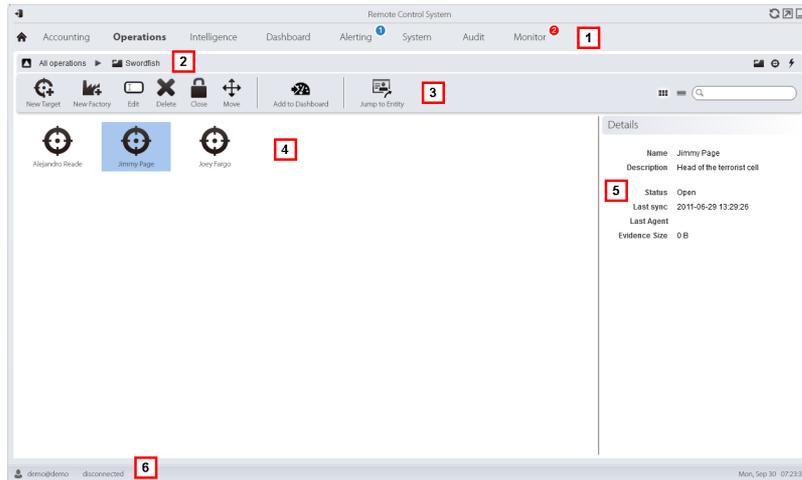
This is what the page looks like:

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

Icon	Function
	Add the target to the dashboard.
	Open the target entity page in intelligence.

Area	Description
4	Target list:

Open target

Closed target

Area	Description
5	Selected target data.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For more information on operations *see "What you should know about operations" on page 18* .
For a description of the data in this window *see "Operation page data" below* .

Operation page data

Selected target data is described below:

Data	*Description*
Name	Target name.
Description	User's description
Status	Defines the target's status:

⊕ Open. If the Technician correctly installs agents, RCS receives the collected evidence.

⊕ Closed, it can no longer be opened.

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

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
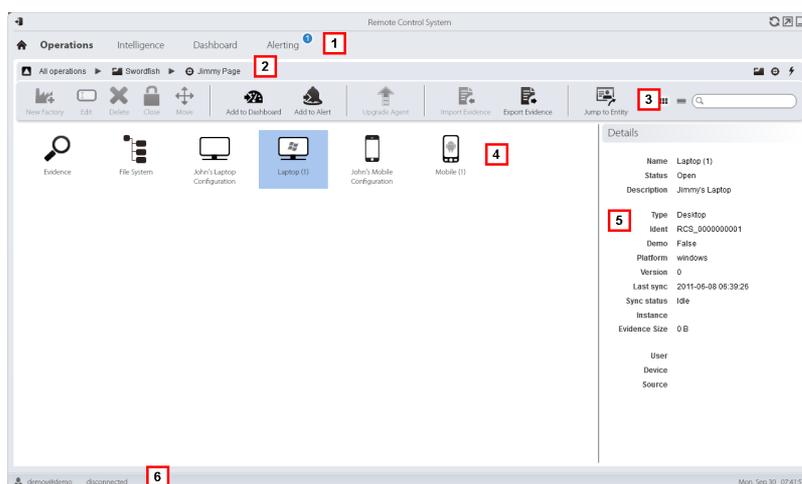
This is what the page looks like:

Area   Description

Area	Description
1	RCS menu.
2	Scroll bar

Area	*Description*
3	Window toolbar. Descriptions are provided below:

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

Icon	*Function*
🎯	Adding the agent to the dashboard.
🔔	Adding the agent to alerts: an alert is generated at each synchronization.
📑	Export target evidence

> ℹ️ NOTE: the function is only enabled if the user has **Evidence export** authorization.

🖼️	Open the target entity page in intelligence.

4	Icons/list of created factories and installed agents.

🖥️ : agent in demo mode.

🖥️ : scout agent awaiting verification.

🖥️ : soldier agent installed.

🖥️ : elite agent installed.

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

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For a description of the data in this window *see "Target page data" on the next page* .

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
	Example of scout agent installed on a desktop Windows device, in Open status.
	Example of soldier agent installed on a desktop Windows device, in Open status.
	Example of elite agent installed on a desktop Windows device, in Open status.
	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.

Data	Description
Level	(agent only) Agent level: scout, soldier, elite.
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.
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

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.
- 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:
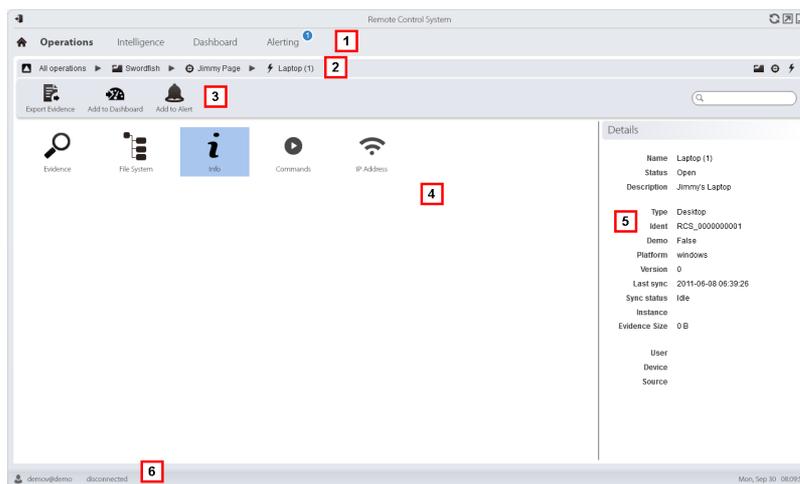
Area	Description
1	RCS menu.
2	Scroll bar

Area	Description
3	Window toolbar.

Icon	Description
	Export agent evidence.
	NOTE: the function is only enabled if the user has **Evidence export** authorization.
	Adding the agent to the dashboard.
	Adding the agent to alerts: an alert is generated at each synchronization.

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)" on page 36* .
	Show the device file system. *See "Retrieve evidence from devices (File System)" on page 49* .
	Show the agent event log (info). *See "Agent event log data" below*
	Show the results of commands run on the device using **Execute** actions. *See "Command page" on the next page* .
	Show the agent synchronization log. *See "Agent synchronization log data" on page 32* .

Area	Description
5	Agent details.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

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.

Command page

| *To manage command results:*	•	**Operations** section, double-click an operation, double-click a target, double-click an agent, double-click **Commands**

Purpose

This function lets you:

- check the results of commands run with the **Execute** action set on the agent
- check executable file results run during file transfer to/from the agent

What the function looks like
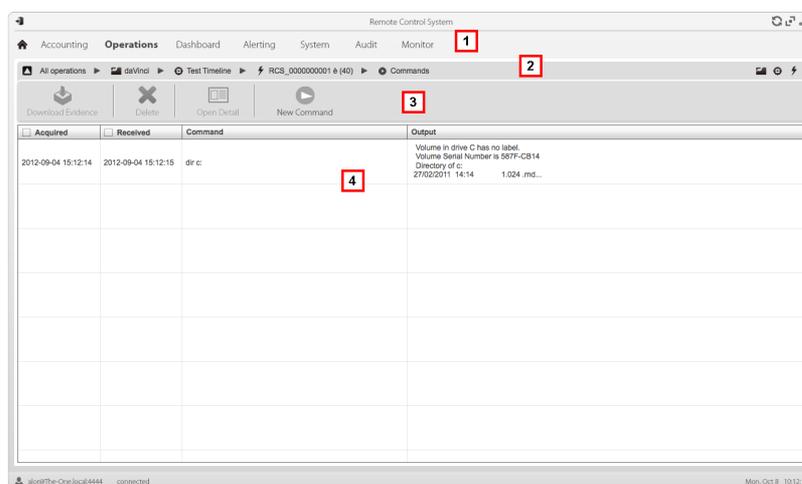
This is what the page looks like:

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

Icon	Description
	Export the selected command to a .txt file.
	Delete the selected commands.
	NOTE: the function requires a user license and is only enabled if the user has **Evidence deletion** authorization.
	Show selected command details.

5	Command list based on set filters.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

Agent synchronization log data

Descriptions are provided below:

Field	Description
Acquired	Synchronization date-time. It can be filtered. **Last 24 hours** is set by default.
IP	IP address used for synchronization.
Address	Site where connection was established.

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

Analysis process

The analysis process is described below:

Phase	Description
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.

Evidence accumulated in the device.

Evidence is sent by the agent to the Collector in order of creation. If a device rarely synchronizes or has a limited bandwidth, evidence probably accumulates on the device and it will take a long time before the most recent data is received.

The same may happen if large-sized evidence is in queue: the most recent evidence can only be sent after having sent this evidence.

For this reason, we suggest you delete older evidence and/or evidence that exceeds a certain size. Evidence is deleted at the next synchronization.

See "Agent page" on page 29 .

Filtering evidence

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

See "Shared interface elements and actions" on page 11

> **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.**

The selected filters can be saved with a short description to be used later.

> **IMPORTANT: if private filters are set, they cannot be used by other users.**

Translating evidence

The RCS Translate module is available upon special license to translate evidence. In fact, it communicates with a third party translation software that returns text translated into the interface language.

RCS Translate translates the following types of evidence:

- clipboard
- chat
- file
- keylog
- message
- screenshot

The translation is displayed in the page with the evidence list and the single piece of evidence detail page.

Delete evidence

This function deletes one or more pieces of evidence no longer deemed useful. This function depends on the type of license installed.

Filters can be used to select the evidence to be deleted (similar to selecting evidence to be exported).

IMPORTANT: the filter only appears when the Delete **and ALT keys are pressed simultaneously.**

.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:

Step	Action
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: • 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
- translate evidence content into the interface language (optional)
- 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:
4	Evidence list based on set filters.
5	RCS status bar.

Window toolbar

Icon	Description
	Show selected evidence details. *See "Evidence details" on page 42*
	Show the total quantities by evidence type.
	Export selected evidence to a .tgz file.
	NOTE: the function is only enabled if the user has **Evidence export** authorization.
	Delete selected evidence.
	Tip: to delete a set of evidence according to certain criteria (i.e.: data range) simultaneously press ALT and this button: a window appears where you can set evidence deletion criteria. For field descriptions *see "Evidence export data" on page 45* , fields are similar.
	NOTE: the function requires a user license and is only enabled if the user has **Evidence deletion** authorization.
	Apply a level of relevance to the selected evidence.
	Apply a bookmark to the selected evidence.
	Edit selected evidence notes.
	Show evidence ID codes.
	Saves currently selected filters or loads previously saved filter settings.

Icon	Description
	Clear all set filters.
	View content in the interface language.
	NOTE: this function requires a user license.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .
For a description of the data in this window *see "Evidence data" on page 40*
For a description of exportable data*see "Evidence export data" on page 45* .
For more information on evidence*see "What you should know about evidence" on page 34*
To view a list of evidence types*see "List of types of evidence" on page 46*

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.
2	• Drag **Relevance** to the required position or • 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.

Step	Action
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" on page 42*

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" on page 45* .
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:

Data	*Description*
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.

Data	Description
Relevance	Level of evidence relevance, automatically assigned by alert rules or manually assigned in this list. The level of relevance is set using: • the **Relevance** command in the menu • short-cut keys

Short-cut key list.

Icon	Short-cut keys	Description
▮▮▮▮	ALT+4	*Maximum relevance*
▮▮▮	ALT+3	*Intermediate relevance*
▮▮	ALT+2	*Normal relevance*
▮	ALT+1	*Minimum relevance*
-	ALT+0	*No relevance*

Data	Description
Type	Type of evidence to be selected. *See "List of types of evidence" on page 46*
Info	Evidence information: text, images, video, audio and so on. Each piece of information is accompanied by various fields (i.e.: field **content**, **program**). It can be filtered by simply indicating the full search word or full field name and search word. For example: • "boss" searches for the word "boss" or "Boss" in all fields • while "**content**:boss" searches for the word "boss" or "Boss" in **content** fields only.
Notes	Notes entered by the Analyst using: • **Edit Note** menu • short-cut key ALT+N
Report	Bookmark, that indicates that evidence may be included/excluded during export. The bookmark is set using: • **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.

NOTE: the function is only enabled if the user has **Evidence editing** authorization.

What the function looks like

This is what audio evidence details looks like:
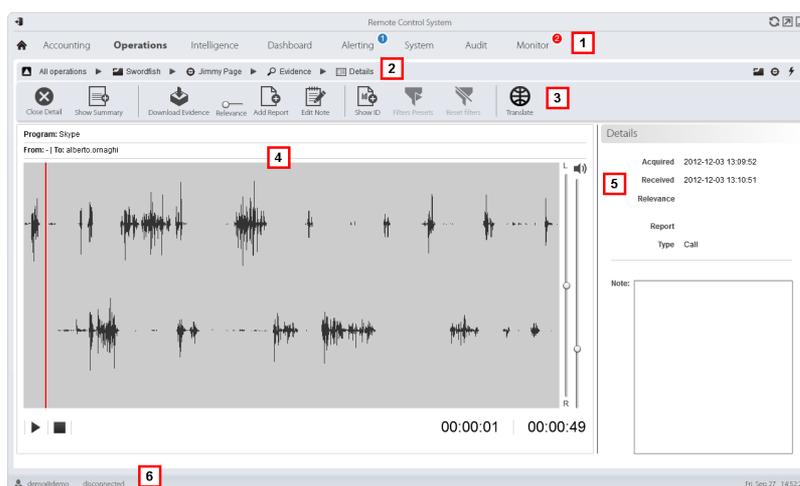
Area	Description
1	RCS menu.
2	Scroll bar

Area	Description
3	Evidence action keys.

Icon	Description
	Closes the details and returns to the evidence list.*See "Evidence analysis (Evidence)" on page 36* .
	Show the total quantities by evidence type.
	Exports evidence to a .tgz file.
	Deletes evidence.
	NOTE: the function requires a user license and is only enabled if the user has **Evidence deletion** authorization.
	Applies a level of relevance.
	Applies a bookmark.
	Edits the notes.
	Displays the ID code.
	Saves currently selected filters or loads previously saved filter settings.
	Clear all set filters.
	View content in the interface language.
	NOTE: this function requires a user license.

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" on page 11* .

For more information on evidence *see "What you should know about evidence" on page 34* .
For a description of the data in this window *see "Evidence data" on page 40* .

Image type evidence actions

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

Icon	*Description*
▬	(screenshot and file type evidence only) Shows the extracted text.
	ℹ NOTE: if the "OCR unavailable" message appears, this means that the document has not yet been converted and indexed. If the button is not displayed, this means that this function was not installed. Contact your system administrator.
👁	(screenshot type evidence only) Return to image view.
🖵	Full screen view.
1:1	Actual image size view.
🔍 🔍	Expand and shrink image.
↺ ↻	Rotate image.
Anti alias	Reduces the image scaling effect.
👤	The image becomes the intelligence entity default image (if the intelligence module is installed).

Audio type evidence actions

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

Icon	*Description*
🔊	Volume adjustment.
❚❚ ■	Start, pause and stop audio.

Icon	Description
L ○ R	Volume balance on local (target) and remote source (speaker).

Evidence export data

Export data

Data required to export evidence is described below.

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

Data	Description
From **To**	Time range for the evidence to be exported.
Acquisition	It considers the date as the evidence acquisition date on the target device.
Receipt	It considers the date as the evidence receipt date.
Relevance	Level of relevance for the evidence to be exported.
Type	Types of evidence to be exported. ℹ 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. Notes can be included or excluded from the export.
Report name	Exported file name. By default, RCS names the file as follows: | *Evidence exported from page*	*File name*
---	---
Target	*target name - agent name* - Evidence Export.tgz
Agent	*agent name* - Evidence Export.tgz	
Export file	Starts file export.
Export to connector	Starts evidence export to the connector.

Export commands

Export evidence commands are described below.

Command	Description
Export to file	Starts file export.
Export to connector	Starts evidence export to the connector.
	NOTE: the function is only enabled if the user has **Connector management** authorization.

List of types of evidence

Available types of evidence are described below:

Module	File type	Recording...
Accessed files	text	*(desktop only) documents or images opened by the target.*
Addressbook	text	*contacts.*
Application	text	*applications used.*
Calendar	text	*calendar.*
Call	audio	*calls (i.e..: GSM and VoIP).*
Camera	image	*Webcam images.*
Chat	text	*chat.*
Clipboard	text	*information copied to the clipboard.*
Device	text	*system information.*
File	text	*files opened by target.*
File System	text	*hard disk structure that can be explored in the File System function. See "Retrieve evidence from devices (File System)" on page 49*
Info	text	*information provided by the agent and defined in settings.*
Keylog	text	*keys pressed on the keyboard.*
Messages	text	*e-mail.*
Money	text	*Information on the cryptocurrency digital wallet (i.e.: Bitcoin).*
Mic	audio	*audio.*
Mouse	image	*mouse click.*

Module	File type	Recording...
Password	text	*password.*
Position	image	*target's geographic position.*
Print	image	*printed pages.*
Screenshots	image	*images on the target's screen.*
URL	text	*visited websites.*

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

Description

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

The FileSystem tree structure can be gradually explored, first reading the first level structure (**Retrieve default** command) and then exploring folders, followed by reading or re-reading the selected folder (**Retrieve subtree** command).

Once the concerned file is found, it can be downloaded and saved as file evidence (**Download** command)

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:

Example	Description
▼ 🖥 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)

NOTE: the function is only enabled if the user had **File system browsing on agent** authorization.
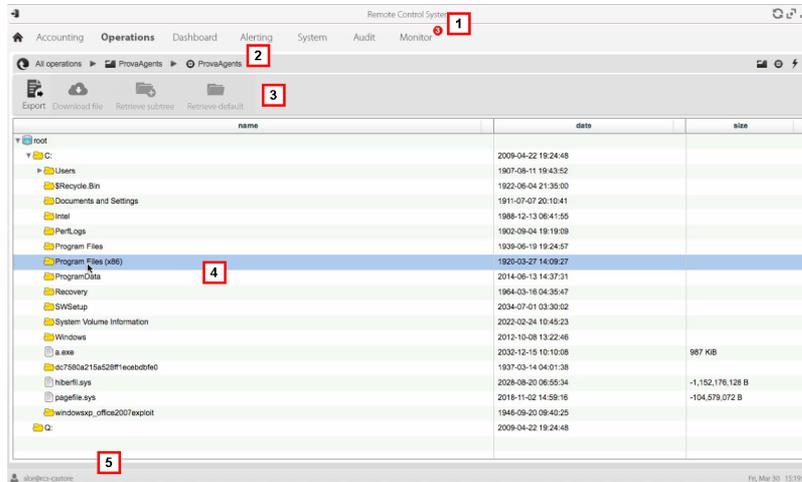
What the function looks like

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 the selected file to **File** type evidence.
	Explore the selected folder content.
	Request the first level disk structure.
	View the list of currently suspended Filesystem requests awaiting next synchronization.

Area	Description
4	Device hard disk structure.
5	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

For more information on exploring the file-system*see "What you should know about retrieving evidence" on page 49*

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.

Intelligence

Presentation

Introduction

The section lets you represent interactions between targets at a high level, matching evidence received by agents with other information already possessed.

Content

This section includes the following topics:

What you should know about intelligence

Presentation

Introduction

The Analyst processes the investigation information in his/her possession in the Intelligence section.

The people under investigation, other people and places involved in the investigation are represented by *entities*. The relations between people and between people and places are represented as *links* between entities.

The system creates new entities and new links between entities based on the evidence received from target devices. The analyst interprets and organizes this information, adding, editing or deleting entities or links according to the evolution of the investigation.

Intelligence section license

Intelligence functions are sold under license.

Without a user license the analyst can only use the Intelligence section to view and add details on targets in the operation; the system does not process information based on collected evidence. The only entities included are the Targets and they can only be viewed as icons or in tables, *see "Entity management: icon and table views" on page 62* .

To learn more

See "*What you should know about entities*" *below*

See "*What you should know about links*" *on page 55*

See "*What you should know about Group entities*" *on page 57*

See "*What you should know about how intelligence works*" *on page 57* .

What you should know about entities

Introduction

The entity represents a person or place involved in an investigation.

Each entity is defined by detailed information that allow the system to identify relations between entities.

People involved in the investigation: Target entities and Person entities

The system defines two types of entities to represent the people involved in an investigation:

- 🔵 :Target type, for the people being tapped

- 🔵 : Person type, for the people not being tapped

The places involved in an investigation: Position entity and Virtual entity

The system defines two types of entities to represent the places involved in an investigation:

- 📍 : Position type, physical sites

- 🖥 : Virtual type, virtual sites like web pages

Managing entities

The analyst manages entities so they represent the evolution of the investigation, thus:

- it adds entities to monitor other people and places deemed of interest
- it adds details to the entities to provide new data to the system to identify relations between entities
- it eliminates entities when the people or places are deemed insignificant to the investigation
- it forms the Group entity for easier information display and analysis,*see "What you should know about Group entities" on page 57*

Target entity

The Target entity is automatically created when the target is created in the Operations section. The name and description are the same ones assigned in the Operations section.

> NOTE: Target entities cannot be eliminated from the Intelligence section. To eliminate them, targets must be eliminated from the Operations section.

> NOTE: the Target name and description can be changed without any impact on the Operations section.

The system adds Target entity details with information gathered from evidence (i.e.: photos, most frequently contacted people). The analyst can add other information in his/her possession.*See "Target entity details" on page 73*

Person entity

The Person entity can be manually created by the analyst or automatically by the system.
The Person entity is defined by IDs s/he uses to communicate, by phone or internet (i.e.: phone number, Skype contact).

NOTE: the more information in the entity detail sheet, the higher the probability the system identifies links between that entity and other entities.

If a Person entity becomes the object of tapping, it can be transformed/changed into a Target entity. This way, the system creates a new target in the corresponding Operation.

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

*See "*Person entity details*" on page 78*

Position entity

The Position entity can be manually created by the analyst or automatically by the system.
The Position entity is defined by the geographic coordinates (latitude and longitude) or address of the site that it represents and a range of precision.

NOTE: the range of precision must be suited to the type of place (i.e.: 50-100m for a building, much more for a park).

*See "*Position entity details*" on page 80*

Virtual entity

The Virtual entity must be manually created by the Analyst.
The Virtual entity is defined by one or more URL addresses for the web page they represent.
*See "*Virtual entity details*" on page 82*

What you should know about links

Introduction

A link is a relationship between entities. There can be only one link between two entities.
There are three types of links:

- ············ Know
- ⸺ Peer
- ---- Identity

Know links

Know links represent a *know* type relationship. Two entities have a Know link when at least one of the two has the other in his/her address book.
A Know link can be directional or bi-directional.

Peer links

Peer links indicate that there was a *contact* between the two entities.

Two entities that represent people have a Peer link when there was a direct communication between the two entities (i.e.: phone call, chat). The relationship can be directional and bi-directional.

An entity that represents a person and one that represents a place have a Peer link when the person was in that place (physical or on the web). The relationship is only directional: from the entity that represents a person to the one that represents a place.

Peer links represent a stronger relationship than know links, thus they replace any Know link between the entities.

Managing Peer and Know links

The analyst manages links so they represent the evolution of the investigation, thus:

- adds or edits links between two entities when in possession of information that prove a relationship between the two
- assigns a level of relevance to links to represent the relationship's relevance in the investigation
- deletes links when in possession of information that prove the lack of relations or that the relationship is insignificant to the investigation.

Identity links

Identity links represent a suggestion of an *identity* relationship between two entities that represent people. This type of link is automatically created by the system when the two entities share at least one identification (i.e.: phone number).

Identity links do not have directions.

Managing Identity links

The analyst must decide the reason for identity links and how to act accordingly:

- if they are the same person, the two entities must be merged;
- if they are two different people that used the same identification, the shared identification must be deleted from one of the entities and the link eliminated.

Link time value

Links are the result of an automatic or manual process completed at a certain time. However, the time the link is created, meaning when the first relationship was formed between entities, is only logged for Peer links automatically created by the system.

This way, an analysis period can be selected to see when certain relationships were created.

For the other links, once they are created (automatically or manually) they are considered as created at the beginning by the system.

## What you should know about Group entities

Introduction

The Group entity groups other entities and can be automatically created by the system or manually by the Analyst.

The Group has two display levels:

- expanded, to view all the entities it represents and their links
- reduced, to occupy less space and facilitate the display of other entities. Connections to and from the group are displayed but not links inside the group.

Example of expanded Group **[1]** and reduced Group **[2].**
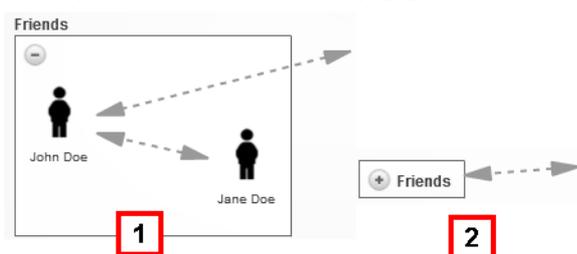
Groups are only displayed in the link view, *see "Entity management: link view" on page 64* .

Group entities created by the system

The system automatically creates a Group only when it finds links between Person or Target entities belonging to two different operations. It creates a Group in both operations, assigning each the name of the other operation.

The created Group represents the Person or Target type entity in the operation that are linked to the entities in the operation being analyzed.

The Group can only be expanded if you have permission to manage the operation in which the entities it represents belong. Otherwise, the only display status is the reduced one.

Group entity created manually.

The Analyst can group any type of entity in a Group, but an entity may only belong to one Group.

Creating a Group can help with data processing. For example, you can decide to create a Group entity called "Rossi family" with entities that represent the people and places associated with the Rossi family.

What you should know about how intelligence works

Introduction

Intelligence supports the analyst in processing the investigation evidence and data.

Intelligence process

Phase	Description
1	The system creates an operation in the Intelligence section when an operation is opened in the Operations section.
2	The system creates a Target entity when a target is created in the Operations section.
3	The system, based on the evidence collected from target devices, creates links with target entities and creates new entities and links. NOTE: the system processes information from targets in all open operations.
4	The analyst adds entities to represent people, places and web pages deemed of interest for the investigation and adds details.
5	The system continues to update entities and their links based on new evidence and information added by the analyst.
6	The analyst interprets and manages entities and their links to propose solutions for the investigation. NOTE: the analyst can set an alert rule to be alerted when the system creates an entity or link.*See "Alert" on page 90* .

Automatic Know link creation criteria

If the evidence indicates that...	The system creates...
targets John and Paul have identification 003214567 in their address book	• a Person entity with identification 003214567 • a directional Know link from John to the Person entity • a directional Know link from John to the Person entity
target John has identification 003214567 for Target/Person entity Paul in his address book	a directional Know link from John to Paul

Automatic Peer link creation criteria with Target and Person entities

If the evidence indicates that...	The system creates...

targets John and Paul communicated with identification 003214567	- a Person entity with identification 003214567 - a directional Peer link from John to the Person entity - a directional Peer link from Paul to the Person entity
target John communicated with Target/Person entity Paul	a directional Peer link from John to Paul
target John often communicates with identification 003214567	- a Person entity with identification 003214567 - a directional Peer link from John to the Person entity

Automatic Peer link creation criteria with Position entities

If the evidence indicates that...	The system creates...
targets John and Paul were in Times Square at the same time	- a Position entity with the geographic coordinates for Times Square - a directional Peer link from John to the Position entity - a directional Peer link from Paul to the Position entity
target John was in the place associated with John's office Position entity	a direction Peer link from John to John's office entity
target John is often in Times Square	- a Position entity with the geographic coordinates for Times Square - a directional Peer link from John to the Position entity

NOTE: for the system, a target visited a place if they were there for at least 15 minutes. Two targets visited the same place at the same time if they were there at the same time for at least 15 minutes.

Automatic Peer link creation criteria with Virtual entities

If the evidence indicates that...	The system creates...
target John visited URL www.secretplaces.com linked to the Virtual entity Secret places website	a direction Peer link from John to Secret places website

Automatic Identity link creation criteria with Target and Person entities

If the system detects that...	The system creates...

Target/Person entity John has 003214567 in his identification data and Target/Person entity Paul has 003214567 in his

Target/Person entity   an Identity link between John and Paul

Automatic link creation criteria between Target/Person entities in different operations

If the system detects that...

conditions are met to create a link between the Drug traffic John Target/Person entity and Weapon traffic Paul Target/Person entity

NOTE: link creation criteria between operations are the same as those for a link inside the operation.

The system creates...

in the Drug traffic operation,
- the Weapons traffic Group entity
- a link between John and the Weapons traffic Group

in the Weapons traffic operation
- the Drug traffic Group entity
- a link between Paul and the Drug traffic Group

NOTE: if the Group entity was created due to a previous relationship, only the link is created.

NOTE: the type and direction of the created link are determined by the same link rules between entities in the same operation.

Intelligence operation management

To manage intelligence operations:

- **Intelligence** section

Purpose
This function lets you:
- view intelligence operations

What the function looks like
This is what the page looks like:
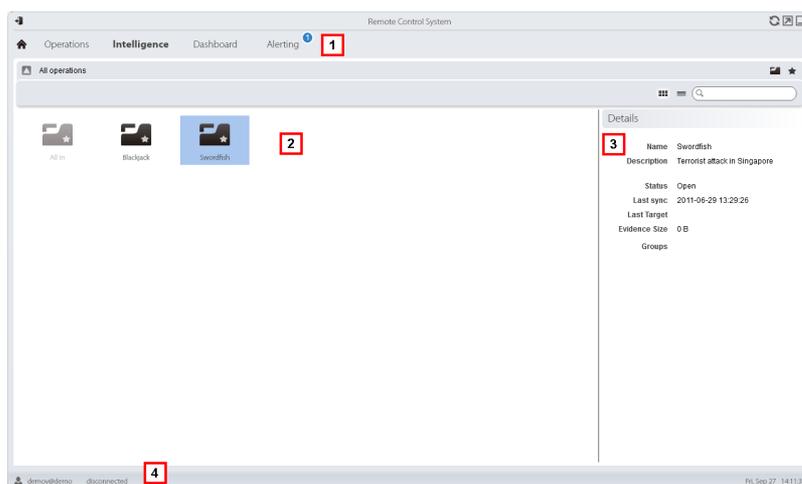
Area	Description
1	RCS menu.
2	Operation list:
	Open operation.
	All operations. Shows entities in all operations.
3	Selected operation data.
4	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

Viewing operation entities

To view operation entities

Step	Action
1	Double-click an operation; the entity management page opens. *See "Entity management: link view" on page 64*

Entity management: icon and table views

To manage entities:	● **Intelligence** section, double-click an operation and click **Icon view** or **Table view**

Purpose

This function lets you:

- view operation entities
- manage operation entities
- open the target page linked to the Target entity

i   NOTE: the only entities viewed and managed without a user license are Target entities.

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

What the function looks like

This is what the page looks like:
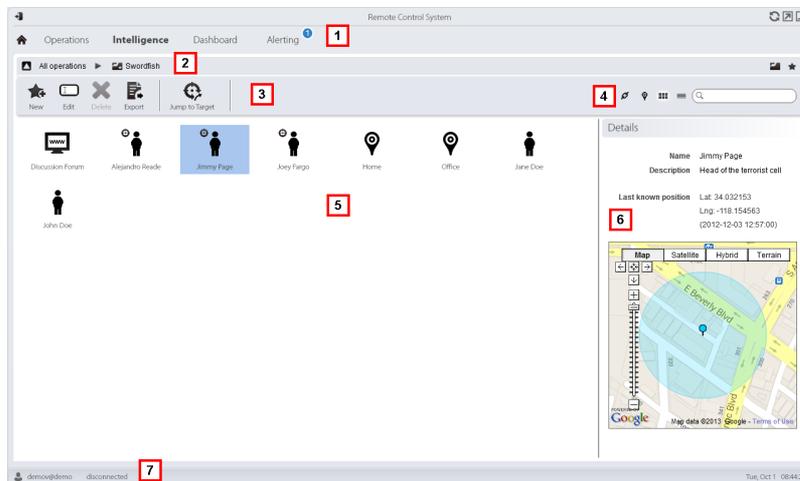
Area   *Description*

1   RCS menu.

2   Scroll bar

Area	Description
3	Window toolbar. Descriptions are provided below:

Icon	Function
	Creates a new entity
	Edits an entity
	Deletes an entity
	Exports entity data in `.html` format
	Opens the target page linked to the entity.*See "Target page" on page 24* .

Area	Description
4	View and search box buttons:

Object	Description
Q John Doe	Search box. Enter part of the name or description to display a list of entities that contain the entered letters.
≡	Displays the entities in a table.
▦	Displays entities as icons
⦿	Displays Target and Position entities and their links on a map. *See "Entity management: Position view" on page 69*
⬭	Displays entities and their links in a graph. *See "Entity management: link view" on the facing page*

Area	Description
5	Entity list
6	Selected entity data.
7	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

To learn more on intelligence *see "What you should know about intelligence" on page 53 see "What you should know about entities" on page 53*

Viewing entity details

To view entity details:

Step	Action
1	Double-click an entity: the detail page opens.

- *"**Target entity details**" on page 73* .
- *"**Person entity details**" on page 78* .
- *"**Position entity details**" on page 80* .
- *"**Virtual entity details**" on page 82* .

Entity management: link view

To manage intelligence entities:	• **Intelligence** section, double-click an operation, click **Link View**

Purpose

This function lets you:

- view operation entities and their links in the operation or in other operations in a graph
- manage entities
- manage entity links
- open the target page linked to the Target entity
- open evidence associated with a link
- dynamically view evidence associated with entity links

NOTE: this function requires a user license. Without a license, the default operation entity view is the icon view, *see "**Entity management: icon and table views**" on page 62* .

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

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.

4 View and search box buttons:

Object	Description
🔍 John Doe	Search box. Enter part of the name or description to display a list of entities that contain the entered letters.
☰	Displays the entities in a table. *See " Entity management: icon and table views" on page 62*
⠿	Displays entities as icons *See "Entity management: icon and table views" on page 62*
📍	Displays Target and Position entities and their links on a map. *See "Entity management: Position view" on page 69*
∅	Displays entities and their links in a graph.

5 Filter area

Area   Description

6	Entity graph and links based on set filters

NOTE: the Know, Identity and manually created links are always displayed regardless of the selected period.

NOTE: the entity with the most links is placed at the center of the graph.

7 Selected entity data.

8 Command that dynamically displays the quantity, direction and frequency of evidence that define the links between the entities displayed in the graph based on the set filters.

9 RCS status bar.

Window toolbar

Icon   Function

Creates a new entity

Editing an entity

Deletes an entity

Exports entity data in `.html` format

Merges two entities

Opens the target page linked to the entity.*See "Target page" on page 24 .*

Opens the evidence associated with the selected link. *See "Evidence analysis (Evidence)" on page 36*

$\varnothing_+$: creates a link

$\varnothing$: edits a link

$\varnothing_-$: deletes a link

: applies a level of relevance to a link

Icon	Function
	: creates a Group entity
	: deletes a Group entity
	Exports the entity graph in `.graphml` format.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

To learn more on intelligence *see "What you should know about intelligence" on page 53 see "What you should know about entities" on page 53*

Viewing entity details

To view entity details:

Step	Action
1	Double-click an entity: the detail page opens.
	• *"Target entity details" on page 73* .
	• *"Person entity details" on page 78* .
	• *"Position entity details" on page 80* .
	• *"Virtual entity details" on page 82* .

Merging two entities in one

To merge two entities in one:

Step	Action
1	Select the two entities holding down the **Ctrl** key on the keyboard.
	NOTE: only a Target entity can be merged with a Person entity or two Person entities.
2	Click **Merge**.
	Result: an entity with the name and description of the first entity is displayed in the graph with the details on both.
	NOTE: if a Target entity is merged with a Person entity, the Target entity remains with the Person entity details.

Creating a link between two entities

To create a link between two entities:

Step	Action
1	Select the two entities holding down the **Ctrl** key on the keyboard.
2	Select the direction, type and level of relevance of the link and click **Save.** **Result**: the link is displayed in the graph

Creating a Group

To create a Group:

Step	Action
1	Select the entities to be grouped holding down the **Ctrl** key on the keyboard.
2	Click **Group, Group.** **Result**: the Group is displayed in the graph.

Dynamically displaying evidence on links between entities

To dynamically display evidence on links between entities:

Step	Action
1	Make sure the entities displayed on the graph and the selected time period are those required. Use the filters to set preferences.

Step	*Action*
2	Click **Play** to display.
	Result : red balls slide along links to represent collected evidence.

 NOTE: the direction in which the ball slides indicates the direction of the evidence (i.e.: the red ball slides from the John entity to the Paul entity if John sent an email to Paul).

 NOTE: the number of balls indicates the quantity of evidence: one ball indicates that at least 10 pieces of evidence were collected, two balls between 10 and 50 pieces, three balls if more than 50 pieces of evidence were collected.

 NOTE: if the link was created on that day, that day is displayed on the map.

| **3** | Click **Stop** to stop the display. |

Entity management: Position view

To manage intelligence entities:	● **Intelligence** section, double-click an operation, click **Position View**

Purpose

This function lets you:

- display Target entities and Position entities for an operation and their links on a map.
- manage Target and Position entities
- manage links between Target and Position entities
- open the target page linked to the Target entity
- open evidence associated with a link
- dynamically display target entity movements

 NOTE: the function requires a user license and is only enabled if the user has **Entity management** authorization.

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.

4 View and search box buttons:

Object	Description
Q John Doe	Search box. Enter part of the name or description to display a list of entities that contain the entered letters.
≡	Displays the entities in a table. *See "Entity management: icon and table views" on page 62* .
⦙⦙⦙	Displays entities as icons *See "Entity management: icon and table views" on page 62* .
⚲	Displays Target and Position entities and their links on a map.
⌀	Displays entities and their links in a graph. *See "Entity management: link view" on page 64* .

5 Filter area

Area	Description
6	Entity map and links based on set filters

NOTE: the target entity is positioned in the last position acquired in the selected period.

NOTE: manually created links are always displayed regardless of the selected period.

7	Selected entity data.
8	Command to display Target entity movements based on set filters.
9	RCS status bar.

Window toolbar

Icon	Function
	Creates a new entity
	Editing an entity
	Deletes an entity
	Exports entity data in `.html` format
	Opens the target page linked to the entity.*See "Target page" on page 24* .
	Opens the evidence associated with the selected link. *See "Evidence analysis (Evidence)" on page 36*

: creates a link

: edits a link

: deletes a link

: applies a level of relevance to a link

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

To learn more on intelligence *see "What you should know about intelligence" on page 53 see "What you should know about entities" on page 53*

Viewing entity details

To view entity details:

Step	Action
1	Double-click an entity: the detail page opens. • *"Target entity details" on the next page* . • *"Person entity details" on page 78* . • *"Position entity details" on page 80* .

Creating a link between two entities

To create a link between two entities:

Step	Action
1	Select a Target entity and Position entity holding down the **Ctrl** key on the keyboard.
2	Select the level of relevance and click **Save.** **Result**: the link is displayed in the graph

Dynamically displaying target movements

To manage dynamically displayed target movements:

Step	Action
1	Make sure the entities displayed on the graph and the selected time period are those required. Use the filters to set preferences.
2	Click **Play** to display. **Result**: the Target entities displayed on the map move according to the movements logged in evidence. NOTE: if there is no evidence on the target position in the selected period, the Target entity remains on the last position acquired but its icon slowly fades until it disappears or appears in the next logged position.
3	Click **Stop** to stop the display.

Target entity details

To view entity details: | ●   **Intelligence**   section, double-click an operation, double-click a **Target** entity

Purpose

This function lets you:

- view detailed information on the Target entity processed by the system
- add detailed information on the Target entity
- create new entities connected to the Target entity

NOTE: some details and some actions are only enabled with the user license.

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

What the function looks like

This is what the page looks like:

Area	Description
1	RCS menu.
2	Scroll bar

Area	Description
Area	*Description*

3   Window toolbar. Descriptions are provided below:

Icon	Function
Icon	*Function*

    Edit entity data.

    Exports entity data in `.html` format

    Opens the target page linked to the entity.*See "*Target page*" on page 24* .

4   Photo of the target linked to the entity. It is the first image captured by the webcam by default.

5   List of target identification data identified by evidence or manually added.

6   Table with the most frequently contacted people and most frequently visited websites based on the selected period.
Double-click to open the page of evidence for that data.

7   Search period.

8   Map indicating:
- last position acquired from the target,
- places most frequently visited in the selected period,
- manually entered places visited by the target.

9   RCS status bar

To learn more

For interface element descriptions *See "*Shared interface elements and actions*" on page 11* .

To learn more on intelligence *see "*What you should know about intelligence*" on page 53 see "*What you should know about entities*" on page 53*

Adding the target photo

To add the photos:

Step	Action

1
- Click **+** and select a photo

or

- in the **Evidence** page open webcam type evidence details and select an image

Result: the selected image becomes the default image.

Adding target identification data

To add identification data:

Step	Action

1   Click **+** and enter data.

NOTE: the **Account** field is the target's true identity (i.e.: john.john@email.com); the **Name** field in an optional name to be linked to the identification data (i.e.: John).

Result: the identification data is added to the list.

Viewing frequently contacted people

To view frequently contacted people:

Step	Action

1   Select the period of interest

2   In the text box next to **Most contacted,** enter the number of people per type of communication means to be viewed.

3   Press **Enter** on the keyboard.

Result: the information on the people most frequently contacted in the selected period appears in the table, *see "Target entity details" on page 77*

Viewing most frequently visited websites

To view the most frequently visited websites:

Step	Action

1   Select the period of interest

Step	Action
2	In the text box next to **Most visited websites,** enter the number of websites to be viewed.
3	Press **Enter** on the keyboard. **Result**: the information on the websites most frequently visited in the selected period appears in the table, *see "Target entity details" on the next page*

Connecting the Target entity with a frequently contacted person

To connect the Target entity with a frequently contacted person:

Step	Action
1	In the **Most Contacted** table, click **Add as Entity** in the required row and enter data. **Result**: a Person entity with the selected identification data is added to the list of operation entities along with a Peer link with the Target entity. NOTE: the result is the same if a Person entity is manually created with the table identification data and a Peer link added between the Target and created entity.

Connecting the target to a frequently visited website

To connect the target to a frequently visited website:

Step	Action
1	In the **Most visited websites** table, click **Add as Entity** in the required row and enter data. **Result**: a Virtual entity with the selected URL is added to the list of operation entities along with a Peer link with the Target entity. NOTE: the result is the same if a Virtual entity is manually created with the table URL address and a Peer link added between the Target and created entity.

View the last acquired position

To view the target's last position on the map:

Step	Action
1	Select the **Last position** combo box. **Result:** a blue flag indicates the corresponding position.

Viewing frequently visited places

To view frequently visited places on the map:

Step	Action
1	Select the **Most visited places combo box.** **Result**: the most visited positions are displayed on the map with red flags.

Adding a Position entity visited by the target

To manually add a Position entity visited by the target:

Step	Action
1	In the map, click **+** and enter data. Tip: add a significant **Name** and a **Description** that help to identify the relationship between the target and place. **Result:** a Position entity with a Peer link with the Target entity is added to the operation list of entities. NOTE: the result is the same if a Position entity is manually created and a Peer link added between the Target and the created entity.

Target entity details

Most contacted people table

Following is a description of the data indicated in the table of people most frequently contacted by the target:

Data	Description
first column	communication method icon and the person's identification data.
second column	number of target contacts with the person in the selected period.

Data	Description
third column	percent of target communications with the person in the selected period. NOTE: calculations are based on the communication mean and considering the displayed contacts.
	button to create a Person entity with that identification data and to create a peer link with the target entity.

Most visited websites table

Following is a description of the data indicated in the most visited websites table:

Data	Description
first column	visited website URL address.
second column	number of target visits to the website in the selected period.
third column	percent of target visits to the website in the selected period. NOTE: calculated considering the displayed websites.
	button to create a Virtual entity with that URL address and to create a Peer link with the Target entity.

Person entity details

To view entity details:	•	**Intelligence** section, double-click an operation, double-click a **Person** entity

Purpose

This function lets you:

- view detailed information on the Person entity
- add detailed information on the Person entity
- create Position entities connected to the Person entity

NOTE: the function requires a user license and is only enabled if the user has **Entity management** authorization.

What the function looks like

This is what the page looks like:
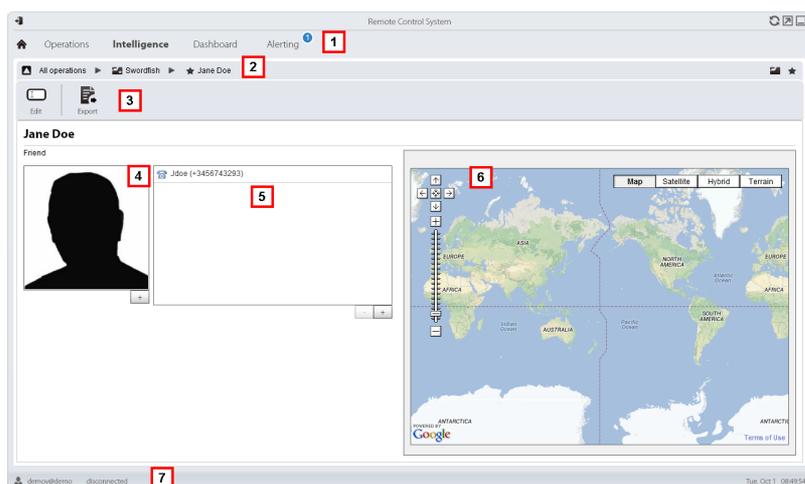
Area **Description**

1 RCS menu.

2 Scroll bar

3 Window toolbar. Descriptions are provided below:

Icon	*Function*
	Edit entity data.
	Exports entity data in `.html` format

4 Photos of the person linked to the entity.

5 List of identification data for people linked to with the entity.

6 Map indicating positions connected to the entity.

7 RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

To learn more on intelligence *see "What you should know about intelligence" on page 53 see "What you should know about entities" on page 53*

Adding a person's picture

To add an image:

Step	Action
1	Click **+** and select a photo **Result**: the selected image becomes the default image.

Adding a person's identification data

To add identification data:

Step	Action
1	Click **+** and enter data. NOTE: the **Account** field is the person's actual identity (i.e.: john.john@email.com); the **Name** field is an optional name to be linked to the identification data (i.e.: John). **Result:** the identification data is added to the list.

Adding a Position entity visited by the entity

To manually add a Position entity visited by the entity:

Step	Action
1	In the map, click **+** and enter data. Tip: add a significant **Name** and a **Description** that help to identify the relationship between the person and place. **Result:** a Position entity with a Peer link with the Person entity is added to the operation list of entities. NOTE: the result is the same if a Position entity is manually created and a Peer link added between the Person entity and the created entity.

Position entity details

To view entity details: • **Intelligence** section, double-click an operation, double-click a **Position** entity

Purpose

This function lets you:

- view detailed information on the Position entity
- add a photo of the place linked to the entity

NOTE: the function requires a user license and is only enabled if the user has **Entity management** authorization.

What the function looks like

This is what the page looks like:
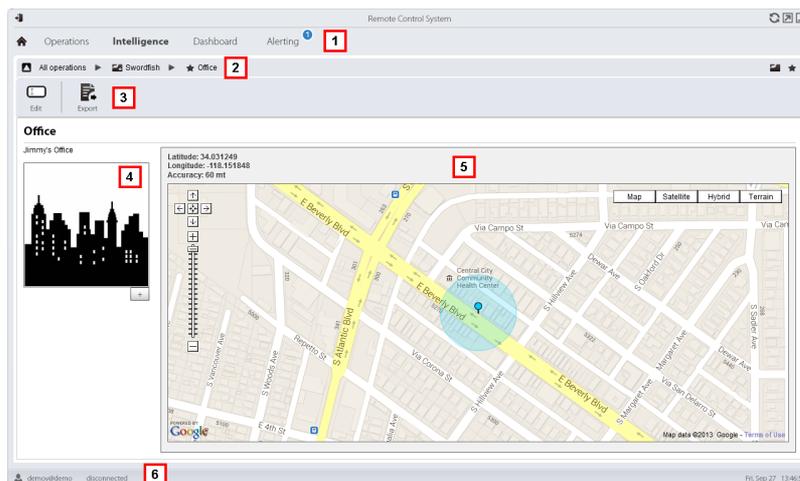
Area	Description
1	RCS menu.
2	Scroll bar
3	Window toolbar. Descriptions are provided below:

Icon	Function
	Edit entity data.
	Exports entity data in `.html` format

4	Photo of the place linked to the entity.

Area	Description
5	Map indicating the place linked to the entity.
6	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .
To learn more on intelligence *see "What you should know about intelligence" on page 53* .

Adding a picture of the site

To add an image:

Step	Action
1	Click **+** and select an image. **Result**: the selected image becomes the default image.

Virtual entity details

To view entity details: | ● **Intelligence** section, double-click an operation, double-click a **Virtual** entity

Purpose

This function lets you:

- view detailed information on the Virtual entity
- add detailed information on the Virtual entity

NOTE: the function requires a user license and is only enabled if the user has **Entity management** authorization.

What the function looks like

This is what the page looks like:
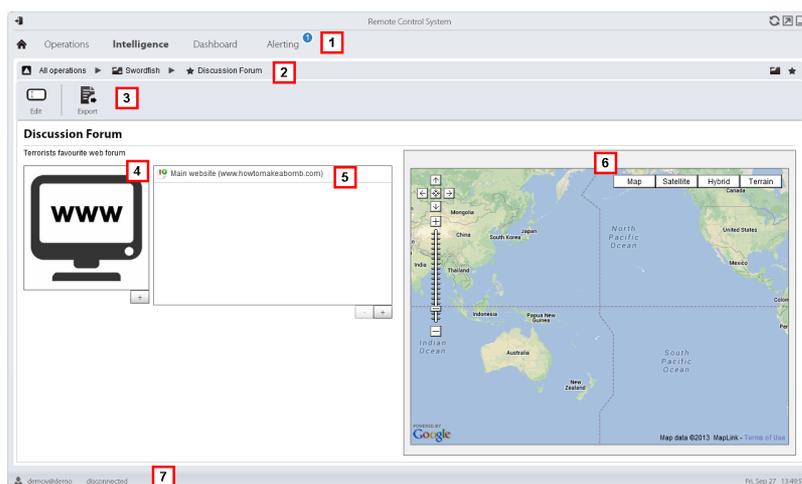
Area	Description
1	RCS menu.
2	Scroll bar
3	Window toolbar. Descriptions are provided below:

Icon	Function
	Edit entity data.
	Exports entity data in `.html` format

4	Image of the address content linked to the entity.
5	List of web addresses linked to the entity.
6	Map indicating the position of the web address automatically identified by the system via IP address.
7	RCS status bar.

To learn more

For interface element descriptions *See "Shared interface elements and actions" on page 11* .

To learn more on intelligence *see "What you should know about intelligence" on page 53 see "What you should know about entities" on page 53*

Adding an image of the web address

To add images:

Step	Action
1	Click **+** and select an image. **Result**: the selected image becomes the default image.

Adding web addresses to the entity

To add web addresses to the entity:

Step	Action
1	Click **+** and enter data. **Result:** the address is added to the list.

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*
Operation evidence: 	Operation targets and the amount of evidence per target appear.
Target evidence: 	The target's evidence and the amount of evidence per type appear.
Agent evidence: 	The agent's evidence and the amount of evidence per type appear.

 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" on page 46* .

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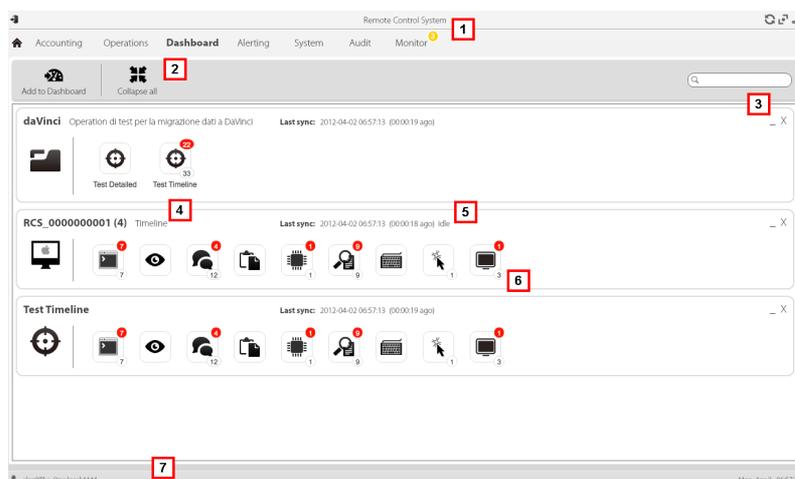
Area	Description
1	RCS menu.
2	Window toolbar. Descriptions are provided below:

Icon	Description
	Add a new element to be monitored.
	Shrink or expand all Dashboard element windows.

Area	Description
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*" *on page 11* .

For more information on the Dashboard *see "What you should know about the Dashboard" on page 86* .

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.

Step	Action
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" on page 24* . For the target element: • double-click the agent: the agent page opens.*See "Agent page" on page 29* . For the agent element: • double-click the evidence type: the evidence page appears. *See "Evidence analysis (Evidence)" on page 36*

Alert

Presentation

Introduction

Alerts signal when evidence is received, agents are synchronized or entities are automatically created or connected by the system. Furthermore, they let you automatically tag evidence and links for analyses and export.

Content

This section includes the following topics:

What you should know about alerts

What are alerts

During the investigation phase, being "alerted" on special events that concern the target in real-time via e-mail or notification on RCS Console, can be helpful.

Alerts can be received when:

- new evidence arrives
- the agent synchronizes
- entities are automatically created and connected (intelligence)

For example, if awaiting evidence from a target for a long time, an alert rule can be created to send an e-mail 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.

Or, if intelligence is used, it could be helpful to be "alerted" when a link is created with a certain entity or a new entity is created in the operation.

Alert rules

Alert rules set which events generate alerts. They can also be used to automatically assign levels of relevance to evidence or intelligence links which can be used in the analysis phase.

Alert rule application field

Rules that alert the arrival of evidence can be created on the following levels:

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

Rules that alert the automatic creation of an intelligence entity can be created on the following levels:

- **Operation**: alerts when an entity is created for that operation

Rules that alert the automatic creation of an intelligence link can be created on the following levels:

- **Operation**: alerts when a link is created for any entity in the operation
- **Entity**: alerts when a link is created for that entity

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

Alert process

The alert process is described below:

NOTE: sending an e-mail is optional.

Phase	Description
1	The Analyst creates rules to be alerted of the arrival of certain evidence, agent synchronizations or the automatic creation of intelligence entities or links. Rules log the alerts, notify them on the RCS Console and send them via e-mail (optional).
2	The system taps the incoming evidence or analyzes the element it is creating and compares it with the alert rules.

If the evidence...	Then...
corresponds to an alert rule	The system saves the evidence as *evidence* or adds the entity or link to the operation, generating an alert that automatically applies the selected level of relevance. An e-mail notification can be sent by the system as an option.
does not correspond to an alert rule	The system saves the evidence as *evidence* or adds the entity or link to the operation without generating an alert.

Phase	Description
3	The Analyst receives an alert e-mail (if set by the alert rule) and checks the alert log. From an alert, directly open the evidence that generated it or the created entity or the link view.
4	After checking, the Analyst deletes the alert logs.

Alerting

|	
To receive alerts from the target:	• **Alerting** section

Purpose

This function lets you:

- receive alerts when a certain type of evidence is tapped, when the target device synchronizes with RCS or when intelligence automatically creates entities or entity links.
- automatically tag evidence or intelligence link by relevance, to facilitate later analysis.
- monitor all logged alerts and directly open the event that generated them.

What the function looks like

This is what the page looks like:
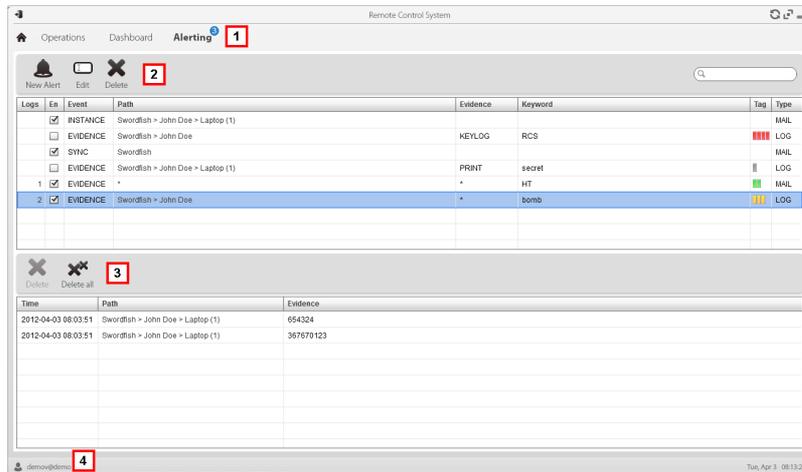
Area	Description
1	RCS menu.

 : 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.

NOTE: the function is only enabled if the user has **Alerts creation** authorization.

| | Edit the selected alert rule. |

| | Delete the selected alert rule. |

CAUTION: all generated notifications are deleted.

Area	*Description*
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" on page 11* .

For a description of the data in this window *see "Alert data " on the next page*

For more information on alerts*see "What you should know about alerts" on page 91* .

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 logs an event 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.

Step	Action
3	Click **Save**: the new alert rule appears in the main work area. An alert is sent as soon as the system logs an event that matches the rule.

Adding a rule to automatically tag certain evidence or certain intelligence links between entities

To automatically tag certain evidence or certain link without logging or sending alerts:

Step	Action
1	Click **New Alert**: data entry fields appear.
2	• Setting criteria to select evidence or links • In **Type** select **None.** • In **Relevance** set the relevance level • 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 events 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	Double-click on the row in the logged alert list. **Result**: it directly opens: • the list of evidence that generated the alert (**Evidence** event). • entity details(**Entity** event) • link view (**Link** event)

Alert data

Alert rule data

Alert rule data is described below:

Data	Description
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: **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. **Entity**: triggers the rule when the system automatically creates a new intelligence entity in the indicated operation. **Link**: triggers the rule when the system automatically creates a link between intelligence entities in an operation or with the indicated entity.
Path	operation, target, entity, agent and factory to be monitored. Thus it indicates the rule application field. For example, for **Evidence** event, if an operation is selected, all operation evidence is monitored. If an agent is selected, that agent's evidence is monitored.
Evidence	(only **Evidence** type events) Type of evidence that generates alerts. Tip: '*****' indicates all types of evidence. For a description of all types *see "List of types of evidence" on page 46*
Keyword	(only **Evidence** type events) Keyword that the evidence must contain to trigger the alert. For example, keyword "password" creates an alert when the evidence (audio, document) contains the word "password".
Tag	(only **Evidence** or **Link** type events) Automatically tags evidence or the link with different levels of relevance to facilitate analysis:

Icon	Description
	Maximum relevance.
	Intermediate relevance.
	Normal relevance.
	Minimum relevance.
	No relevance.

Data	*Description*
Type	Type of alert to be received when evidence arrives: • **Log**: alert logged and notified on the RCS Console. • **Mail**: e-mail and alert logged • **None**: no logged alert nor e-mail. Useful to automatically tag evidence by relevance (**Tag**)
Suppression Time	(only **Mail** type alerts) Latency time for sending identical alert e-mails. Used to avoid identical e- mails after the first. For example, if the target has not communicated its evidence for a while and e-mail alert was selected, you may be bombarded with e- mails when the first evidence arrives. Set a 30- minute **Suppression time** to receive one e-mail every 30 minutes. NOTE: this setting only limits e-mail delivery. Events are always logged.

Log data

Alert logs are described below:

Data	*Description*
Date	alert time-date.
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.
Info	Quantity and type of events that generated the alert.

]Hacking**Team**[