

]HackingTeam[

RCS 9.6

The hacking suite for governmental interception

Administrator manual



Information ownership

© COPYRIGHT 2015, HT S.r.l.

All rights reserved in all countries.

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

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

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

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

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

HT S.r.l.

via della Moscova, 13

20121 Milan (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

Contents

Guide introduction	1
Helpful information on the guide	1
Manual goals	1
New guide features	1
Supplied documentation	2
Print concepts for notes	2
Print concepts for format	2
Product and guide addressees	3
Software author identification data	4
RCS Console for the Administrator	5
Starting the RCS Console	6
Introduction	6
Restoring disabled users who entered incorrect passwords	6
What the login page looks like	6
Open RCS Console	7
Homepage description	7
Introduction	7
What it looks like	7
Wizards in the homepage	8
Introduction	8
What it looks like	8
Shared interface elements and actions	9
Introduction	9
What the RCS Console looks like	9
Change interface language or password	11
Converting the RCS Console date-time to the actual time zone	11
Table actions	12
Administrator's procedures	14
Introduction	14
Preparing the RCS for use by other users	14
Opening an investigation	14
Closing an investigation	14

Monitoring the system	15
Managing RCS login	16
What you should know about users and groups	17
Introduction	17
Login privileges	17
Functions enabled by single role	17
User groups per operation	18
User groups for system alarm alerts	18
User management	18
Purpose	18
Next steps	18
What the function looks like	19
To learn more	20
Registering and enabling a user for RCS	20
Enabling/Disabling a user	20
Immediately disconnecting a user	20
Editing user data	21
User data	21
Privilege data	22
Group management	24
Purpose	24
What the function looks like	24
To learn more	25
Creating a group and linking users and operations	25
Editing group data and removing users and operations	25
Operation and target	27
What you should know about operations	28
What is an operation	28
Assigning the operation to a user group	28
What happens when a new operation is created	28
What happens when an operation is closed	28
What you should know about targets	28
What is a target	28
Administrator tasks	28

What happens when a target is created	29
What happens when a target is closed	29
Opening and closing an operation	29
Operation management	29
Purpose	29
Next steps	30
What the function looks like	30
To learn more	31
Creating an operation	31
Editing operation data	31
Closing an operation	31
Deleting an operation	31
Operation data	32
Operation page	32
Purpose	32
What the function looks like	32
To learn more	33
Creating a target	34
Closing a target	34
Editing target data	34
Deleting a target	34
Operation page data	34
Monitoring users	36
What you should know about user monitoring (Audit)	37
What is user monitoring	37
How signaled actions are read	37
Selecting specific actions using filters	37
Exportable data	37
User monitoring (Audit)	38
Purpose	38
What you can do	38
What the function looks like	38
To learn more	39
Selecting actions in a time range	39

Selecting actions based on proposed data	39
Removing one or more filters	39
Exporting displayed actions	40
User monitoring data (Audit)	40
System monitoring	41
System monitoring (Monitor)	42
Purpose	42
What the function looks like	42
To learn more	43
Define the alerting group or temporarily enable/disable it	43
System monitoring data (Monitor)	44
Glossary	46

Guide introduction

Helpful information on the guide

Manual goals

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

- create users and workgroups
- open and close investigations
- monitor RCS users
- monitor the system

New guide features

List of release notes and updates to this online help.

Release date	Code	Software version.	Description
March 15, 2015	Administrator manual 1.7 MAR-2013	9.6	Added automatic incorrect password entry disabling and restore procedures, see " Starting the RCS Console " on page 6.
November 24, 2014	Administrator manual -	9.5	No documentation update.
September 20, 2014	Administrator manual -	9.4	No documentation update.
June 23, 2014	Administrator manual -	9.3	No documentation update.
February 19, 2014	Administrator manual -	9.2	No documentation update.
September 30, 2013	Administrator manual 1.4 SET - 2013	9	Updated documentation due to improvements to the user interface. Improved the contents.

Supplied documentation

The following manuals are supplied with RCS software:

Print concepts for notes

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



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



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



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



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



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



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

Print concepts for format


A key to print concepts is provided below:

<i>Example</i>	<i>Style</i>	<i>Description</i>
See " <i>User data</i> "	<i>italic</i>	this indicates a chapter, section, sub-section, paragraph, table or illustration heading in this manual or other publication of reference.
<ddmmyyy>	<aaa>	indicates text that must be specified by the user according to a certain syntax. In the example <ddmmyyy> is a date and could be "14072011".
Select one of the listed servers [2].	[x]	indicates the object specified in the text that appears in the adjacent image.

<i>Example</i>	<i>Style</i>	<i>Description</i>
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	capital first letter	indicates a keyboard key name.
See: Network Injector Appliance.	-	suggests you compare the definition of a word in the glossary or content with another word or content.

Product and guide addressees

Following is the list of professionals that interact with RCS:

<i>Addressee</i>	<i>Activity</i>	<i>Skills</i>
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 Milan (MI)

Italy

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

e-mail: info@hackingteam.com

RCS Console for the Administrator

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.

The Administrator's role

The *Administrator's* role is:

- to manage system access by assigning users the various roles foreseen by the application
- to create and close investigations
- to define the involved targets
- to inform the *Technician* user of the types of evidence to be tapped
- to monitor actions run by users
- to monitor licenses available for RCS components

Functions enabled for the Administrator

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

- **Accounting**
- **Operations**
- **Audit**
- **Monitor**

Content

This section includes the following topics:

Starting the RCS Console	6
Homepage description	7
Wizards in the homepage	8
Shared interface elements and actions	9
Administrator's procedures	14

Starting the RCS Console

Introduction

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



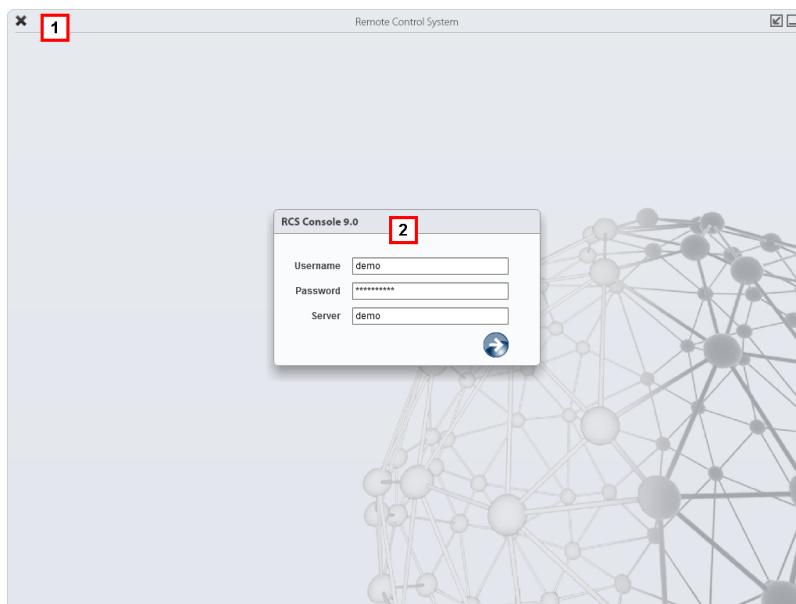
IMPORTANT: if the wrong password is entered five times in a row, the user is automatically disabled by the system and can no longer login to RCS Console.

Restoring disabled users who entered incorrect passwords




To restore a user, enter the **Accounting** section and set the user status to **Enabled**.

What the login page looks like

This is what the login page looks like:





Area Description

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

Open RCS Console

To open RCS Console functions:

Step Action

- 1 In **Username** and **Password**, enter the credentials as assigned by the Administrator.
- 2 In **Server**, enter the name of the machine or server address to connect to.
- 3  Click : the homepage appears with the menus enabled according to your account privileges. See "[Homepage description](#)" below.

Homepage description

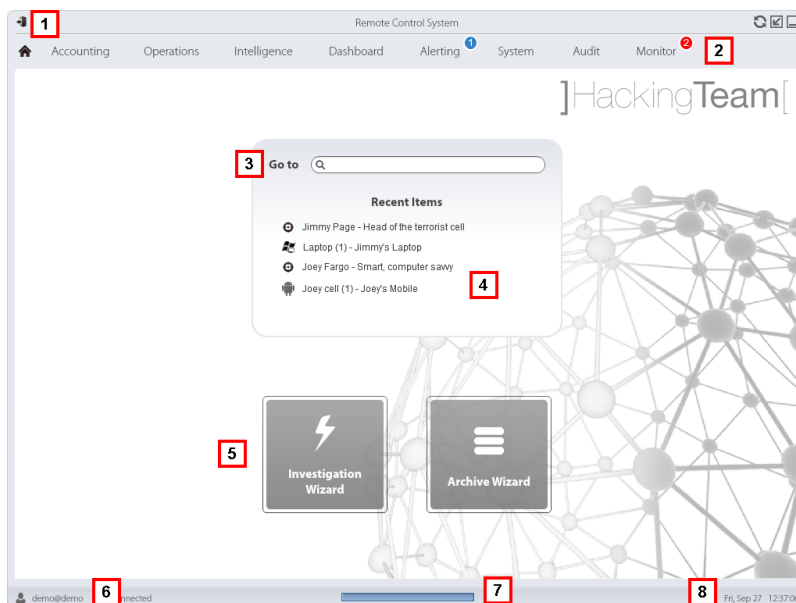
To view the homepage:  click 

Introduction

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

What it looks like

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



Area Description

- 1 Title bar with command buttons.
- 2 RCS menu with functions enabled for the user.
- 3 Search box to search operations, targets, agents and entities, by name or description.
- 4 Links to the last five elements opened (operation in the **Operations** section, operation in the **Intelligence** section, target, agent and entity).
- 5 Wizard buttons.
- 6 Logged in user with possibility of changing the language and password.
- 7 Download area with ability to view progress during export or compiling.
- 8 Current date and time with possibility of changing the time zone.

Wizards in the homepage

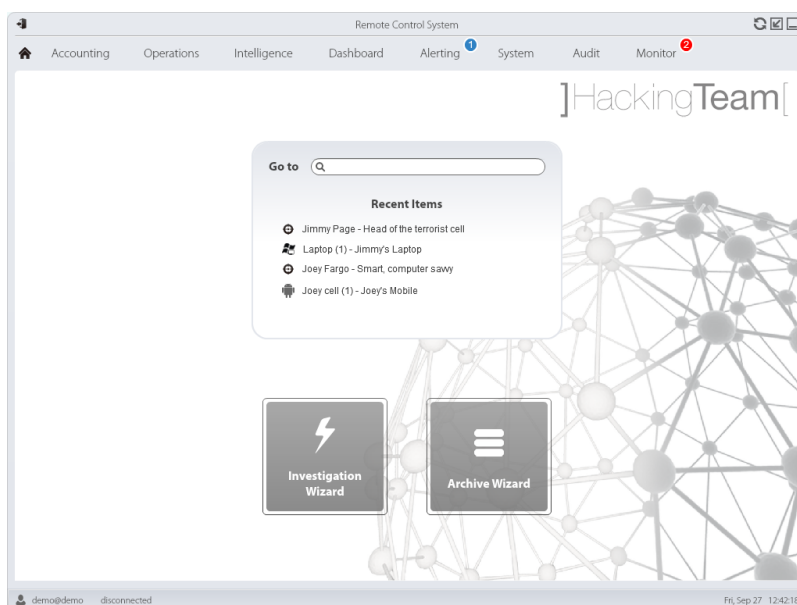
To view the homepage: | • click 

Introduction

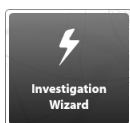
For users with certain privileges, RCS Console displays buttons that run wizards.

What it looks like

This is how the homepage is displayed with enabled wizards:



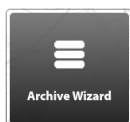
Button	Function
--------	----------



Open the wizard to quickly create an agent.



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



Open the wizard to quickly save operation and target data.



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

Shared interface elements and actions

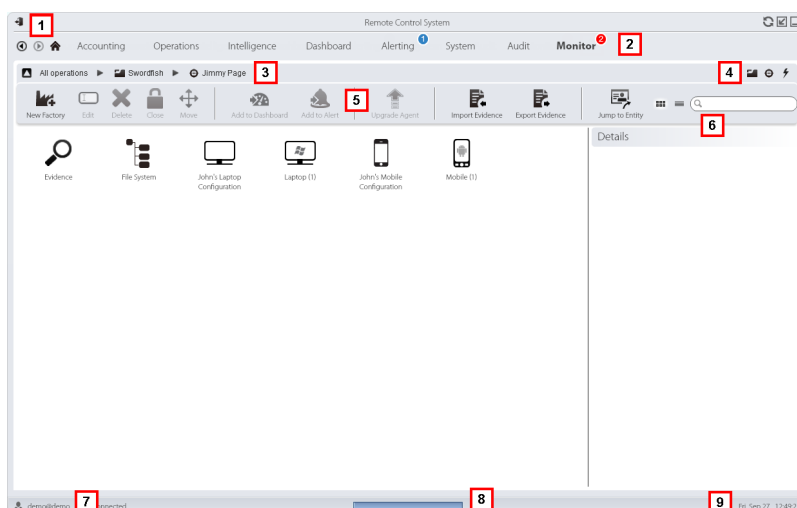
Introduction

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

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





What the RCS Console looks like

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






Area Description

1 Title bar with command buttons:








-  Logout from RCS.
-  Page refresh button.
-  Expand window button.
-  Shrink window button.

2








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

RCS menu with functions enabled for the user.

3 Operation navigation bar. Descriptions are provided below:

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

Area Description

- 4** Buttons to display all elements regardless of their group membership. Descriptions are provided below:
-  Show all operations.
 -  Show all targets.
 -  Show all agents.
 -  Show all entities.
- 5** Window toolbar.
- 6** Search buttons and box:
-  Search box. Enter part of the name to display a list of elements that contain the entered letters.
 -  Display elements in a table.
 -  Display elements as icons.
- 7** Logged in user with possibility of changing the language and password.
- 8** Download area with ability to view progress during export or compiling. Files are downloaded to the desktop in RCS Download folder.
- Top bar: percent generation on server.
 - Bottom bar: percent download from server to RCS Console.
- 9** Current date and time with possibility of changing the time zone.

Change interface language or password

To change the interface language or password:

Step Action

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

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

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

Step Action

- 1** Click **[9]** to display a dialog window with the current date-time.
 - UTC time:** Greenwich mean time (GMT)
 - Local time:** date-time where the RCS server is installed
 - Console time:** date-time of the console used that can be converted.

Step Action

- 2 Change the time zone and click **Save** to confirm and exit: all displayed dates-times are converted as requested.

Table actions

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

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

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

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

Event	Path
SYNC	Swordfish
INSTANCE	Swordfish > J
EVIDENCE	*

Filter a text

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

 Info

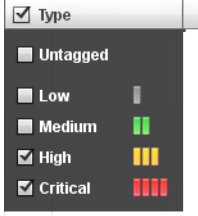
The example shows elements with descriptions like:

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

Sort based on an option

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

 Acquired
 Last 24 Hours
 Last Week
 From / To
 Action User

<i>Action</i>	<i>Description</i>
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.

Administrator's procedures

Introduction

Procedures typically performed by the Administrator are indicated below with references to their pertinent chapters.

Preparing the RCS for use by other users

Following are the procedures typically performed to prepare RCS for use by others:

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

- | | |
|---|--|
| 1 | In the Accounting section, Users set the people who will have access to RCS.
See " User management " on page 18 |
| 2 | In the Accounting section, Groups create the user group (usually composed of system administrators and not linked to any operation) that will receive the system alarm e-mail notifications
See " Group management " on page 24 |
| 3 | In the Monitor section, select the group that will receive the system alarm e-mail notifications.
See " System monitoring (Monitor) " on page 42 |

Opening an investigation

Procedures typically performed to open an investigation are indicated below:

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

- | | |
|---|--|
| 1 | In the Accounting section, Users set the people who will belong to the investigation team and their roles.
See " User management " on page 18 |
| 2 | In the Accounting section, Groups set the team enabled to view investigation data and receive system alarms.
See " Group management " on page 24 |
| 3 | In the Operations section, open the investigation and link one or more groups.
See " Operation management " on page 29 and " Operation page " on page 32 |
| 4 | Inform the RCS Technician of the types of evidence to be collected. |
| 5 | In the Audit section, monitor system access by the team and check their actions.
See " User monitoring (Audit) " on page 38 |

Closing an investigation

The typical procedure performed to close an investigation is indicated below:

Step Action

- 1 In the **Operations** section, close the investigation.
See "[Operation management](#)"
- 2 If necessary, ask the System administrator to save evidence in a Backup file.

Monitoring the system

The typical procedures performed to monitor RCS use are indicated below:

Step Action

- 1 In the **Monitor** section, monitor system messages and licenses used.
See "[System monitoring \(Monitor\)](#)" on page 42
- 2 In the **Audit** section, monitor actions performed by Technicians, Analysts and other Administrators.
See "[User monitoring \(Audit\)](#)" on page 38

Managing RCS login

Presentation

Introduction

Managing users and groups is essential to guarantee data confidentiality and security.

Content

This section includes the following topics:

What you should know about users and groups	17
User management	18
Group management	24

What you should know about users and groups





Introduction

To guarantee maximum data confidentiality and security, RCS provides the Administrator the opportunity of assigning login privileges to each user and grouping users in workgroups for specific operations. The structure adapts to both situations where tasks are highly fragmented and situations where all tasks are performed by a few people.

By managing users, the Administrator can also quickly disconnect a suspected user and temporarily disable his/her RCS login.

Login privileges

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

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



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

Functions enabled by single role

Following is the list of RCS functions reserved to users in a specific role:

<i>Role</i>	<i>Enabled functions</i>
System Administrator	<ul style="list-style-type: none"> • System • Monitor
Administrator	<ul style="list-style-type: none"> • Accounting • Operations • Audit • Monitor
Technician	<ul style="list-style-type: none"> • Operations • System
Analyst	<ul style="list-style-type: none"> • Operations • Intelligence • Dashboard • Alerting

User groups per operation

Groups allow users to be grouped to assign them specific operations. This way, several operations can be managed simultaneously, guaranteeing maximum data confidentiality amongst workgroups.

See "[Operation management](#)" on page 29



IMPORTANT: operation assignments to a workgroup will be effective the next time the user in that group logs in.

User groups for system alarm alerts

A group of users exclusively intended to receive an e-mail in the event of system alarm can be created.

This way, fast System administrator intervention can be guaranteed in the event of serious faults.

See "[System monitoring \(Monitor\)](#)" on page 42

User management

To manage
users:

- Accounting section, Users

Purpose

This function lets you:

- register a user and allow him/her access to certain RCS functions. Once registered, the user can login and view functions based on assigned roles
- temporarily disable user login, for example, in the event of prolonged absence
- immediately disconnect the user from RCS, for example, in the event of alleged illegal access to RCS
- monitor the date-time and IP address of the user's last connection to RCS and other pertinent data



Tip: to block a user and prevent any access to RCS, we suggest you immediately disconnect him/her (if connected) and disable him/her.



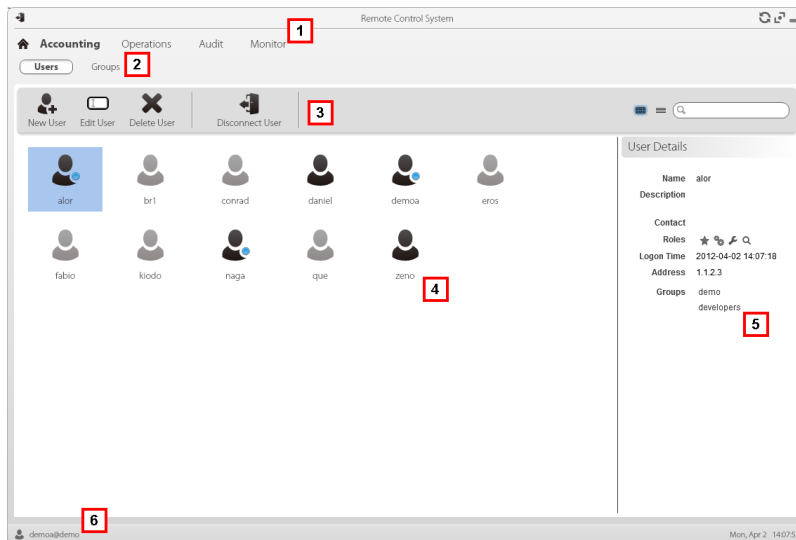
NOTE: the function is only enabled with **User and group administration** permissions.

Next steps








Several users can be linked to a workgroup, to assign them specific operations or send system alarms. See "[Group management](#)" on page 24.

What the function looks like

This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 **Accounting** menu.
- 3 Window toolbar. Descriptions are provided below:
 -  Adds a user
 -  Edits the selected user.
 -  Deletes the selected user.
 -  Disconnects the selected user.
- 4 Main work area with list of registered users:
 -  Registered user currently logged into RCS.
 -  User registered but not currently logged into RCS.
 -  User registered but not enabled to login. The user cannot have access to RCS.
- 5 Selected user data.
- 6 RCS status bar.

To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 9.


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

For more information on users and groups see "[What you should know about users and groups](#)" on page 17.

Registering and enabling a user for RCS

To register a new user:



Step Action

- 1 Click **New User**: data entry fields appear.
- 2 Enter the required data and make sure the **Enabled** box is selected if you want the user to login to RCS.
- 3 Click **Save**: the new user with the  icon appears in the main work area.

Enabling/Disabling a user

To enable or disable a user to login to RCS:

Step Action

- 1 Double-click a user: his/her data appear.
- 2 Click **Enabled** to enable or disable.
- 3 Click **Save**: the new user appears in the main work area with icon 
(enabled) or  (disabled).



IMPORTANT: if the user is logged in, she/he will continue to work but the next login will be denied. To immediately disconnect a user see "[Immediately disconnecting a user](#)" below.

Immediately disconnecting a user

To immediately disconnect a logged in user:

Step Action

- 1 Click on a user  and click **Disconnect user**: the user appears with icon  in the main work area.



IMPORTANT: if the user is logged in, she/he will immediately be disconnected. The next login will be permitted unless the user is disabled. To disable the user see "[Enabling/Disabling a user](#)" on the previous page.

Editing user data


To edit user data:





Step Action

- 1 Double-click a user: his/her data appear.
- 2 Edit data and click **Save**: data is considered from the next login or next alert messages.

User data

Selected user data is described below:


<i>Data</i>	<i>Description</i>
Enabled	Select to enable user login to RCS. Do not select to leave the user registered but deny login to RCS.
Name	Name used to login to RCS.
Description	User's description
E-mail	User's e-mail.  IMPORTANT: if the user has Analyst privileges, evidence alerts will be sent to this address. The e-mail cannot be changed by the user.
Password	User's password. The user can change it later from the status bar.

<i>Data</i>	<i>Description</i>
Roles	<p>Privileges assigned to the user:</p> <ul style="list-style-type: none">  System administrator  Administrator  Technician  Analyst <p>For a detailed description of privileges see "Privilege data" below</p>
Advanced permissions	<p>Opens the window to assign authorizations for each privilege. For a detailed description of authorizations see "Privilege data" below</p>
Language	RCS Console interface language. The user can change it later from the status bar.
Console time zone	Time zone used by the RCS Console to display time.
Groups	User's groups. The user can only see the operations assigned to the group.

Privilege data

Administrator authorizations

Following is a description of the authorizations assigned to Administrators:

<i>Data</i>	<i>Description</i>
User and group administration	<p>Enables the Accounting section.</p> <p> NOTE: users with this authorization can naturally change their own and others' authorizations.</p>
Operation management	Enables Operations management.
Target management	Enables target management.
Audit management	Enables the Audit section.
Change license	Allows the license to be updated.

System administrator authorizations

Following is a description of the authorizations assigned to System Administrators:

<i>Data</i>	<i>Description</i>
Frontend management	Enables the System, Frontend section.
Backend management	Enables the System, Backend section.
System backup and restore	Enables the System, Backup section.
Network Injector management	Enables the System, Network Injector section.
Connector management	Enables the Connectors section .


Technician authorizations

Following is a description of the authorizations assigned to Technicians:

<i>Data</i>	<i>Description</i>
Factory build	Allows factories to be created and set.
Injection vector build	Allows installation vectors to be compiled.
Agent configuration	Allows agent configurations to be edited.
Run commands on an agent	Allows commands to be run on agents.
Upload file to agent	Allows files to be sent to agent.
Import evidence	Allows evidence to be imported
Network Injector rule management	Allows rules to be added for Network Injectors.

Analyst authorizations

Following is a description of the authorizations assigned to Analysts

<i>Data</i>	<i>Description</i>
Alert build	Allows alert rules to be created.
Explore agent file system	Allows the agent's file system to be browsed.
Edit evidence	Allows priorities to be assigned to evidence and notes added.
Delete evidence	Allows evidence to be deleted.  NOTE: this authorization is never enabled by default since it requires a user license.
Export evidence	Allows evidence to be exported
Entity management	Allows intelligence entities to be managed.

Group management

To manage groups:

- Accounting section, Groups

Purpose

This function lets you:

- organize users in work groups to assign specific operations
- create an alerting group to receive system alarm e-mails



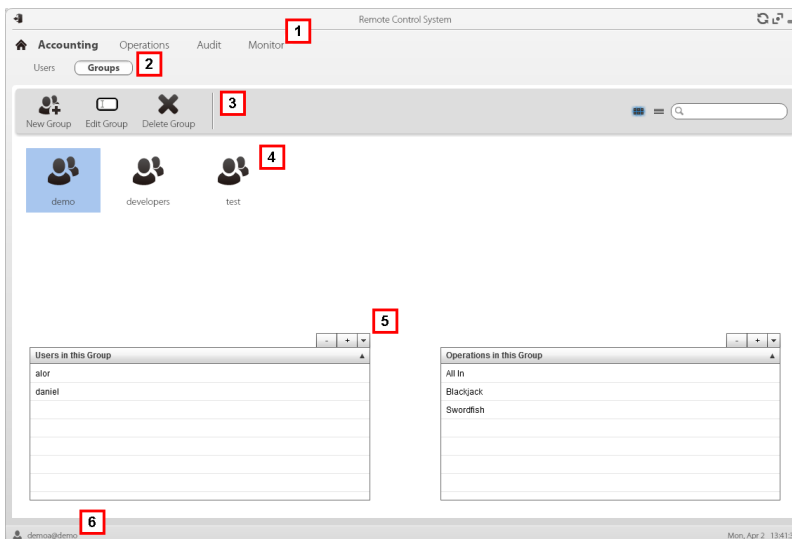
Tip: to simply and quickly group and manager users intended to receive RCS alarms, create an "alerting" group that contains all users to be alerted in the event of alarm without linking it to any operation. See "[User management](#)" on page 18



NOTE: the function is only enabled with **User and group administration** permissions.

What the function looks like




This is what the page looks like:



Area Description

- 1 RCS menu.
- 2 **Accounting** menu.

Area Description

- 3 Window toolbar. Descriptions are provided below:
 -  Adds a group.
 -  Edits the selected group.
 -  Deletes the selected group.
- 4 Group list.
- 5 Users and operation assigned to the selected group.
- 6 RCS status bar.

To learn more



For interface element descriptions see "[Shared interface elements and actions](#)" on page 9.

For more information on groups and users see "[What you should know about users and groups](#)".

Creating a group and linking users and operations

To create a new group:

Step Action

- 1 Click **New group**: enter a name to be assigned to the group.
- 2 Enter the required data and click **Save**: the new group is displayed in the main work area.
- 3 In the **Users in this Group** table, click  to add users to the group.
- 4 In the **Operations in this Group** table, click  to add operations to the group: the next time group users login, they will see the added operations in the list.



IMPORTANT: if an operation is linked to a user who is currently logged in, the user will only be able to view the operation the next time she/he logs in.



Editing group data and removing users and operations

To edit group data:

Step Action

- 1 Double-click a group.
- 2 Edit the name and click **Save**.

Step Action

- 3 In the **Users in this Group** table, click  to remove users from the group.
- 4 In the **Operations in this Group** table, click  to remove operations from the group: the next time group users login, they will no longer see the operations in the list.



IMPORTANT: if an operation is removed from a user who is currently logged in, the user will no longer view the operation the next time she/he logs in.

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	28
What you should know about targets	28
Operation management	29
Operation page	32

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.

Assigning the operation to a user group

To guarantee maximum data confidentiality, we recommend you only link an operation to the RCS users assigned to the investigation. Users not linked to the operation will not see any operation data or collected evidence. For this reason, the person who creates the operation must be part of at least one of the groups linked to the operation when created.

What happens when a new operation is created

When an operation is created it is already declared open thus operation targets can be created and the Technician can generate and install agents. When the operation is open, agents begin to collect data and send it to RCS.

What happens when an operation is closed

The operation must be closed when the investigation is closed, and it is certain that all agents have already transmitted all the collected evidence to the Backend.

Closing the operation automatically closes the targets and agents. When an agent is closed, uninstallation occurs at the first synchronization, leaving the device clean.

A closed operation cannot be re-opened. Only the operation data and collected evidence are left in the database.



CAUTION: *for infrequent synchronizations, for example, every four days, wait for the last planned synchronization before closing the operation.*

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.

Administrator tasks

The Administrator manages targets on the general organizational level; the Technician sets and works on targets according to the Administrator's instructions.

The Administrator is in charge of:

- creating a new target within an operation
- instruct the Technician on activation schedules and the types of evidence to be collected through a certain target's agents, based on the instructions received from legal authorities
- monitoring correct instruction application through Audits
- closing a target

What happens when a target is created

When a target is created it is already declared *open* and thus the Technician can be asked to generate and install agents.

What happens when a target is closed

A target can be closed, for example, when closing investigations for that target.

Closing a target automatically closes its agents. When an agent is closed, uninstallation occurs at the first synchronization, leaving the device clean.

A closed target cannot be re-opened. Only the target data and those sent by agents are left in the database.



CAUTION: *when a target is closed, all linked agents are automatically uninstalled. Only close a target when certain to have all the required data.*



CAUTION: *for infrequent synchronizations, for example, every four days, wait for the last planned synchronization before closing the target.*



Tip: only close the target when you are sure that agents have downloaded all the required information.

Opening and closing an operation

When an operation is closed, all of its targets are irreversibly closed and all their agents are uninstalled. See "[What you should know about operations](#)" on the previous page.

Operation management

To manage operations:

- Operations section

Purpose

This function lets you:

- create a new operation
- assign the operation to a user group



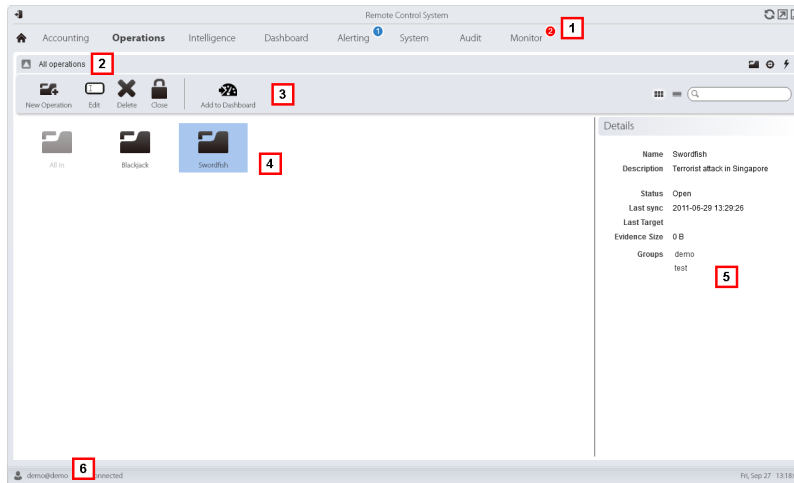
NOTE: the function is only enabled if the user has **Operation management** authorization.

Next steps







One or more targets must be linked to the operation. See "[Operation page](#)" on page 32.

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:
 -  Adds an operation.
 -  Edits the selected operation.
 -  Deletes the selected operation.
 -  Closes the operation.
- 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 9.


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

For more information on operations see "[What you should know about operations](#)" on page 28.

Creating an operation

To create a new operation:

Step Action

- 1 Click **New Operation**: data entry fields appear.
- 2 Select the group (or groups) to be assigned to the operation.
 NOTE: the user who is creating the operation must belong to at least one of the linked groups.
- 3 Enter the required data and click **Save**: the new operation appears in the main work area in Open status.

Editing operation data

To edit operation data:

Step Action

- 1 Select an operation and click **Edit**: its data appears.
- 2 Edit the required data and click **Save**.

Closing an operation

To close an operation and begin uninstalling agents on all targets:

Step Action

- 1 Select an operation and click **Closed**.
- 2 Confirm close: all targets are closed and agent uninstall is requested. Data is left available on the database.



CAUTION: closing an operation is irreversible see "[What you should know about operations](#)" on page 28

Deleting an operation

To delete an operation:

Step Action


- 1 Select an operation and click **Delete**.
- 2 Confirm the action by clicking **Yes**: operation data, targets, agents and all evidence is deleted from databases.



CAUTION: deleting an action is irreversible and all data linked to that operation is lost.

Operation data

Selected operation data is described below:

<i>Data</i>	<i>Description</i>
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	<p>Operation status and close command:</p> <p>Open: the operation is open. If targets were set and agents correctly installed, the RCS receives the collected evidence.</p> <p>Closed: the operation is closed and can not be re-opened. Agents no longer send data but evidence already received can still be viewed.</p> <p> CAUTION: closing an operation is irreversible. See "What you should know about operations" on page 28.</p>
Groups	<p>Groups that can see the operation.</p> <p>See "Group management" on page 24</p>

Operation page

To view an operation: | • [Operations](#) section, double-click an operation

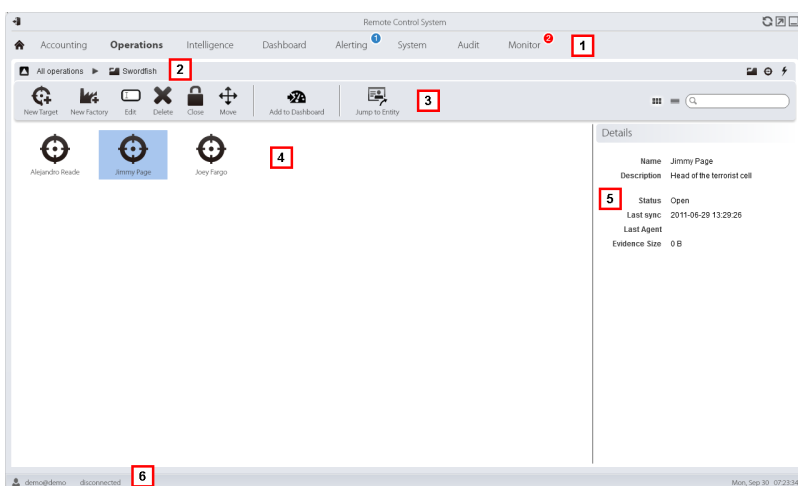
Purpose

This function lets you:

- create one or more targets to be monitored during an operation
- manage target activation/deactivation.

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:



Adds a target.



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



Edits the selected target.



Deletes the selected target.



Closes the target.



Moves the target to another operation.

- 4 Target list:



open target



closed target

- 5 Selected target data.
- 6 RCS status bar.

To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 9.

For more information on operations see "[What you should know about operations](#)" on page 28.

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

Creating a target

To create a new target:

Step Action

- 1 Click **New target**: data entry fields appear.
- 2 Enter the required data and click **Save**: the new target appears in the main work area in Open status, meaning it is ready to be used by a Technician.

Closing a target

To close a target and begin uninstalling its agents:

Step Action

- 1 Select a target and click **Close**.
- 2 Confirm close: the target is closed and agent uninstallation is automatically launched. Data is left available on the database.



CAUTION: closing a target is irreversible see "[What you should know about targets](#)" on page 28

Editing target data

To edit target data:

Step Action

- 1 Select a target and click **Edit**: its data appears.
- 2 Edit the required data and click **Save**.

Deleting a target

To delete a target:

Step Action



- 1 Select a target and click **Delete**.
- 2 Confirm the action by clicking **Yes**: target data, its agents and all evidence is deleted from databases.



CAUTION: deleting a target is irreversible and all data linked to that target will be lost.

Operation page data

Selected target data is described below:

Data	Description
Name	Target name.
Description	User's description
Status	Defines the target's status: <ul style="list-style-type: none"> Open. If the Technician correctly installs agents, RCS receives the collected evidence. Closed. Closed, it can no longer be opened.

Monitoring users

Presentation

Introduction

Monitoring RCS users guarantees correct investigations and the observance of rules and indications issued by any authority that requested the investigations.

Content

This section includes the following topics:

What you should know about user monitoring (Audit)	37
User monitoring (Audit)	38

What you should know about user monitoring (Audit)

What is user monitoring

The Audit is a list of actions taken by all Administrator, Technician and Analyst users in RCS. Its purpose is to guarantee correct investigations and the observance of rules and indications issued by any authority that requested the investigations.

This way, the Administrator can monitor system access by enabled users and trace special actions over time such as, for example, target creation.

How signaled actions are read

The Audit records all actions run on the system by each single user in a table.

Four pieces of information are always included in each action:

- action date-time,
- user that performed the action,
- action type,
- description of the action

The other fields are only populated according to the type of action. For example, if a user logs into the system, the Audit records the user's name in **Actor** and the "login" action type in **Action**.

If a Technician creates agents, an action appears in the list for each agent with the name of the user, the "target.create" type of action, the operation name, target name and agent's name.



NOTE: : audit records are not localized and only available in English.

Selecting specific actions using filters

The function normally displays actions performed in the last 24 hours. The filter on the **Date** column is thus the only filter that is always set by default but can be changed as needed. For this reason, the corresponding check box is always selected.

A filter can be set for all other columns to refine the search. If the check box next to the heading is selected, the filter on that column is active.

Each heading thus allows you to select which data should be displayed.

Only the **Description** column lets you enter part of the text to be searched, for example, if "log" is entered, all actions whose descriptions contain the text "log" will be displayed. For example:

- "User 'xxx' logged in"
- "Log file created"

Exportable data

RCS lets you export recorded actions for Administrators, Technicians and Analysts. The file will be downloaded to the RCS Download folder on the desktop.

User monitoring (Audit)

To monitor users:

- Audit section

Purpose

This function lets you monitor Administrator, Technician and Analyst actions in RCS. For example, you can monitor correct operation progress, target activation/deactivation schedules and the Technician's correct application of the types of agents authorized for a specific operation.

What you can do

You can select only the actions run in a certain period and apply filters to search, for example, for detailed information on specific operations or users. In the event of need, actions can always be exported in CSV format files.



IMPORTANT: if the page is kept open, it must be refreshed to view the most recent actions. See "[Homepage description](#)" on page 7



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

What the function looks like



This is what the page looks like:

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Date	Actor	Action	User	Group	Operation	Target	Agent	Description	
2012-04-02 13:10:16	admin	user.update						Updated 'privs' to [ADMIN, TECH, VIEW] for user 'test'	
2012-04-02 13:10:16	admin	user.update						Updated 'desc' to 'This is a test user' for user 'test'	
2012-04-02 13:10:16	alor	login						User 'alor' logged in	
2012-04-02 13:10:16	admin	user.update						Updated 'desc' to 'This is a test user' for user 'test'	
2012-04-02 13:10:16	admin	user.update						Updated 'contact' to 'ask@me.it' for user 'test'	
2012-04-02 13:10:16	alor	user.create						Created a new user 'disgruntled'	
2012-04-02 13:10:16	admin	user.update						Changed password for user 'test'	
2012-04-02 13:10:16	admin	user.update						Updated 'privs' to [ADMIN, TECH] for user 'admin'	
2012-04-02 13:10:16	alor	logout						User 'alor' logged out	

Area Description

- 1 RCS menu.

Area Description

- 2 Window toolbar. Descriptions are provided below:
 -  Exports displayed actions to a CSV format file (can be imported in Excel).
 -  Removes all filters applied to table data.
- 3 List of actions run by RCS users.
- 4 RCS status bar.

To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 9.

For a description of the data in this window see "[User monitoring data \(Audit\)](#)".

For more information on the audit see "[What you should know about user monitoring \(Audit\)](#)" on page 37.

Selecting actions in a time range

To only view actions in a certain time range:

Step Action

- 1 Click on the **Date** column heading.
- 2 Click on the required time range.



NOTE: the date filter is always on, set on actions in the last 24 hours. Only the criteria can be changed.

Selecting actions based on proposed data

To increase result accuracy:

Step Action

- 1 Click on one or more column headings: a search field appears where you can enter data.
- 2 Enter the word to be searched and press **Enter**. Information in the column will be filtered and ordered according to the entered search word.

Removing one or more filters

To remove a filter and display all data:

<i>If you want to remove...</i>	<i>Then...</i>
---------------------------------	----------------

a single filter	unselect the check box in the column heading.
------------------------	---

<i>If you want to remove...</i>	<i>Then...</i>
all filters simultaneously	click Remove filters .



NOTE: the date filter is always on, set on actions in the last 24 hours. Only the time criteria can be changed.

Exporting displayed actions

To export displayed actions:

Step Action

- 1 Click **Export**: data entry fields appear.
- 2 Enter the name of the file to be exported and click **OK**: a progress bar indicates operation progress. To check progress, click on the bar.

User monitoring data (Audit)

Audit table columns are described below:

<i>Column</i>	<i>Description</i>
Date	Action date-time.
Actor	Name of the logged in user that caused the action.
Action	Type of action run by the logged in user. The action is displayed as <i>individual.action</i> . For example "user.update" means that a user was updated. This makes selecting the same types of actions easier.
User	User concerned by the action, for example, created by an Administrator. It should not be confused with the name in Actor which is the user who caused the action.
Group	Group concerned by the action, for example, the group linked to an operation.
Operation	Operation concerned by the action, for example, the operation closed by an Administrator.
Target	Target concerned by the action, for example, the target closed by an Administrator.
Agent	Agent concerned by the action, for example, agent created by a Technician.
Description	Brief description of the action.



NOTE: all actions are displayed in English.

System monitoring

Presentation

Introduction

System monitoring guarantees constant control of component status and license usage.

Content

This section includes the following topics:

System monitoring (Monitor)	42
--	-----------

System monitoring (Monitor)

To monitor the system: • Monitor section

Purpose

This function lets you:

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



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

What the function looks like

This is what the page looks like:









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

Area Description

1 RCS menu.

Monitor¹: indicates the current number of system alarms triggered.

Area Description

- 2** Window toolbar.
Descriptions are provided below:
-  Defines the alerting group.
 -  NOTE: the function is only enabled with **User and group administration** permissions.
 -  Displays license status
 -  Loads a new license file.
 -  NOTE: the function is only enabled if the user has **License modification** authorization.
- 3** List of RCS components and their status:
-  Alarm (generates an e-mail sent to the alerting group)
 -  Warning
 -  Component running
- 4** RCS status bar.

To learn more

For interface element descriptions see "[Shared interface elements and actions](#)" on page 9.

For a description of the data in this window see "[System monitoring data \(Monitor\)](#)" on the next page.

Define the alerting group or temporarily enable/disable it

To select the alerting group:

Step Action

- 1** Click **Set alerting**.
- 2**
 - To turn off e-mail notifications, select **None**.

or

 - To enable notifications via e-mail to a group, select **Select a group to be alerted via e-mail** and the alerting group from the drop down menu. Each time a system alarm is triggered, the selected group will receive an e-mail with its description.
- 3** Click **Save**.











Tip: to simply and quickly group and manager users intended to receive RCS alarms, create an "alerting" group that contains all users to be alerted in the event of alarm without linking it to any operation. See "[User management](#)" on page 18

System monitoring data (Monitor)

System component monitoring data

System monitoring data is described below:


<i>Data</i>	<i>Description</i>
Type	Monitored component type and name.
Name	Some examples are provided below: <ul style="list-style-type: none">  Anonymizer  Carrier  Collector  Database  Network Controller
Address	Component's IP address.
Last contact	Last synchronization date-time.
Status	Component status at last synchronization: <ul style="list-style-type: none">  Alarm: the component is not running, contact the alerting group for immediate service.  Warning: the component signals a risky situation, contact the system administrator for necessary checks.  Component running.
CPU Proc	% CPU use by the single process.
CPU Host	% CPU use by server.
Free disk	% free disk space.

License monitoring data

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



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

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

Glossary

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

A

Accounting

Console section that manages RCS access.

acquisition sequence

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

Administrator

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

Agent

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

alert rules

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

Alerting

Console section that manages new evidence alerts.

alerting group

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

Analyst

Person in charge of analyzing the data collected during operations.

Anonymizer

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

Audit

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

B

back end

Environment designed to decrypt and save collected information. It includes Master Node and Shard databases.

BRAS

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

BSSID

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

C

Carrier

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

Collector

Collector Service: receives data sent by agents, via the Anonymizer chain.

console

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

D

Dashboard

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

DSLAM

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

E

Elite agent

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

entity

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

ESSID

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

evidence

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

evidence alerts

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

Exploit

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

F

factory

A template for agent configuration and compiling.

front end

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

G

Group

Intelligence entity that groups several entities.

I

injection rules

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

M

Monitor

Console section that monitors components and license status.

N

Network Controller

Collector Service: checks Network Injector and Anonymizer status and sends them new configurations and software updates.

Network Injector

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

Network Injector Appliance

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

O

operation

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

P

Person

Intelligence entity that represents a person involved in the investigation.

Position

Intelligence entity that represents a place involved in the investigation.

R

RCS

(Remote Control System) the product documented hereto.

RCS Console

Software designed to interact with the RCS Server.

RCS receiver

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

RCS sender

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

RCS Server

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

S

Scout agent

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

Soldier agent

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

SSH

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

System

Console section that manages the system.

System administrator

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

T

Tactical Network Injector

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

TAP

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

target

The physical person under investigation. It is represented by the Target entity in the intelligence section.

Technician

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

V

Virtual

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

VPS

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

W

WPA

(WiFi Protected Access) WiFi network protection.

WPA 2

(WiFi Protected Access) WiFi network protection.

]HackingTeam[

RCS 9.6 Administrator manual
Administrator manual 1.7 MAR-2013
© COPYRIGHT 2015
info@hackingteam.com

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