]HackingTeam[

RCS 9.4

The hacking suite for governmental interception

Manuale dell'amministratore

Proprietà delle informazioni

richieste di ulteriori copie di questo manuale o di informazioni tecniche sul prodotto, devono essere indirizzate a:

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

Sommario

Glossario dei termini

Di seguito i termini utilizzati in questo manuale e loro definizione.

A

Accounting
Sezione della console dedicata alla gestione degli accessi a RCS.

Agent
Sonde software installate sui dispositivi sotto monitoraggio. Progettate per raccogliere prove e comunicarle al Collector.

Agent elite
Agente installato su dispositivi sicuri. Permette di raccogliere tutti i tipi di evidence disponibili.

Agent scout
Sostituto dell'agent inviato sul dispositivo per verificarne il livello di sicurezza prima di installare gli agent veri e propri (elite o soldier).

Agent soldier
Agente installato su dispositivi non completamente sicuri. Permette di raccogliere solo alcuni tipi di evidence.

Alerting
Sezione della console dedicata alle segnalazioni di nuove prove.

Amministratore
Colui che abilita l'accesso al sistema agli utenti, crea i gruppi di lavoro e definisce le indagini in essere, gli obiettivi e il tipo di dati da raccogliere.

Amministratore di sistema
Colui che installa i server e le console, si occupa degli aggiornamenti software e del ripristino dei dati in caso di malfunzionamento.

Analista
Persona incaricata dell'analisi dei dati raccolti durante le indagini.

Anonymizer
(opzionale) Protegge il server da attacchi esterni e consente l'anonimato durante le operazioni di indagine. Trasferisce i dati degli agent ai Collector.

Audit
Sezione della console che riporta tutte le azioni degli utenti e del sistema. Utilizzata per controllare abusi di RCS.

avvisi da evidence
Avvisi, normalmente email, inviati agli analisti per avvisarli che una nuova evidence corrisponde alle regole impostate.

B

back end
Ambiente destinato alla decodifica e salvataggio delle informazioni raccolte. Include il Master Node e i database Shard.

BRAS
(Broadband Remote Access Server) instrada il traffico da/a DSLAM verso la rete dell'ISP e fornisce l'autenticazione per gli iscritti dell'ISP.

BSSID
(Basic Service Set IDentifier) Identificativo dell'Access Point e dei suoi client.

C

Carrier
Servizio del Collector: invia i dati ricevuti dagli Anonymizer agli shard o al Master Node.

Collector
Servizio del Collector: riceve i dati inviati dagli agent, tramite la catena di Anonymizer.

console
Computer su cui è installato RCS Console. Accede direttamente a RCS Server o al Master Node.

D

Dashboard
Sezione della console dedicata all'Analista. Usata per avere una rapida panoramica dello stato delle investigazioni, dei target e degli agent più importanti.

DSLAM
(Digital Subscriber Line Access Multiplexer) apparato di rete, spesso collocato negli scambi telefonici dell'operatore telefonico. Connette più interfacce DSL a un canale di comunicazione digitale ad alta velocità usando le tecniche di multiplexing.

E

entità
Insieme di informazioni di intelligence associate al target e a persone e luoghi coinvolti nell'indagine.

ESSID
(Extended Service Set IDentifier) Conosciuto anche come SSID, identifica la rete WiFi.

evidence
Dati delle prove raccolti. Il formato dipende dal tipo di evidence (es.: immagine).

Exploit
Codice che, sfruttando un bug o una vulnerabilità, porta all'esecuzione di codice non previsto. Utilizzato per infettare i dispositivi dei target.

F

factory
Un modello per la configurazione e la compilazione di agent.

front end
Ambiente destinato a comunicare con gli agent per raccogliere informazioni e impostare la loro configurazione. Include i Collector.

G

Gruppo
Entità di intelligence che raggruppa più entità.

gruppo di alerting
Raggruppa gli utenti che devono ricevere notifiche via mail ogni volta che si genera un allarme di sistema (per esempio, il database ha superato il limite di spazio libero disponibile). Normalmente, questo gruppo è associato a nessuna operation.

M

Monitor
Sezione della console dedicata alle segnalazioni degli stati dei componenti e delle licenze.

N

Network Controller
Servizio del Collector: controlla lo stato dei Network Injector e degli Anonymizer, spedendo loro le nuove configurazioni o aggiornamenti software.

Network Injector
Componente hardware che controlla il traffico di rete del target e inietta un agent nelle risorse Web selezionate. Fornito in due versioni, Appliance o Tactical: Appliance è per installazioni presso ISP, mentre Tactical è utilizzato sul campo.

Network Injector Appliance
Versione rack di Network Injector, per l'installazione presso l'ISP. Cfr.: Tactical Network Injector.

O

operation
Investigazione verso uno o più target, i cui dispositivi saranno i destinatari degli agent.

P

Person
Entità di intelligence che rappresenta una persona coinvolta in un'indagine.

Position
Entità di intelligence che rappresenta un luogo coinvolto in un'indagine.

R

RCS
(Remote Control System) il prodotto oggetto di questo manuale.

RCS Console
Software dedicato all'interazione con RCS Server.

RCS mittente
Sistema RCS che riceve le evidence dagli agent e li trasferisce ad altri sistemi RCS riceventi (vedi) tramite le regole di connessione. È un sistema RCS completo.

RCS ricevente
Sistema RCS che riceve le evidence da un altro sistema RCS mittente (vedi) e non direttamente dagli agent. Rispetto a RCS nella sua forma completa, RCS ricevente offre solo le funzioni per elaborare le evidence.

RCS Server
Una o più macchine, in base all'architettura di installazione, dove sono installati i componenti alla base di RCS: i database Shard, i Network Controller e Collector.

regole di alert
Regole che creano alert quando una nuova evidence viene salvata o quando l'agent sincronizza per la prima volta.

regole di injection
Impostazioni che definiscono come identificare traffico HTTP, quale risorsa da infettare e quale metodo usare per l'infezione.

S

sequenze di acquisizione
Insieme di eventi, azioni e moduli di acquisizione complessi che costituiscono la configurazione avanzata di un agent.

SSH
(Secure SHell) protocollo di rete per sessioni remote cifrate, servizi remoti o esecuzioni comandi.

System
Sezione della console dedicata alla gestione del sistema.

T

Tactical Network Injector
Versione portatile di Network Injector, per utilizzo tattico. Cfr.: Network Injector Appliance.

TAP
(Test Access Port) dispositivo hardware inserito in reti informatiche che permette il monitoraggio passivo del flusso dati in transito.

target
La persona fisica sotto investigazione. Nella sezione intelligence è rappresentata dall'entità Target.

Tecnico
Colui che su mandato dell'Amministratore crea e gestisce gli agent.

V

Virtual
Entità di intelligence che rappresenta un luogo virtuale (es. un sito web) coinvolto in un'indagine.

VPS
(Virtual Private Server) server remoto su cui installare l'Anonymizer. Normalmente disponibile a noleggio.

W

WPA

(WiFi Protected Access) Protezione per le reti WiFi.

WPA 2

(WiFi Protected Access) Protezione per le reti WiFi.

1

Introduzione a questa Guida

Presentazione

Obiettivi del manuale

Questo manuale guida l'*Amministratore* a utilizzare RCS Console per:

- creare gli utenti e i gruppi di lavoro
- aprire e chiudere indagini
- fare il monitoraggio degli utenti di RCS
- fare il monitoraggio del sistema

Di seguito sono presentate le informazioni necessarie alla consultazione del manuale.

Contenuti

Questa sezione include i seguenti argomenti:

Novità della guida

Elenco note di rilascio e aggiornamenti di questa guida in linea.

Data rilascio	*Codice*	*Versione software*	*Descrizione*
20 Settembre 2014	Manuale dell'amministratore -	9.4	Nessun aggiornamento alla documentazione.
23 Giugno 2014	Manuale dell'amministratore -	9.3	Nessun aggiornamento alla documentazione.
19 Febbraio 2014	Manuale dell'amministratore -	9.2	Nessun aggiornamento alla documentazione.
30 Settembre 2013	Manuale dell'amministratore 1.4 SET - 2013	9	Aggiornata documentazione per migliorie apportate all'interfaccia utente. Migliorato sommario.

Documentazione fornita

A corredo del software RCS sono forniti i seguenti manuali:

Manuale	*Destinatari*	*Codice*	*Formato di distribuzione*
Manuale dell'amministratore di sistema	Amministratore di sistema	Manuale dell'amministratore di sistema 1.7 SET-2014	PDF
Manuale dell'amministratore (questo manuale)	Amministratori	Manuale dell'amministratore 1.5 SET-2014	PDF
Manuale del tecnico	Tecnici	Manuale del tecnico 1.8 SET-2014	PDF
Manuale dell'analista	Analisti	Manuale dell'analista 1.7 SET-2014	PDF

Convenzioni tipografiche per le segnalazioni

Di seguito le segnalazioni previste in questo documento (Microsoft Manual of Style):

AVVERTENZA: indica una situazione rischiosa che se non evitata, può causare danni fisici all'utente o alle attrezzature.

PRUDENZA: indica una situazione rischiosa che se non evitata, può causare la perdita di dati.

IMPORTANTE: offre indicazioni essenziali al completamento del compito. Mentre le note possono essere trascurate e non inficiano il completamento del compito, le indicazioni importanti non devono essere trascurate.

NOTA: informazioni neutre e positive che enfatizzano o aggiungono informazioni a dei punti nel testo principale. Fornisce informazioni che possono essere applicate solo in casi speciali.

Suggerimento: consiglia l'utente nell'applicare le tecniche e le procedure descritte nel testo ai loro bisogni specifici. Può suggerire un metodo alternativo e non è fondamentale alla comprensione del testo.

Richiede assistenza: l'operazione può essere portata a termine solo su indicazioni dell'assistenza tecnica.

Convenzioni tipografiche per la formattazione

Di seguito la legenda di alcune convenzioni tipografiche:

Esempio	***Stile***	***Descrizione***
*Vedi "**Dati degli utenti**"*	*corsivo*	indica il titolo di un capitolo, una sezione, una sottosezione, un paragrafo, una tabella o una figura di questo manuale, o di un'altra pubblicazione di riferimento.
<ggmmaaaa>	<aaa>	indica un testo che dovrà essere specificato dall'utente secondo una certa sintassi. Nell'esempio <ggmmaaaa> è una data e può diventare "14072011".
Selezionare uno dei server elencati **[2]**.	**[x]**	indica l'oggetto citato nel testo e che compare nell'immagine adiacente.

Esempio	*Stile*	*Descrizione*
Fare clic su **Add**. Selezionare il menu **File, Save data.**	**grassetto**	indica una scritta sull'interfaccia operatore, sia di un elemento grafico (es.: tabella, scheda) sia di un pulsante a video.
Premere Enter	prima lettera maiuscola	indica il nome di un tasto della tastiera.
Cfr.: Network Injector Appliance	-	suggerisce di confrontare la definizione di un termine in glossario o contenuto con altro termine o contenuto.

Destinatari del prodotto e di questa guida

Di seguito le figure professionali che interagiscono con RCS.

Destinatario	*Attività*	*Competenze*
Amministratore di sistema	Segue le indicazioni dell'assistenza HackingTeam fornite in fase contrattuale. Installa e aggiorna i server RCS, i Network Injector e le RCS Console. Programma e gestisce i backup. Ripristina i backup in caso di sostituzione dei server.  **AVVERTENZA: l'amministratore di sistema deve avere tutte le competenze necessarie richieste. HackingTeam non si assume alcuna responsabilità di malfunzionamenti o danni alle attrezzature arrecati da una installazione non professionale.**	Tecnico di reti esperto
Amministratore	Crea gli account e i gruppi autorizzati. Crea operation e target. Controlla lo stato del sistema e delle licenze.	Responsabile dell'indagine
Tecnico	Crea gli agent e li configura. Configura le regole di un Network Injector.	Tecnico specializzato in intercettazioni
Analista	Analizza le evidence e le esporta.	Operativo

Dati di identificazione dell'autore del software

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 Console per l'Amministratore

Presentazione

Introduzione

RCS (Remote Control System) è una soluzione a supporto delle investigazioni che intercetta attivamente e passivamente dati e informazioni dai dispositivi dei bersagli di tali investigazioni. RCS infatti crea, configura e installa nell'assoluto anonimato degli agenti software che raccolgono dati e informazioni e inviano i risultati al database centrale per la decodifica e il salvataggio.

Ruolo dell'Amministratore

Il ruolo dell'*Amministratore* è:

- gestire l'accesso al sistema attribuendo ai diversi utenti i ruoli previsti dall'applicazione
- aprire e chiudere le indagini
- definire i target coinvolti
- indicare all'utente *Tecnico* i tipi di prove da intercettare
- controllare le azioni svolte dagli utenti
- controllare le licenze disponibili per i componenti di RCS

Funzioni abilitate per l'Amministratore

Per completare le attività che gli competono, l'Amministratore ha accesso alle seguenti funzioni:

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

Contenuti

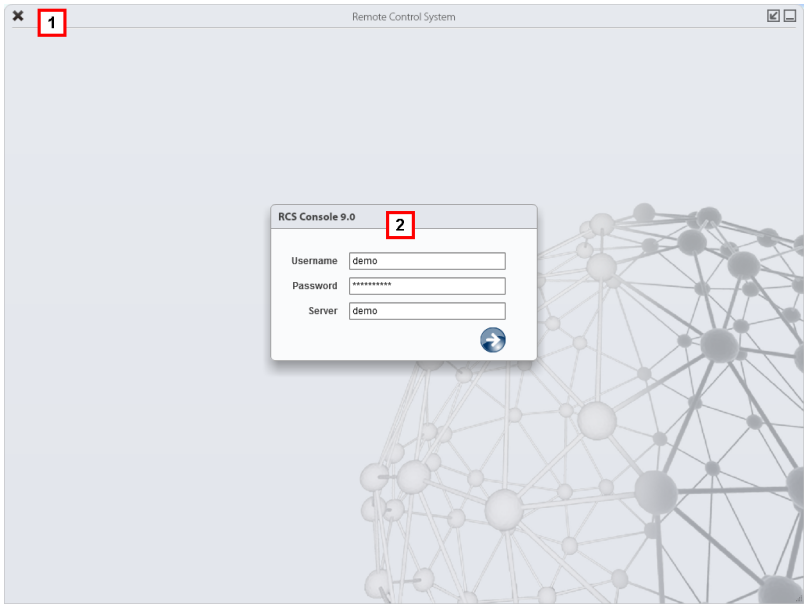
Questa sezione include i seguenti argomenti:

Avvio di RCS Console

All'avvio, RCS Console chiede di inserire le proprie credenziali precedentemente impostate dall'Amministratore.

Come si presenta la pagina di login

Ecco come viene visualizzata la pagina di login:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Chiusura di RCS Console. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	Finestra di dialogo per inserimento delle proprie credenziali.

Accedere a RCS Console

Per accedere alle funzioni di RCS Console:

Passo	*Azione*
1	In **Username** e **Password** inserire le credenziali come assegnate dall'Amministratore.
2	In **Server** inserire il nome della macchina o l'indirizzo del server cui ci si vuole collegare.
3	Fare clic su  : si presenta l'homepage con i menu abilitati in base ai privilegi del proprio account. *Vedi "**Descrizione della homepage**" nel seguito .*

Descrizione della homepage

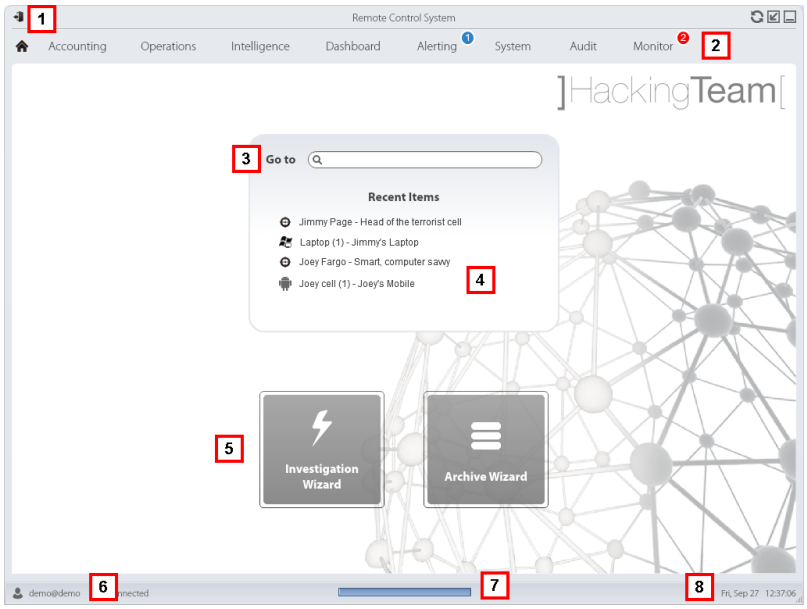
Per visualizzare l'homepage:	• fare clic su 

Introduzione

RCS Console presenta all'avvio questa homepage, unica per tutti gli utenti. I menu abilitati dipendono dai ruoli assegnati al proprio account.

Come si presenta

Ecco come viene visualizzata l'homepage con già presente una cronologia degli argomenti recenti. Per il dettaglio degli elementi e le azioni comuni:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando.
2	Menu di RCS con le funzioni abilitate per l'utente.
3	Casella di ricerca per cercare tra i nomi di operation, target, agent ed entità, per nome o descrizione.
4	Collegamenti agli ultimi cinque elementi aperti (operation della sezione **Operations**, operation della sezione **Intelligence**, target, agent ed entità).
5	Pulsanti per avvio dei wizard.
6	Utente connesso con la possibilità di cambiare la lingua e la password.
7	Area download con possibilità durante una esportazione o una compilazione di vedere lo stato di avanzamento.
8	Data e ora attuale con la possibilità di cambiare il fuso orario.

Descrizione dei wizard da homepage

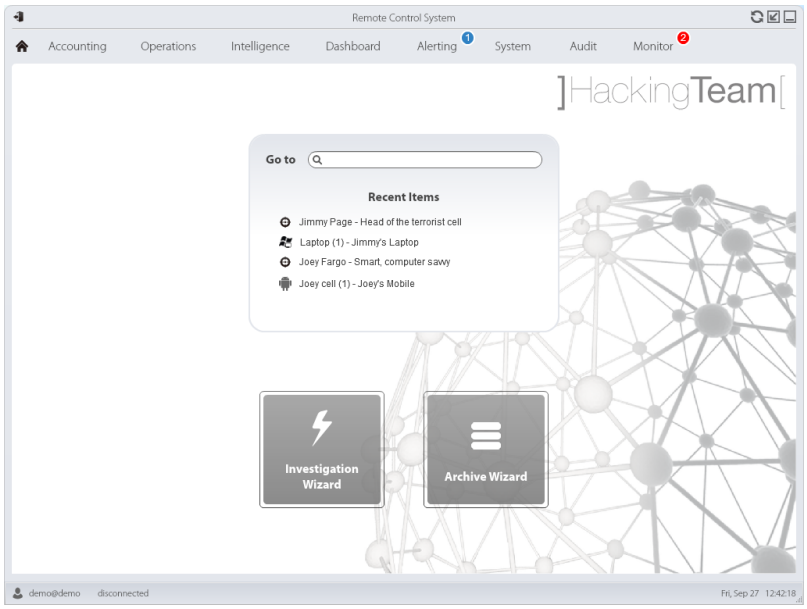
Per visualizzare l'homepage:	• fare clic su 

Introduzione

Per utenti con certi privilegi RCS Console presenta dei pulsanti che attivano dei wizard.

Come si presenta

Ecco come viene visualizzata l'homepage con i wizard abilitati:



Pulsante	*Funzione*
	Apre il wizard per la creazione rapida di un agent.  NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Tecnico.
	Apre il wizard per l'archiviazione rapida dei dati di operation e target.  NOTA: pulsante abilitato solo per utenti con privilegi di Amministratore e di Amministratore di sistema.

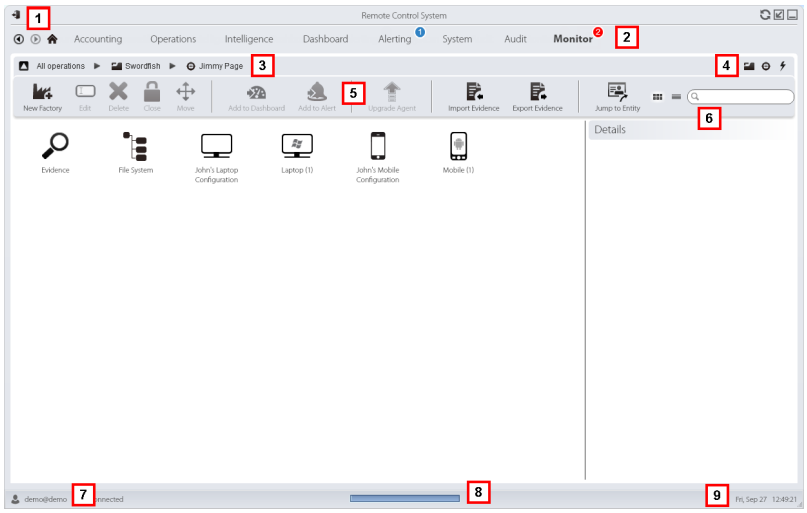
Elementi e azioni comuni dell'interfaccia

Ogni pagina del programma utilizza elementi comuni e permette azioni simili tra loro.

Per facilitare la consultazione di questo manuale, sono stati descritti in questo capitolo elementi e azioni comuni ad alcune funzioni.

Come si presenta RCS Console

Ecco come viene visualizzata una pagina tipica di RCS Console. In questo esempio mostriamo la pagina di un target:



Area	*Descrizione*
1	Barra del titolo con pulsanti di comando: Logout da RCS. Pulsante di aggiornamento della pagina. Pulsante di ingrandimento della finestra. Pulsante di riduzione a icona della finestra.
2	• Pulsante per tornare indietro nella cronologia di navigazione • Pulsante per andare avanti nella cronologia di navigazione • Pulsante per tornare alla homepage • Menu di RCS con le funzioni abilitate per l'utente

Area	*Descrizione*
3	Barra di navigazione per l'operation. Di seguito la descrizione:

Icona	*Descrizione*
	Torna al livello superiore.
	Mostra la pagina dell'operation (sezione **Operations**).
	Mostra la pagina del target.
	Mostra la pagina della factory.
	Mostra la pagina dell'agent.
	Mostra la pagina dell'operation (sezione **Intelligence**).
	Mostra la pagina dell'entità.

4	Pulsanti per visualizzare tutti gli elementi indipendentemente dalla loro appartenenza. Di seguito la descrizione:

Icona	*Descrizione*
	Mostra tutte le operation.
	Mostra tutti i target.
	Mostra tutti gli agent.
	Mostra tutte le entità.

5	Barre con i pulsanti della finestra.
6	Pulsanti e casella di ricerca:

Oggetto	*Descrizione*
	Casella di ricerca. Inserendo parte del nome compare l'elenco degli elementi che contengono le lettere inserite.
	Visualizza gli elementi in una tabella.
	Visualizza gli elementi come icone.

7	Utente connesso con possibilità di cambiare la lingua e la password.

Area	*Descrizione*
8	Area download con possibilità durante una esportazione o una compilazione di vedere lo stato di avanzamento. I file sono scaricati sul desktop nella cartella RCS Download. • Barra superiore: percentuale di generazione sul server. • Barra inferiore: percentuale di download dal server su RCS Console.
9	Data e ora attuale con la possibilità di cambiare il fuso orario.

Azioni sempre disponibili sull'interfaccia

Cambiare la lingua dell'interfaccia o la propria password

Per cambiare la lingua dell'interfaccia o la propria password:

Passo	*Azione*
1	Fare clic su **[7]**: compare una finestra di dialogo con i dati dell'utente.
2	Cambiare lingua o password e fare clic su **Salva** per confermare e uscire.

Convertire le date-ora di RCS Console al proprio fuso orario

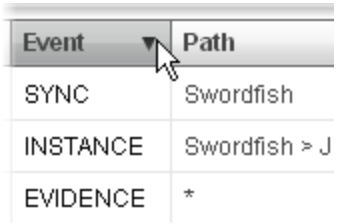
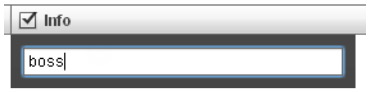
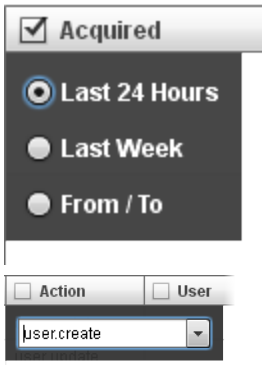
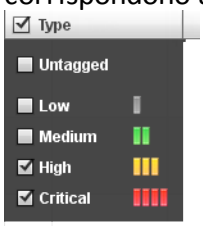
Per convertire tutte le date-ora al proprio fuso orario:

Passo	*Azione*
1	Fare clic su **[9]**: compare una finestra di dialogo con la data-ora attuale. **Ora UTC**: data-ora di Greenwitch (GMT) **Ora Locale**: data-ora dove è installato il server RCS **Ora Console**: data-ora della console da cui si sta lavorando e che può essere convertita
2	Cambiare il fuso orario e fare clic su **Salva** per confermare e uscire: tutte le date-ora visualizzate sono convertite come richiesto.

Azioni sulle tabelle

RCS Console mostra diversi dati in forma di tabella. Le tabelle permettono di:

- ordinare i dati per colonna in ordine crescente/decrescente
- filtrare i dati per ogni colonna

Azione	*Descrizione*
Ordinare per colonna	Fare clic sull'intestazione per ottenere l'ordine per quella colonna, crescente o decrescente. 
Filtrare un testo	Inserire parte del testo che si sta cercando: compaiono solo gli elementi che contengono il testo digitato.  L'esempio mostra elementi con descrizioni tipo: • "my**boss**" • "**boss**anova"
Filtrare in base a una opzione	Selezionare una opzione: compaiono gli elementi che corrispondono all'opzione scelta. 
Filtrare in base a più opzioni	Selezionare una o più opzioni: compaiono gli elementi che corrispondono a tutte le opzioni scelte. 
Cambiare la dimensione delle colonne	Selezionare il bordo della colonna e trascinarlo.

Procedure dell'Amministratore

Introduzione

Di seguito le procedure tipiche dell'Amministratore con un rimando ai capitoli interessati.

Procedure

Predisporre RCS all'uso di altri utenti

Di seguito le procedure tipiche per predisporre RCS all'uso da parte di altre persone:

Passo	*Azione*
1	Nella sezione **Accounting**, **Utenti** definire le persone che avranno accesso a RCS. *Vedi "**Gestione degli utenti**" a pagina 19*
2	Nella sezione **Accounting, Gruppi** creare un gruppo di utenti (tipicamente composto da amministratori di sistema, non associati ad alcuna operation) cui destinare le e-mail di segnalazione di sistema in allarme. *Vedi "**Gestione dei gruppi**" a pagina 26*
3	Nella sezione **Monitor** selezionare il gruppo destinato a ricevere e-mail di segnalazione di sistema in allarme. *Vedi "**Monitoraggio del sistema (Monitor)**" a pagina 46*

Aprire un'indagine

Di seguito le procedure tipiche per aprire un'indagine:

Passo	*Azione*
1	Nella sezione **Accounting**, **Utenti** definire le persone che faranno parte della squadra coinvolta nell'indagine e i loro ruoli. *Vedi "**Gestione degli utenti**" a pagina 19*
2	Nella sezione **Accounting**, **Gruppi** definire la squadra abilitata a vedere i dati dell'indagine e a ricevere gli allarmi di sistema. *Vedi "**Gestione dei gruppi**" a pagina 26*
3	Nella sezione **Operations** aprire l'indagine e associarvi uno o più gruppi. *Vedi "**Gestione delle operation**" a pagina 32 e "**Pagina dell'operation**" a pagina 35*

Passo	Azione
4	Comunicare al Tecnico di RCS i tipi di prove da raccogliere.
5	Nella sezione **Audit** controllare l'accesso al sistema da parte della squadra e verificare le loro azioni. *Vedi "**Monitoraggio utenti (Audit)**" a pagina 41*

Chiudere un'indagine

Di seguito la procedura tipica per chiudere un'indagine:

Passo	Azione
1	Nella sezione **Operations** chiudere l'indagine. *Vedi "**Gestione delle operation**"*
2	Se necessario richiedere all'Amministratore di sistema il salvataggio delle evidence in un Backup.

Monitorare il sistema

Di seguito le procedure tipiche per monitorare l'utilizzo di RCS:

Passo	Azione
1	Nella sezione **Monitor** controllare eventuali segnalazioni del sistema e le licenze utilizzate. *Vedi "**Monitoraggio del sistema (Monitor)**" a pagina 46*
2	Nella sezione **Audit** controllare le azioni compiute da Tecnici, Analisti e altri Amministratori. *Vedi "**Monitoraggio utenti (Audit)**" a pagina 41*

3

Gestione dell'accesso a RCS

Presentazione

Introduzione

La gestione degli utenti e dei gruppi è fondamentale per garantire la riservatezza e la sicurezza dei dati.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere su utenti e gruppi

Introduzione

Per garantire la massima riservatezza e sicurezza dei dati RCS offre all'Amministratore la possibilità di assegnare privilegi di accesso a ogni suo utente e raccogliere gli utenti in gruppi di lavoro cui affidare specifiche operation. La struttura si adatta sia alle realtà dove i compiti sono molto frammentati sia alle realtà dove tutti i compiti ricadono su poche persone.

Con la gestione degli utenti l'Amministratore può inoltre disconnettere rapidamente un utente sospetto e disabilitarlo temporaneamente dall'accesso a RCS.

Privilegi di accesso

RCS è stato progettato per garantire la massima sicurezza dei server e dei dati raccolti. Per raggiungere questo obiettivo sono stati definiti quattro ruoli distinti che corrispondono tipicamente alle figure professionali che possono accedere al sistema:

- Amministratore di sistema: responsabile esclusivo dell'installazione hardware e software e dei backup
- Amministratore: responsabile di tutti gli accessi al sistema, delle indagini e degli obiettivi dell'indagine
- Tecnico: responsabile della configurazione e dell'installazione degli agent di intercettazione
- Analista: responsabile dell'analisi dei dati

Suggerimento: a un utente è possibile assegnare più ruoli, per esempio un Amministratore può anche avere i privilegi del Tecnico.

Funzioni abilitate per il singolo ruolo

Di seguito l'elenco delle funzioni di RCS il cui accesso è previsto solo per gli utenti in possesso di quel ruolo:

Ruolo	*Funzioni abilitate*
Amministratore di sistema	• System • Monitor
Amministratore	• Accounting • Operations • Audit • Monitor

Ruolo	*Funzioni abilitate*
Tecnico	• Operations • System
Analista	• Operations • Intelligence • Dashboard • Alerting

Gruppi di utenti per ogni operation

I gruppi permettono di raggruppare più utenti per assegnare loro operation specifiche. In questo modo è possibile gestire più operation contemporaneamente garantendo la massima riservatezza dei dati tra i gruppi di lavoro.

Vedi "Gestione delle operation" a pagina 32

IMPORTANTE: le assegnazioni delle operation a un gruppo di lavoro saranno effettive alla successiva login dell'utente che appartiene al gruppo.

Gruppi di utenti per avvisi su allarmi di sistema

È possibile creare un gruppo di utenti esclusivamente destinato a ricevere una e-mail nel caso di allarmi di sistema.

In questo modo è possibile garantire interventi rapidi degli Amministratori di sistema in caso di malfunzionamenti gravi.

Vedi "Monitoraggio del sistema (Monitor)" a pagina 46

Gestione degli utenti

Per gestire gli utenti:	• **sezione Accounting, Utenti**

Scopo

Questa funzione permette di:

- registrare un utente e permettergli l'accesso a determinate funzioni di RCS. Da quel momento l'utente potrà collegarsi e vedere le funzioni in base ai ruoli assegnati
- disabilitare temporaneamente l'utente all'accesso, per esempio in caso di assenza prolungata
- disconnettere immediatamente l'utente da RCS, per esempio in caso di sospetto di accesso illegale a RCS

- controllare la data-ora e l'indirizzo IP dell'ultima connessione dell'utente a RCS e altri suoi dati

Suggerimento: per bloccare un utente e impedirgli un qualsiasi accesso a RCS si suggerisce di disconnetterlo immediatamente (se è connesso) e subito disabilitarlo.

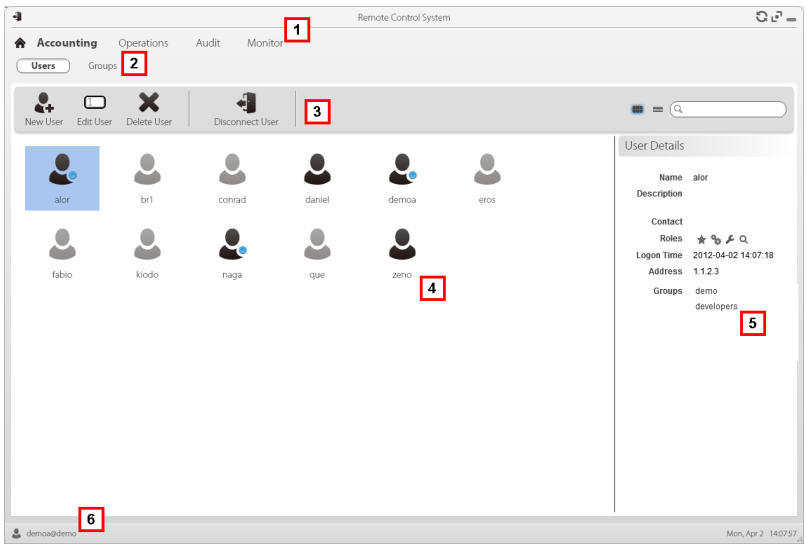
NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione utenti e gruppi**.

Passi successivi

È possibile associare più utenti a un gruppo di lavoro, per assegnare loro solo specifiche operation o per destinare eventuali allarmi di sistema. *Vedi "Gestione dei gruppi" a pagina 26* .

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **Accounting.**

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge un utente.
	Modifica l'utente selezionato.
	Elimina l'utente selezionato.
	Disconnette l'utente selezionato.

4	Area di lavoro principale con elenco degli utenti registrati:  Utente registrato e connesso attualmente a RCS.  Utente registrato ma non connesso attualmente a RCS.  Utente registrato ma non abilitato al login. L'utente non può avere accesso a RCS.
5	Dati dell'utente selezionato.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati degli utenti**" a pagina 23* .

Per saperne di più sugli utenti e gruppi *vedi "**Cose da sapere su utenti e gruppi**" a pagina 18* .

Registrare e abilitare un utente all'accesso a RCS

Per registrare un nuovo utente:

Passo	*Azione*
1	Fare clic su **Nuovo utente**: compaiono i dati da compilare.
2	Compilare i dati richiesti e assicurarsi che la casella **Abilitato** sia selezionata se si desidera che l'utente possa già accedere a RCS.
3	Fare clic su **Salva**: nell'area di lavoro principale compare il nuovo utente con l'icona  .

Abilitare/disabilitare un utente

Per abilitare o disabilitare un utente ad accedere a RCS:

Passo	*Azione*
1	Fare doppio clic su un utente: compaiono i suoi dati.
2	Fare clic su **Abilitato** per abilitare o disabilitare.
3	Fare clic su **Salva**: nell'area di lavoro principale il nuovo utente compare con l'icona  (abilitato) o  (disabilitato).  **IMPORTANTE: se l'utente è connesso continuerà a lavorare ma il successivo accesso gli sarà negato. Per disconnettere l'utente *vedi "Disconnettere un utente immediatamente" nel seguito* .**

Disconnettere un utente immediatamente

Per disconnettere immediatamente un utente connesso:

Passo	*Azione*
1	Fare clic su un utente  e fare clic su **Disconnetti Utente**: nell'area di lavoro principale l'utente compare con l'icona  .  **IMPORTANTE: se l'utente è connesso verrà immediatamente disconnesso. Ma il successivo accesso gli sarà permesso a meno che non lo si disabiliti. Per disabilitarlo*vedi "Abilitare/disabilitare un utente" in precedenza* .**

Modificare i dati di un utente

Per modificare i dati di un utente:

Passo	*Azione*
1	Fare doppio clic su un utente: compaiono i suoi dati.
2	Modificare i dati e fare clic su **Salva**: i dati vengono considerati a partire da successive login o da successivi messaggi di avviso.

Dati degli utenti

Di seguito la descrizione dei dati dell'utente selezionato:

Dato	*Descrizione*
Abilitato	Selezionare per abilitare l'utente alla connessione a RCS. Non selezionare per lasciare l'utente registrato, ma non permettergli l'accesso a RCS.
Nome	Nome utilizzato per accedere a RCS.
Descrizione	Descrizione libera.
E-mail	E-mail dell'utente.  **IMPORTANTE: se l'utente ha i privilegi di Analista questa è l'e-mail dove l'utente riceverà gli avvisi delle evidence. L'e-mail non può essere cambiata dall'utente.**
Password	Password dell'utente. L'utente potrà successivamente modificarla dalla barra di stato.
Ruoli	Privilegi assegnati all'utente:  Amministratore di sistema  Amministratore  Tecnico  Analista Per la descrizione dettagliata dei privilegi *vedi "**Dati dei privilegi**" alla pagina successiva*
Permessi avanzati	Apre la finestra per l'attribuzione delle autorizzazioni per ogni privilegio. Per la descrizione dettagliata delle autorizzazioni *vedi "**Dati dei privilegi**" alla pagina successiva*

Dato	*Descrizione*
Lingua	Lingua dell'interfaccia di RCS Console. L'utente potrà successivamente modificarla dalla barra di stato.
Fuso Orario Console	Fuso orario per la rappresentazione degli orari in RCS Console.
Gruppi	Gruppi cui appartiene l'utente. L'utente potrà vedere solo le operazioni assegnate al gruppo.

Dati dei privilegi

Autorizzazioni dell'Amministratore

Di seguito la descrizione delle autorizzazioni assegnate all'utente con il ruolo di Amministratore:

Dato	*Descrizione*
Gestione utenti e gruppi	Abilita la sezione **Accounting**.  NOTA: chi possiede questa autorizzazione può cambiare le proprie autorizzazioni e quelle altrui.
Gestione operation	Abilita alla gestione delle operation.
Gestione target	Abilita alla gestione dei target.
Gestione Audit	Abilita la sezione **Audit**.
Modifica della licenza	Permette di aggiornare la licenza.

Autorizzazioni dell'Amministratore di sistema

Di seguito la descrizione delle autorizzazioni assegnate all'utente con il ruolo di Amministratore di sistema:

Dato	*Descrizione*
Gestione Frontend	Abilita la sezione **System, Frontend**.
Gestione Backend	Abilita la sezione **System, Backend**.
Backup e ripristino sistema	Abilita la sezione **System, Backup**.

Dato	*Descrizione*
Gestione Network Injector	Abilita la sezione **System, Network Injector**.
Gestione connettori	Abilita la sezione **Connettori.**

Autorizzazioni del Tecnico

Di seguito la descrizione delle autorizzazioni assegnate all'utente con il ruolo di Tecnico:

Dato	*Descrizione*
Creazione factory	Permette di creare le factory e configurarle.
Creazione vettori di infezione	Permette di compilare i vettori di installazione.
Configurazione agent	Permette di modificare la configurazione degli agent.
Esecuzione comandi su agent	Permette di eseguire dei comandi sugli agent.
Upload file verso agent	Permette di inviare file agli agent.
Importazione evidence	Permette di importare le evidence.
Gestione regole Network Injector	Permette di aggiungere regole per i Network Injector.

Autorizzazioni dell'Analista

Di seguito la descrizione delle autorizzazioni assegnate all'utente con il ruolo di Analista:

Dato	*Descrizione*
Creazione alert	Permette di creare le regole di alert.
Esplorazione file system agent	Permette di esaminare il file system dell'agent.
Modifica evidence	Permette di assegnare alle evidence le priorità e di aggiungere note.
Cancellazione evidence	Permette di eliminare le evidence.  NOTA: questa autorizzazione non è mai abilitata di default perché sottoposta a licenza d'uso.
Esportazione evidence	Permette di esportare le evidence.
Gestione entità	Permette di gestire le entità di intelligence.

Gestione dei gruppi

Per gestire i gruppi:	• **sezione Accounting, Gruppi**

Scopo

Questa funzione permette di:

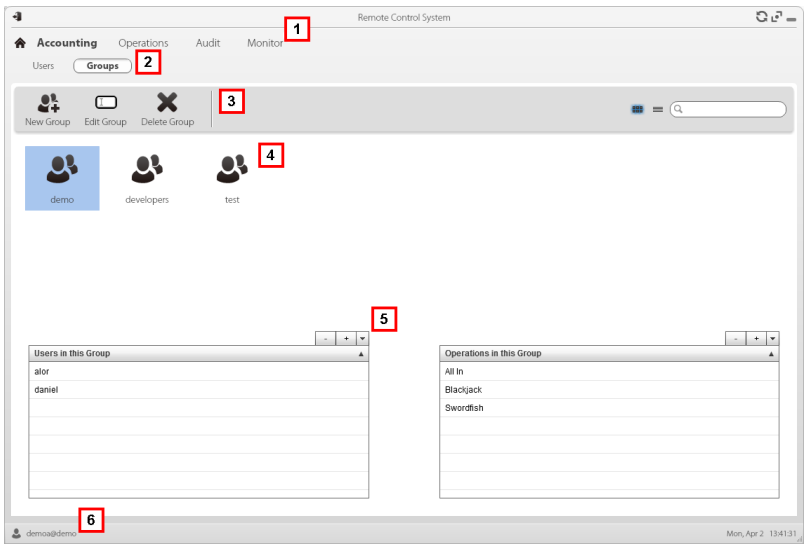
- organizzare gli utenti in gruppi di lavoro per assegnare loro specifiche operation
- creare un gruppo di alerting, che riceverà le e-mail di allarmi del sistema

Suggerimento: per raggruppare e gestire gli utenti destinati a ricevere gli allarmi di RCS in modo più semplice e immediato, creare un gruppo "di alerting" senza associarlo a una operation, ma che contenga tutti gli utenti da avvertire in caso di allarme. *Vedi "**Gestione degli utenti**" a pagina 19*

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione utenti e gruppi**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Menu **Accounting.**
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge un gruppo.
	Modifica il gruppo selezionato.
	Elimina il gruppo selezionato.

4	Elenco dei gruppi.
5	Utenti e operation assegnati al gruppo selezionato.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .
Per saperne di più sui gruppi e sugli utenti *vedi "**Cose da sapere su utenti e gruppi**".*

Creare un gruppo e associarvi utenti e operation

Per creare un nuovo gruppo:

Passo	*Azione*
1	Fare clic su **Nuovo Gruppo**: viene richiesto il nome da assegnare al gruppo.
2	Compilare i dati richiesti e fare clic su **Salva**: nell'area di lavoro principale compare il nuovo gruppo.

Passo	*Azione*
3	Nella tabella **Utenti in questo gruppo** fare clic su  per aggiungere gli utenti al gruppo.
4	Nella tabella **Operation in questo gruppo** fare clic su  per aggiungere le operation al gruppo: alla successiva login gli utenti appartenenti al gruppo vedranno le operation in elenco.  **IMPORTANTE: se si associa una operation a un utente attualmente connesso, quell'utente potrà vedere l'operation solo dalla successiva login.**

Modificare i dati di un gruppo e disassociare utenti e operation

Per modificare i dati di un gruppo:

Passo	*Azione*
1	Fare doppio clic su un gruppo.
2	Modificarne il nome e fare clic su **Salva.**
3	Nella tabella **Utenti in questo gruppo** fare clic su  per escludere utenti dal gruppo.
4	Nella tabella **Operation in questo gruppo** fare clic su  per escludere le operation visibili al gruppo: alla successiva login gli utenti appartenenti al gruppo non vedranno più le operation escluse.  **IMPORTANTE: se si esclude una operation da un utente attualmente connesso, quell'utente non vedrà più l'operation solo dalla successiva login.**

4

Operation e target

Presentazione

Introduzione

La gestione delle operation stabilisce i target da sottoporre a intercettazione.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sulle operation

Cos'è un'operation

L'operation rappresenta l'indagine da eseguire. Un'operation contiene uno o più target, ovvero le persone fisiche da intercettare. Il Tecnico assegna al target uno o più agent di tipo *desktop* o *mobile*. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Assegnare l'operation a un gruppo di utenti

Per garantire il massimo della riservatezza dei dati si suggerisce di associare un'operation solo agli utenti di RCS incaricati dell'indagine. Utenti non associati all'operation non vedranno alcun dato dell'operation e delle evidence raccolte. Per questo motivo è necessario che chi crea un operation faccia parte di almeno uno dei gruppi associati ad essa al momento della creazione.

Cosa avviene quando si crea una nuova operation

Quando un'operation viene creata è già dichiarata aperta, quindi è possibile creare i target dell'operation e chiedere al Tecnico la generazione e l'installazione degli agent. Ad operation aperta gli agent iniziano a raccogliere i dati e a inviarli a RCS.

Cosa avviene quando si chiude un'operation

L'operation deve essere chiusa alla chiusura effettiva dell'indagine, quando si è sicuri che tutti gli agent hanno già trasmesso tutte le evidence raccolte al Backend.

La chiusura provoca automaticamente la chiusura dei target e la chiusura degli agent. Quando un agent viene chiuso, alla prima sincronizzazione viene disinstallato lasciando così pulito il dispositivo.

Un'operation chiusa non può più essere riaperta. Solo i dati dell'operation e le evidence raccolte restano nel database.

PRUDENZA: in caso di sincronizzazioni non frequenti, per esempio ogni quattro giorni, attendere l'ultima sincronizzazione pianificata prima di chiudere l'operation.

Cose da sapere sui target

Cos'è un target

Il target rappresenta la persona fisica da investigare. Il Tecnico assegna al target uno o più agent di tipo desktop o mobile. Così l'agent può essere installato su un computer o su un dispositivo mobile.

Compiti dell'Amministratore

Il ruolo dell'Amministratore nella gestione dei target è a un livello di organizzazione generale; è compito del Tecnico configurare e lavorare operativamente sui target secondo le disposizioni dell'Amministratore.

L'Amministratore ha il compito di:

- creare un nuovo target all'interno di un'operation
- dare disposizioni al Tecnico sulle tempistiche di attivazione e la tipologia delle prove da raccogliere attraverso gli agent di un determinato target, in base alle caratteristiche del mandato ricevuto dall'autorità giudiziaria
- verificare la corretta applicazione delle disposizioni attraverso il controllo dell'Audit
- chiudere un target

Cosa avviene quando si crea un target

Quando un target viene creato è già dichiarato *aperto* , quindi è possibile chiedere al Tecnico la generazione e l'installazione degli agent.

Cosa avviene quando si chiude un target

È possibile chiudere un target, per esempio alla chiusura effettiva dell'indagine su quel target.

La chiusura di un target chiude automaticamente i suoi agent. Quando un agent viene chiuso, alla prima sincronizzazione viene disinstallato lasciando così pulito il dispositivo.

Un target chiuso non può più essere riaperto. Solo i dati del target stesso e quelli già inviati dagli agent restano nel database.

PRUDENZA: quando si chiude un target, si disinstallano automaticamente tutti gli agent associati. Chiudere un target solo quando si è certi di avere tutti i dati che servono.

PRUDENZA: in caso di sincronizzazioni non frequenti, per esempio ogni quattro giorni, attendere l'ultima sincronizzazione pianificata prima di chiudere il target.

Suggerimento: chiudere un target solo quando si è sicuri che gli agent hanno già scaricato tutte le informazioni di cui si ha bisogno.

Apertura e chiusura di un'operation

Nel caso di chiusura di una operation, tutti i target associati sono irrevocabilmente chiusi, e tutti i loro agent disinstallati. *Vedi "**Cose da sapere sulle operation**" alla pagina precedente* .

Gestione delle operation

Per gestire le operation:	• sezione **Operations**

Scopo

Questa funzione permette di:

- creare una nuova operation
- assegnare l'operation a un gruppo di utenti

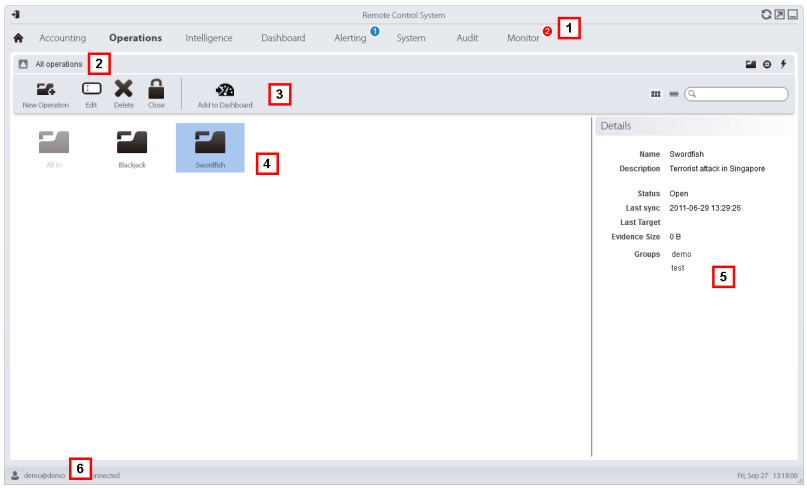
NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione operation**.

Passi successivi

Uno o più target devono essere associati all'operation. *Vedi "Pagina dell'operation" a pagina 35 .*

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.

Area	*Descrizione*
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Aggiunge un'operation.
	Modifica l'operation selezionata.
	Elimina l'operation selezionata.
	Chiude l'operation.

4 Elenco delle operation create:

 Operation aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, si ricevono le evidence raccolte.

 Operation chiusa. Tutti i target sono chiusi e gli agent disinstallati. È comunque possibile vedere tutti i suoi target e tutte le sue evidence.

5 Dati dell'operation selezionata.

6 Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati delle operation**" a pagina 35* .

Per saperne di più sulle operation *vedi "**Cose da sapere sulle operation**" a pagina 30* .

Creare un'operation

Per creare una nuova operation:

Passo	*Azione*
1	Fare clic su **Nuova Operation**: compaiono i dati da compilare.
2	Selezionare il gruppo (o i gruppi) da assegnare all'operation. NOTA: almeno uno dei gruppi associati deve contenere l'utente che sta creando l'operation.
3	Compilare i dati richiesti e fare clic su **Salva**: nell'area di lavoro principale compare la nuova operation in stato aperto.

Modificare i dati di un'operation

Per modificare i dati di un'operation:

Passo	*Azione*
1	Selezionare un'operation, quindi fare clic su **Modifica**: compaiono i suoi dati.
2	Modificare i dati e fare clic su **Salva**.

Chiudere un'operation

Per chiudere un'operation e attivare la disinstallazione degli agent su tutti i target:

Passo	*Azione*
1	Selezionare un'operation, quindi fare clic su **Chiudi**.
2	Confermare la chiusura: vengono chiusi tutti i target e viene richiesta la disinstallazione degli agent. I dati restano disponibili sul database. ***PRUDENZA: la chiusura dell'operation è irreversibile, vedi "Cose da sapere sulle operation" a pagina 30***

Eliminare un'operation

Per eliminare un'operation:

Passo	*Azione*
1	Selezionare un'operation, quindi fare clic su **Cancella**.
2	Confermare l'azione facendo clic su **Sì**: vengono eliminati dai database i dati dell'operation, dei target, degli agent e tutte le evidence.

PRUDENZA: eliminare un'operation è un'azione irreversibile e causa la perdita dei dati associati a quella operation.

Dati delle operation

Di seguito la descrizione dei dati dell'operation selezionata:

Dato	*Descrizione*
Nome	Nome dell'operation.
Descrizione	Descrizione libera.
Contatto	Campo descrittivo per definire, ad esempio, il nome di un referente (Giudice, Magistrato, e così via).
Stato	Stato di un'operation e comando di chiusura: **Open**: l'operation è aperta. Se sono stati definiti dei target e sono stati installati correttamente degli agent, RCS riceve le evidence raccolte. **Closed**: l'operation è chiusa, senza più possibilità di riaprirla. Gli agent non inviano più i dati, ma è possibile consultare le evidence già ricevute.  ***PRUDENZA: la chiusura dell'operation è irreversibile.Vedi "Cose da sapere sulle operation" a pagina 30***
Gruppi	Gruppi abilitati a visualizzare l'operation. *Vedi "Gestione dei gruppi" a pagina 26*

Pagina dell'operation

Per entrare in una operation:	• sezione **Operations**, doppio-clic su una operation

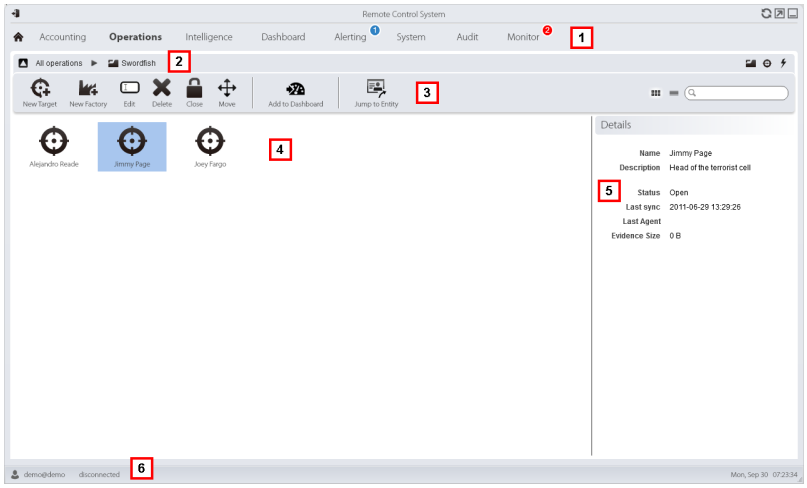
Scopo

Questa funzione permette di:

- creare uno o più target da monitorare durante un'operation
- gestire l'attivazione/disattivazione di un target

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barra di navigazione.
3	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Funzione*
	Aggiunge un target.  NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione target.**
	Modifica il target selezionato.
	Elimina il target selezionato.
	Chiude il target.
	Sposta il target in un'altra operation.

Area	*Descrizione*
4	Elenco dei target:  target aperto  target chiuso
5	Dati del target selezionato.
6	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .

Per saperne di più sulle operation *vedi "**Cose da sapere sulle operation**" a pagina 30* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati della pagina di un'operation**" alla pagina successiva* .

Creare un target

Per creare un nuovo target:

Passo	*Azione*
1	Fare clic su **Nuovo Target**: compaiono i dati da compilare.
2	Compilare i dati richiesti e fare clic su **Salva**: nell'area di lavoro principale compare il nuovo target in stato aperto, ovvero pronto per essere utilizzato da un Tecnico.

Chiudere un target

Per chiudere un target e attivare la disinstallazione dei suoi agent:

Passo	*Azione*
1	Selezionare un target, quindi fare clic su **Chiudi**.
2	Confermare la chiusura: viene chiuso il target e viene automaticamente avviata la disinstallazione dei suoi agent. I dati restano disponibili sul database.  ***PRUDENZA: la chiusura del target è irreversibile, vedi "Cose da sapere sui target" a pagina 30***

Modificare i dati di un target

Per modificare i dati di un target:

Passo	*Azione*
1	Selezionare un target, quindi fare clic su **Modifica**: compaiono i suoi dati.
2	Modificare i dati e fare clic su **Salva**.

Eliminare un target

Per eliminare un target:

Passo	*Azione*
1	Selezionare un target, quindi fare clic su **Cancella**.
2	Confermare l'azione facendo clic su **Sì**: vengono eliminati dai database i dati del target, dei suoi agent e tutte le evidence.

PRUDENZA: eliminare un target è un'azione irreversibile e causa la perdita dei dati associati a quel target.

Dati della pagina di un'operation

Di seguito la descrizione dei dati del target selezionato:

Dato	*Descrizione*
Nome	Nome del target.
Descriztione	Descrizione libera.
Stato	Definisce lo stato di un target:  Aperto. Se il Tecnico ha installato correttamente gli agent, RCS riceve le evidence raccolte.  Chiuso. Chiuso senza più possibilità di riaprirlo.

5

Monitoraggio degli utenti

Presentazione

Introduzione

Il monitoraggio degli utenti di RCS garantisce la correttezza di una indagine, il rispetto delle regole e delle indicazioni dettate da un qualsiasi ente che richiede attività investigative.

Contenuti

Questa sezione include i seguenti argomenti:

Cose da sapere sul monitoraggio utenti (Audit)

Cos'è il monitoraggio utenti

L'Audit è l'elenco delle azioni intraprese in RCS da tutti gli utenti tipo Amministratori, Tecnici e Analisti. Serve a garantire la correttezza di una indagine, il rispetto delle regole e delle indicazioni dettate da un qualsiasi ente che richiede attività investigative.

In questo modo l'Amministratore può controllare l'accesso al sistema da parte di tutti gli utenti abilitati ed eventualmente risalire nel tempo ad azioni particolari, quali per esempio la creazione di un target.

Come si leggono le azioni segnalate

L'Audit riassume in una tabella ogni azione effettuata nel sistema da ogni singolo utente.

In ogni azione sono sempre presenti quattro informazioni:

- data-ora dell'azione,
- utente che ha eseguito l'azione,
- tipo di azione,
- descrizione dell'azione.

Le altre caselle sono popolate solo in relazione al tipo di azione. Ad esempio, se un utente accede al sistema, l'Audit registra il nome dell'utente in **Attore** e il tipo di azione "login" in **Azione**.

Se un Tecnico crea degli agent, nell'elenco compare un'azione per ogni agent con il nome dell'utente, il tipo di azione "target.create" , il nome dell'operation, il nome del target e il nome dell'agent.

NOTA: le registrazioni della azioni sono disponibili solo in lingua Inglese.

La selezione delle azioni interessanti tramite i filtri

La funzione mostra normalmente le azioni eseguite nelle ultime 24 ore. Il filtro sulla colonna **Data** è quindi l'unico filtro che è sempre impostato di default ma che può essere modificato a piacimento. Per questo motivo la casella di controllo corrispondente è sempre selezionata.

Per tutte le altre colonne è possibile impostare un filtro per limitare la ricerca. Se la casella di controllo di fianco all'intestazione è selezionata, allora c'è un filtro attivo su quella colonna.

Ogni intestazione permette quindi di selezionare quali dati visualizzare.

Solo la colonna **Descrizione** accetta l'inserimento di parte del testo da cercare, per esempio se si inserisce "log" saranno visualizzate tutte le azioni la cui descrizione contiene il testo "log". Per esempio:

- "User 'xxx' **log**ged in"
- "**Log** file created"

Dati esportabili

RCS permette di esportare le azioni registrate per Amministratori, Tecnici e Analisti. Il file sarà salvato nella cartella RCS Download sul desktop.

Monitoraggio utenti (Audit)

Per monitorare gli utenti: • sezione **Audit**

Scopo

Questa funzione permette di controllare le azioni in RCS di Amministratori, Tecnici e Analisti. Per esempio è possibile verificare il corretto svolgimento di un'operation, il rispetto delle tempistiche di attivazione/disattivazione di un target, l'applicazione corretta da parte del Tecnico delle tipologie di agent autorizzate per una specifica operation.

Cosa è possibile fare

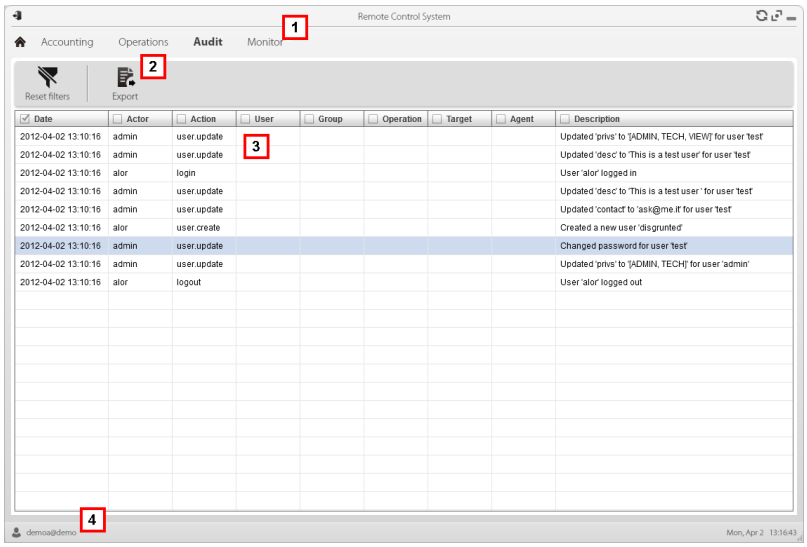
È possibile selezionare solo le azioni svolte in un certo periodo e applicare dei filtri per ricercare, per esempio, informazioni dettagliate su specifiche operation o di specifici utenti. In caso di necessità, è possibile esportare le azioni in un file in formato CSV.

IMPORTANTE: se la pagina viene tenuta aperta, è necessario aggiornarla per ottenere le azioni più recenti. ***Vedi "Descrizione della homepage" a pagina 8***

NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione Audit**.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS.
2	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Esporta le azioni visualizzate in un file in formato CSV (importabile in Excel).
	Rimuove tutti i filtri applicati ai dati della tabella.

3	Elenco azioni svolte dagli utenti di RCS.
4	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi di interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati del monitoraggio utenti (Audit)**"*

Per saperne di più sull'audit *vedi "**Cose da sapere sul monitoraggio utenti (Audit)**" a pagina 40* .

Selezionare le azioni di un periodo di tempo

Per visualizzare solo le azioni di un periodo di tempo:

Passo	*Azione*
1	Fare clic sull'intestazione di colonna **Data.**
2	Fare clic sull'intervallo di tempo di interesse.

NOTA: il filtro sulla data è sempre attivo, impostato sulle azioni delle ultime 24 ore. È possibile solo modificarne i criteri.

Selezionare le azioni in base ai dati proposti

Per aumentare l'accuratezza del risultato :

Passo	*Azione*
1	Fare clic sull'intestazione di una o più colonne: compare un campo di ricerca da compilare.
2	Inserire la parola da ricercare e premere il tasto **Invio**. Le informazioni all'interno della colonna sono filtrate e ordinate in base alla parola chiave inserita.

Rimuovere uno o più filtri

Per rimuovere un filtro e visualizzare tutti i dati:

Se volete rimuovere...	*Allora...*
un singolo filtro	deselezionare la casella di controllo nell'intestazione della colonna desiderata.
tutti i filtri contemporaneamente	fare clic su **Rimuovi filtri.**

NOTA: il filtro sulla data è sempre attivo, impostato sulle azioni delle ultime 24 ore. È possibile solo modificarne i criteri di intervallo.

Esportare le azioni visualizzate

Per esportare le azioni visualizzate:

Passo	*Azione*
1	Fare clic su **Esporta**: compaiono i dati da compilare.
2	Inserire il nome del file da esportare e fare clic su **OK:** un indicatore di stato mostra l'avanzamento dell'operazione. Per controllarne l'avanzamento fare clic sulla barra.

Dati del monitoraggio utenti (Audit)

Di seguito la descrizione delle colonne della tabella Audit:

Colonna	*Descrizione*
Data	Data-ora dell'azione.
Attore	Nome dell'utente connesso che ha causato l'azione.
Azione	Tipo di azione intrapresa dall'utente connesso. L'azione viene rappresentata con *soggetto.azione*. Per esempio "user.update" significa che è stato aggiornato un utente. Questo facilita la selezioni di azioni dello stesso tipo.
Utente	Utente interessato dall'azione, per esempio creato da un Amministratore. Da non confondere con il nome in Attore che è l'utente che ha causato l'azione.
Gruppo	Gruppo interessato dall'azione, per esempio il gruppo associato a una operation.
Operation	Operation interessata dall'azione, per esempio l'operation chiusa da un Amministratore.
Target	Target interessato dall'azione, per esempio il target chiuso da un Amministratore.
Agent	Agent interessato dall'azione, per esempio l'agent creato da un Tecnico.
Descrizione	Breve descrizione esplicativa dell'azione.

NOTA: tutte le azioni sono visualizzate in lingua Inglese.

6

Monitoraggio del sistema

Presentazione

Introduzione

Il monitoraggio del sistema permette il controllo costante dello stato dei componenti e dell'uso delle licenze.

Contenuti

Questa sezione include i seguenti argomenti:

Monitoraggio del sistema (Monitor)

Per fare il monitoraggio del sistema:	• sezione **Monitor**

Scopo

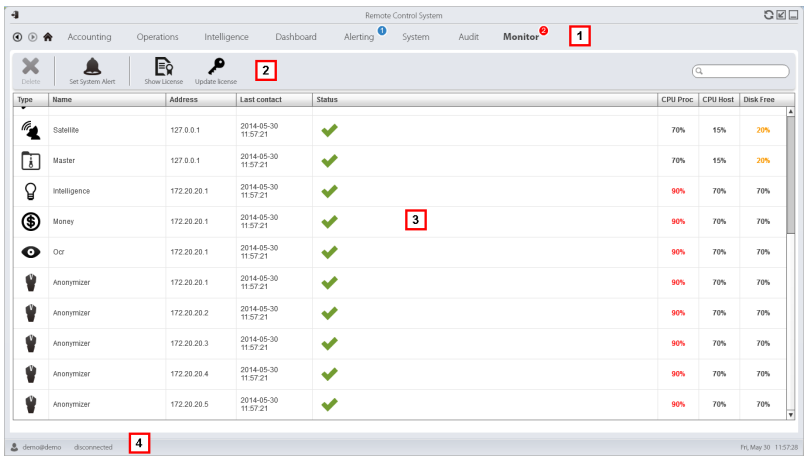
Questa funzione permette di:

- monitorare lo stato del sistema in termini di componenti hardware e software
- monitorare le licenze utilizzate rispetto a quelle acquistate
- definire il gruppo di alerting, destinatario delle e-mail di segnalazione nel caso di allarmi di sistema

Richiede assistenza: contattare il vostro Account Manager HackingTeam se sono necessarie licenze aggiuntive.

Come si presenta la funzione

Ecco come viene visualizzata la pagina:



Area	*Descrizione*
1	Menu di RCS. Monitor 1 : indica la quantità di allarmi di sistema in corso.
2	Barre con i pulsanti della finestra. Di seguito la descrizione:

Icona	*Descrizione*
	Definisce il gruppo di alerting. NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Gestione utenti e gruppi**.
	Visualizza lo stato delle licenze
	Carica un nuovo file licenza. NOTA: la funzione è abilitata solo se si è in possesso dell'autorizzazione **Modifica licenza**.

3	Elenco componenti di RCS con relativo stato: Allarme (genera l'invio di una e-mail al gruppo di alerting) Avvertenza Componente funzionante
4	Barra di stato di RCS.

Per saperne di più

Per la descrizione degli elementi dell'interfaccia *Vedi "**Elementi e azioni comuni dell'interfaccia**" a pagina 10* .

Per la descrizione dei dati presenti sulla finestra *vedi "**Dati del monitoraggio del sistema (Monitor)**" alla pagina successiva* .

Definire il gruppo di alerting o disattivarlo/attivarlo temporaneamente

Per selezionare il gruppo di alerting:

Passo	*Azione*
1	Fare clic su **Imposta Alerting**.
2	• Per disattivare le notifiche via e-mail, selezionare **Nessuno**. oppure • Per attivare le notifiche via e-mail a un gruppo, selezionare **Seleziona un gruppo da avviare via e-mail** e il gruppo di alerting dal menu a tendina. Il gruppo selezionato riceverà a ogni allarme di sistema una notifica via e-mail con la descrizione dell'allarme.
3	Fare clic su **Salva.**

Suggerimento: per raggruppare e gestire gli utenti destinati a ricevere gli allarmi di RCS in modo più semplice e immediato, creare un gruppo "di alerting" senza associarlo a una operation, ma che contenga tutti gli utenti da avvertire in caso di allarme. *Vedi "Gestione degli utenti" a pagina 19*

Dati del monitoraggio del sistema (Monitor)

Dati di monitoraggio dei componenti del sistema

Di seguito la descrizione dei dati del monitoraggio di sistema:

Dato	*Descrizione*
Tipo **Nome**	Tipo e nome del componente controllato. Di seguito alcuni esempi:  Anonymizer  Carrier  Collector  Database  Network Controller
Indirizzo	Indirizzo IP del componente.
Ultimo contatto	Data-ora ultima sincronizzazione.

Dato	*Descrizione*
Stato	Stato del componente dall'ultima sincronizzazione:  Allarme: il componente non sta funzionando, contattare il gruppo di alerting per un intervento rapido.  Avvertenza: il componente segnala una situazione di rischio, contattare l'Amministratore di sistema per le verifiche del caso.  Componente funzionante.
CPU Proc	% utilizzo CPU del singolo processo.
CPU Host	% utilizzo CPU del server.
Disco libero	% di unità disco libera.

Dati di monitoraggio delle licenze

Di seguito la descrizione dei dati del monitoraggio delle licenze. Nel caso di licenze limitate il formato è "x/y" dove x è la quantità di licenze attualmente usate dal sistema e y la quantità massima di licenze.

PRUDENZA: se la quantità di licenze si esaurisce, eventuali nuovi agent saranno accodati in attesa che si liberi una licenza o che se ne acquistino di nuove.

Dato	*Descrizione*
Tipo di licenza	Tipo di licenza attualmente in uso per gli agent. **reusable**: è possibile riutilizzare la licenza di un agent dopo la sua disinstallazione. **oneshot**: la licenza di un agent ha validità solo per una installazione.  NOTA: è possibile aggiornare la licenza solo se si è in possesso dell'autorizzazione **Modifica licenza**.
Utenti	Quantità di utenti attualmente usati dal sistema e quantità massima ammessa.
Agent	Quantità di agent attualmente usati dal sistema e quantità massima ammessa.
Desktop Mobile	Rispettivamente quantità di agent desktop e di agent mobile attualmente usati dal sistema e quantità massima ammessa.
Server distribuiti	Quantità di database attualmente usati dal sistema e quantità massima ammessa.

Dato	*Descrizione*
Collectors	Quantità di Collector attualmente usati dal sistema e quantità massima ammessa.
Anonymizers	Quantità di Anonymizer attualmente usati dal sistema e quantità massima ammessa.

]HackingTeam[

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

RCS 9.4 Manuale dell'amministratore
Manuale dell'amministratore 1.5 SET-2014

info@hackingteam.com