]HackingTeam[

RCS 9.5

La suite de hacking para intercepción gubernamental

Manual del administrador

Propiedad de la información

las solicitudes de copias adicionales de este manual o de la información técnica del producto se deben enviar a:

HT S.r.l.

via della Moscova, 13

20121 Milan (MI)

Italia

Tel.: + 39 02 29 060 603

Fax: + 39 02 63 118 946

Correo electrónico: info@hackingteam.com

Contenido

Glosario

A continuación se detallan las definiciones utilizadas en este manual.

A

Accounting
Sección de la consola en la que se administra el acceso a RCS.

Administrador
Es la persona que permite el acceso al sistema, crea grupos de trabajo y define las operations, los targets y los tipos de datos que se recopilarán.

Administrador del sistema
Persona que instala los servidores y las consolas, actualiza el software y restaura los datos en caso de alguna falla.

Agent
Software de sondeo instalado en los dispositivos a monitorear. Está diseñado para reunir evidence y transmitirla al Collector.

Agent elite
Agent instalado en dispositivos seguros. Le permite recopilar todos los tipos de evidence disponibles.

Agent scout
Reemplaza al agent enviado al dispositivo para verificar el nivel de seguridad antes de instalar agents reales (elite o soldier).

Agent soldier
Agent instalado en dispositivos que no son completamente seguros. Solo le permite recopilar algunos tipos de evidence.

Alerting
Sección de la consola en la que se administran los alerts de nueva evidence.

alerts de evidence
Alertas, usualmente en forma de correos electrónicos, que se envían a los analistas cuando hay nueva evidence que coincide con las reglas establecidas.

Analista
Persona encargada de analizar los datos recopilados durante las operations.

Anonymizer
(opcional) Protege al servidor contra ataques externos y permite permanecer anónimo durante las investigaciones. Transfiere los datos del agent a los Collectors.

Audit
Sección de la consola que reporta las acciones de todos los usuarios y el sistema. Se utiliza para controlar el abuso de RCS.

B

back end
Entorno diseñado para desencriptar y guardar la información que se recopila. Incluye el Master Node y las bases de datos shard.

BRAS
(Broadband Remote Access Server) Dirige el tráfico hacia o desde el DSLAM a la red del ISP y administra la autentificación de los suscriptores del ISP.

BSSID
(Basic Service Set IDentifier) Punto de acceso y su identificador cliente.

C

Carrier
Servicio del Collector: envía los datos recibidos de los Anonymizers a las bases de datos shard o al Master Node.

Collector
Servicio de Collector: recibe los datos que envían los agents a través de la cadena de Anonymizers.

consola
Computadora en la que se instala RCS Console. Accede directamente a RCS Server o al Master Node.

D

Dashboard
Sección de la consola utilizada por el analista. Se usa para tener un resumen rápido del estado de las operations, targets y agents más importantes.

DSLAM
(Digital Subscriber Line Access Multiplexer) Dispositivo de red que usualmente se encuentra en la central telefónica de los operadores de telecomunicaciones. Conecta varias interfaces de líneas de abonados digitales (DSL) a un canal de comunicaciones de alta velocidad digital usando técnicas de multiplexión.

E

Emisor de RCS
Sistema RCS que recibe evidence de los agents y la transfiere a otros sistemas RCS (consultar) a través de las reglas de conexión. Es un sistema RCS completo.

entidad
Grupo de información de Intelligence vinculada con el target y con las personas y lugares involucrados en la investigación.

ESSID
(Extended Service Set IDentifier) También conocido como SSID. Permite identificar la red Wi-Fi.

evidence
Evidence de datos recopilados. El formato depende del tipo de evidence (p. ej.: imagen).

Exploit
Código que se aprovecha de un error o vulnerabilidad y ejecuta un código imprevisto. Se utiliza para infectar a los dispositivos de los targets.

F

factory
Una plantilla para la configuración y compilación de un agent.

front end
Entorno diseñado para comunicarse con los agents para recopilar información y establecer su configuración. Incluye Collectors.

G

Grupo
Entidad de Intelligence que agrupa a varias entidades.

grupo de alerting
Grupo de usuarios que reciben notificaciones por correo cuando se activa una alarma del sistema (por ejemplo, cuando la base de datos excede los límites de espacio disponible). Usualmente este grupo no está vinculado con ninguna operation.

M

Monitor
Sección de la consola en la que se monitorea el estado de los componentes y la licencia.

N

Network Controller
Servicio del Collector: verifica el estado del Network Injector y el Anonymizer y les envía nuevos parámetros de configuración y actualizaciones de software.

Network Injector
Componente de hardware que controla el tráfico de la red del target e inyecta un agent en los recursos web seleccionados. Viene en dos versiones, Appliance o Tactical: la primera es para la implementación en el ISP, la segunda se usa en el campo.

Network Injector Appliance
Versión apilable del Network Injector, para instalarlo en el ISP. Consulte: Tactical Network Injector.

O

operation
Investigación dirigida a uno o más targets, cuyos dispositivos tendrán agents.

P

Person
Entidad de Intelligence que representa a una persona involucrada en la investigación.

Position
Entidad de Intelligence que representa a un lugar involucrado en la investigación.

R

RCS
(Remote Control System). El producto que aquí se documenta.

RCS Console
Software diseñado para interactuar con RCS Server.

RCS Server
Una o más computadoras, según la arquitectura de instalación, donde se instalan los componentes esenciales de RCS: las bases de datos shard, los Network Controller y el Collector.

Receptor de RCS
Sistema RCS que recibe evidence de otros sistemas RCS emisores (consultar) pero nunca directamente de los agents. En comparación con un RCS completo, el receptor de RCS solo cuenta con las funciones de procesamiento de evidence.

reglas de alert
Reglas que crean alerts cuando se almacena nueva evidence o los agents se comunican por primera vez.

reglas de inyección
Opciones de configuración que definen cómo identificar el tráfico HTTP, qué recurso debe inyectarse y qué método se usará para la inyección.

S

secuencia de obtención
Grupo de eventos, acciones y módulos de obtención complejos, que forman parte de la configuración avanzada de agents.

SSH
(Secure SHell) Protocolo de red para la transmisión segura de datos, los servicios del intérprete de comandos remoto o la ejecución de comandos.

System
Sección de la consola en la que se administra el sistema.

T

Tactical Network Injector
Versión portátil del Network Injector, para uso táctico. Consulte: Network Injector Appliance.

TAP
(Test Access Port) Dispositivo de hardware que se instala en una red y que monitorea de forma pasiva el flujo de datos transmitido.

target
La persona física bajo investigación.Se representa por medio de la entidad Target en la sección Intelligence.

Técnico
Persona designada por el administrador para crear y administrar agents.

V

Virtual
Entidad de Intelligence que representa a una ubicación virtual (p. ej.: sitio web) involucrado en la investigación.

VPS
(Virtual Private Server) Servidor remoto en el que se instala el Anonymizer. Usualmente se alquila.

W

WPA

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

WPA 2

(Wi-Fi Protected Access) Protección de la red Wi-Fi.

1

Introducción a esta guía

Presentación

Objetivos de este manual

Este manual sirve como guía para el *Administrador* sobre cómo usar RCS Console para:

- crear usuarios y grupos de trabajo
- abrir y cerrar investigaciones
- monitorear a los usuarios de RCS
- monitorear el sistema

A continuación se muestra la información necesaria para consultar el manual.

Contenido

En esta sección se incluyen los siguientes temas:

Nuevas funciones de la guía

Lista de notas publicadas y actualizaciones a esta ayuda en línea.

Fecha de publicación	*Código*	*Versión de software.*	*Descripción*
24 de noviembre de 2014	Manual del administrador -	9.5	No se actualizó la documentación.
20 de septiembre de 2014	Manual del administrador -	9.4	No se actualizó la documentación.
23 de junio de 2014	Manual del administrador -	9.3	No se actualizó la documentación.
19 de febrero de 2014	Manual del administrador -	9.2	No se actualizó la documentación.
30 de septiembre de 2013	Manual del administrador 1.4 SEP - 2013	9	Se actualizó la documentación debido a las mejoras a la interfaz de usuario. Se mejoró el contenido.

Documentación incluida

Los siguientes manuales se incluyen con el software RCS:

Manual	*Destinatarios*	*Código*	*Formato de distribución*
Manual del administrador del sistema	Administrador del sistema	Manual del administrador del sistema 1.8 NOV-2014	PDF
Manual del administrador (este manual)	Administradores	Manual del administrador 1.6 NOV-2014	PDF
Manual del técnico	Técnicos	Manual del técnico 1.9 NOV-2014	PDF
Manual del analista	Analistas	Manual del analista 1.8 NOV-2014	PDF

Convenciones tipográficas de notas

Las notas previstas en este documento se detallan a continuación (Manual de estilo de Microsoft):

ADVERTENCIA: indica una situación de riesgo que, si no se evita, podría causar lesiones físicas en el usuario o daños en el equipo.

PRECAUCIÓN: indica una situación de riesgo que, si no se evita, puede causar la pérdida de datos.

IMPORTANTE: indica las acciones necesarias para realizar una tarea. Si bien pueden pasarse por alto algunas notas sin que esto afecte a la realización de la tarea, no se deberían omitir las indicaciones importantes.

NOTA: información neutral y positiva que enfatiza o complementa la información del texto principal. Proporciona información que puede aplicarse solo en casos especiales.

Sugerencia: recomendación para la aplicación de técnicas y procedimientos descritos en el texto de acuerdo a ciertas necesidades especiales. Puede sugerirse un método alternativo y no es esencial para la comprensión del texto.

Llamada al servicio: la operation solo puede completarse con la ayuda del servicio técnico.

Convenciones tipográficas de formato

A continuación se muestran las explicaciones de algunas convenciones tipográficas:

Ejemplo	***Estilo***	***Descripción***
*Consulte "**Datos del usuario**"*	*cursiva*	indica el título de un capítulo, una sección, una subsección, un párrafo, una tabla o una imagen de este manual u otra publicación a la que se hace referencia.
<ddmmaaaa>	<aaa>	indica un texto que el usuario debe ingresar de acuerdo a cierta sintaxis. En el ejemplo, <ddmmaaaa> es una fecha y un posible valor podría ser “14072011”.
Seleccione uno de los servidores de la lista **[2]**.	**[x]**	indica el objeto citado en el texto que aparece en la imagen adyacente.

Ejemplo	*Estilo*	*Descripción*
Haga clic en **Agregar**. Seleccione el menú **Archivo, Guardar datos**.	**negrita**	indica el texto en la interfaz del operador, que puede ser un elemento gráfico (como una tabla o pestaña) o un botón en la pantalla (como mostrar).
Presione Entrar	primera letra mayúscula	indica el nombre de una tecla en el teclado.
Consulte: Network Injector Appliance.	-	sugiere que compare la definición de una palabra en el glosario o contenido con otra palabra o contenido.

Destinatarios del producto y de esta guía

A continuación se muestra una lista de los profesionales que interactúan con RCS.

Destinatario	*Actividad*	*Habilidades*
Administrador del sistema	Sigue las indicaciones de HackingTeam que se suministran durante la fase contractual. Instala y actualiza los RCS Servers, los Network Injectors y las RCS Cosoles. Programa y se encarga de realizar las copias de seguridad. Restaura las copias de seguridad si se reemplazan los servidores.  **ADVERTENCIA: el administrador del sistema debe tener las habilidades necesarias. HackingTeam no se hace responsable en caso de mal funcionamiento del equipo o de posibles daños ocasionados por la instalación por parte de una persona no profesional.**	Técnico de red experto
Administrador	Crea cuentas y grupos autorizados. Crea operations y targets. Monitorea el estado del sistema y de las licencias.	Administrador de investigación
Técnico	Crea agents y los configura. Establece las reglas de Network Injector	Técnico especialista en intercepciones
Analista	Analiza la evidence y la exporta.	Operativo

Datos de identificación del autor del software

HT S.r.l.

via della Moscova, 13
20121 Milan (MI)
Italia
Tel.: + 39 02 29 060 603
Fax: + 39 02 63 118 946
Correo electrónico: info@hackingteam.com

2

RCS Console para el administrador

Presentación

Introducción

RCS (Remote Control System) es una solución que soporta investigaciones por medio de la intercepción activa y pasiva de los datos y la información de los dispositivos bajo investigación. De hecho, RCS crea, configura e instala agents de software de forma anónima que recopilan datos e información y envían los resultados a la base de datos central para decodificarlos y guardarlos.

El rol del administrador

El rol del *administrador* es:

- administrar el acceso al sistema por medio de la asignación de funciones a los diversos usuarios previstos por la aplicación
- crear y cerrar investigaciones
- definir los targets involucrados
- informar al usuario *técnico* sobre los tipos de evidence que deben interceptarse
- monitorear las acciones ejecutadas por los usuarios
- monitorear las licencias disponibles para los componentes de RCS

Funciones activadas por el administrador

Para realizar sus actividades, el administrador tiene acceso a las siguientes funciones:

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

Contenido

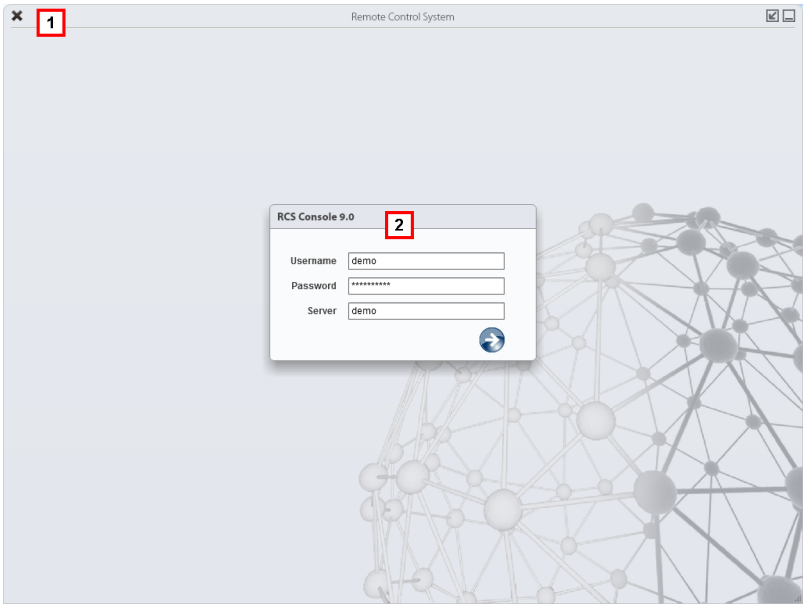
En esta sección se incluyen los siguientes temas:

Pantalla inicial de RCS Console

Cuando se abre RCS Console, se le pide que ingrese sus datos de inicio de sesión que estableció el administrador.

Cómo se ve la página de inicio de sesión

Así es como se ve la página de inicio de sesión:



Área	*Descripción*
1	Barra de título con botones de comando: Cierra RCS Console. Botón para ampliar la ventana. Botón para minimizar la ventana.
2	Ventana de diálogo para ingresar al sistema.

Acceso a RCS Console

Para acceder a las funciones de RCS Console:

Paso	*Acción*
1	En **Nombre de usuario** y **Contraseña,** ingrese sus datos de inicio de sesión asignados por el administrador.
2	En **Servidor,** ingrese el nombre del equipo o la dirección del servidor al que desea conectarse.
3	Haga clic en : aparecerá la página principal con los menús activados según los privilegios de su cuenta. *Consulte "**Descripción de la página principal**" abajo* .

Descripción de la página principal

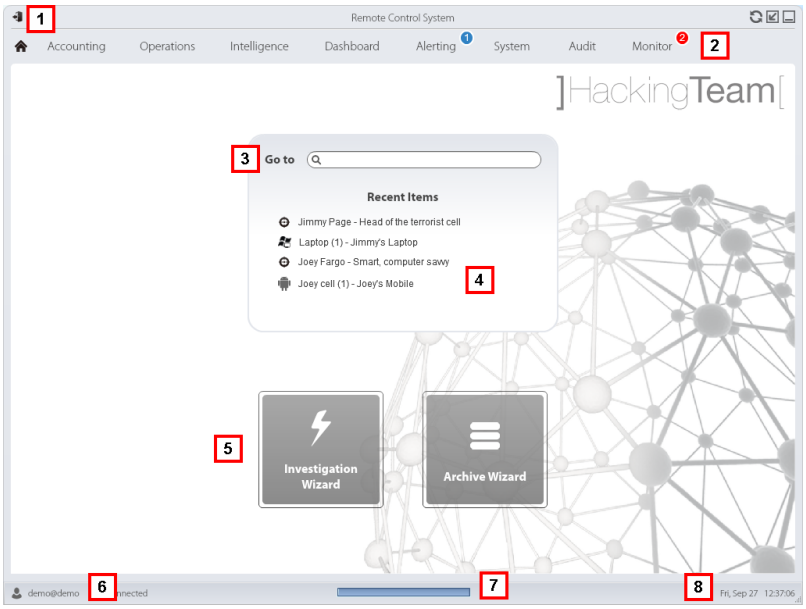
Para ver la página principal:	• haga clic en

Introducción

Al abrir RCS Console se mostrará la página principal. Todos los usuarios verán la misma página. Los menús se verán activos según los privilegios asignados a la cuenta.

Cómo se ve

Así es como se ve la página principal, con elementos guardados que se abrieron recientemente. Detalle de los elementos y las acciones comunes:



Área	*Descripción*
1	Barra de título con botones de comando.
2	Menú de RCS con las funciones activas para el usuario.
3	Cuadro de búsqueda para buscar operations, targets, agents y entidades, por nombre o descripción.
4	Enlaces a los cinco elementos abiertos (operation en la sección **Operations**, operation en la sección **Intelligence**, target, agent y entidad).
5	Botones del asistente.
6	Usuario conectado con opciones para cambiar el idioma y la contraseña.
7	Área de descarga con una barra de progreso durante la exportación o compilación.
8	Fecha y hora actuales con opciones para cambiar la zona horaria.

Asistentes en la página principal

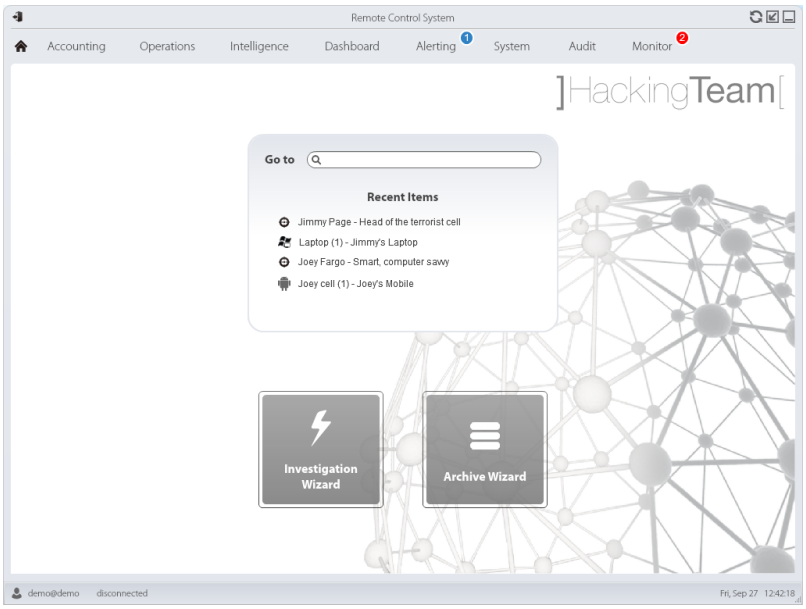
Para ver la página principal:	• haga clic en 

Introducción

Para los usuarios con ciertos privilegios, en RCS Console se muestran los botones que permiten abrir los asistentes.

Cómo se ve

Así es como se ve la página principal con los asistentes activados:



Botón	*Función*
	Abre el asistente para crear rápidamente un agent. NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Técnico.
	Abre el asistente para guardar rápidamente los datos de operation y target. NOTA: el botón solo se activa para los usuarios con privilegios Administrador y Administrador del sistema.

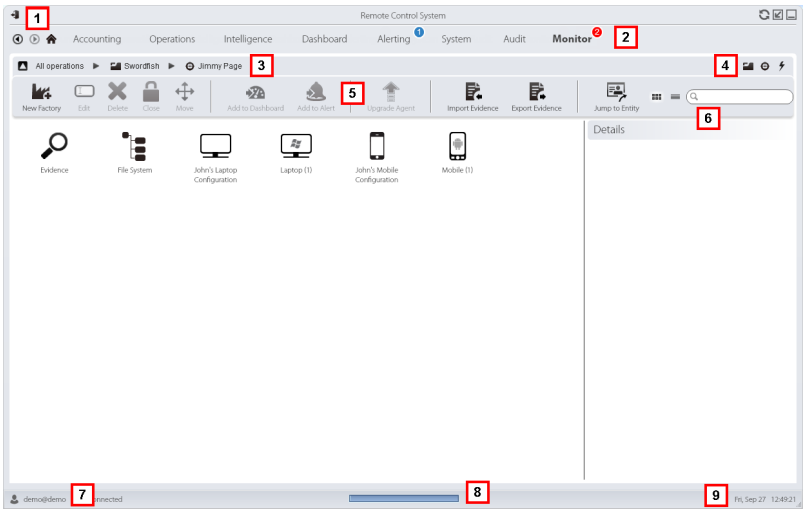
Elementos y acciones comunes de la interfaz

Cada página del programa usa elementos comunes y permite realizar acciones similares.

Para facilitar la comprensión del manual, en este capítulo se describirán los elementos y acciones compartidos por ciertas funciones.

Cómo se ve RCS Console

Así es como se ve usualmente la página de RCS Console. En este ejemplo se muestra la página de un target:



Área	*Descripción*
1	Barra de título con botones de comando: Salir de RCS. Botón para volver a cargar la página. Botón para ampliar la ventana. Botón para minimizar la ventana.
2	• Botón Anterior del historial de navegación • Botón Siguiente del historial de navegación • Botón para regresar a la página principal • Menú de RCS con las funciones activas para el usuario.

Área	*Descripción*
3	Barra de navegación de la operation. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Regresar al nivel superior.
	Muestra la página de la operation (sección **Operations**).
	Muestra la página del target.
	Muestra la página de la factory.
	Muestra la página del agent.
	Muestra la página de la operation (sección **Intelligence**).
	Muestra la página de la entidad.

4	Botones que permiten mostrar todos los elementos, independientemente del grupo al que pertenecen. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Muestra todas las operations.
	Muestra todos los targets.
	Muestra todos los agents.
	Muestra todas las entidades.

5	Barra de herramientas de la ventana.
6	Botones y cuadro de búsqueda:

Objeto	*Descripción*
	Cuadro de búsqueda. Escriba parte del nombre para que aparezca una lista con los elementos que contienen esas letras.
	Muestra los elementos en una tabla.
	Muestra los elementos como íconos.

7	Usuario conectado con opciones para cambiar el idioma y la contraseña.

Área	*Descripción*
8	Área de descarga con una barra de progreso durante la exportación o compilación. Los archivos se descargan en el escritorio, en la carpeta Descarga de RCS. • Barra superior: porcentaje de generación en el servidor • Barra inferior: porcentaje de descarga desde el servidor a RCS Console.
9	Fecha y hora actuales con opciones para cambiar la zona horaria.

Acciones siempre disponibles en la interfaz

Cambiar el idioma de la interfaz o la contraseña

Para cambiar el idioma de la interfaz o la contraseña:

Paso	*Acción*
1	Haga clic en **[7]** para que aparezca una ventana de diálogo con los datos del usuario.
2	Cambie el idioma o la contraseña y haga clic en **Guardar** para confirmar y salir.

Cambiar la fecha y la hora de RCS Console a su zona horaria

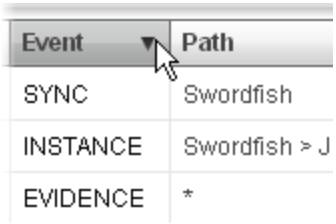
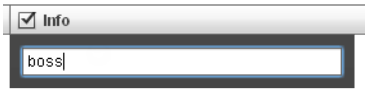
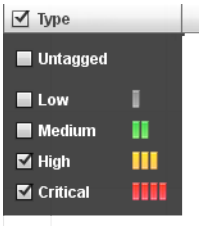
Para convertir todas las fechas y horas a su zona horaria:

Paso	*Acción*
1	Haga clic en **[9]** para que aparezca una ventana de diálogo con la fecha y la hora actuales: **Hora UTC**: hora media de Greenwich (GMT) **Hora local**: fecha y hora donde se encuentra instalado el RCS Server **Hora de la consola**: fecha y hora de la consola que se está utilizando y que se puede cambiar.
2	Cambie la zona horaria y haga clic en **Guardar** para confirmar y salir: todas las fechas y horas se cambiarán según lo que haya indicado.

Acciones relacionadas con las tablas

RCS Console muestra varios datos en forma de tablas. Las tablas le permiten:

- ordenar los datos por columna en orden ascendente o descendente
- filtrar datos por columna

Acción	*Descripción*
Ordenar por columna	Haga clic en el encabezado de la columna para ordenarla de forma ascendente o descendente. 
Filtrar un texto	Escriba una parte del texto que desea buscar: se mostrarán solo los elementos que contengan esas letras.  Al escribir el mismo texto que en el ejemplo se mostrarán elementos con una descripción como: • "my**boss**" • "**boss**anova"
Filtrar en base a una opción	Seleccione una opción: se mostrarán los elementos que coincidan con la opción seleccionada. 
Filtrar en base a varias opciones	Seleccione una o más opciones: se mostrarán los elementos que coincidan con las opciones seleccionadas. 
Cambiar el tamaño de la columna	Seleccione el borde de la columna y arrástrelo.

Procedimientos del administrador

Introducción

A continuación se indican los procedimientos realizados usualmente por el administrador con referencias a los capítulos pertinentes.

Procedimientos

Preparar el sistema RCS para que otros usuarios lo usen

A continuación se describen los procedimientos que se realizan usualmente para preparar el sistema RCS para que otros usuarios lo usen:

Paso	*Acción*
1	En la sección **Accounting**, en **Users,** defina las personas que tendrán acceso a RCS. *Consulte "**Administración de usuarios**" en la página 19*
2	En la sección **Accounting, Groups** cree el grupo de usuarios (usualmente compuesto por administradores del sistema no vinculados con ninguna operation) que recibirán notificaciones de alarmas del sistema por correo electrónico *Consulte "**Administración de grupo**" en la página 26*
3	En la sección **Monitor**, seleccione el grupo que recibirá las notificaciones de alarmas del sistema por correo electrónico. *Consulte "**Monitoreo del sistema (Monitor)**" en la página 46*

Abrir una investigación

A continuación se detallan los procedimientos que se realizan usualmente para abrir una investigación:

Paso	*Acción*
1	En la sección **Accounting**, **Users** defina las personas que pertenecerán al equipo de investigación y sus funciones. *Consulte "**Administración de usuarios**" en la página 19*
2	En la sección **Accounting**, **Groups** defina el equipo que tendrá permiso para ver los datos de la investigación y recibir alarmas del sistema. *Consulte "**Administración de grupo**" en la página 26*

Paso	Acción
3	En la sección **Operations**, abra la investigación y vincule uno o más grupos. *Consulte "**Administración de operations**" en la página 32 y "**Página de la operation**" en la página 35*
4	Informe a los técnicos de RCS sobre los tipos de evidence que se recopilarán.
5	En la sección **Audit**, monitoree el acceso del equipo al sistema y se controlan sus acciones. *Consulte "**Monitoreo de los usuarios (Audit)**" en la página 41*

Cerrar una investigación

A continuación se detalla el procedimiento que se realiza usualmente para cerrar una investigación:

Paso	Acción
1	En la sección **Operations**, cierre la investigación. *Consulte "**Administración de operations**"*
2	En caso de ser necesario, pida al administrador del sistema que guarde la evidence en un archivo de respaldo.

Monitoreo del sistema

A continuación se detallan los procedimientos que se realizan usualmente para monitorear el uso de RCS:

Paso	Acción
1	En la sección **Monitor**, monitoree los mensajes del sistema y las licencias utilizadas. *Consulte "**Monitoreo del sistema (Monitor)**" en la página 46*
2	En la sección **Audit**, monitoree las acciones realizadas por los técnicos, analistas y otros administradores. *Consulte "**Monitoreo de los usuarios (Audit)**" en la página 41*

3

Administración del acceso a RCS

Presentación

Introducción

La administración de grupos y usuarios es esencial para garantizar la confidencialidad y seguridad de los datos.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de los usuarios y los grupos

Introducción

Para garantizar la confidencialidad y seguridad máximas de los datos, RCS ofrece al administrador la posibilidad de asignar privilegios de acceso a cada usuario y a los usuarios de los grupos de trabajo para operations específicas. La estructura se adapta tanto a situaciones en las que las tareas se encuentran muy fragmentadas como a situaciones en las que pocas personas son las que realizan todas las tareas.

Por medio de la administración de los usuarios, el administrador también tiene la posibilidad de desconectar rápidamente a un usuario sospechoso y desactivar temporalmente su acceso a RCS.

Privilegios de registro

RCS está diseñado para garantizar la máxima seguridad del servidor y de los datos recopilados. Para lograrlo, se definieron cuatro roles que normalmente corresponden a los profesionales que pueden registrarse en el sistema:

- Administrador del sistema: está a cargo exclusivamente de la instalación de hardware y software, y de las copias de seguridad.
- Administrador: está a cargo de todos los acceso al sistema, las investigaciones y las metas de investigación.
- Técnico: está a cargo de la configuración y de la instalación de los agents de intercepción
- Analista: está a cargo del análisis de los datos.

Sugerencia: se pueden asignar varios roles al mismo usuario; por ejemplo, un administrador también puede tener privilegios de técnico.

Funciones activadas por rol

A continuación se muestra una lista de las funciones de RCS reservadas a los usuarios en un rol específico:

Rol	*Funciones activadas*
System administrador	• System • Monitor
Administrador	• Accounting • Operations • Audit • Monitor

Rol	*Funciones activadas*
Técnico	• Operations • System
Analista	• Operations • Intelligence • Dashboard • Alerting

Grupos de usuario por operation

Los grupos permiten que los usuarios se agrupen para asignarles operations específicas. De esta forma, se pueden administrador varias operations de forma simultánea, lo cual garantiza la máxima confidencialidad entre los grupos de trabajo.

*Consulte "**Administración de operations**" en la página 32*

IMPORTANTE: la asignación de operations a un grupo de trabajo comenzará a funcionar la siguiente vez que el usuario de ese grupo inicie sesión.

Grupos de usuarios para las alertas del sistema

Es posible crear un grupo de usuarios exclusivamente destinado a recibir un correo electrónico en caso de una alarma de sistema.

De esta forma, se puede garantizar una intervención rápida del administrador del sistema en caso de fallas graves.

*Consulte "**Monitoreo del sistema (Monitor)**" en la página 46*

Administración de usuarios

Para administrar usuarios:	• **Sección Accounting, Users**

Propósito

Esta función le permite:

- registrar un usuario y permitirle acceder a ciertas funciones de RCS. Una vez registrado, el usuario puede iniciar sesión y ver las funciones según los roles asignados
- desactivar temporalmente el acceso a un usuario, por ejemplo, en caso de una ausencia prolongada
- desconectar inmediatamente a un usuario de RCS, por ejemplo, en caso de supuesto acceso ilegal a RCS

- monitorear la fecha y la hora, y la dirección IP de la última conexión del usuario a RCS y otros datos relevantes

Sugerencia: para bloquear a un usuario e impedir su acceso a RCS, recomendamos que lo desconecte inmediatamente (si es que está conectado) y que desactive su cuenta.

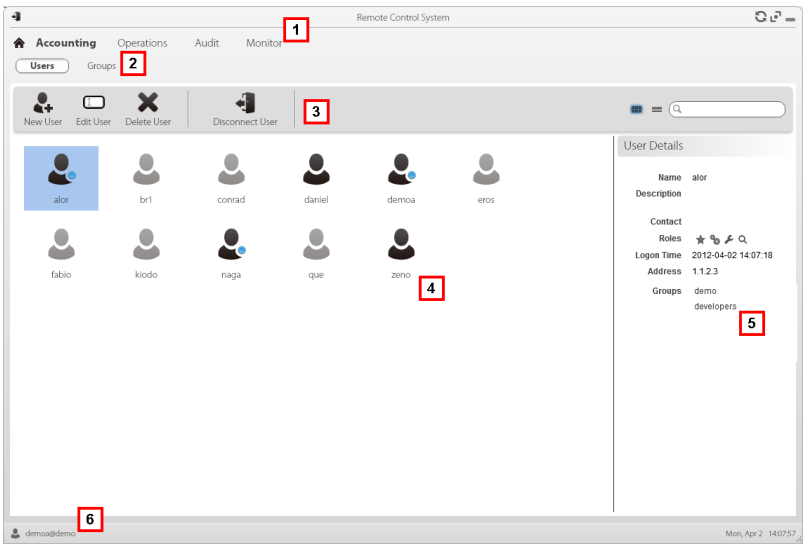
NOTA: la función solo se activa con los permisos **Administración de usuarios y de grupos**.

Próximos pasos

Es posible vincular a varios usuarios a un grupo de trabajo, para asignarles operations específicas o para enviarles alarmas del sistema. *Consulte "Administración de grupo" en la página 26 .*

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **Accounting**.

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Permite agregar un usuario
	Permite editar al usuario seleccionado.
	Elimina al usuario seleccionado.
	Desconecta al usuario seleccionado.

4	Área de trabajo principal con una lista de los usuarios registrados:  Usuarios registrados que actualmente están conectados a RCS.  Usuarios registrados pero que actualmente no están conectados a RCS.  Usuarios registrados pero sin acceso al sistema. El usuario no puede acceder a RCS.
5	Datos del usuario seleccionado.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos del usuario**" en la página 23* .

Para obtener más información acerca de los usuarios y los grupos, *consulte "**Qué debería saber acerca de los usuarios y los grupos**" en la página 18* .

Registro y activación de un usuario para el acceso a RCS

Para registrar a un nuevo usuario:

Paso	*Acción*
1	Haga clic en **Nuevo usuario**: se mostrarán los campos para ingresar datos.
2	Ingrese los datos solicitados y, si desea que el usuario tenga acceso a RCS, asegúrese de que el cuadro **Activado** esté seleccionado.
3	Haga clic en **Guardar**: aparecerá el nuevo usuario con el ícono  en el área de trabajo principal.

Activar/desactivar a un usuario

Para permitir o cancelar el acceso de un usuario a RCS:

Paso	*Acción*
1	Haga doble clic en un usuario: aparecerán sus datos.
2	Haga clic en **Activado** para activarlo o desactivarlo.
3	Haga clic en **Guardar**: aparecerá el nuevo usuario en el área de trabajo principal con el ícono  (activado) o  (desactivado).  **IMPORTANTE: si el usuario está conectado al sistema, continuará trabajando pero se le negará el acceso la siguiente vez que inicie sesión. Para desconectar a un usuario inmediatamente *consulte "Desconectar a un usuario inmediatamente" abajo* .**

Desconectar a un usuario inmediatamente

Para desconectar inmediatamente a un usuario que está conectado al sistema:

Paso	*Acción*
1	Haga clic en el usuario  y luego en **Desconectar usuario**: el usuario aparecerá con el ícono  en el área de trabajo principal.  **IMPORTANTE: si el usuario está conectado al sistema, perderá la conexión de forma inmediata. El usuario podrá acceder la siguiente vez que inicie sesión, a menos que lo desactive. Para desactivar al usuario *consulte "Activar/desactivar a un usuario" arriba* .**

Edición de los datos de un usuario

Para editar los datos de un usuario:

Paso	*Acción*
1	Haga doble clic en un usuario: aparecerán sus datos.
2	Edite los datos y haga clic en **Guardar**: se tendrán en cuenta los cambios la siguiente vez que se inicie sesión o en los próximos mensajes de alert.

Datos del usuario

A continuación se describen los datos del usuario seleccionado:

Datos	*Descripción*
Activado	Si se selecciona esta opción se activará el acceso de los usuarios a RCS. Si no se selecciona, los usuarios quedarán registrados pero se les negará el acceso a RCS.
Nombre	Nombre usado para acceder a RCS.
Descripción	Descripción del usuario
Correo electrónico	Correo electrónico del usuario.  **IMPORTANTE: si un usuario tiene privilegios de analista, los alerts de evidence se enviarán a esta dirección. El usuario no puede cambiar el correo electrónico.**
Contraseña	Contraseña del usuario. El usuario puede cambiarla más adelante desde la barra de estado.
Roles	Privilegios asignados al usuario:  Administrador del sistema  Administrador  Técnico  Analista Para ver una descripción detallada de los privilegios *consulte "**Datos de privilegios**" en la página siguiente*
Permisos avanzados	Abre la ventana para asignar autorizaciones para cada privilegio. Para ver una descripción detallada de las autorizaciones *consulte "**Datos de privilegios**" en la página siguiente*

Datos	*Descripción*
Idioma	Idioma de la interfaz de RCS Console. El usuario puede cambiarla más adelante desde la barra de estado.
Zona horaria de la consola	Zona horaria utilizada por RCS Console para mostrar la hora.
Grupos	Grupos de usuarios. El usuario solo puede ver las operations asignadas al grupo.

Datos de privilegios

Autorizaciones del administrador

A continuación se describen las autorizaciones asignadas a los administradores:

Datos	*Descripción*
Administración de usuarios y grupos	Activa la sección **Accounting**.  NOTA: los usuarios con esta autorización obviamente pueden cambiar su propias autorizaciones o las de los demás.
Administración de operations	Activa la administración de operations.
Administración de targets	Activa la administración de targets.
Administración de audit	Activa la sección **Audit**.
Cambiar licencia	Permite actualizar la licencia.

Autorizaciones del administrador del sistema

A continuación se describen las autorizaciones asignadas a los administradores del sistema:

Datos	*Descripción*
Administración de frontend	Activa la sección **System, Frontend**.
Administración de backend	Activa la sección **System, Backend**.
Copia de seguridad y restauración del sistema	Activa la sección **System, Backup**.

Datos	*Descripción*
Administración del Network Injector	Activa la sección **System, Network Injector**.
Administración de conectores	Activa la **sección Connectors**.

Autorizaciones de los técnicos

A continuación se describen las autorizaciones asignadas a los técnicos:

Datos	*Descripción*
Creación de factory	Permite crear y configurar las factories.
Creación del vector de inyección	Permite compilar vectores de instalación.
Configuración de agents	Permite hacer cambios en la configuración de los agents.
Comandos de ejecución de un agent	Permite ejecutar comandos en los agents.
Enviar archivos a agents	Permite enviar archivos a los agents.
Importar evidence	Permite importar evidence.
Administración de las reglas del Network Injector	Permite agregar reglas a los Network Injectors.

Autorizaciones de los analistas

A continuación se describen las autorizaciones asignadas a los analistas

Datos	*Descripción*
Crear alert	Permite crear reglas de alert.
Explorar el sistema de archivos del agent	Permite explorar el sistema de archivos del agent.
Editar evidence	Permite asignar prioridades a la evidence y agregar notas.
Eliminar evidence	Permite eliminar evidence.  NOTA: esta autorización nunca está activada de forma predeterminada, ya que requiere una licencia de usuario.

Datos	*Descripción*
Exportar evidence	Permite exportar evidence.
Administración de entidades	Permite administrar las entidades Intelligence.

Administración de grupo

Para administrar grupos:	• **Sección Accounting, Groups**

Propósito

Esta función le permite:

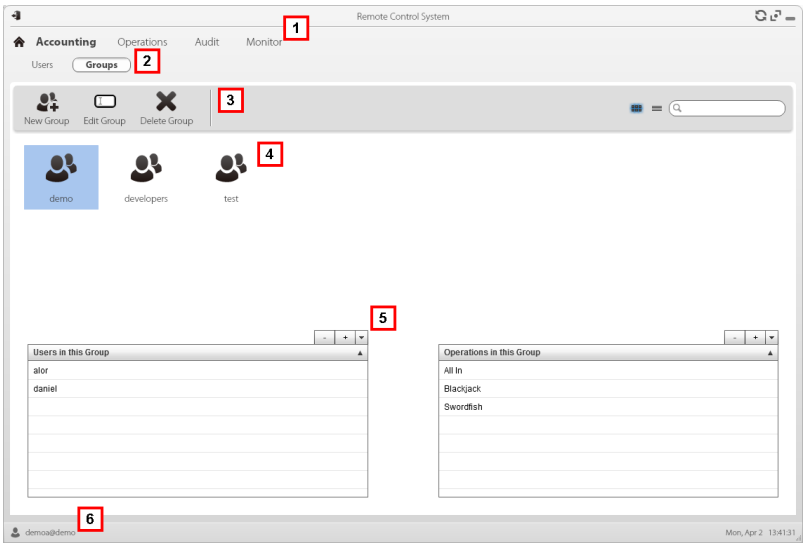
- organizar usuarios en grupos de trabajo para asignarles operations específicas
- crear un grupo de alerting para recibir alertas del sistema por correo electrónico

Sugerencia: para agrupar fácil y rápidamente a los usuarios que recibirán las alarmas de RCS, cree un grupo de "alerting" que contenga a todos los usuarios que deben recibir una alerta en caso de que haya una alarma no vinculada con ninguna operation. *Consulte "**Administración de usuarios**" en la página 19*

NOTA: la función solo se activa con los permisos **Administración de usuarios y de grupos**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Menú **Accounting**.
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Agrega un grupo.
	Permite editar el grupo seleccionado.
	Elimina el grupo seleccionado.

4	Lista de grupos.
5	Usuarios y operations asignados al grupo seleccionado.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información acerca de los grupos y los usuarios, consulte *"**Qué debería saber acerca de los usuarios y los grupos**"*.

Crear un grupo y vincular usuarios y operations

Para crear un nuevo grupo:

Paso	*Acción*
1	Haga clic en **Nuevo grupo**: escriba el nombre que desea asignarle al grupo.
2	Escriba los datos solicitados y haga clic en **Guardar**: el nuevo grupo se mostrará en el área de trabajo principal.
3	En la tabla **Usuarios en este grupo**, haga clic en  para agregar usuarios al grupo.
4	En la tabla **Operations en este grupo**, haga clic en  para agregar operations al grupo: la próxima vez que los usuarios inicien sesión, verán en la lista las operations que se agregaron.  **IMPORTANTE: si una operation está vinculada a un usuario que actualmente está conectado al sistema, este usuario no podrá ver la operation hasta la próxima vez que inicie sesión.**

Edición de los datos del grupo y eliminación de usuarios y operations

Para editar los datos de un grupo:

Paso	*Acción*
1	Haga doble clic en un grupo.
2	Cambie el nombre y haga clic en **Guardar.**
3	En la tabla **Usuarios en este grupo**, haga clic en  para quitar a los usuarios del grupo.
4	En la tabla **Operations en este grupo**, haga clic en  para quitar operations del grupo: la próxima vez que los usuarios inicien sesión, ya no verán esas operations en la lista.  **IMPORTANTE: si se quita una operation de un usuario que actualmente está conectado al sistema, la próxima vez que inicie sesión ya no podrá ver la operation.**

4

Operation y target

Presentación

Introducción

La administración de operations establece los targets que serán interceptados.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca de las operations

Qué es una operation

Una operation es una investigación que se llevará a cabo. Una operation contiene uno o más targets, es decir, las personas físicas que se van a interceptar. El técnico asigna uno o más agents, de *escritorio* o *móviles,* al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Asignación de la operation a un grupo de usuarios

Para garantizar la máxima confidencialidad de los datos, le recomendamos vincular cada operation exclusivamente a los usuarios de RCS asignados a esa investigación. Los usuarios no vinculados con la operation no verán ningún dato de la evidence recopilada en esa operation. Por este motivo, la persona que crea la operation debe ser parte de cuando menos uno de los grupos vinculados con la operation al momento de la creación.

Qué sucede cuando se crea una nueva operation

Cuando se crea una nueva operation ya se declara abierta, por lo que se pueden crear los targets de la operation y los técnicos pueden generar e instalar agents. Cuando la operation se considera abierta, los agents comienzan a recopilar datos y a enviarlos a RCS.

Qué sucede cuando se cierra una operation

La operation debe cerrarse cuando se cierra la investigación y se tiene la certeza de que todos los agents ya transmitieron toda la evidence recopilada al Backend.

Al cerrar la operation automáticamente se cierran los targets y los agents. Cuando se cierra el agent, la desinstalación se realiza en la siguiente sincronización, lo cual deja el dispositivo limpio.

Una operation cerrada no podrá volver a abrirse. Solo los datos y la evidence recopilada de la operation permanecen en la base de datos.

PRECAUCIÓN: en caso de sincronizaciones infrecuentes, por ejemplo, cada cuatro días, espere a que ocurra la última sincronización planificada antes de cerrar la operation.

Qué debería saber acerca de los targets

Qué es un target

Un target es una persona física que va a ser investigada. El técnico asigna uno o más agents, de escritorio o móviles, al target. Por lo tanto, es posible instalar agents en una computadora o teléfono móvil.

Tareas del administrador

El administrador se encarga de administrar los targets a nivel de organización general; el técnico configura y trabaja con targets de acuerdo con las instrucciones del administrador.

El administrador está a cargo de:

- crear un nuevo target dentro de la operation
- instruir al técnico sobre los tiempos de activación y los tipos de evidence que deben recopilarse a través de determinados agents de targets, según las instrucciones recibidas de las autoridades legales
- monitorear mediante auditorías la aplicación correcta de las instrucciones
- cerrar targets

Qué ocurre cuando se crea un target

Cuando se crea un target, se lo declara *abierto*. A partir de esto se le puede pedir a un técnico que genere e instale agents.

Qué ocurre cuando se cierra un target

Un target se puede cerrar, por ejemplo, cuando se cierran las investigaciones para dicho target.

Al cerrar un target, automáticamente se cierran sus agents correspondientes. Cuando se cierra el agent, la desinstalación se realiza en la siguiente sincronización, lo cual deja el dispositivo limpio.

Un target cerrado no se puede volver a abrir. Solo los datos del target y los que son enviados por agents permanecen en la base de datos.

PRECAUCIÓN: cuando se cierra un target, todos los agents vinculados se desinstalan automáticamente. Cierre un target solo cuando esté seguro de tener todos los datos que necesita.

PRECAUCIÓN: en caso de sincronizaciones infrecuentes, por ejemplo, cada cuatro días, espere a que ocurra la última sincronización planificada antes de cerrar la operation.

Sugerencia: solo cierre el target cuando esté seguro de que los agents hayan descargado toda la información requerida.

Abrir y cerrar una operation

Cuando se cierra una operation, todos sus targets se cierran irreversiblemente, y se desinstalan todos sus agents. *Consulte "**Qué debería saber acerca de las operations**" en la página precedente .*

Administración de operations

Para administrar operations:	• Sección **Operations**

Propósito

Esta función le permite:

- crear una operation
- asignar la operation a un grupo de usuarios

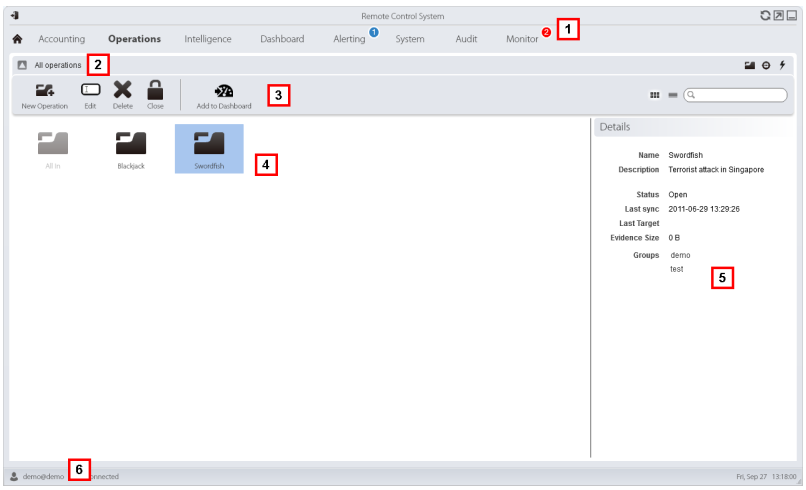
NOTA: la función solo se activa si el usuario tiene autorización **Administración de operations**.

Próximos pasos

Deben vincularse uno o más targets a la operation. *Consulte "Página de la operation" en la página 35 .*

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación

Área	*Descripción*
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Permite agregar una operation.
	Permite editar la operation seleccionada.
	Elimina la operation seleccionada.
	Cierra la operation.

4	Lista de operations creadas:  Operation abierta. Si se establecieron targets y se instalaron agents correctamente, se recibirá la evidence recopilada.  Operation cerrada. Todos los targets están cerrados y los agents desinstalados. Aún se pueden ver todos los targets y la evidence .
5	Datos de una operation seleccionada.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de la operation**" en la página 35* .

Para obtener más información sobre las operations *consulte "**Qué debería saber acerca de las operations**" en la página 30* .

Crear una operation

Para crear una operation:

Paso	*Acción*
1	Haga clic en **Nueva operation**: aparecerán los campos para ingresar datos.
2	Seleccione el grupo (o los grupos) que se asignará a la operation. NOTA: el usuario que está creando la operation debe pertenecer cuando menos a uno de los grupos vinculados.
3	Escriba los datos solicitados y haga clic en **Guardar**: la nueva operation se mostrará en el área de trabajo principal, en estado Abierto.

Edición de los datos de una operation

Para editar los datos de una operation:

Paso	*Acción*
1	Seleccione una operation y haga clic en **Editar**: aparecerán sus datos.
2	Edite los datos indicados y haga clic en **Guardar.**

Cerrar una operation

Para cerrar una operation y comenzar a desinstalar los agents en todos los targets:

Paso	*Acción*
1	Seleccione una operation y haga clic en **Cerrado**.
2	Confirme el cierre: todos los targets están cerrados y se solicita la desinstalación de todos los agents. Los datos quedarán disponibles en la base de datos. ***PRECAUCIÓN: el cierre de una operation es irreversible consulte "Qué debería saber acerca de las operations" en la página 30***

Eliminación de una operation

Para eliminar una operation:

Paso	*Acción*
1	Seleccione una operation y haga clic en **Eliminar**.
2	Para confirmar la acción haga clic en **Sí**: se eliminarán los datos de la operation, los targets, los agents y toda la evidence de la base de datos.

PRECAUCIÓN: la eliminación de una acción es irreversible, por lo que se perderán todos los datos vinculados con dicha operation.

Datos de la operation

A continuación se describen los datos de la operation seleccionada:

Datos	*Descripción*
Nombre	Nombre de la operation.
Descripción	Descripción del usuario
Contacto	Los campos descriptivos se utilizan para definir, por ejemplo, el nombre de una persona de contacto (juez, abogado, etc.).
Estado	Estado de la operation y comando de cierre: **Abierta**: la operation está abierta. Si se establecieron targets y se instalaron agents correctamente, RCS recibe la evidence recopilada. **Cerrada**: la operation está cerrada y no podrá volver a abrirse. Los agents ya no enviarán más datos, pero todavía podrá consultar la evidence que ya se recibió.  ***PRECAUCIÓN: el cierre de una operation es irreversible. Consulte "Qué debería saber acerca de las operations" en la página 30***
Grupos	Grupos que pueden ver la operation. *Consulte "Administración de grupo" en la página 26*

Página de la operation

Para ver una operation:	• En la sección **Operations**, haga doble clic en una operation

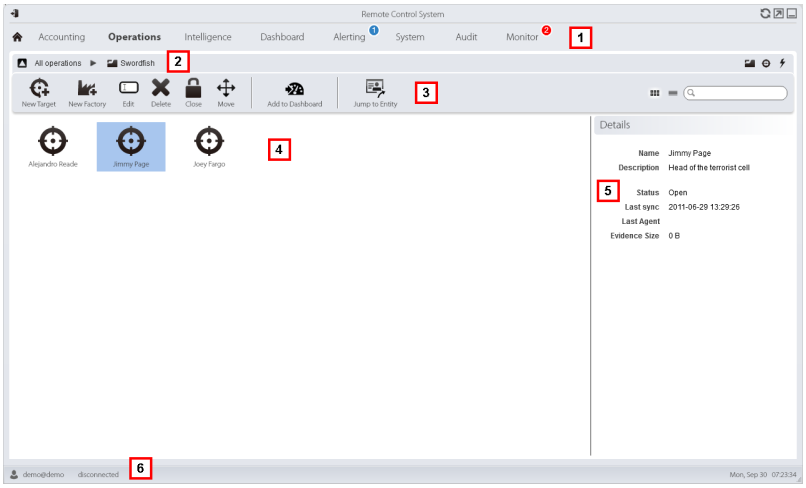
Propósito

Esta función le permite:

- crear uno o más targets que serán monitoreados durante una operation
- administrar la activación y desactivación de targets.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de navegación
3	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Función*
	Permite agregar un target.  NOTA: la función solo se activa si el usuario tiene autorización **Administración de targets**.
	Permite editar el target seleccionado.
	Elimina el target seleccionado.
	Cierra el target.
	Cambia el target a otra operation.

Área	*Descripción*
4	Lista de targets:  target abierto  target cerrado
5	Datos de un target seleccionado.
6	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para obtener más información sobre las operations *consulte "**Qué debería saber acerca de las operations**" en la página 30* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de la página de la operation**" en la página siguiente* .

Crear un target

Para crear un nuevo target:

Paso	*Acción*
1	Haga clic en **Nuevo target**: aparecerán los campos para ingresar datos.
2	Escriba los datos solicitados y haga clic en **Guardar**: el nuevo target se mostrará en el área de trabajo principal, en estado Abierto, lo cual significa que está listo para que el técnico lo utilice.

Cierre de un target

Para cerrar un target y comenzar a desinstalar sus agents:

Paso	*Acción*
1	Seleccione un target y haga clic en **Cerrar**.
2	Confirme el cierre: el target se cerrará y se iniciará automáticamente la desinstalación del agent. Los datos quedarán disponibles en la base de datos.  ***PRECAUCIÓN: el cierre de un target es irreversible consulte "Qué debería saber acerca de los targets" en la página 30***

Editar los datos de un target

Para editar los datos de un target:

Paso	*Acción*
1	Seleccione un target y haga clic en **Editar**: aparecerán sus datos.
2	Edite los datos indicados y haga clic en **Guardar.**

Eliminar un target

Para eliminar un target:

Paso	*Acción*
1	Seleccione un target y haga clic en **Eliminar**.
2	Para confirmar la acción, haga clic en **Sí**: los datos del target, sus agents y toda la evidence se eliminarán de la base de datos.

PRECAUCIÓN: la eliminación de un target es irreversible, por lo que se perderán todos los datos vinculados con dicho target.

Datos de la página de la operation

A continuación se describen los datos del target seleccionado:

Datos	*Descripción*
Nombre	Nombre del target.
Descripción	Descripción del usuario
Estado	Define el estado del target:  Abierto. Si el técnico instala los agents correctamente, RCS recibirá la evidence recopilada.  Cerrado. Cerrado, ya no se podrá volver a abrir.

5

Monitoreo de los usuarios

Presentación

Introducción

El monitoreo de los usuarios de RCS garantiza la integridad de las investigaciones, el respeto de las reglas y las indicaciones emitidas por la autoridad correspondiente que solicite las investigaciones.

Contenido

En esta sección se incluyen los siguientes temas:

Qué debería saber acerca del monitoreo de los usuarios (Audit)

Qué es el monitoreo de los usuarios

Audit es una lista de las acciones que realizaron todos los usuarios de tipo administrador, técnico y analista en RCS. Su propósito es garantizar la integridad de las investigaciones, el respeto de las reglas y las indicaciones emitidas por la autoridad correspondiente que solicite las investigaciones.

De esta forma, el Administrador puede monitorear el acceso al sistema mediante la activación de usuarios y el seguimiento de las acciones especiales a través del tiempo, tales como, por ejemplo, la creación de targets.

Cómo se leen las acciones señaladas

Audit registra en una tabla todas las acciones que cada usuario ejecuta en el sistema.

En cada acción se incluyen cuatro datos:

- fecha y hora de la acción
- usuario que realizó la acción
- tipo de acción
- descripción de la acción

Los otros campos solo se llenan de acuerdo al tipo de acción. Por ejemplo, si un usuario accede al sistema, Audit registra el nombre del usuario en **Actor** y el tipo de acción “inicio de sesión” en **Acción.**

Si un técnico crea agents, en la lista aparece una acción para cada agent con el nombre del usuario, el tipo de acción "target.create" (target.crear), el nombre de la operation, el nombre del target y el nombre del agent.

NOTA: los registros audit no están traducidos a otros idiomas, solo están disponibles en inglés.

Selección de acciones específicas usando los filtros

La función usualmente muestra las acciones realizadas en las últimas 24 horas. El filtro en la columna **Fecha** es el único que siempre se muestra de forma predeterminada, pero se puede modificar según sea necesario. Por este motivo, siempre está seleccionado el cuadro de verificación.

Se puede establecer un filtro para el resto de las columnas si se desea refinar la búsqueda. Si se selecciona el cuadro de verificación junto al encabezado, se activará el filtro en esa columna.

Cada encabezado le permite seleccionar qué datos se deben mostrar.

Solo la columna **Descripción** le permite ingresar parte del texto que desea buscar; por ejemplo, si se ingresa "registra", se mostrarán todas las acciones cuya descripción contenga la palabra "registra". Por ejemplo:

- "El usuario 'xxx' está **registra**do en"
- "...se **registra** en el archivo"

Datos exportables

RCS le permite exportar las acciones registradas de los administradores, técnicos y analistas. El archivo se descargará en la carpeta Descarga de RCS que se encuentra en el escritorio.

Monitoreo de los usuarios (Audit)

Para monitorear a los usuarios:	• Sección **Audit**

Propósito

Esta función le permite monitorear las acciones del administrador, el técnico y el analista en RCS. Por ejemplo, puede monitorear el progreso correcto de la operation, los tiempos de activación/desactivación de los targets y la aplicación correcta de los tipos de agents autorizados para una operation específica por parte del técnico.

Qué puede hacer

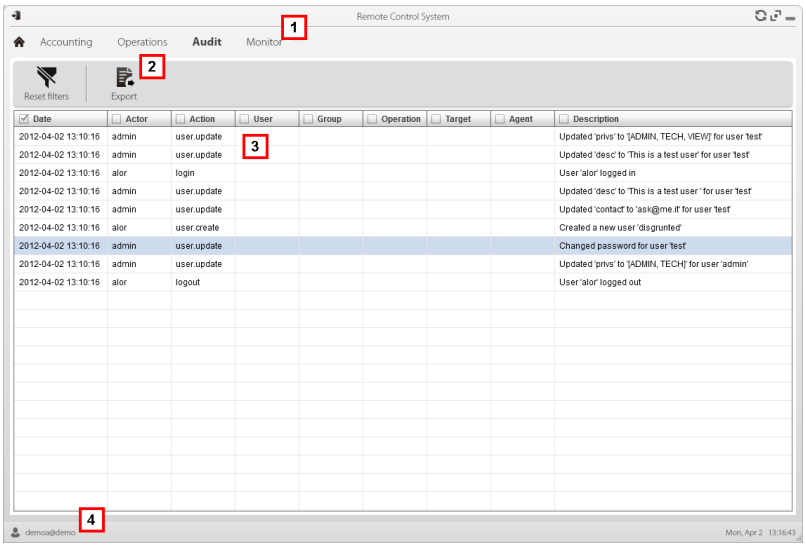
Puede seleccionar solo las acciones que se ejecutan en cierto período y aplicar filtros a la búsqueda; por ejemplo, para la información detallada sobre las operations o usuarios específicos. En caso de ser necesario, es posible exportar los archivos en formato CSV.

IMPORTANTE: si se mantiene la página abierta, se debe volver a cargar para ver las acciones más recientes. ***Consulte "Descripción de la página principal" en la página 8***

NOTA: la función está activada solo si el usuario tiene autorización **Administración de alerts**.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS.
2	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Exporta las acciones que se muestran en un archivo con formato CSV (se puede importar en Excel).
	Elimina todos los filtros que se aplicaron a los datos de la tabla.

3	Lista de acciones ejecutadas por los usuarios de RCS.
4	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de monitoreo de los usuarios (auditoría)**"*.

Para obtener más información acerca de audit, *consulte "**Qué debería saber acerca del monitoreo de los usuarios (Audit)**" en la página 40* .

Seleccionar acciones en un rango de tiempo

Para ver acciones en un cierto rango de tiempo determinado:

Paso	*Acción*
1	Haga clic en el encabezado de la columna **Fecha**.
2	Haga clic en el rango de tiempo deseado.

NOTA: el filtro fecha siempre está activado, su valor son las acciones de las últimas 24 horas. Solo se puede cambiar el criterio de búsqueda.

Seleccionar acciones en base a la fecha propuesta

Para aumentar la exactitud de los resultados:

Paso	*Acción*
1	Haga clic en uno o más encabezados de columnas: aparecerá un campo de búsqueda donde puede ingresar datos.
2	Escriba la palabra que desea buscar y presione **Entrar.** Se filtrará y ordenará la información de esta columna en base a la palabra de búsqueda ingresada.

Eliminar uno o más filtros

Para eliminar un filtro y mostrar todos los datos:

Si desea eliminar...	*Entonces...*
un solo filtro	desmarque el cuadro de verificación en el encabezado de la columna.
todos los filtros simultáneamente	haga clic en **Eliminar filtros.**

NOTA: el filtro fecha siempre está activado, su valor son las acciones de las últimas 24 horas. Solo se puede cambiar el criterio tiempo.

Exportar las acciones que se muestran

Para exportar las acciones que se muestran:

Paso	*Acción*
1	Haga clic en **Exportar**: aparecerán los campos para ingresar datos.
2	Ingrese el nombre del archivo que desea exportar y haga clic en **Aceptar:** el progreso de la operation se muestra en la barra de progreso. Para consultar el progreso, haga clic en la barra.

Datos de monitoreo de los usuarios (Audit)

Las columnas de la tabla de Audit se describen a continuación:

Columna	*Descripción*
Fecha	Fecha y hora de la acción.
Actor	Nombre del usuario conectado al sistema que causó la acción.
Acción	Tipo de acción ejecutado por el usuario conectado al sistema. La acción se muestra como *persona.acción*. Por ejemplo "user.update" (usuario.actualizar) significa que se actualizó un usuario. Esto facilita la selección de los mismos tipos de acciones.
Usuario	Usuario afectado por la acción; por ejemplo, creado por un Administrador. No debe confundirse con el nombre del Actor, que es el usuario que causó la acción.
Grupo	Grupo afectado por la acción; por ejemplo, el grupo vinculado con una operation.
Operation	Operation afectada por la acción; por ejemplo, la operation cerrada por un Administrador.
Target	El target afectado por la acción; por ejemplo, el target cerrada por un Administrador.
Agent	Agent afectado por la acción; por ejemplo, un agent creado por un Técnico.
Descripción	Breve descripción de la acción.

NOTA: todas las acciones se muestran en inglés.

6

Monitoreo del sistema

Presentación

Introducción

El monitoreo del sistema garantiza el control constante del estado de los componentes y el uso de la licencia.

Contenido

En esta sección se incluyen los siguientes temas:

Monitoreo del sistema (Monitor)

Para monitorear el sistema:	• Sección **Monitor**

Propósito

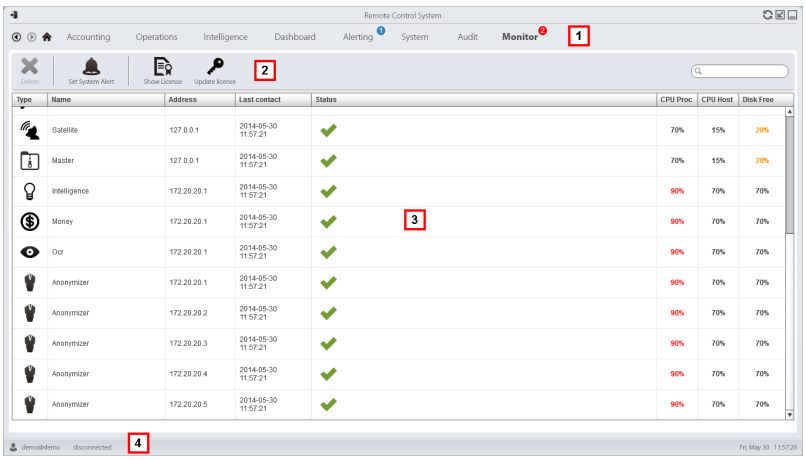
Esta función le permite:

- monitorear el estado del sistema en términos de hardware y software
- monitorear las licencias usadas en comparación con las que se compraron
- definir el grupo de alerting y un destinatario de alerts por correo electrónico en caso de alarmas del sistema

Llamada al servicio: póngase en contacto con su gerente de cuenta de HackingTeam si necesita más licencias.

Cómo se ve la función

Así es como se ve la página:



Área	*Descripción*
1	Menú de RCS. Monitor 1 : indica la cantidad actual de alarmas del sistema que se activaron.
2	Barra de herramientas de la ventana. A continuación se muestra la descripción de cada elemento:

Ícono	*Descripción*
	Define el grupo de alerting.  NOTA: la función solo se activa con los permisos **Administración de usuarios y de grupos**.
	Muestra el estado de las licencias
	Carga un nuevo archivo de licencias.  NOTA: la función solo se activa si el usuario tiene autorización **Modificación de licencias**.

3	Lista de componentes de RCS y su estado:  Alarma (genera y envía un correo electrónico al grupo de alerting)  Advertencia  Componente en funcionamiento
4	Barra de estado de RCS.

Para obtener más información

Para ver las descripciones de los elementos de la interfaz *Consulte "**Elementos y acciones comunes de la interfaz**" en la página 10* .

Para ver una descripción de los datos en esta ventana *consulte "**Datos de monitoreo del sistema (Monitor)**" en la página siguiente* .

Define el grupo de alerting o lo activa/desactiva temporalmente

Para seleccionar el grupo de alerting:

Paso	*Acción*
1	Haga clic en **Establecer alert**.
2	• Para desactivar las notificaciones por correo electrónico, seleccione **Ninguna**. o • Para activar las notificaciones por correo electrónico para un grupo, seleccione **Seleccionar un grupo que reciba alertas por correo electrónico** y el grupo de alerting del menú desplegable. Cada vez que se active una alarma de sistema, el grupo seleccionado recibirá un correo electrónico con su descripción.
3	Haga clic en **Guardar**.

Sugerencia: para agrupar fácil y rápidamente a los usuarios que recibirán las alarmas de RCS, cree un grupo de "alerting" que contenga a todos los usuarios que deben recibir una alerta en caso de que haya una alarma no vinculada con ninguna operation. *Consulte "**Administración de usuarios**" en la página 19*

Datos de monitoreo del sistema (Monitor)

Datos del monitoreo de los componentes del sistema

A continuación se muestran los datos de monitoreo del sistema:

Datos	*Descripción*
Tipo	Tipo y nombre de los componentes monitoreados.
Nombre	A continuación se muestran algunos ejemplos:  Anonymizer  Carrier  Collector  Database  Network Controller
Dirección	Dirección IP del componente.
Último contacto	Fecha y hora de la última sincronización.

Datos	*Descripción*
Estado	Estado del componente en la última sincronización:  Alarma: el componente no está funcionando, póngase en contacto con el grupo de alerting para repararlo de inmediato.  Advertencia: el componente indica una situación de riesgo, póngase en contacto con el administrador del sistema para que realice las revisiones necesarias.  Componente en funcionamiento.
Proceso de CPU	% de uso de CPU por parte del proceso particular.
Host de CPU	% de uso de CPU por parte del servidor.
Espacio libre en el disco	% de espacio libre en el disco.

Datos de monitoreo de la licencia

A continuación se describen los datos de monitoreo de la licencia: para las licencias restringidas, el formato es "x/y", donde "x" es la cantidad de licencias que el sistema utiliza actualmente e "y" es la cantidad máxima de licencias.

PRECAUCIÓN: si todas las licencias están en uso, cualquier agent nuevo quedará en una cola de espera hasta que se libere una licencia o se compren más licencias.

Datos	*Descripción*
Tipo de licencia	Tipo de licencia actualmente en uso para los agents. **reusable**: una licencia de agent puede volver a utilizarse después de que se desinstala. **oneshot**: la licencia de un agent solo es válida para una instalación.  NOTA: la licencia solo puede actualizarse si el usuario tiene autorización **Modificación de licencias**.
Usuarios	Cantidad de usuarios actualmente en uso por parte del sistema y cantidad máxima admitida.
Agent	Cantidad de agents actualmente utilizados por el sistema y cantidad máxima admitida.

Datos	*Descripción*
De escritorio **Móvil**	Cantidad de agents de escritorio y móviles actualmente utilizados por el sistema y cantidades máximas admitidas, respectivamente.
Servidores distribuidos	Cantidad de bases de datos actualmente utilizadas por el sistema y cantidad máxima admitida.
Collectors	Cantidad de Collectors actualmente utilizados por el sistema y cantidad máxima admitida.
Anonymizers	Cantidad de Anonymizers actualmente utilizados por el sistema y cantidad máxima admitida.

]HackingTeam[

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

RCS 9.5 Manual del administrador
Manual del administrador 1.6 NOV-2014

info@hackingteam.com