

ViRobot Intranet Security Management System 3.5

5.5



Herramientas



ViRobot

www.hauri-la.com

Contenido



1. Pruebas y Actualizaciones

2. ViRobot

3. Editar Configuración

4. Traer Información

5. Comandos Remotos

6. Tareas de Nodos/Clientes

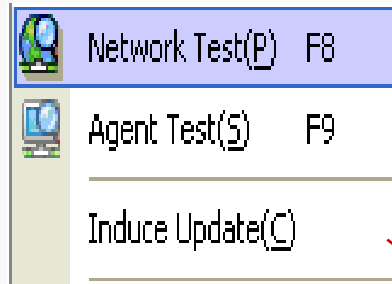
7. Respuesta a Epidemias



1. PRUEBAS Y ACTUALIZACIONES



Pruebas y actualizaciones : Se pueden realizar diferentes pruebas de funcionalidad así como forzar a los clientes para que se actualicen desde VISMS 3.5.



Prueba de Red: Manda solicitudes de eco entrante (ping) a los clientes, para saber que equipos se encuentran encendidos.

Prueba de Agente: Manda una petición al agente del cliente, y este responde si esta funcionando de manera correcta.

Forzar la actualización: Manda las actualizaciones a los clientes sin esperar a que ellos la soliciten.



2. VIROBOT.



ViRobot : Escaneos remotos, configuración, pausa del escaneo residente, quitar pausa de escaneo Residente, así como el control de la operación de ViRobot (Escaneo en tiempo real, Firewall, Control de Acceso y Protección de Correo)

The image shows a context menu for ViRobot with the following items and their corresponding callout boxes:

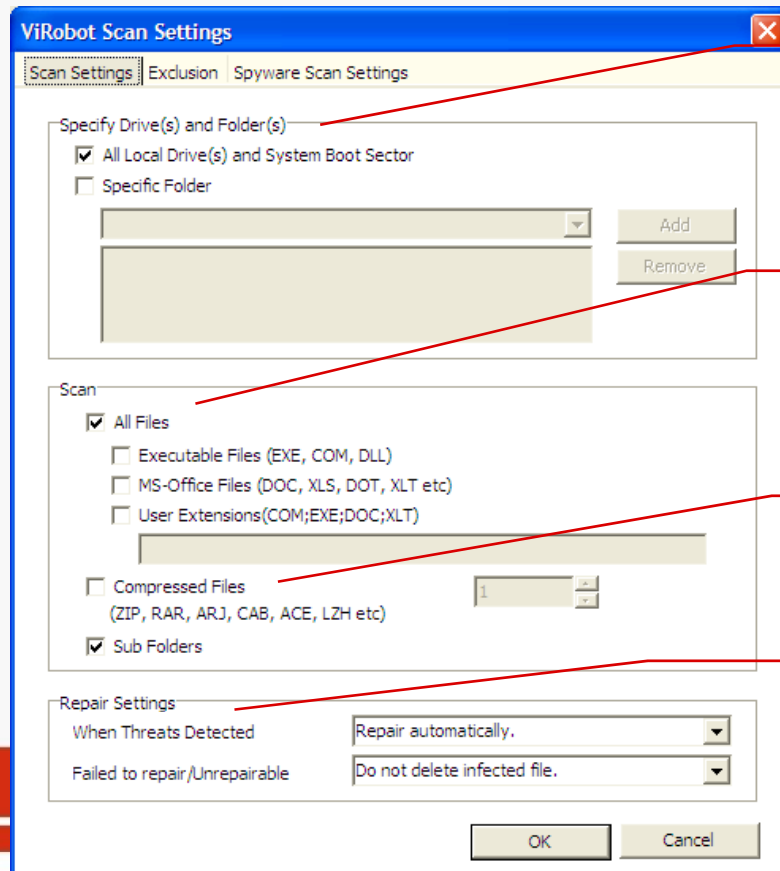
- Remote Virus Scan(Y)**: Manda la instrucción para iniciar el escaneo remoto del cliente seleccionado.
- Remote ViRobot Scan Settings**: Configuración del escaneo remoto.
- Pause Resident Scan**: Pausar el escaneo residente.
- Restart Resident Scan**: Reiniciar el escaneo residente.
- Control of Real-time ViRobot Operation**: Control de Operación de ViRobot.



2. ViRobot (Escaneo Remoto)



Configuración del escaneo : Especificas las unidades, archivos, nivel de compresión y subcarpetas para que sean analizados



Especificas las unidades o carpetas a escanear

Especificas el tipo de archivos vas a escanear

Nivel de compresión que deberá de analizar el escaneo remoto

Configuración de Reparación

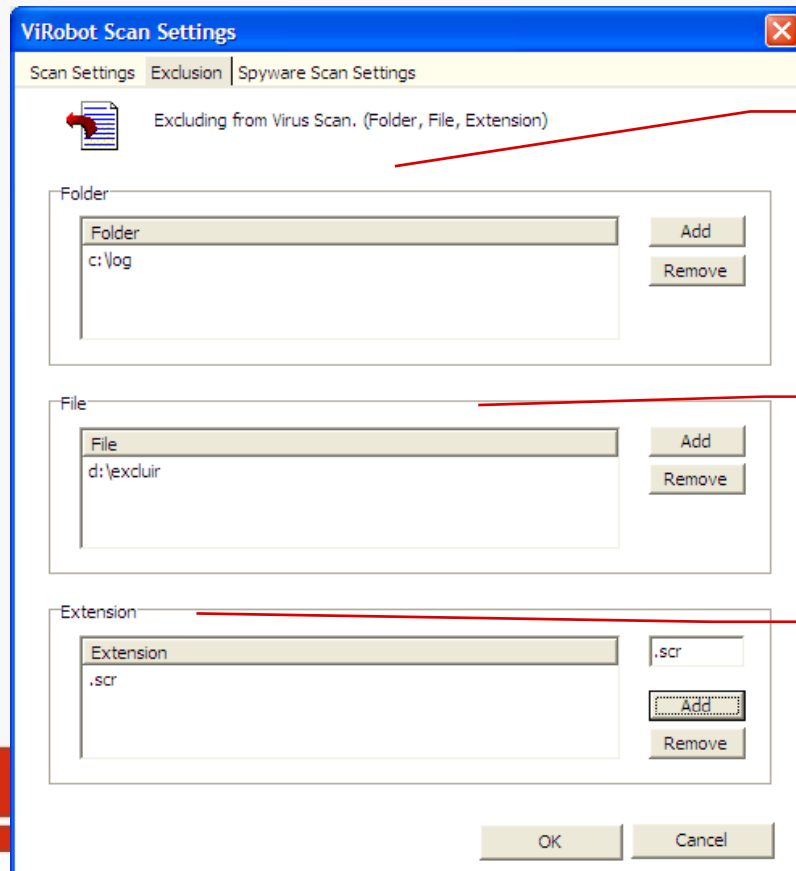
ViRobot



2. ViRobot (Escaneo Remoto)



Exclusiones: En esta parte, se pueden excluir carpetas, archivos o extensiones de archivos que no se desea escanear.



Opción para excluir carpetas.

Opción para excluir archivos.

Opción para excluir extensiones de archivos.

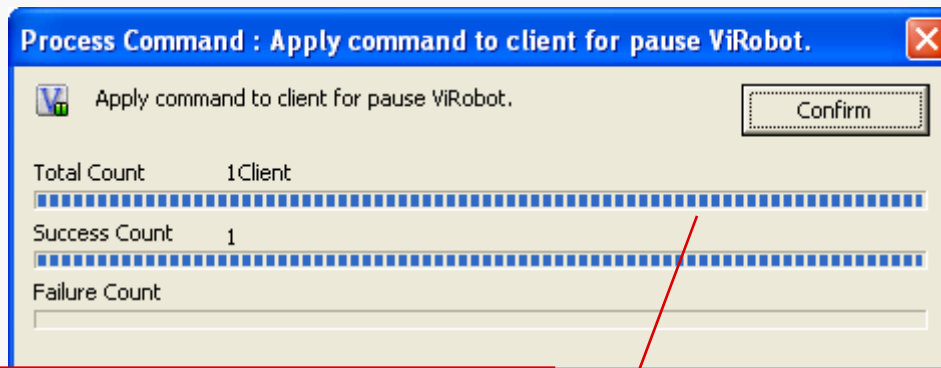


2. ViRobot (Pausa)



Pausa el escaneo Residente: El escaneo en tiempo real se puede pausar (si es necesario)

- Clientes totales: Es el número total de clientes incluidos en el nodo seleccionado.
- Conexión exitosas: Por una respuesta normal, el cliente será incluida en conexión exitosa.
- Cuentas Fallidas: Por la falta de una respuesta normal, el cliente será incluida en cuentas fallidas.



Envío de comando remoto de pausa al cliente.

En la consola de VISMS en información del cliente, te muestra que el escaneo residente esta detenido (cuando la conexión fue exitosa).

Total Nodes - File					
Computer Name	Telephone Number	Engine Version	Identifier	Resident Scan	OS
MORENO	123	2008-01-22.03 (890427) : ViRobot Desktop 5.5		Paused	Microsoft Windows XP ...
PROTEKTN-332849		2008-01-22.03 (890427) : ViRobot Desktop 5.5			Microsoft Windows XP ...

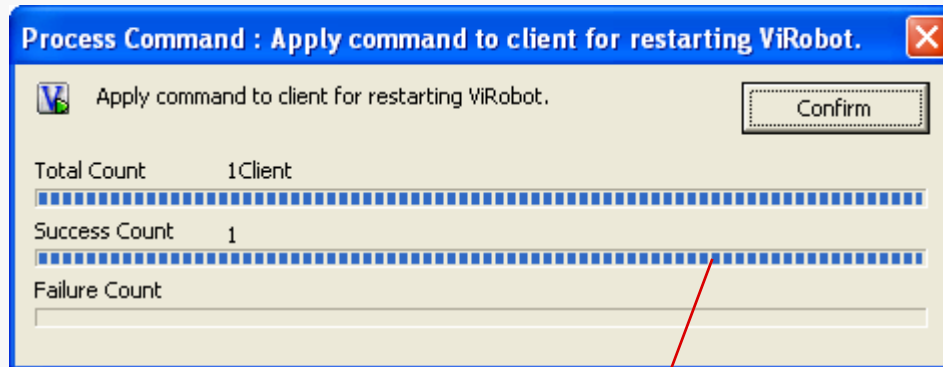


2. ViRobot (Reiniciar)



Reiniciar el escaneo Residente: Reinicia el escaneo en tiempo real.

- Clientes totales: Es el número total de clientes incluidos en el nodo seleccionado.
- Conexión exitosas: Por una respuesta normal, el cliente será incluida en conexión exitosa.
- Cuentas Fallidas: Por la falta de una respuesta normal, el cliente será incluida en cuentas fallidas.



En la consola de VISMS en información del cliente, te muestra que el escaneo residente no esta detenido o pausado (cuando la conexión fue exitosa).

Envío de comando remoto de reiniciar al cliente.

Total Nodes - File					
Computer Name	Telephone Number	Engine Version	Identifier	Resident Scan	OS
MORENO	123	2008-01-22.03 (890427) : ViRobot Desktop 5.5			Microsoft Windows XP ...
PROTEKTN-332849		2008-01-22.03 (890427) : ViRobot Desktop 5.5			Microsoft Windows XP ...



2. ViRobot (Tiempo Real)



Control de la operación en tiempo real de ViRobot: Permite iniciar/detener los servicios que ofrece ViRobot



Capacidad para iniciar/detener los servicios de los clientes de la VISMS 3.5. Estos servicios son

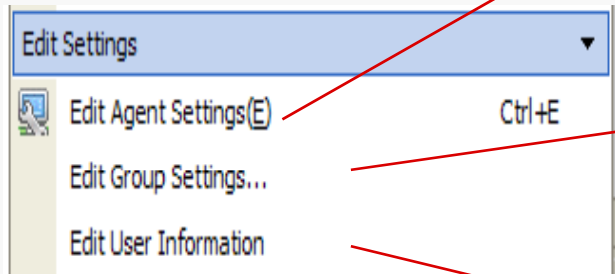
- Escaneo Residente
- Firewall del PC
- Control de Acceso
- Protección de Correo



3. EDITAR CONFIGURACION



Editar la Configuración: Este menú, nos da la opción de editar la configuración del Agente por usuario, grupo, así como la información del usuario.



Editar la configuración del Agente por usuario.

Editar la configuración del Agente por Grupos.

Editar la configuración del Usuario. (Teléfono, nombre del usuario, etc.)



3. Configuración del Agente (Configuración del Usuario)



Editar la Configuración: Este menú, nos arroja información del cliente, además, nos da la opción de editar la información del usuario.

The screenshot shows the 'Client Environment Settings' window for a client named 'Cmoreno'. The window is divided into two main sections: 'Node Information' on the left and 'Client' settings on the right. The 'Node Information' section includes fields for Type (Client), Path (Main server\Cmoreno\), Address (127.0.0.1), ID (00-15-00-3D-27-8F), and various product and engine details. The 'Client' section has tabs for 'User Settings', 'General', 'Restriction Policy', 'Display', and 'Update'. The 'User Settings' tab is active, showing fields for Name (Cmoreno), Department (Virtual), Telephone (0), and Number. There is also a text area for 'Other Description' and a status bar at the bottom.

- Tipo: Cliente
- Ruta: Servidor Principal (Es decir, es cliente del servidor principal)
- Dirección IP: IP del Cliente.
- ID: Dirección MAC

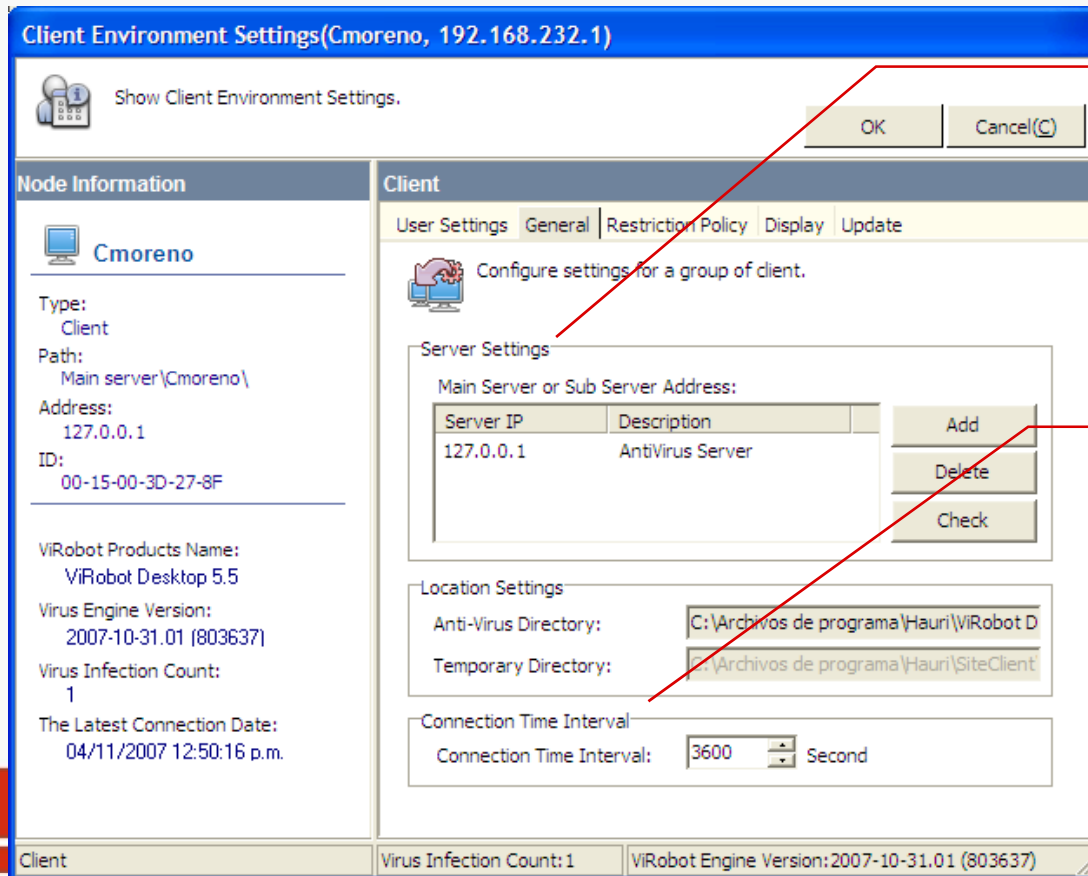
- Nombre: Nombre del Equipo
- Departamento: Grupo/Departamento al que pertenece el cliente
- Teléfono
- Numero



3. Configuración del Agente (General)



Editar la Configuración del Agente (General): Esta opción reporta la IP del servidor principal así como el intervalo de conexión del cliente al VISMS 3.5



Determinar la IP del o los Servidores a los cuales reportara el agente para descargar las actualizaciones y enviar reporte

Establecer los intervalos de tiempo para las actualizaciones de las listas de virus, motor y versión de productos. **Las actualizaciones no requieren reinicio del sistema**



3. Configuración del Agente (Restricciones)



Editar la Configuración del Agente (Restricciones): Nos permite restringir al usuario para que no pueda hacer modificación alguna a la configuración del cliente del VISMS 3.5

Client Environment Settings(Cmoreno, 192.168.232.1)

Show Client Environment Settings. [OK] [Cancel(C)]

Node Information

Cmoreno

Type: Client
Path: Main server\Cmoreno\
Address: 127.0.0.1
ID: 00-15-00-3D-27-8F

ViRobot Products Name: ViRobot Desktop 5.5
Virus Engine Version: 2007-10-31.01 (803637)
Virus Infection Count: 1
The Latest Connection Date: 04/11/2007 12:50:16 p.m.

Client

User Settings | General | **Restriction Policy** | Display | Update

Apply a restriction policy to selected VMS clients in order to prevent them from configuring certain ViRobot options.

Lockdown Option in Client Settings
Select Lockdown Option : No modifiable All

Un-installation Password:
Enter a password to prevent clients from removing VMS Client (Default: agentdown)
Uninstallation Password : agentdown
 No Password

Restrict Update Time Settings
Update is restricted during the time. Please set restrict update time.
 Set Restriction Time Release Restriction
Time : 02:26:53 p.m. - 03:26:53 p.m.

Client | Virus Infection Count:1 | ViRobot Engine Version:2007-10-31.01 (803637)

Se pueden establecer los privilegios de cambios en la Configuración del Agente.

Allow All Modification

– Acceso a todo

Disallow All modification

– Restricción Total

Establecer una contraseña para la desinstalación del Agente (ViRobot ISMS Client 3.5). **Nota:** La Desinstalación del Agente es independiente a la del ViRobot Desktop.

En el caso de que en la red se realicen procesos los cuales utilizan amplio ancho de banda, es posible determinar intervalos de tiempo en los cuales no se realizan actualizaciones

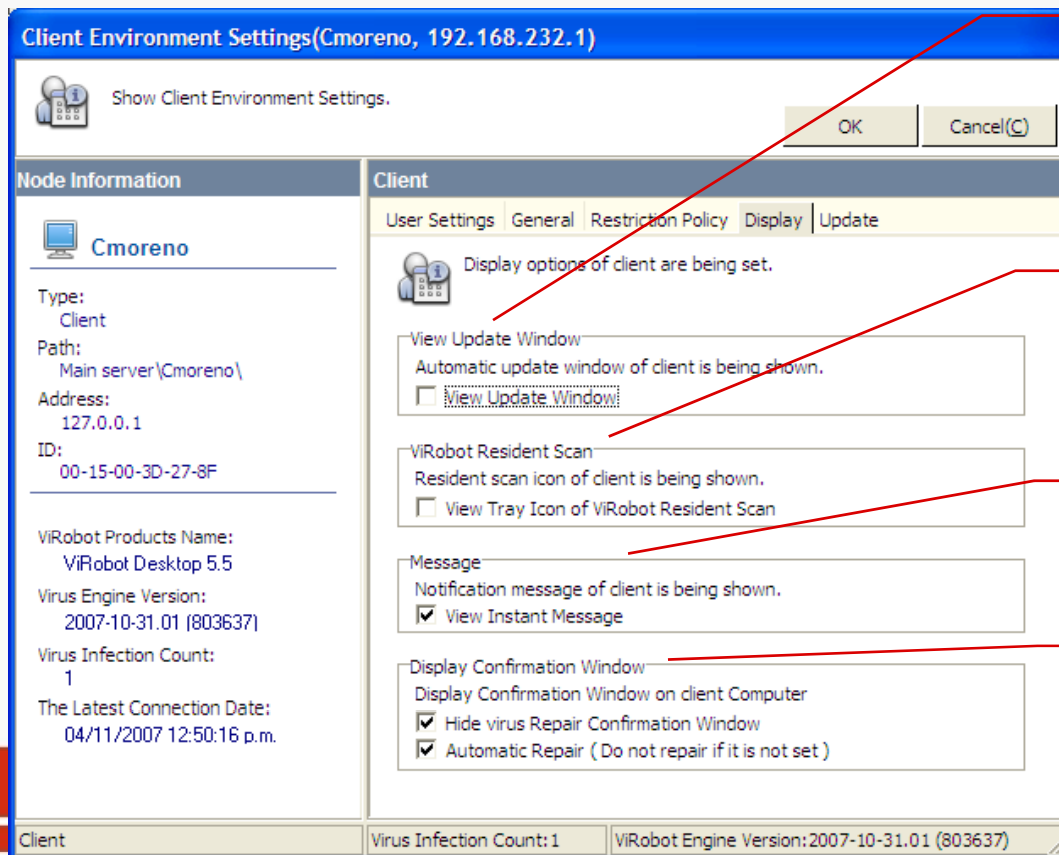
ViRobot



3. Configuración del Agente (Pantallas)



Configuración del Agente (Pantallas): Configuración para que no muestre las actualizaciones a los Clientes, mostrar/esconder el icono de ViRobot, desplegar mensajes, esconder ventanas de detección.



Autorizar que el usuario vea las actualizaciones que realiza el servidor en el Agente. **Nota: Recomendamos ocultar este proceso por transparencia al usuario.**

Esconder o mostrar el icono de el ViRobot. **Nota: Recomendamos ocultar este proceso por transparencia al usuario**

Desplegar Mensajes de Texto de las Actividades del Agente

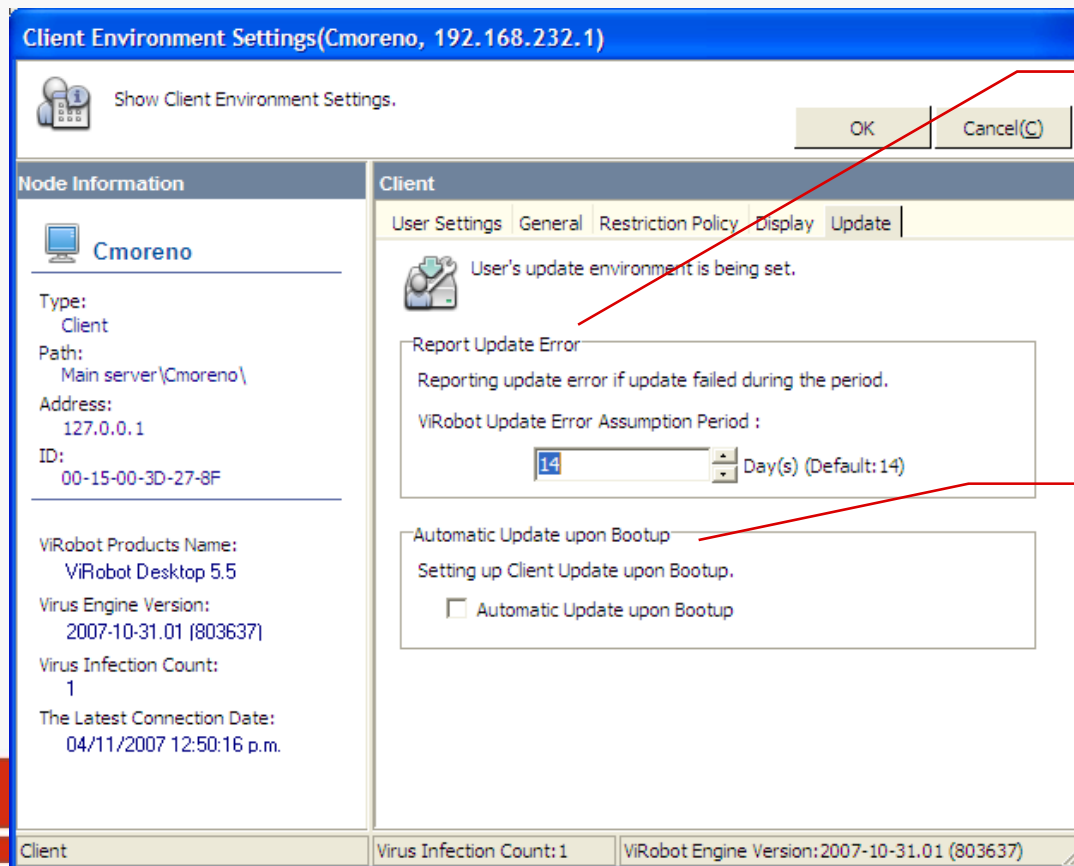
Reparar el clientes de Windows. Esconde el mensaje de confirmación al momento que ViRobot detecta un virus y repara Automáticamente. **Nota: Se deben de activar estas 2 Opciones.**



3. Configuración del Agente (Actualizaciones)



Configuración del Agente (Actualizaciones): Reporte de error si las actualizaciones no se realizan en el numero determinado de días que se configure y configuración de actualización en el inicio del sistema.



Con esta configuración se generara un reporte de error si algún cliente no se actualiza después de el tiempo definido.

Actualización automática.
Actualiza al cliente automáticamente al iniciar sesión.

ViRobot



3. Configuración por Grupo (General)



Configuración por Grupo (General): En esta opción se puede establecer la configuración básica
El intervalo de actualizaciones y establecer la IP del VISMS 3.5

Edit Group Settings

General | Restriction Policy | Notify | Update | ViRobot Resident

Configure settings for a group of client.

Basic Information

Department: **HAURI MEXICO**

Use computer name as user name

Use workgroup name as group name

Connection Time Interval

In every: **3600** second(s)

Server Settings

Main Server or Sub-server IP Address:

Server Address	Description
----------------	-------------

Add

Remove

OK Cancel(C)

Puedes cambiar el nombre del departamento y cambiar el nombre del usuario por el nombre de la computadora (del grupo seleccionado).

Determinar el Intervalo de conexión de los Agentes hacia el SiteServer.

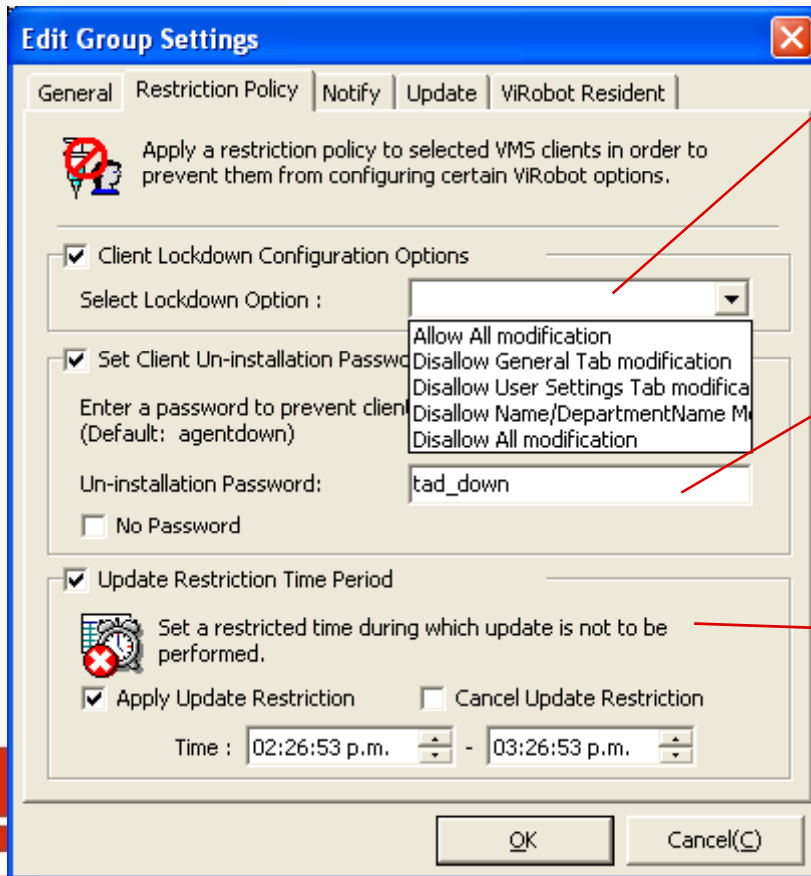
Establece las IP de o los Servidores a los cuales los Agentes buscaran las actualizaciones.



3. Configuración por Grupo (Políticas de Restricción)



Editar la Configuración por Grupo (Restricciones): Nos permite restringir al usuario para que no pueda hacer modificación alguna a la configuración del cliente del VISMS 3.5



Se pueden establecer los privilegios de cambios en la Configuración del Agente.
Allow All Modification
– Acceso a todo
Disallow All modification
– Restricción Total

Establecer una contraseña para la desinstalación del Agente (ViRobot ISMS Client 3.5). **Nota:** La Desinstalación del Agente es independiente a la del ViRobot Desktop.

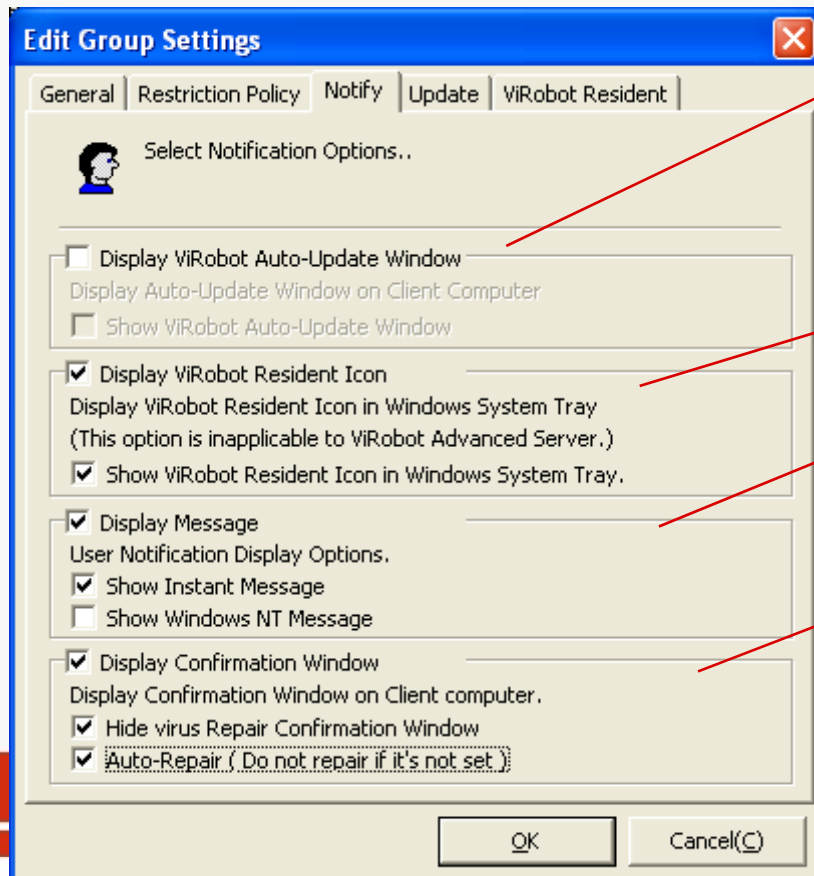
En el caso de que en la red se realicen procesos los cuales utilizan amplio ancho de banda, es posible determinar intervalos de tiempo en los cuales no se realizan actualizaciones



3. Configuración por Grupo (Notificación)



Configuración por Grupo (Notificación): Configuración para que no muestre las actualizaciones a los Clientes, mostrar/esconder el icono de ViRobot, desplegar mensajes, esconder ventanas de detección.



Autorizar que el usuario vea las actualizaciones que realiza el servidor en el Agente. **Nota: Recomendamos ocultar este proceso por transparencia al usuario.**

Esconder o mostrar el icono de el ViRobot.

Desplegar Mensajes de Texto de las Actividades del Agente

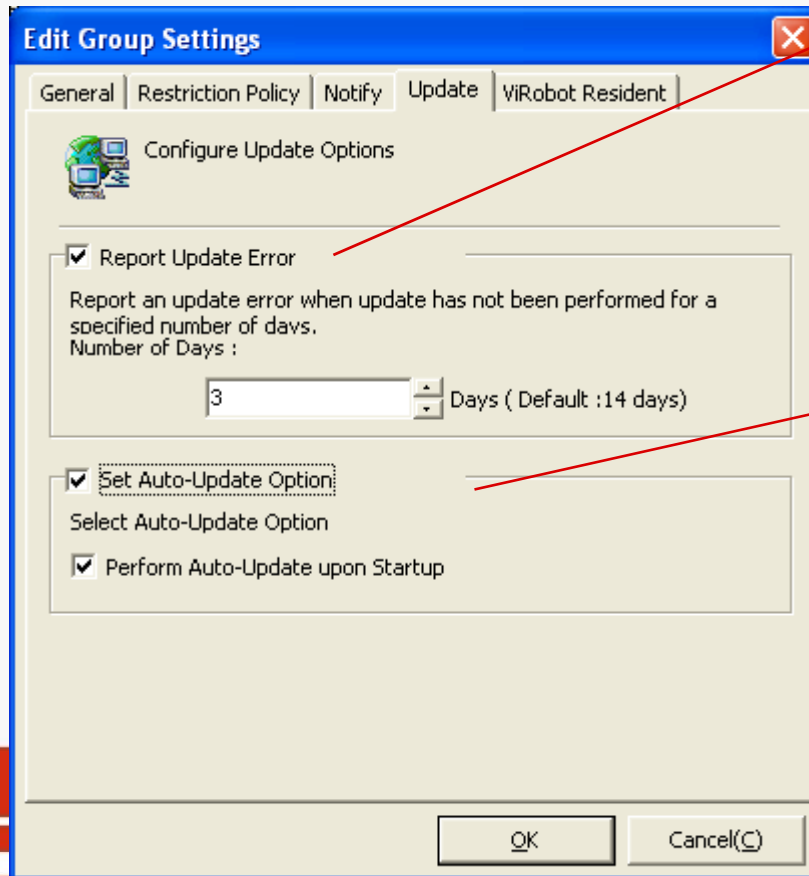
Reparar el clientes de Windows. Esconde el mensaje de confirmación al momento que ViRobot detecta un virus y repara Automáticamente. **Nota: Se deben de activar estas 2 Opciones.**



3. Configuración por Grupo (Actualizaciones)



Configuración por Grupo (Actualizaciones): Reporte de error si las actualizaciones no se realizan en el numero determinado de días que se configure y configuración de actualización en el inicio del sistema.



Con esta configuración se generara un reporte de error si algún cliente no se actualiza después de el tiempo definido.

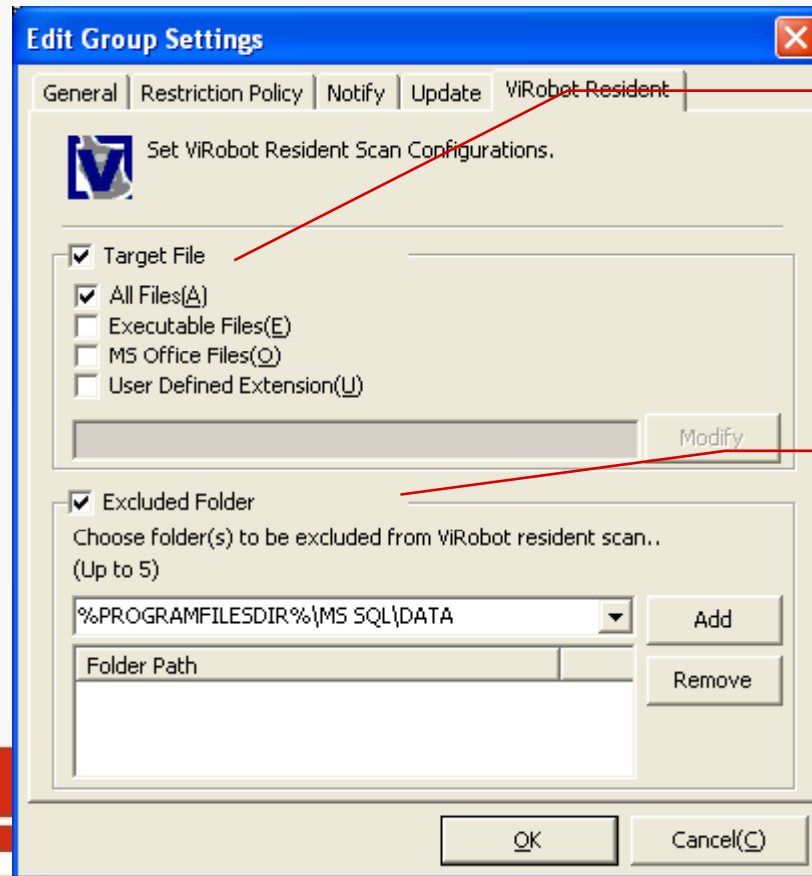
Actualización automática.
Actualiza al cliente automáticamente al iniciar sesión.



3. Configuración por Grupo (ViRobot Residente)



Configuración por Grupo (ViRobot Residente): Configuración para el escaneo de archivos en tiempo real, así como la posibilidad de excluir carpetas de este escaneo.



Escaneo en tiempo real para los clientes.
NOTA: En equipos con Windows 98, Me, Se recomienda dejar:

- Executables
- MS-Office Files

Opción para excluir carpetas en el escaneo en tiempo real.
NOTA: Se recomienda excluir carpetas solamente con archivos no infectables, tales como Bases de datos, etc.

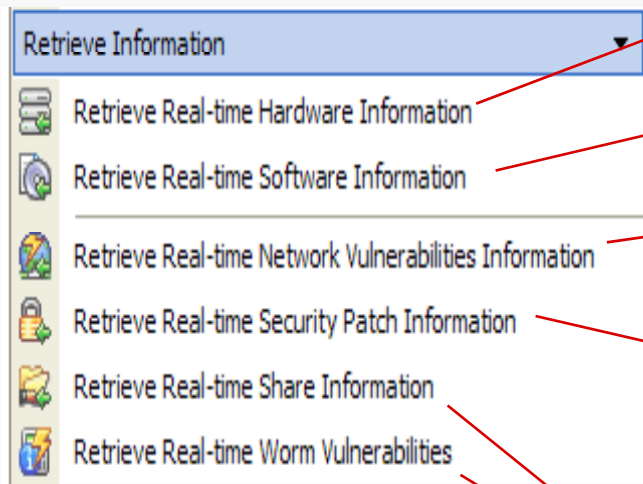
ViRobot



4. RECOLECCION DE INFORMACION



Traer Información: En este menú, podemos traernos diferente información de nuestros clientes como Información de Hardware, Software, Vulnerabilidades de Red, Parches de Seguridad, Carpetas compartidas, Vulnerabilidades explotadas por Gusanos.



Información de Hardware en Tiempo Real

Información de Software en Tiempo Real

Información de Vulnerabilidades de Red en Tiempo Real

Información de Parches de Seguridad de MS en Tiempo Real

Información de Carpetas Compartidas en Tiempo Real

Información de Vulnerabilidades explotadas por Gusanos en Tiempo Real

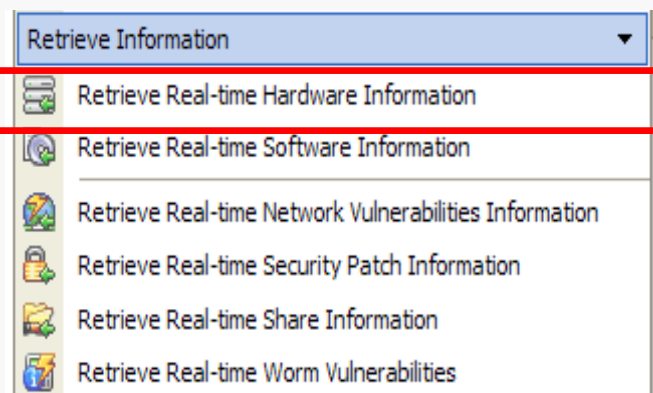


4. Información de Hardware en Tiempo Real



Inventario de Hardware: Aquí podemos traernos la información del Inventario de Hardware en tiempo real de los clientes de la VISMS 3.5

Traerse la información del Inventario de Hardware en Tiempo Real



Información de Hardware del Cliente, BIOS Versión, Sistema Operativo, Tipo de CPU, Memoria Principal, etc.

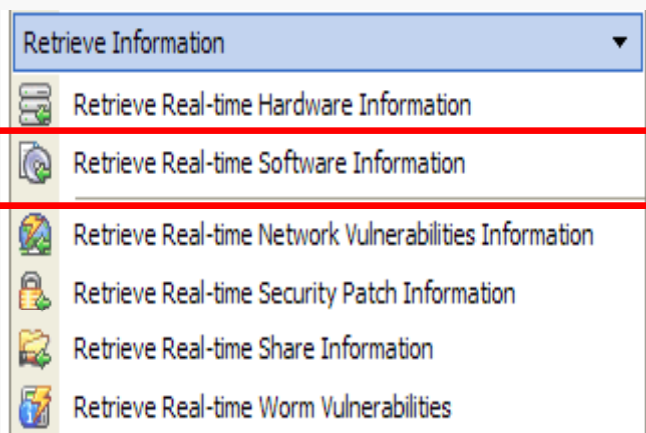
Item	Contents
ViRobot Version	2008-01-22.03 (890427)
Agent Version	Version 2006.427 (Release 0, BuildNo 244)
Name	Moreno
Department Name	Produccion
Company Name	
Telephone	123
Mobile	
BIOS Date	09/16/05
BIOS Version	HP - 16090520
Operating System	Microsoft Windows XP Version 5.1 BuildNo(2..
Windows Directory	C:\WINDOWS
CPU Type	Intel(R) Pentium(R) M processor 1.73GHz
Screen Size	1024 X 768
Input Method Editor(IME)	None
Main Memory	1528MB



4. Información de Software en Tiempo Real



Inventario de Software: Aquí podemos traernos la información del Inventario de Software en tiempo real instalado en los clientes de la VISMS 3.5.



Traerse la información del Inventario de Software en Tiempo Real

Item	Version	Contents
Revisión de Windows XP - KB884575	20040827....	C:\WINDOWS\\$\NtUninstallKB884575\$\spuninst\sp...
Revisión de Windows XP - KB885464	20040927....	C:\WINDOWS\\$\NtUninstallKB885464\$\spuninst\sp...
Revisión de Windows XP - KB885855	20040930....	C:\WINDOWS\\$\NtUninstallKB885855\$\spuninst\sp...
Revisión de Windows XP - KB888239	20041124....	C:\WINDOWS\\$\NtUninstallKB888239\$\spuninst\sp...
Revisión de Windows XP - KB892559	20050125....	C:\WINDOWS\\$\NtUninstallKB892559\$\spuninst\sp...
Simplite-MSN 2.2	02.02.2011	M:\Program Files\MSN\MSN22\MSN22.exe
Sonic DLA	4.97	C:\Program Files\Sonic\DLA\DLA.exe
SoundMAX	5.12.0	C:\Program Files\SoundMAX\SoundMAX.exe
Texas Instruments PCIxx21/x515 drivers.	1.10.0	C:\Program Files\Texas Instruments\PCIxx21\Driver\7\INT...
ViRobot Desktop 5.5		C:\Program Files\ViRobot\ViRobot Desktop 5.5\ViRobot Desktop 5.5.exe
ViRobot ISMS Client 3.5		C:\Program Files\ViRobot\ISMS Client 3.5\ISMS Client 3.5.exe
ViRobot ISMS Server 3.5	3.5	C:\Program Files\ViRobot\ISMS Server 3.5\ISMS Server 3.5.exe
Windows Live Messenger	8.1.0170.00	C:\Program Files\Windows Live\Messenger\msiexec.exe
Windows Media Format Runtime		"C:\Archivos de programa\Windows Media Player\...

Información del Software instalado, se puede salvar en un archivo, hacer desinstalación remota, ver usuarios con algún software determinado, etc.



4 Información de Vulnerabilidades de Red en Tiempo Real



Información de Vulnerabilidades de Red: Nos podemos traer la información de las conexiones actuales en tiempo real ya sean por TCP o UDP, su estado, de los clientes de la VISMS 3.5.

Obtencion de Información de Vulnerabilidades de Red en Tiempo Real

Información de los protocolos actuales (TCP, UDP) puertos, estado, etc.

Group Name	User Name	Local IP	Local Port	Remote IP	Remote P...	PID	Path
Produccion	Moreno	192.16...	139	0.0.0.0	0	4	System
Produccion	Moreno	192.16...	1034	213.186...	80	2160	C:\Archivos de programa\Secway\Si...
Produccion	Moreno	192.16...	1052	207.46....	1863	2160	C:\Archivos de programa\Secway\Si...
Produccion	Moreno	192.16...	3238	192.168...	2441	2564	C:\Archivos de programa\MSN Mess...

En caso de actividad maliciosa, el proceso se puede bloquear, terminar y borra después de que se haya terminado.

Path	Status	Exploitable Vulnerability
System	Listen	Chode, Fire HackeR, Msinit, Nimda, Opaserv, Qaz
C:\Archivos de programa\Secway\Si...	Waiting for Close	KWM
C:\Archivos de programa\Secway\Si...	Establis	it Daemon
C:\Archivos de programa\MSN Mess...	Establis	
C:\Archivos de programa\MSN Mess...	Establis	
C:\Archivos de programa\MSN Mess...	Establis	
C:\ARCHIV~1\MOZILL~1\FIREFOX...	Established	

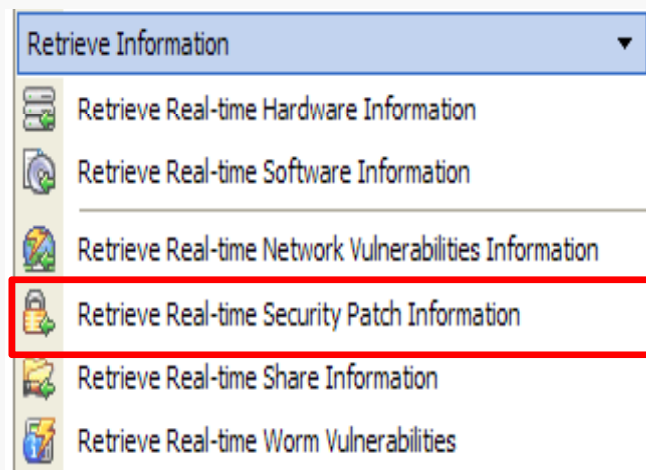
- Block Session
- Terminate Process
- Delete after terminating process



4. Información de Parches de Seguridad de MS en Tiempo Real



Información de Parches Críticos de Microsoft: En esta opción podemos revisar que parches de Seguridad críticos de Microsoft tiene el equipo instalado.



Traerse la Información de Parches de Seguridad de MS en Tiempo Real

Item	Contents
Operating System	Microsoft Windows XP
Operating System ServicePack	Service Pack 2
Internet Explorer	6.0.2900.2180
OS Hotfix #1	MS02-009
OS Hotfix #2	MS03-011
OS Hotfix #3	MS04-038
OS Hotfix #4	MS06-074
IE Hotfix #1	SP2

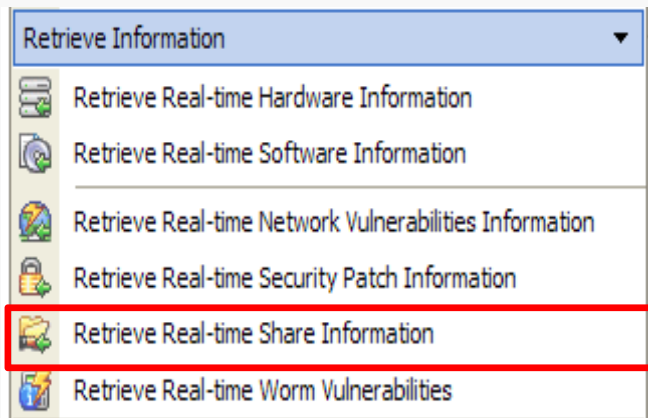
Información parches de Seguridad. Consigue la información sobre los parches de seguridad de el cliente (usted puede traer la lista de los parches de seguridad de los cliente que selecciono) Dando clic en Retrieve Real-Time Security Patch Information.



4. Información de Carpetas Compartidas en Tiempo Real



Información de Carpetas Compartidas: Nos permite ver que carpetas compartidas tiene el cliente, que permisos tiene, modificarlos o remover el recurso compartido.



Información de Carpetas Compartidas en Tiempo Real

Podemos aplicar permisos de solo lectura, todos los permisos, remover el recurso, etc.



Muestra el nombre del recurso compartido, así como al grupo que pertenece, nombre del usuario, Dirección IP, la ruta del recurso compartido, los permisos de lectura, escritura y ejecución, etc.

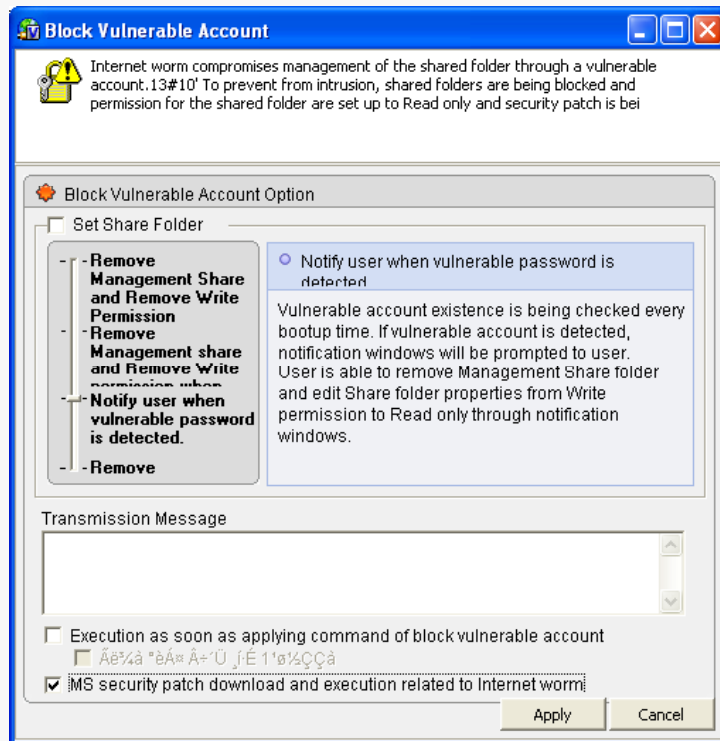
Share Name	Group Name	User Name	Address	Path	Description	Permission	Password
Sistema	Produccion	Moreno	192.168.4.17	D:\Mis Documentos\E...		Classified Permissions	Classified Permissions
Programas	Produccion	Moreno	192.168.4.17	D:\Mis Documentos\E...		Classified Permissions	Classified Permissions



4. Información de Vulnerabilidades explotadas por Gusanos



Infamación de Vulnerabilidades: Nos da información de vulnerabilidades que actualmente explotan los Gusanos para poder infectar nuestros equipos, y nos informa que parche nos hace falta.



Opción de remover recursos compartidos (Admin\$, C\$, D\$) y remover permisos de escritura, notificar al usuario cuando utiliza una cuenta vulnerable, o simplemente remover recurso compartidos.

Información de parches de Seguridad críticos faltantes que pueden ser explotados por Gusanos

Group Name	User Name	Address	Worm Virus Res...	Vulnerable Account	Worms Vulnerabilities Security Patch List
Production	Moreno	192.168.4.17	Not specified	Administrador(123456789);	MS05-043;MS05-047;MS05-051;MS06-002;



5.- COMANDOS REMOTOS



Comandos Remotos: Respuesta rápida, envío de mensajes, archivos, ejecución de programas, editar el registro, revisar el administrador de tareas, explorador remoto, control remoto, apagar equipos, todo esto se puede hacer de forma remota desde la consola.

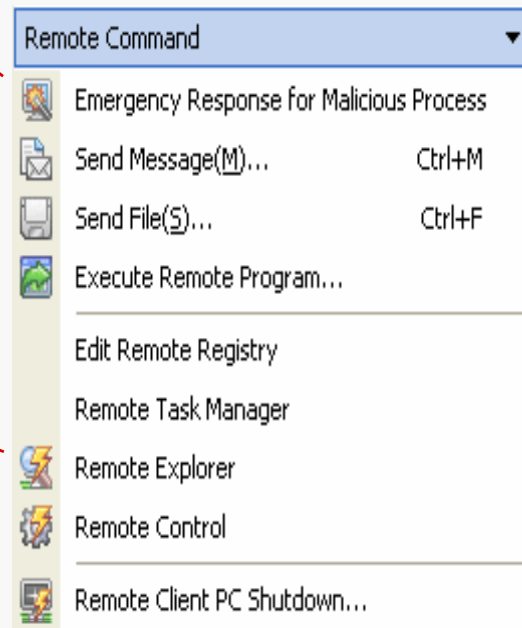
Respuesta rápida a emergencias

Envío de archivos.

Editar el registro.

Explorador remoto.

Apagar los equipos.



Envío de mensajes

Ejecutar programas.

Abrir el administrador de tareas

Control remoto hacia el cliente



5. Respuesta rápida de emergencia contra procesos maliciosos



Respuesta de emergencia: Con esta poderosa herramienta tenemos la opción de terminar algún Proceso malicioso, así como borrar la entrada que haya generado en el registro y sacar un Log de estas acciones.

Emergency Response for Malicious Process

Please enter program name, file name, registry value for the command of emergency response for malicious program. In case of relative path, please use the registered path.

Terminate Malicious Process

Please register running malicious process name.

Process Name: C:\Windows\System32\sysconf.exe

Delete file after terminating process

Delete Registry Value

Deleting start value of registry registered by malicious process.

Value Name: Video Process

Create Log File

Creation Path: C:\malicious.log

Open(O)... Save(S) Ok(O) Cancel(C)

Terminar el proceso malicioso, dándole la ruta de donde se encuentra.

Aquí le damos el nombre con el que este proceso se encuentra en el registro

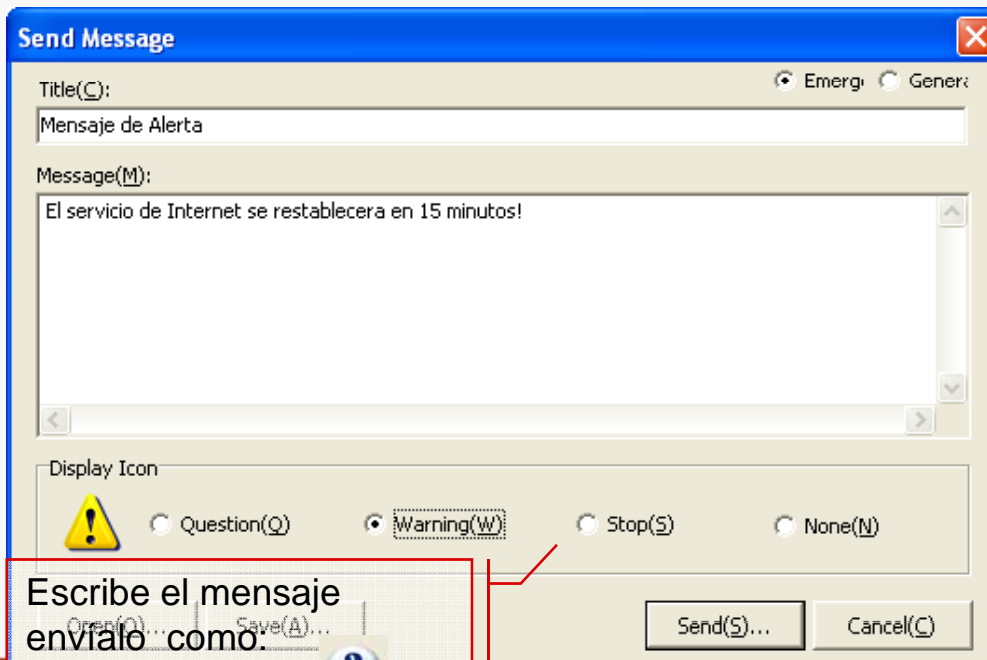
Le asignamos un nombre al Log y ubicación para consultarlo posteriormente



5. Envió de mensajes



Envió de mensajes: Sistema de Mensajería interno, a través de los puertos del Agente Antivirus. se pueden enviar mensajes de alerta a los usuarios, ejerciendo una posición pro-activa frente a nuevos ataques.



Escribe el mensaje
envíalo como:

•Pregunta



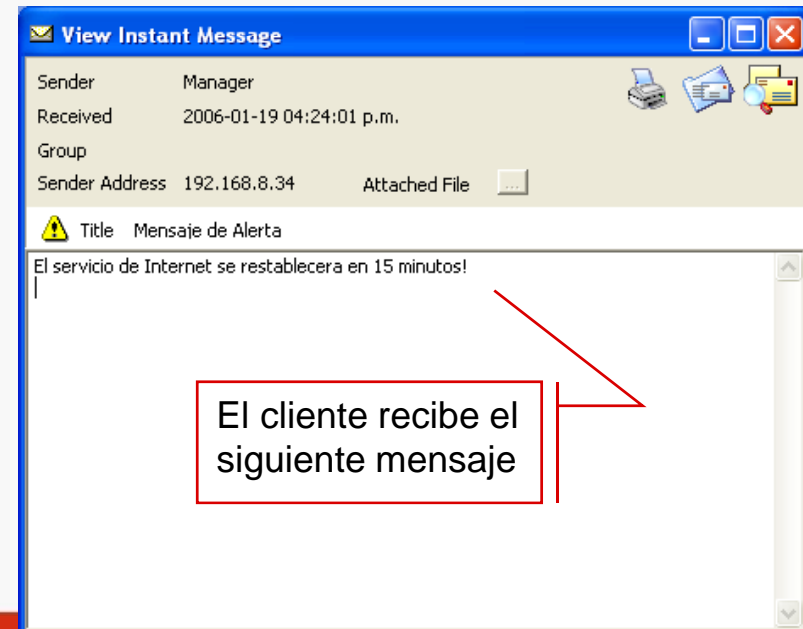
•Cuidado



•Stop

•Notificación

•Da clic en Send.



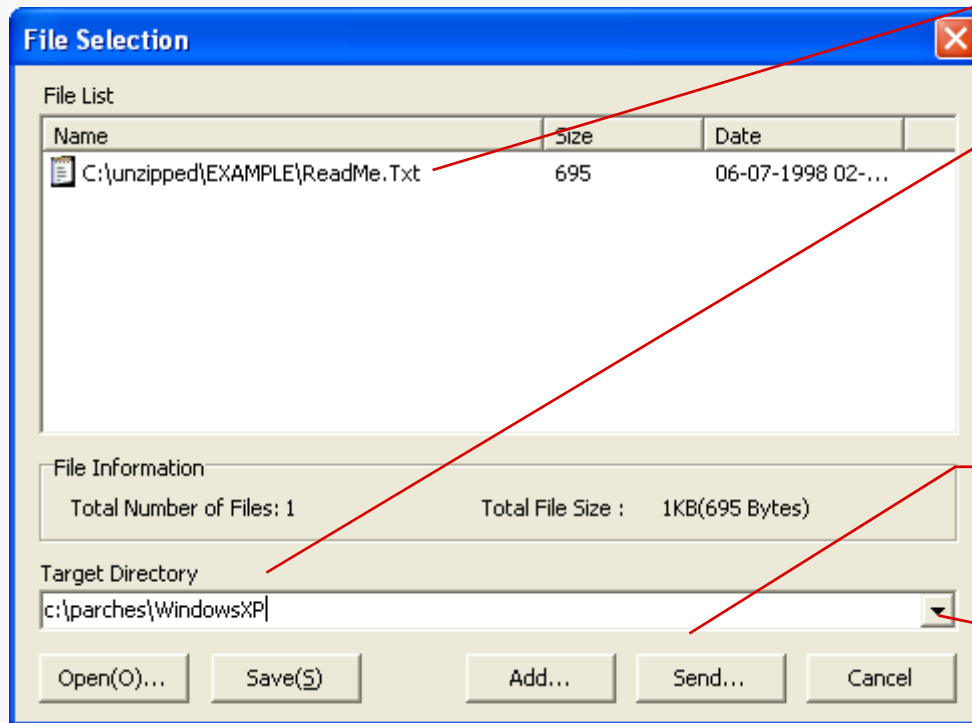
El cliente recibe el
siguiente mensaje



5. Envió de archivos



Envió de archivos: Envió de archivos, a través de los puertos del Agente Antivirus. se pueden enviar archivos



Archivo a enviar.

- Directorio de Instalación
- Archivos Comunes
- Archivos de Programa
- Directorio de Windows
- Sistema de Windows
- Directorio del Agente

Da clic en Send para enviar el archivo.

Selecciona la ruta donde se desea enviar el archivo.

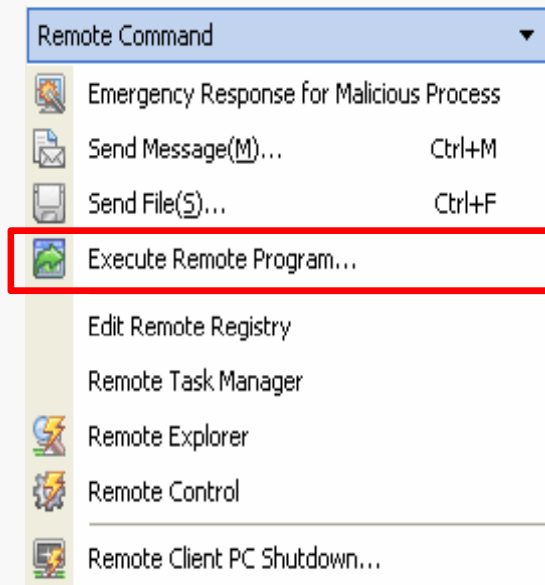


5. Ejecutar comandos remotos



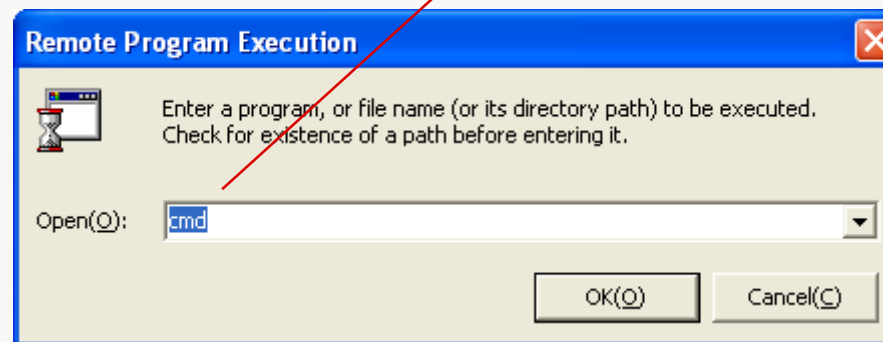
Ejecutar comandos remotos: Desde la consola VISMS es posible ejecutar líneas de comando remotos para ejecutar aplicaciones o procesos.

Nota: Es posible ejecutar los paquetes enviados por el administrador.



Ejecutar programas.

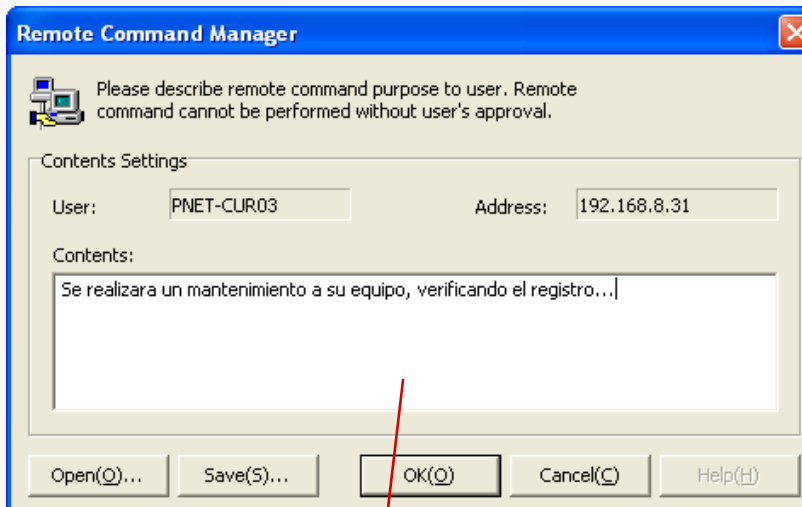
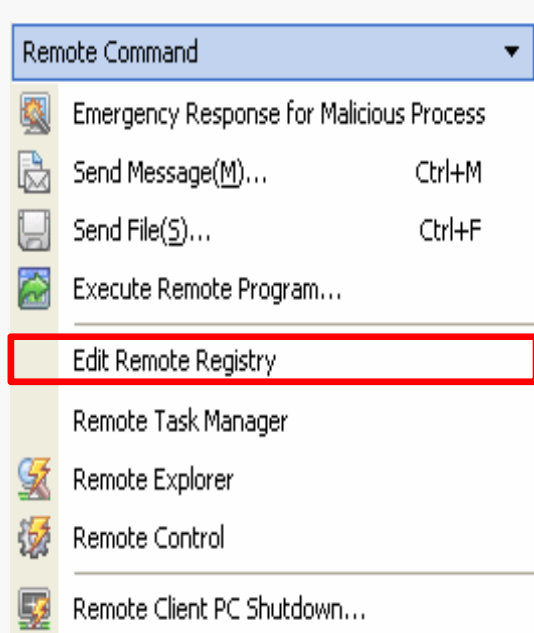
Tecleamos el comando que queremos ejecutar.



5. Editar el Registro



Editar el Registro: El administrador puede hacer una petición para revisar el registro del cliente sin necesidad de molestarlo o moverlo de su lugar.



El administrador hace la petición al usuario y pide su aprobación.

El usuario ve el mensaje y decide si acepta o no la petición.

Editar el registro del cliente.

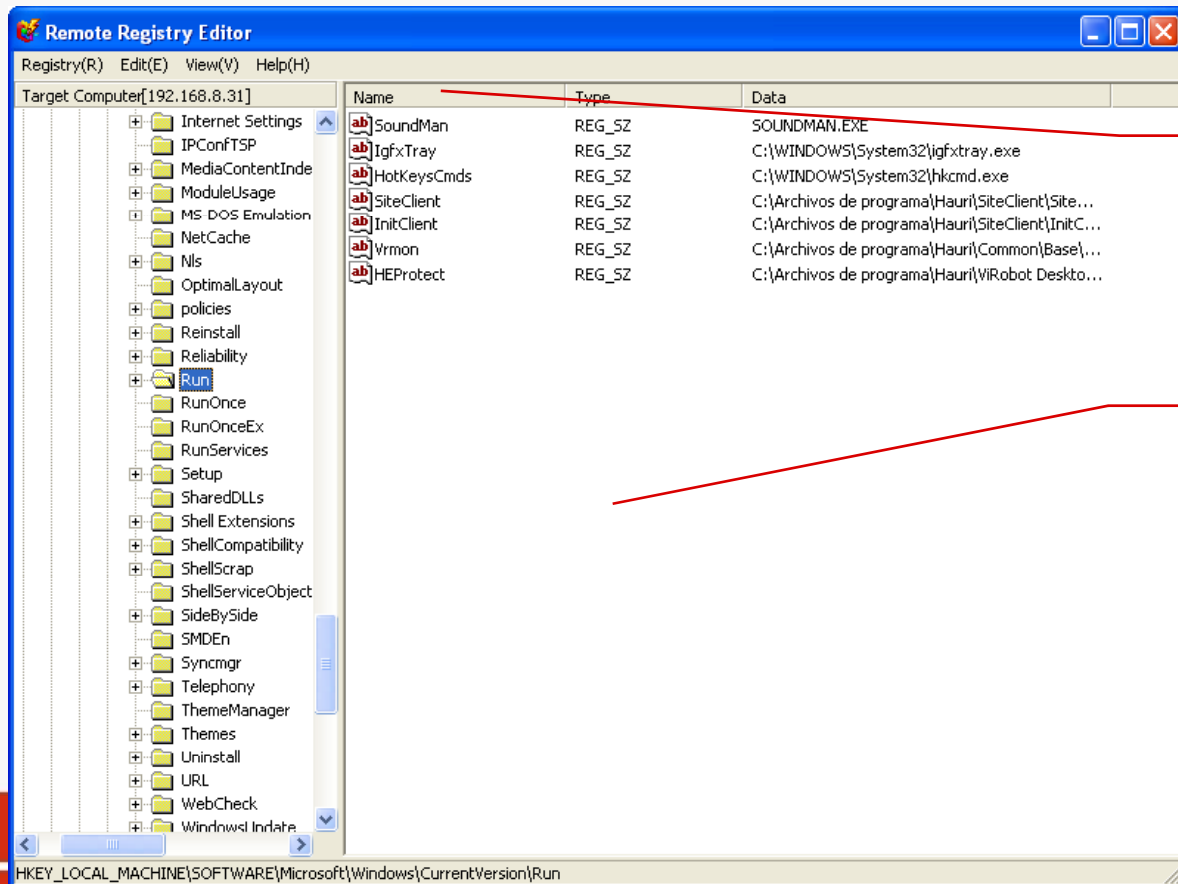


ViRobot

5. Editar el Registro



Editar el Registro: Una vez aprobada la petición, el administrador tendrá acceso total al registro del cliente.



Dirección IP del usuario

Control total sobre el registro de Windows del cliente, excelente para corroborar que ningún proceso malicioso se este iniciando cuando el equipo es encendido.

ViRobot



5. Administrador de Tareas Remoto



Administrador de tareas remoto: El administrador puede hacer una petición para revisar el administrador de tareas del cliente, para verificar que no este levantado algún proceso extraño sin necesidad de molestarlo o moverlo de su lugar.

The image shows a sequence of three screenshots illustrating the remote task manager process:

- Remote Command Manager:** A dialog box titled "Remote Command Manager" with a close button. It contains the text: "Please describe remote command purpose to user. Remote command cannot be performed without user's approval." Below this is a "Contents Settings" section with "User:" set to "PNET-CUR03" and "Address:" set to "192.168.8.31". A "Contents:" text area contains the message: "Se realizara mantenimiento a su equipo, revisando el administrador de tareas...". At the bottom are buttons for "Open(O)...", "Save(S)...", "OK(O)", "Cancel(C)", and "Help(H)".
- Remote Task Manager:** A menu item in the "Remote Command" dropdown, highlighted with a red box.
- Administrator is requesting user's approval:** A dialog box with a close button. It contains the text: "Administrator is waiting for user's approval for remote approach. Please click 'Cancel' if you disagree." Below this are fields for "Task Command:" (Remote Task Manager), "Administrator:" (192.168.8.34), and "Task Description:" (Se realizara mantenimiento a su equipo, revisando el administrador de tareas...). On the right are buttons for "Accept(A)", "Decline(C)", and "Help(H)".

Explanatory text boxes with red borders and arrows:

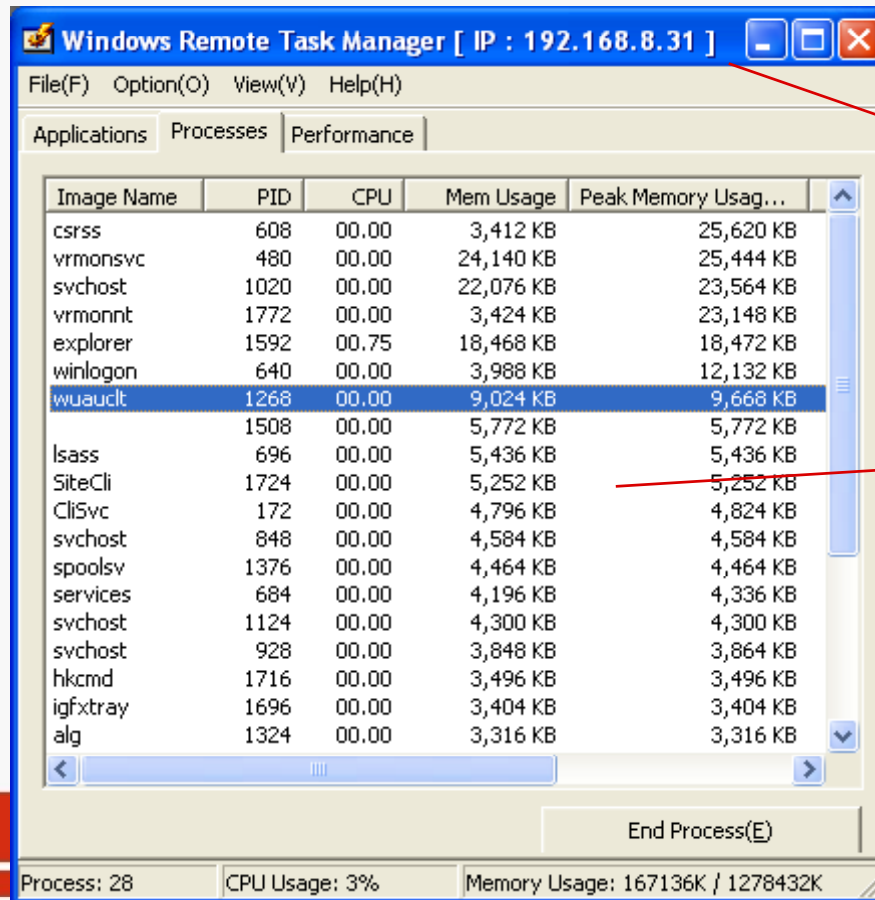
- Pointing to the "Remote Task Manager" menu item: "Administrador de tareas remoto."
- Pointing to the "Remote Command Manager" dialog: "El administrador hace la petición al usuario y pide su aprobación."
- Pointing to the "Contents" text area: "El usuario ve el mensaje y decide si acepta o no la petición."

ViRobot

5. Administrador de Tareas Remoto



Editar el Registro: Una vez aprobada la petición, el administrador tendrá acceso total al Administrador de Tareas del Cliente.



Dirección IP del usuario

Control total sobre el Administrador de Tareas de Windows del cliente, excelente para corroborar que ningún proceso malicioso este arriba.

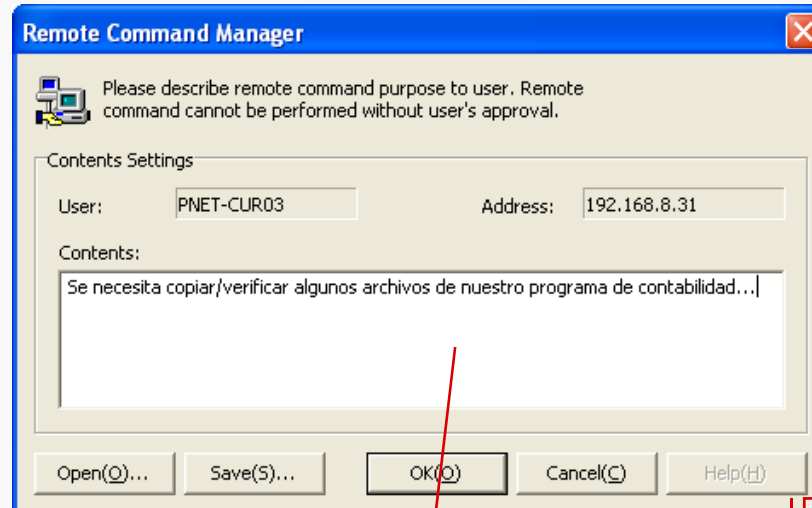
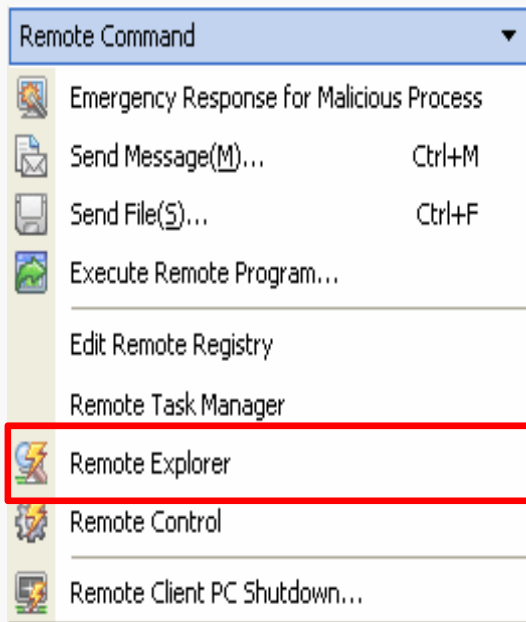
ViRobot



5. Explorador Remoto



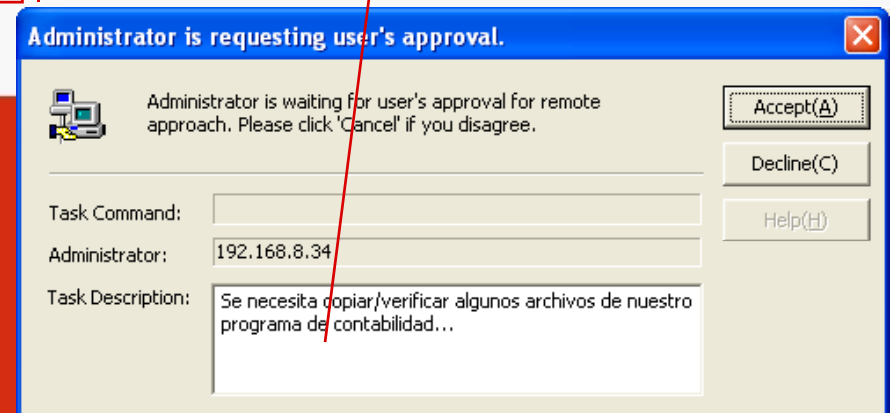
Explorador remoto: El administrador puede hacer una petición al usuario para explorar los discos locales, copiar/verificar/sobrescribir archivos sin necesidad de molestarlo o moverlo de su lugar.



El administrador hace la petición al usuario y pide su aprobación.

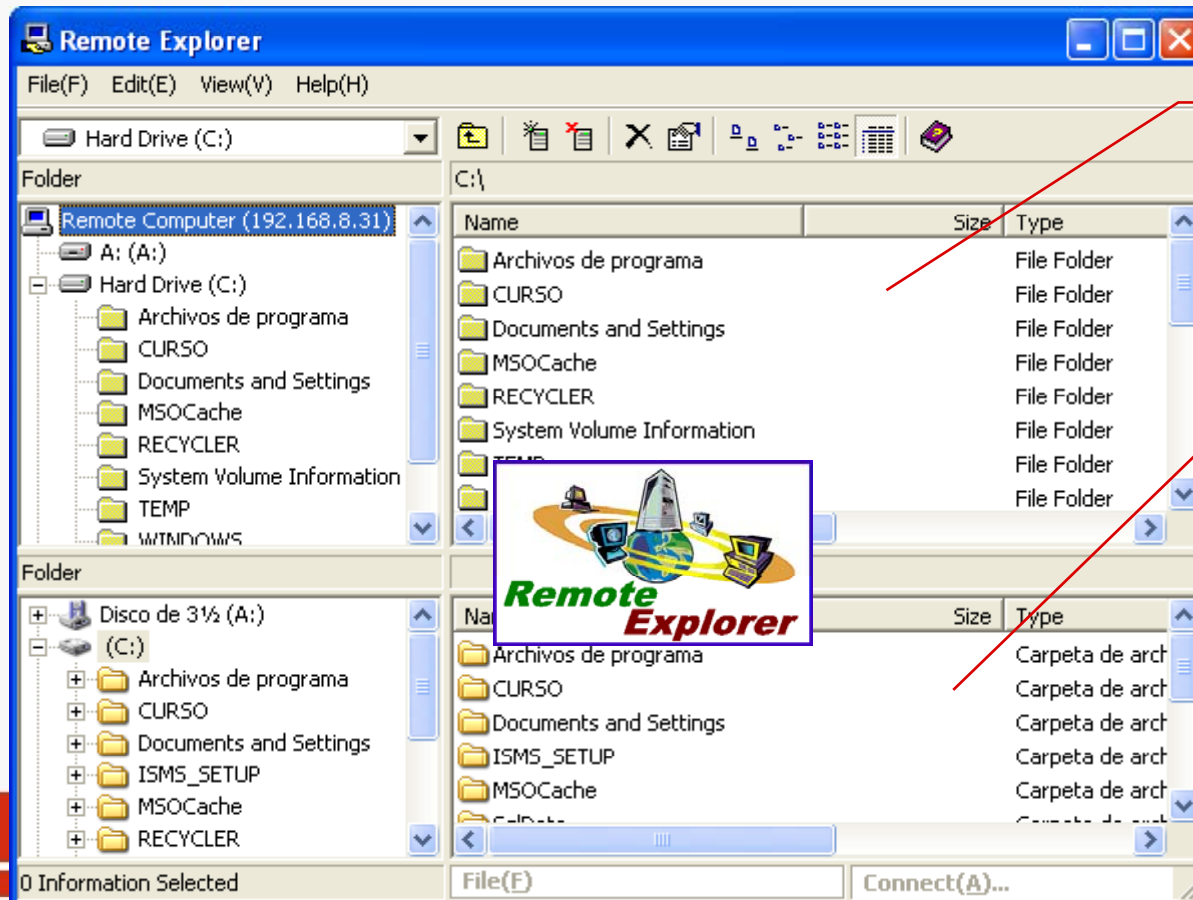
El usuario ve el mensaje y decide si acepta o no la petición.

Explorador Remoto de discos locales.



5. Explorador Remoto

Explorador Remoto: Una vez aprobada la petición, el administrador tendrá acceso total a los discos duros locales del cliente.



Discos duros locales del equipo remoto

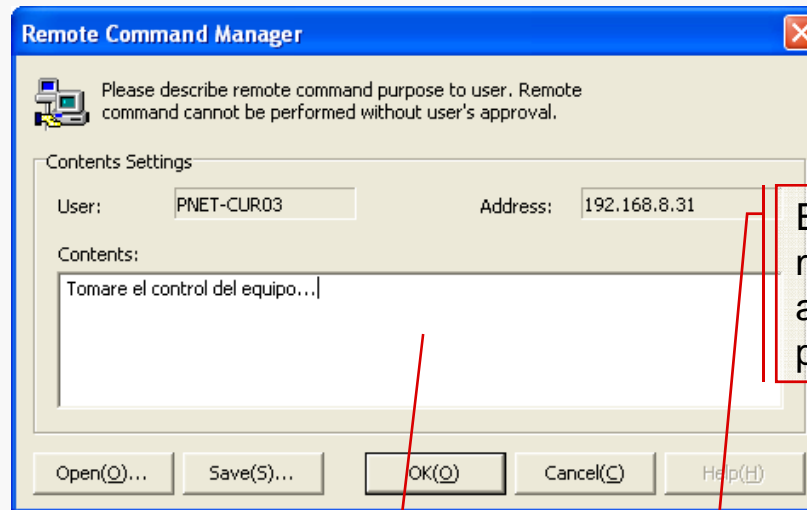
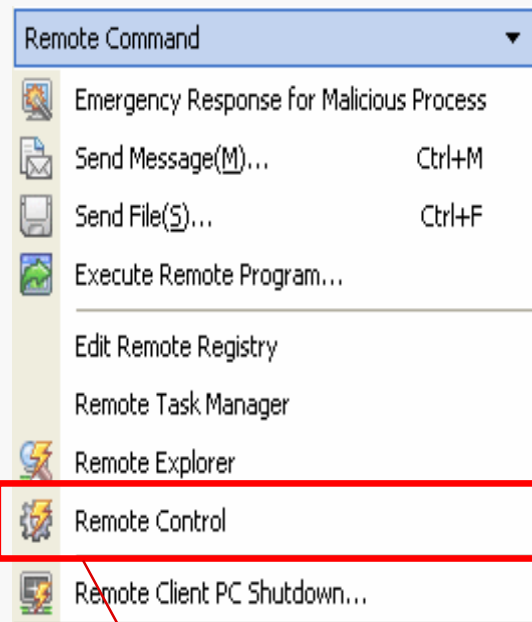
Discos duros locales del Administrador.



5. Control Remoto



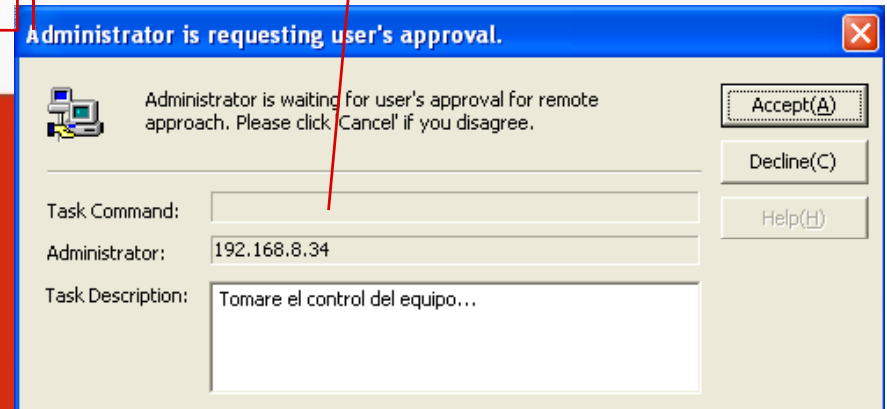
Control remoto: El administrador puede hacer una petición al usuario para tomar el control remoto del equipo, de este modo, los tiempos de respuesta por parte del administrador en caso de una emergencia son mucho mas rápidos.



El usuario ve el mensaje y decide si acepta o no la petición.

El administrador hace la petición al usuario y pide su aprobación.

Control remoto hacia el cliente.



ViRobot

5. Control Remoto

Habilita y deshabilita el Mouse del cliente.

Deshabilita y Habilita el teclado del cliente.

Ventana de Chat del administrador.

Ventana de Chat cliente.

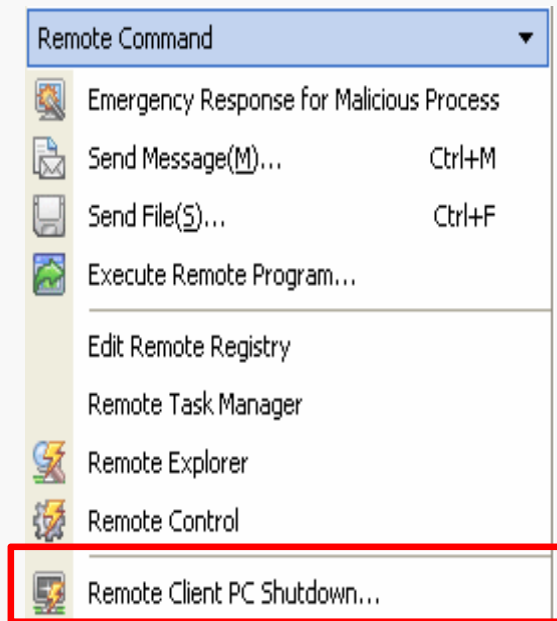
El cliente y el administrador pueden enviar un archivo

The screenshot shows the Remote Control Server interface (Ver 2.0) and the Remote Control Client interface. The server window has a menu bar with File(F), View(V), Tool(T), Window(W), and Help. The client window displays a system message: "System Administrator is using remote control feature. You can disconnect in order to stop remote control." The client interface includes a "Connected:" status bar showing "00:03:53" and an "Advanced >>" button. Below this is an "Advanced" chat window with a text area containing the following messages: "- 192.168.4.17: prueba de mensaje", "- 192.168.4.15: envio de prueba exitosa", "- 192.168.4.15: otro envio", and "- 192.168.4.17: recibido". A "Send" button is located at the bottom of the chat area. Below the chat area is a "File Transfer" section with a file selection field and a "Send" button. The server window also features a "Chat Window" on the left side with a similar message log and a "Send" button. At the bottom of the server window, there is a "Send File" section with a file selection field and a "Send" button. The status bar at the bottom of the server window shows "Number of All Users:1", "Connected User:192.168.4.15", "Connection Starting Time:17:01", and "192.168.4.15 Connected".

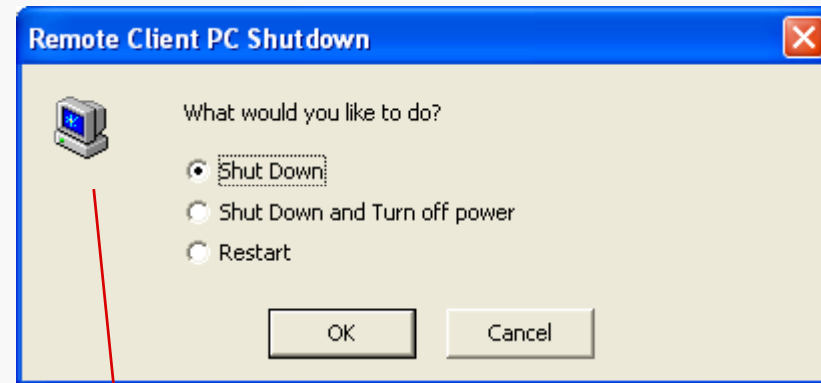
5. Apagar los equipos



Apagar los equipos: Con esta herramienta el administrador puede apagar, reiniciar los equipos en caso de ser necesario.



Apagar los equipo de forma remota



- Cerrar
- Cerrar y apagar el equipo.
- Reiniciar

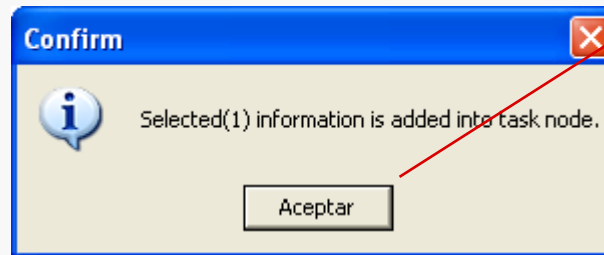
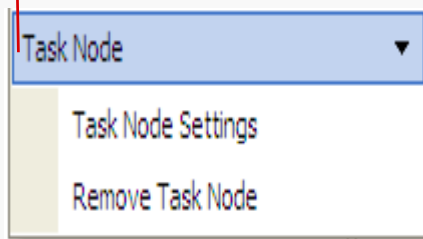


6. Tarea de Nodos



Tarea de Nodos: Aquí podemos asignar las tareas que estén dadas de alta, a algún nodo y de igual manera removerles las tareas a dichos nodos.

1. Seleccionamos el nodo que deseamos, y aplicamos la tarea.

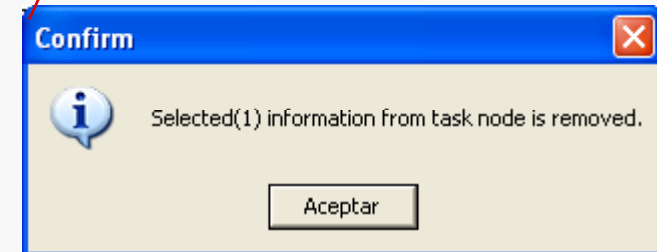


2. Confirmación de tarea asignada

3. Nodo con tarea asignada

Total Nodes - File						
User Name	Group Name	Address	Latest Connection Date	Sever Address	Computer Name	
PNET-CUR03	HAURI MEXICO	192.168.8.31	20-01-2006 11-48-22 a.m.	192.168.8.34	PNET-CUR03	
PNET-CUR02	HAURI MEXICO	192.168.8.35	11-01-2006 08-08-36 p.m.	192.168.8.34	PNET-CUR02	
PNET-CUR04	PROTEKTNET	192.168.8.34	20-01-2006 12-00-55 p.m.	192.168.8.34	PNET-CUR04	

4. Confirmación de tarea removida.





Gracias!

Departamento de Soporte Técnico.

Hauri Latinoamerica.
www.hauri-la.com

soporte@huri-la.com



01 800 801 7000