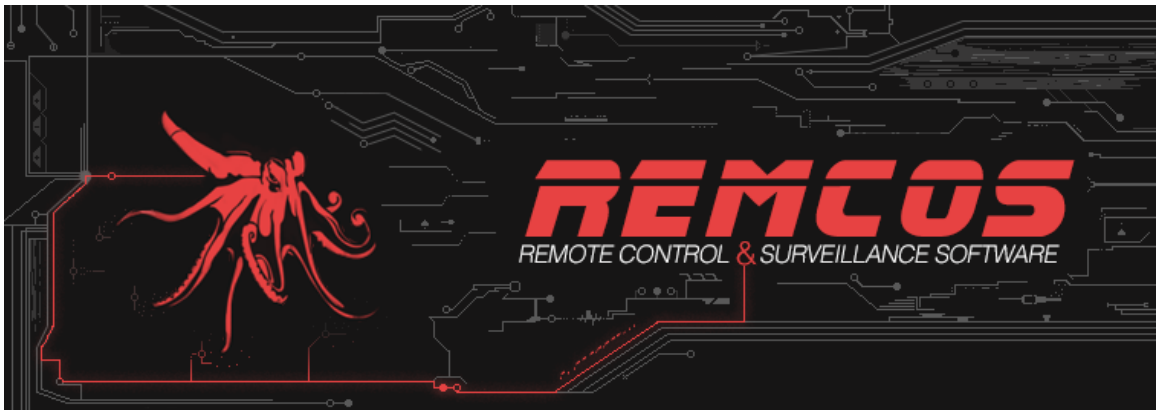


INSTRUCTION MANUAL

Revision 16

--
Remcos v2.3.0

TABLE OF CONTENTS

CHAPTER 1
-
Introduction to Remcos

USAGE CASES

Remcos is a powerful tool designed to carry on many operations related to remote computer control.

You can use Remcos for:

- Remote Control of your own computers remotely;
- Remote Administration of one or many Company/Classroom/Lab/Factory computers;
- Remote Support and Technical Assistance: Remote Desktop, Chat, File Manager, etc.;
- Remote Surveillance of your systems, against unauthorized access, insider threats etc.;
- Remote Proxy;
- Remote Anti-Theft;
- Penetration Testing purposes.

USAGE AGREEMENT

To use Remcos you are obliged to comply to local laws and to BreakingSecurity.net Terms of Service.
By law, any user must be noticed that a surveillance system is in place, and user activity could be monitored. Avoiding to provide a notice may lead to violation of laws concerning privacy and a ban of your Remcos license.
As our Terms of Service state,
you hereby acknowledge and agree that you may not and warrant that you will not:

(A) use the Breaking-Security.net software for any illegal purpose, or in violation of any laws, including, without limitation, laws governing privacy, data protection and intellectual property;
(B) install and/or use Breaking-Security.net software on any computer which you do not have explicit permission to do so on;
(C) install a surveillance software (such as Remcos) without providing a notice to users that such surveillance software is installed and their activity could be monitored;
(D) remove, circumvent, disable, damage or otherwise interfere with security-related features of the Breaking-Security.net software, features which prevent or restrict use or copying of any licensed content, or features that enforce limitations on use of the Breaking-Security.net software;
(E) intentionally interfere with or damage operation of Breaking-Security.net or any user's enjoyment of them, by any means, including spreading trojan horses or other malware;
(F) post, store, send, transmit, or disseminate any information or material which infringes any patents, trademarks, trade secrets, copyrights, or any other proprietary or intellectual property rights;
(G) resell our software to third parties, without explicit authorization and contract from Breaking-Security.net

COMPATIBILITY & DEVELOPMENT

Remcos is programmed in

- C++ (Agent)
- Delphi (Controller)

The skillful development in these programming languages provides maximum performance, compatibility, and lightweight operation.

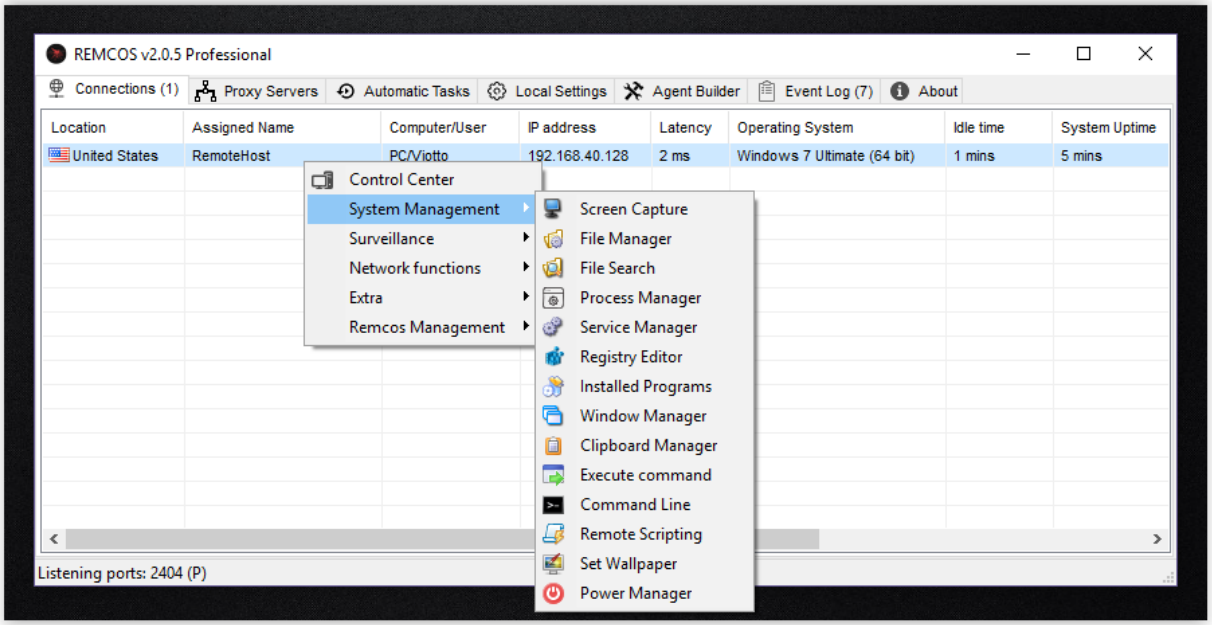
Remcos is completely native and runs without any dependencies (except the default Windows ones), on **any Windows version, from WinXP to Win10**,
on both 32-bit and 64-bit platforms.

Remcos agent, written in C++, while it provides access to an extremely wide array of functions,
is just ~120 kb in size:
That's just one of the many things in Remcos where you can view how performance, speed and lightweight operation have always been a priority in the development.

STRUCTURE

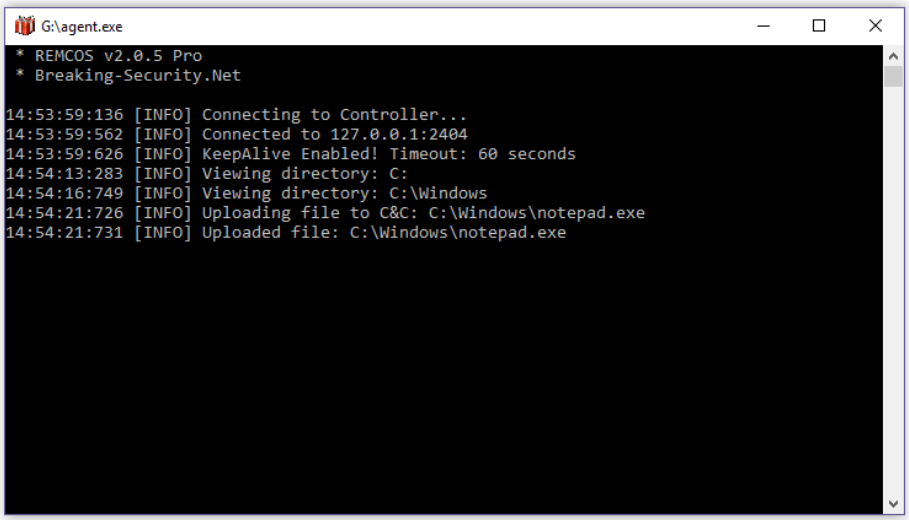
Structurally, Remcos is composed by two main parts:

- **Controller**:
  This is the Remcos component which is used to administrate and control the remote systems.
  It provides a Command&Control Interface, and also provides Agent Builder functionality.
  With the Builder, you can create Remcos Agents with your own custom configuration.



Remcos Controller

- **Agent**:
  The agent must be run on the systems which you wish to control.
  It will connect to the Controller and receive commands from it.



Remcos Agent

CHAPTER 2
-
Network Setup

Remcos uses an encrypted TCP connection between the Controller and the Agent,
without any intermediate servers.
This allows maximum privacy, speed and security for your connections.

To ensure that the two Remcos Endpoints (Controller & Agent) can successfully connect,
connection must be properly configured.

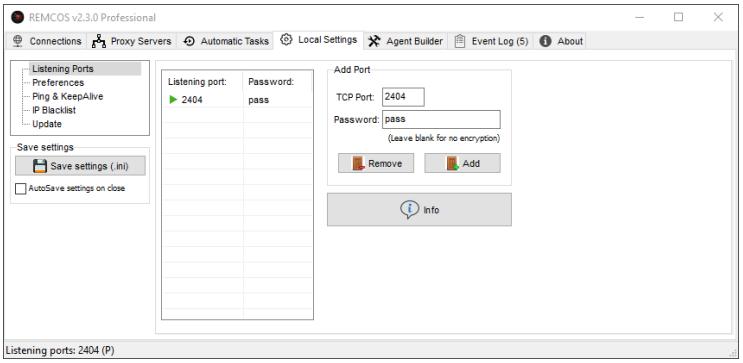
- **Remcos Controller** will act as a TCP **server**,
  and can be configured from ***Local Settings -> Listening Ports***.

- **Remcos Agent** will act as a TCP **client**, and can be configured from ***Agent Builder***.

CONFIGURE CONTROLLER (SERVER) CONNECTION

In Remcos, go to **Local Settings -> Listening Ports**.

Here you can add a TCP port.
You can use the default Remcos port, which is 2404,
or any other available.
Port numbers range up to 65535.
The port you want to use must be available and not
already used by other programs.



Local Settings -> Listening ports

If you get an error adding a port, probably it is already used by some other program.
Try another port.

Ensure that Remcos connection is allowed by the local firewall and security software.

If you enter a password along with the port, connection will be encrypted.

Password will serve 2 purposes:

1. **Encrypt your connection:**
   100% of data transmitted between Controller and Agent will be encrypted.
   This will protect you from traffic sniffers, man-in-the-middle attacks,
   and anybody who is trying to monitor your traffic.

2. **Protect your remote systems from unauthorized access:**
   Even if an intruder gets access to your Controller system, or your IP/DNS address,
   he won't be able to access your remote systems using Remcos without a valid password.

PORT FORWARDING

In case you are connecting Remcos through WAN or VPN, you will have to ensure that your TCP ports are correctly forwarded.
If ports are not forwarded, connection will be blocked by the router.

Port Forwarding steps depend on your router or VPN.
Port Forwarding references:

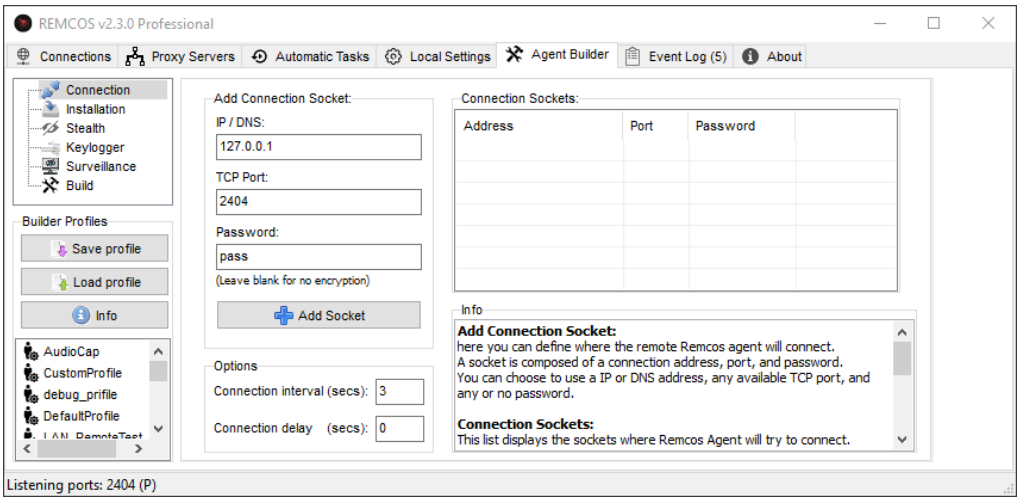
- https://PortForward.com
- https://en.wikipedia.org/wiki/Port_forwarding

You can use the free online service CanYouSeeMe.org to check if your port is opened and reachable from the Internet.

CONFIGURE AGENT CONNECTION

In Remcos, go to **Agent Builder -> Connection**.

From here you can setup how the Agent will connect to the Controller.



Agent Builder -> Connection

1. **IP / DNS:**
   Here you must insert the IP address of the Controller.
   If you are connecting Remcos inside a LAN, you can use the **ipconfig** command to view your IP address.
   If you are connecting Remcos through WAN, this will be the router address.
   If you are connecting Remcos through a VPN, this will be the VPN address.

   A DNS address can be used instead of an IP:
   this is useful in case your IP is dynamic and is subject to change;
   you can use a DNS to dynamically point to the updated IP address.

2. **TCP Port:**
   Here you should enter the same port where the Controller is listening to.

3. **Password:**
   Here you should enter the same password that the Controller is using for that Port.

Finally, go to **Agent Builder -> Build** and click the **Build Button** to create your custom **agent.exe**.

Deploy the **agent** file on your system to be controlled and execute it.
At this point, a connection should popup in the Controller Connections tab.

COMMON ISSUES AND SOLUTIONS

1. **No connection is received from the Controller.**
   Remcos Agent does not connect, and is stuck on the "Connecting to Controller…" message.

   Possible issues:

   a. **Network is offline.**
   Check that both Remcos endpoints are connected to internet (if connection is via WAN), or are in the same Network (if connection is via LAN).

   b. **Controller system is not reachable.**
   Check that you can reach the Controller from the Agent system, using a ping command with the IP or DNS address of the Controller.

   c. **Controller's TCP port is not opened.**
   Check that the agent is trying to connect to a Port which is opened and listening on the Controller's side.

   d. **Controller's TCP port is not forwarded.**
   Check that the port is reachable from the Agent system and is correctly forwarded.

   e. **Controller's connection is blocked by a firewall or security software.**
   Make an exception for Remcos Controller in your firewall rules, or disable firewall.

   f. **IP address of the Controller system has changed.**
   Some IP addresses are dynamic, and are subject to change, for example when there is a network reset.
   Be sure to use a static IP address, or use a Dynamic DNS, which updates the IP address on each change.

   g. **DNS address of the Controller points to a wrong or outdated IP address.**
   If you are connecting using a DNS address, be sure that it is updated to the correct IP address of the Controller.
   You can check this from your DNS service. Most DNS services provide you with a webpanel or software to update your DNS address to the new IP.

2. Invalid Connection Attempt errors are displayed in the Event Log.

Possible issues:

a. **Mismatching Connection Password.**
Make sure that the connection password for the Agent and the Controller is the same on the same port.

b. **Something (which is not Remcos) is trying to connect to the Remcos port.**
It is possible that some application is trying to connect to the same port of Remcos.
Make sure that you are using the port only for Remcos.
Remcos is programmed to automatically drop invalid and unauthorized connections.

CHAPTER 3
-
Agent Setup

As seen in previous chapters,
to be able to use Remcos, you must first create an Agent,
which will be later deployed on the systems you wish to control.
The Agent will be in form of an executable .exe file.

A quick configuration of Remcos Agent is already provided in Chapter 2.
If you want to view instructions which cover more advanced configurations, go on to this chapter.

To build an Agent, go to the **Agent Builder** tab.

CONNECTION

How to setup Remcos Agent connection has been covered in Chapter 2.

INSTALLATION

From the Installation tab you can set whether Remcos should start automatically with Windows.
If you check "**Install remote agent**", Remcos Agent will run automatically on each Windows restart.
It is usually recommended to use the default options, unless you are expert with Windows system and registry.

Watchdog:

Watchdog module (Persistence) will protect Remcos process, file and registry entries from corruption or deletion.
In case of accidental program termination, watchdog module will resume Remcos functionality.
This way the remote administrator can be sure to never lose control with the remote side, without having to restart Remcos manually and physically on the remote-controlled machine if something goes wrong.

Protect Registry Entries (Registry Persistence):
This separate watchdog module will protect Remcos registry entries (startup values and software key) from deletion or corruption.

STEALTH

From the Stealth tab you can configure different stealth modules for the Remcos Agent.
You can set the Agent in Visible (default) or Invisible mode.

By law, any user must be noticed that a surveillance system is in place, and user activity could be monitored.
Avoiding to provide a notice may lead to violation of laws concerning privacy and a ban of your Remcos license.

Visibility Mode:

- **Visible:**
  Default, standard option.
  Remcos Agent starts fully visible, with window and tray icon.
  Details such as connection status are displayed,
  and the user can close Remcos anytime by closing the Agent Window.
  You can left-click on the tray icon to show/hide Remcos window.
  This is the recommended mode for remote administration and support sessions.

- **Visible Minimized:**
  Remcos starts in visible mode, but minimized in tray icon.
  As in the normal Visible mode, you can left-click on the icon to show/hide Remcos window.
  This is the recommended mode for remote administration and medium-grade surveillance.

- **Invisible:**
  Remcos Agents starts without creating any window and tray icon.
  This is the recommended mode for high-grade surveillance.

KEYLOGGER

Keylogger can be used to monitor keyboard activity.
Useful for surveillance and monitoring of the remote systems.
Remcos offers many keylogger modes.

Log Everything:
Keylogger will be always active.

Selective Keylogger (Window Filter):
Keylogger will be activated only when user is inside the specified windows.
A window can also be a program or webpage name.

CLEAR COOKIES AND LOGINS

Each time Remcos Agent starts, Clear Logins function will delete all your browsers stored passwords and logins.
This will increase system and accounts security against password grabbing.

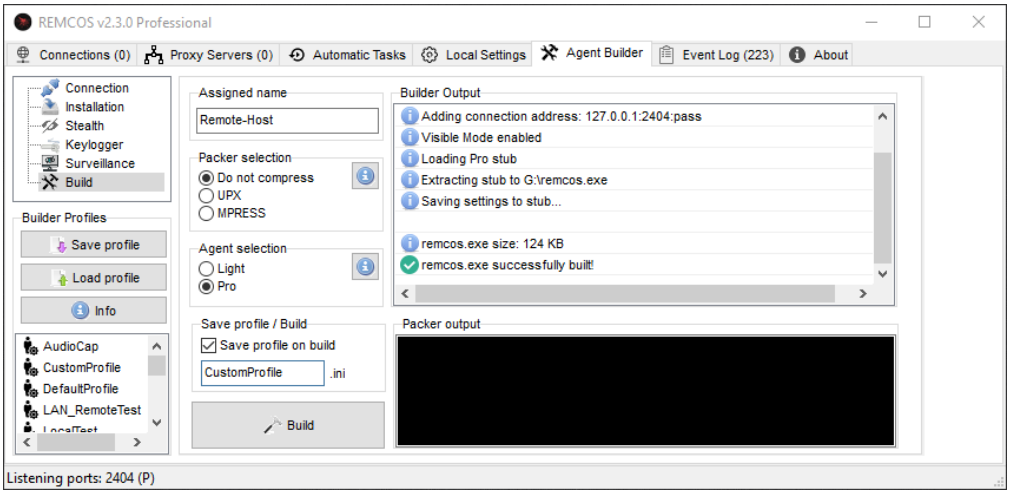
SURVEILLANCE

From the **Surveillance** tab you can enable the ScreenLogger and Offline Audio Capture functions.

BUILDER

From the **Builder** tab you can build your remcos_agent.exe file.

You can save your **Builder Profile** and use it for later agent builds.
Loading a Builder Profile will set all your builder configuration automatically.



Agent Builder -> Build

CHAPTER 4
-
Usage

REMOTE ADMINISTRATION

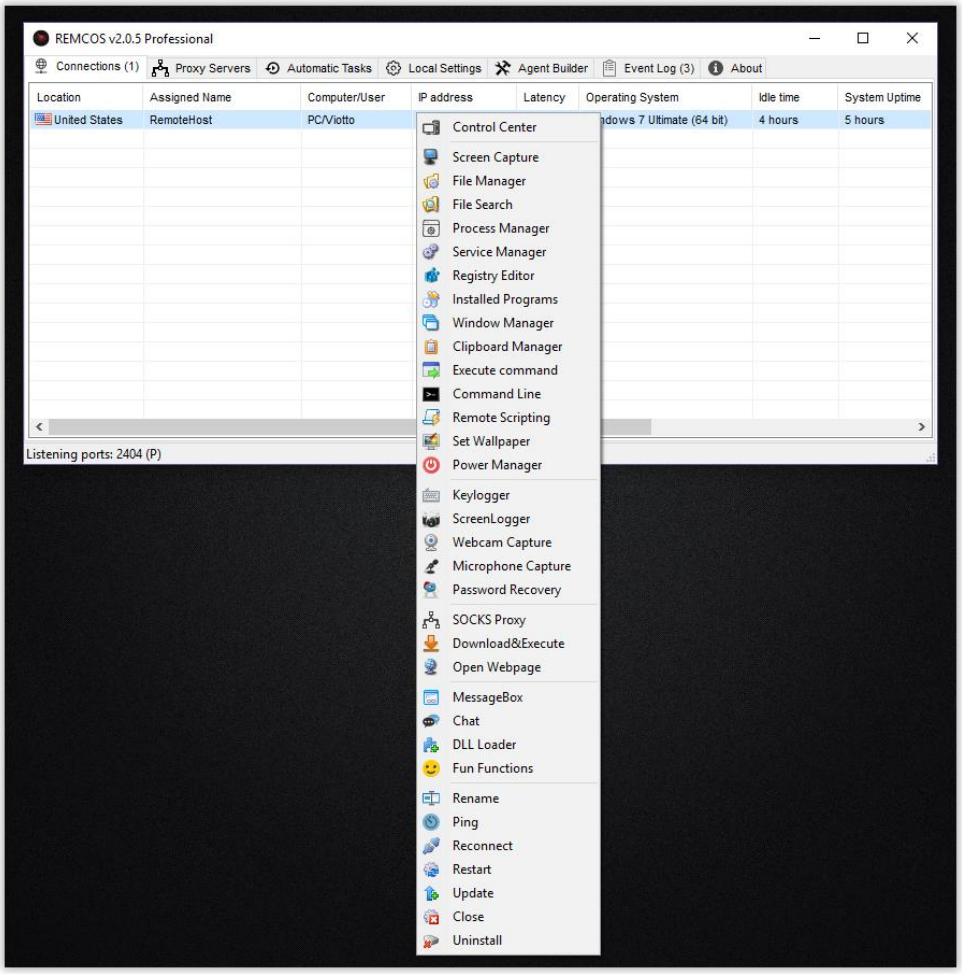
You can administrate and control your remote hosts from the **Connections Tab**.

You have various ways to access Remcos Functions:

1. Functions Menu
2. Shortcut Keys
3. Control Center

Functions Menu:

Right Click on one or more hosts to open the **Functions Menu**. From the Functions Menu you can open any function.
By **selecting multiple hosts** and opening the Functions Menu, you will run the specified function on all the selected ones.



Functions Menu in Expanded Mode

To change the Functions Menu style from Categorized to Expanded, go to **Local Settings -> Preferences -> Functions Menu Style**.

Shortcut Keys:

Most of Remcos functions can be ran using a shortcut key.

Examples:

- **[Ctrl + C]** Control Center
- **[F1]** Screen Capture
- **[F2]** File Manager
- **[F3]** File Search
- **[C]** Chat
- **[P]** SOCKS Proxy

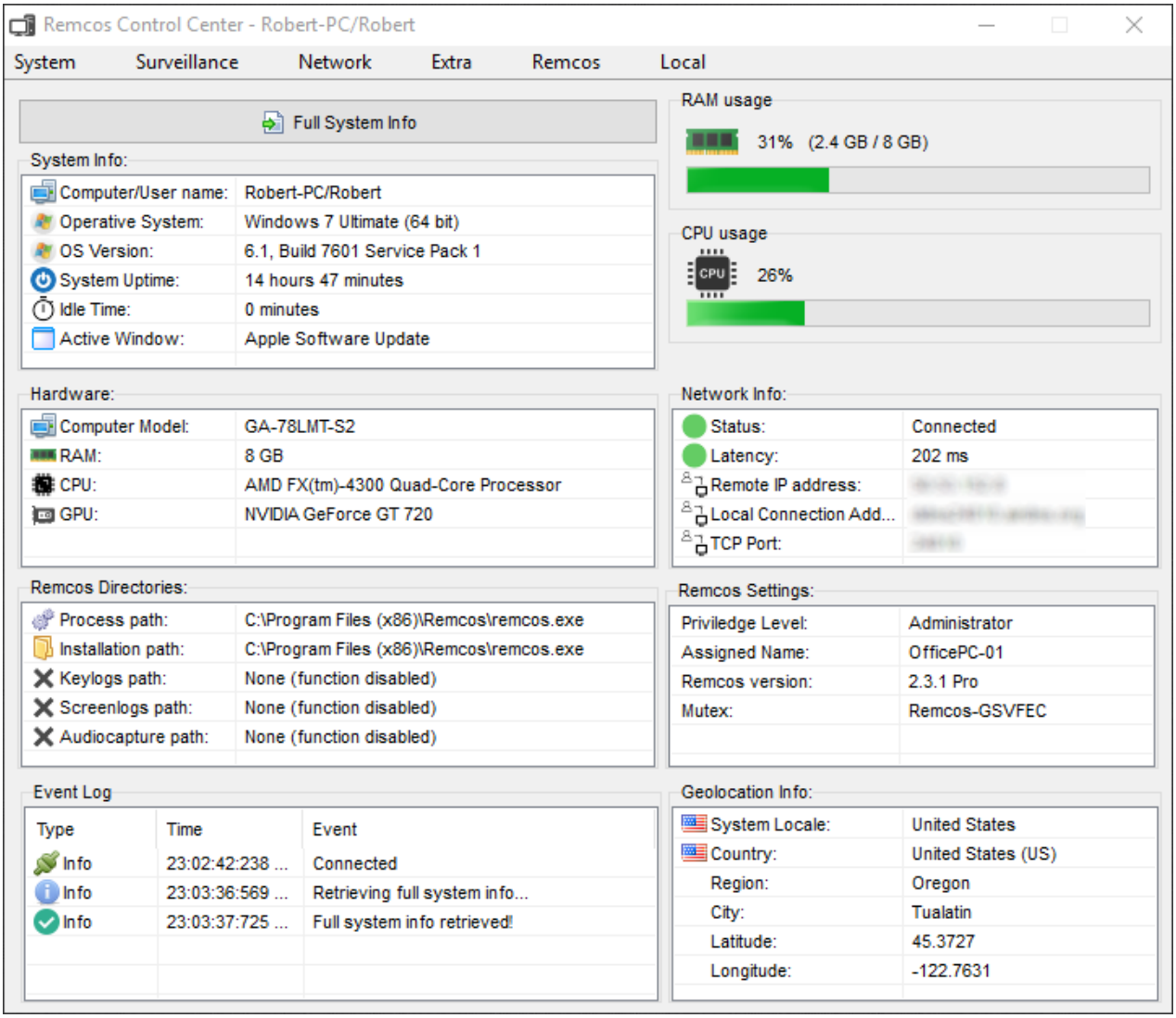
To view shortcut keys, go to:
Local Settings -> Preferences -> Show Shortcut Keys.

Favorite Function
Double-click a remote host to open the Favorite Function.
The Favorite function is the Control Center by default.
You can change the **Double-Click Function** from **Local Settings -> Preferences**.

CONTROL CENTER

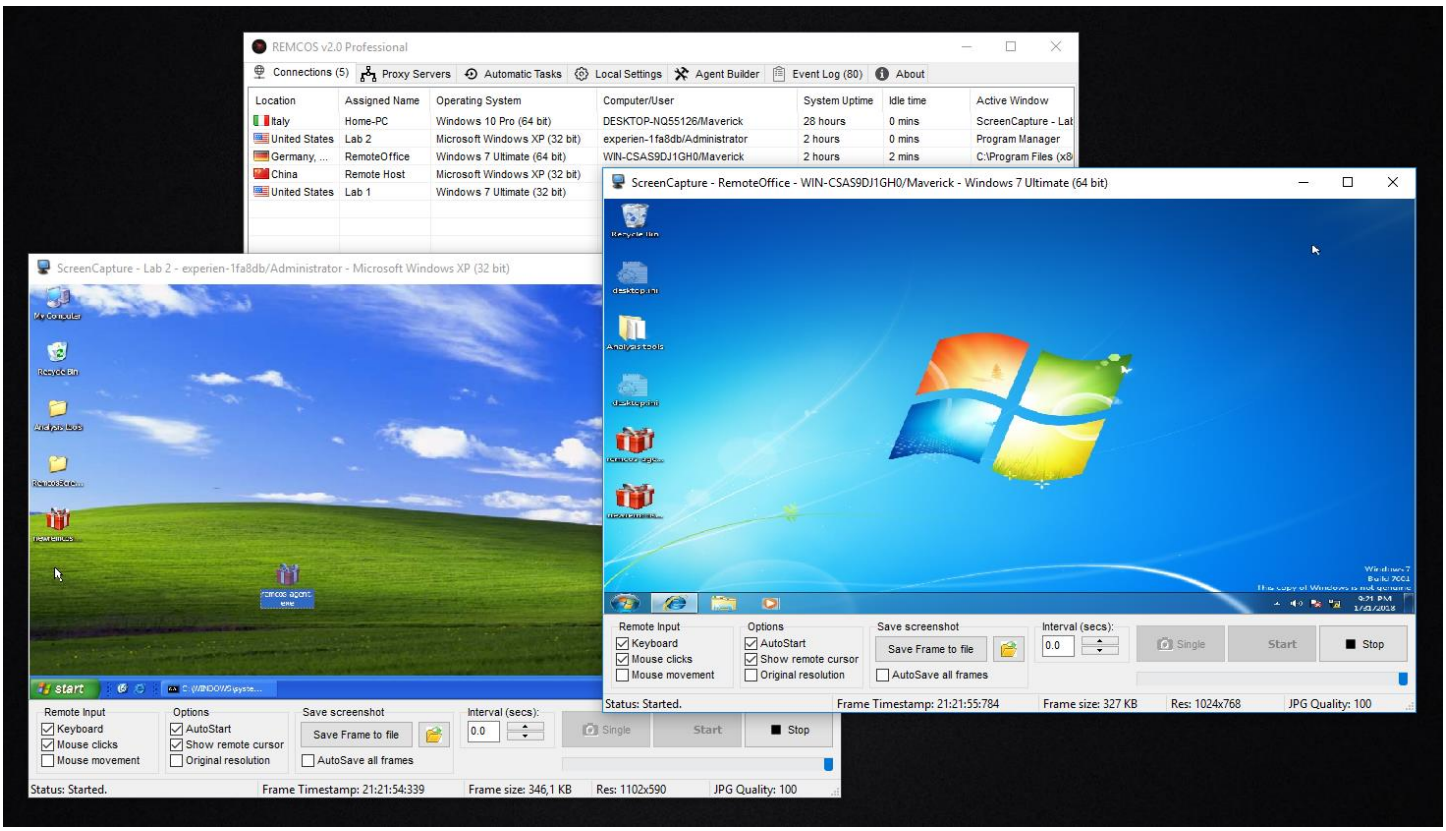
Double Click on a host, or press **[Ctrl + C]** to open the **Control Center**.

The **Control Center** is a convenient method to administrate your remote machine, since you have all the info and functions available in one place.
From the Control Center's Main Menu you can open all the needed functions.



SCREEN CAPTURE

Screen Capture (shortcut key: **F1**) lets you view and control the remote screen(s).
Screen Capture is the most important function for most of Remote Administration needs.



Remote Input:

- **Keyboard**: Let's you type remotely.
- **Mouse Clicks**: Let's you send mouse clicks remotely.
- **Mouse Movement**: Will transfer mouse movement in real time.

Options:

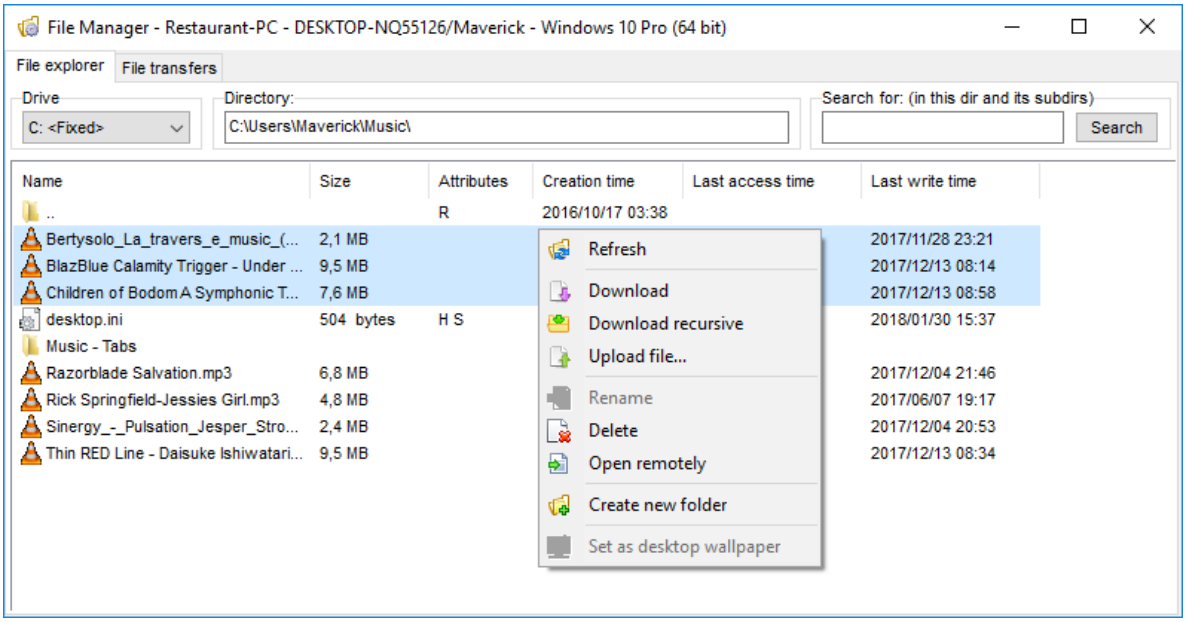
- **Original Resolution**: display the captured screen in the original resolution of the remote screen.
- **Show Remote Cursor**: show or hide the remote mouse cursor.
- **AutoStart**: automatically start Screen Capture when opening function.

Quality:

Adjust the quality of the received video feed.
You can lower the quality in case of slow connection and poor frames-per-second rate.

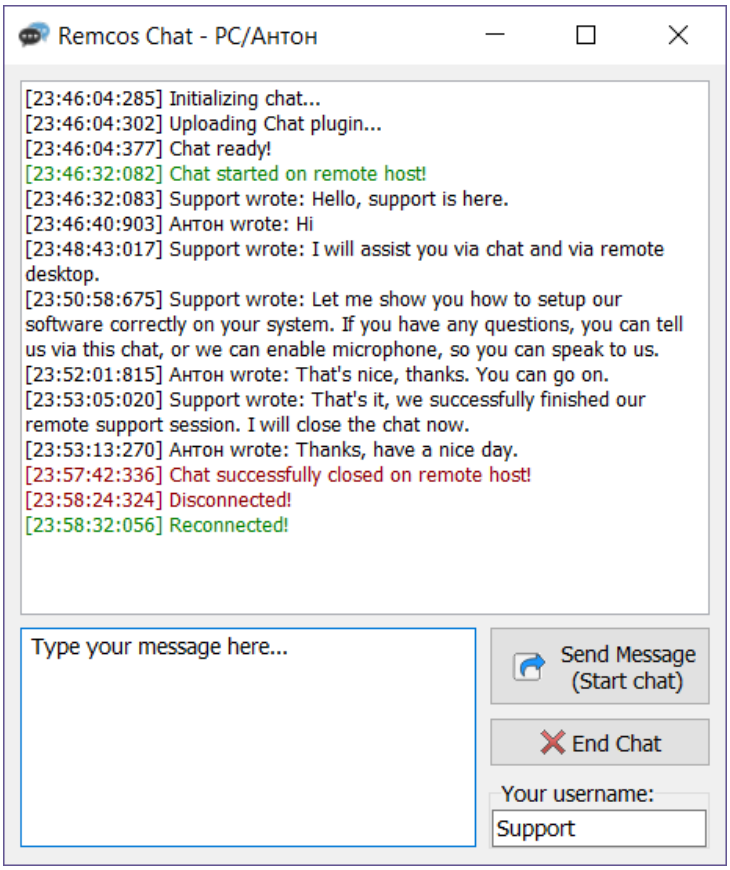
FILE MANAGER

File Manager (key: **F2**)
let’s you manage and transfer files between the systems.



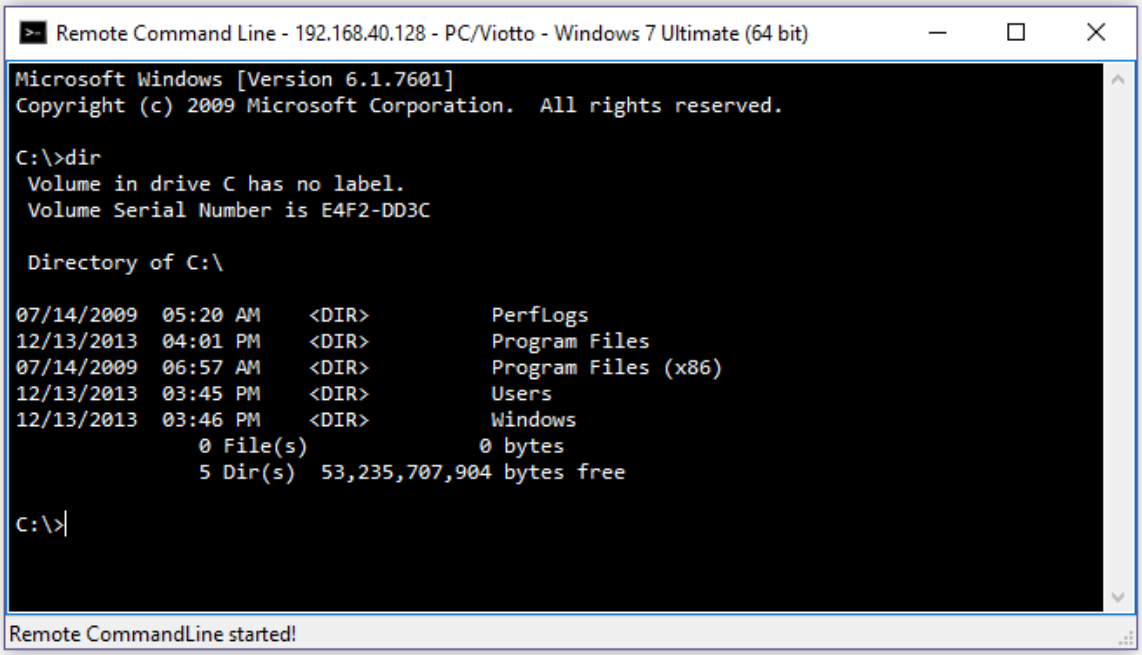
CHAT

Remcos Chat (key: **C**)
provides you an efficient channel of communication when performing **Remote Support** sessions.



REMOTE COMMAND LINE

Remote Command Line (key: **F12**)
opens a Remote Shell on the system,
letting you use its command line remotely.

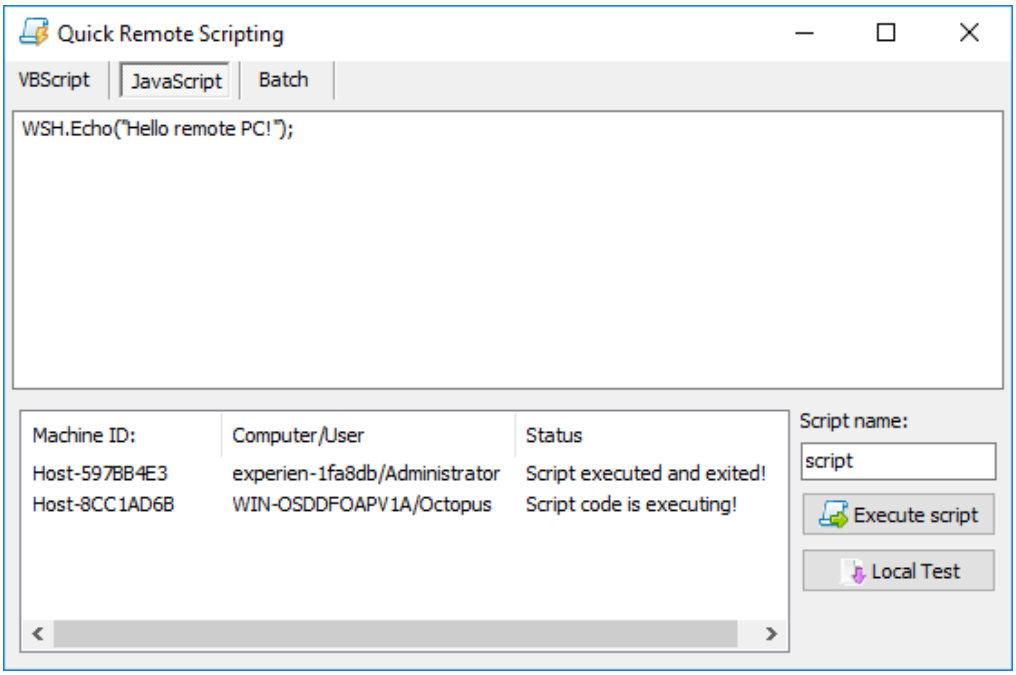


REMOTE SCRIPTING

Remote Scripting (key: **Ctrl + F1**)
can extend Remcos functionality almost indefinitely thanks to the power of scripting and programming!

You can code scripts and use them to upload/download files from servers, set tasks and timed actions, and anything else that you need (and can code:)

With Remcos you can also run the script on multiple machines to carry on automatically pre-programmed complex tasks on all the desired machines at once.



Remcos supports Batch, JavaScript and VBScript languages.

REMOTE ANTI-THEFT

Remcos can help you if somebody steals your computer:

- Use the **File Manager** to **retrieve your most important files**.
- Use the **File Manager** to **delete sensible files**, which you don't want in bad hands.
- **Trace the IP address** of the connection to view where the thief is connecting from.
  You can use the IP address as an information to give to the authorities in case you want to report the case.
- Use the **Webcam Capture** to view and save pictures of who's using your computer.
- Use the **Clear Logins** function to clear all stored browser cookies and logins:
  this will prevent the thief from entering your accounts.

REMOTE SURVEILLANCE

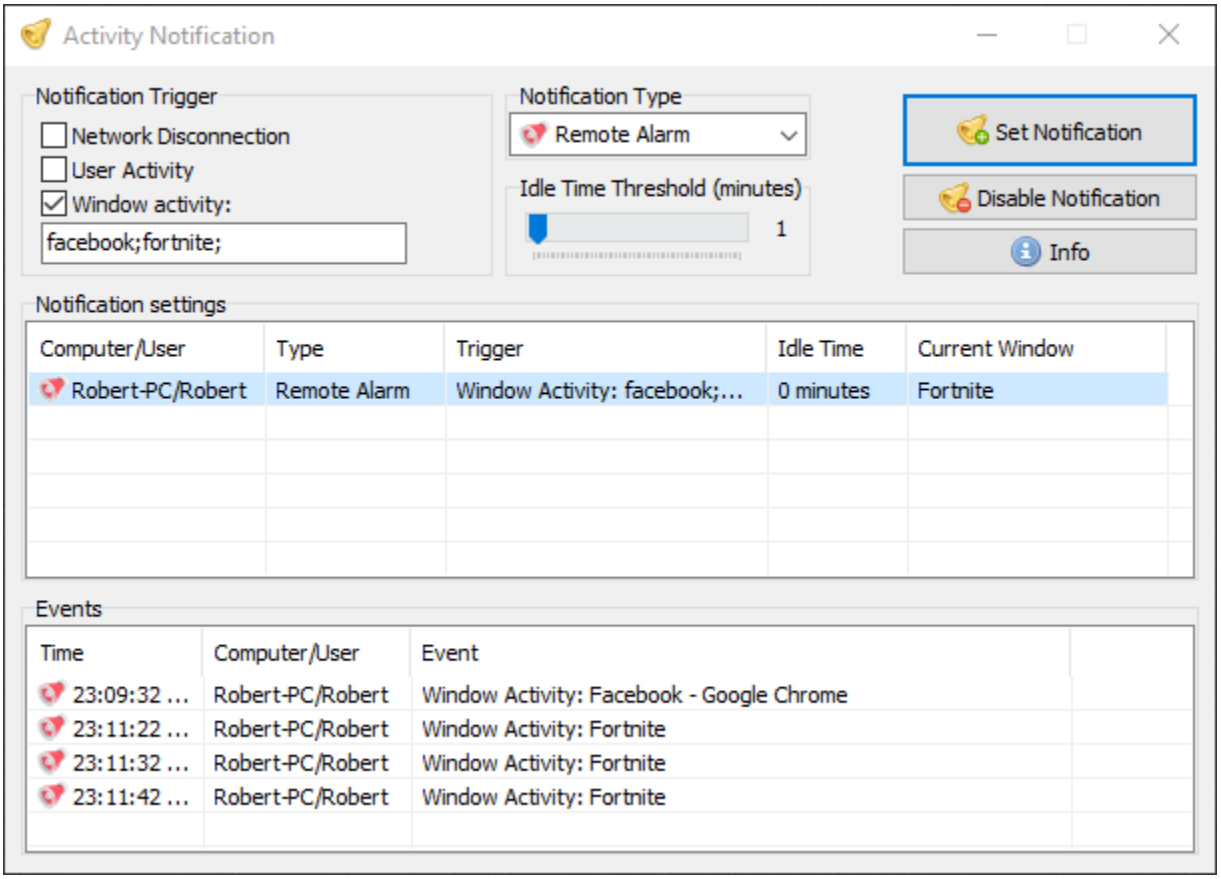
Remcos can transform your computer in a stealth surveillance station.
This can be used, for example, to monitor unallowed actions on computers which need a very high level of safety, and must be accessed only by authorized personnel to perform controlled actions.

- Be sure to comply to the local laws and our Terms of Service.
- **Webcam Capture**: use your computer as an IP camera.
- **Microphone Capture**: activate the computer's microphone and listen to it remotely.
- **Keylogger**: use the Keylogger to see what has been typed on the keyboard.
- **Screen Logger**: Saves screenshots at intervals or when inside specified applications.
- **Browsers History**: View the browsing history.
- **Password Recovery:** recovers stored passwords.
- **Activity Notification:** sets a local or remote alarm for certain actions you want to monitor, such as user activity or network disconnections.

ACTIVITY NOTIFICATION

Activity Notification can be used to:

- Detect accesses to a restricted computer;
- Detect activity on specified programs and windows;
- Notify any network disconnections on systems which should be always online;
- Sound an alarm on the Controller or on the Monitored system when an unauthorized action is detected.



NOTIFICATION TYPES:

Log:
Silent Notification. Log event only.

Notification:
Sound Notification (Controller) + Log Event.

Alarm:
Sound Alarm (Controller) + Log Event.
Alarm will play on Controller system, until stopped by Remcos user.

Remote Alarm:
An alarm will sound on the monitored computer.
This can be a great method to deter unauthorized people from accessing your computer,
and prevent unauthorized activities.
Alarm will briefly sound on Controller system as well.

TRIGGERS:

Network Disconnection:
Alarm will be triggered when you lose control of the remote agent (disconnection).
If Remote Alarm is set for Disconnection event, it wont be triggered in case of Controller-side disconnection (Controller Close or Port Close).
The Reconnection command will still trigger the Alarm.

User Activity:
Alarm will be triggered whenever anybody touches mouse or keyboard.
Very useful for surveillance purposes of restricted-access systems.

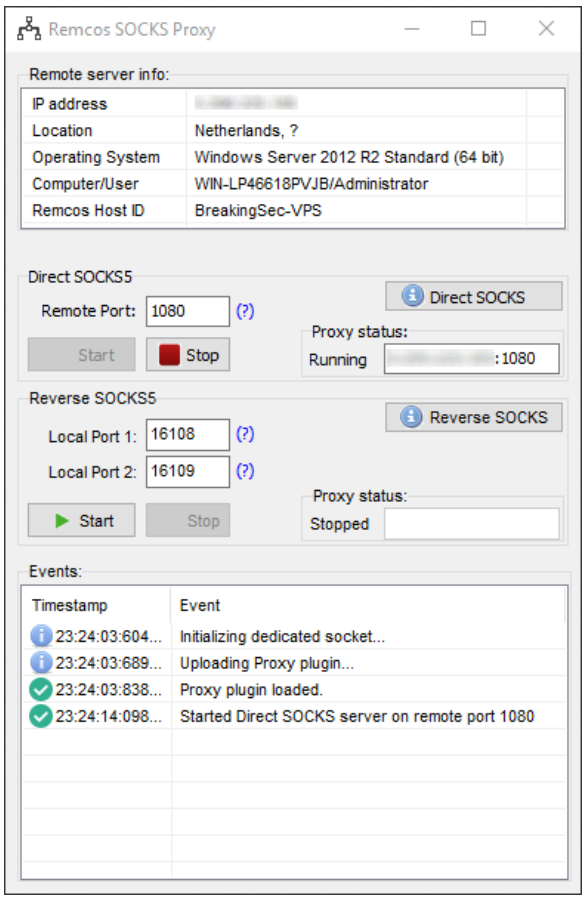
Idle Time Threshold:
User Activity notification will be triggered only if idle time exceeds threshold.
Example: A 5 minutes Threshold will trigger User Activity Notification only if user comes back after 5 minutes or more.
This is useful if you plan to active the notification only after a certain time.

Window Activity:
Alarm will be triggered whenever user opens windows, programs and webpages of your choice.

REMOTE PROXY

Remcos SOCKS proxy allows you to route your internet traffic via your remote machine, and bypass internet restrictions, blocks and censorships.

Remcos Proxy supports SOCKS5 protocol,
in both Direct and Reverse modes.



Remcos SOCKS Proxy

Direct SOCKS:

Proxy Server (Remcos Agent) <--> Client Application

Direct SOCKS function will start a SOCKS5 proxy server on the remote machine.
The remote proxy server will listen for incoming connections on the specified port.
In Direct mode, client applications (such as your browser) will connect directly to the remote proxy system.

To be able to use Direct mode, the remote server IP and port must be reachable and not blocked by router/firewall.
If the remote ports are not reachable, you can either:

1) Use Reverse Proxy mode, or
2) Configure firewall and router on the remote machine, to allow incoming connections on proxy port.

If proxy ports are not blocked on the remote system, it's usually recommended to use Direct mode, since it is faster than Reverse mode.
Direct mode is faster because connection is direct client<-->server, without Controller/Agent tunnel.

Usually, Windows Servers and VPS providers do not block most of incoming connections and ports, so you can probably use Direct Proxy mode on these kind of systems.

If Remcos Controller disconnects, the Direct proxy server will be kept running, until stop command.
This lets users use the proxy even when Remcos is closed.

Remote Port:
Use this port to connect your applications to the Remcos SOCKS proxy.
Port is opened on remote machine.

Reverse SOCKS:

Proxy Server (Remcos Agent) <--> Proxy Intermediary (Remcos Controller) <--> Client Application

You can use the Reverse mode when it is not possible to open a regular, direct proxy on the remote system, due to router or firewall restrictions, which may block ports and incoming connections.

Unlike Direct mode, in Reverse mode no ports are opened on the remote machine.
Proxy server and ports will be opened locally (Controller system).

In Reverse mode, the remote proxy server will connect via reverse connection to the Intermediary Server (Remcos Controller).
In Reverse mode, client applications (such as your browser) will connect to the Intermediary Server, which will route traffic to the remote proxy server.

Reverse mode can be used if remote firewall or router do not allow, or cannot be configured to allow incoming connections, so it is not possible to use Direct Mode.
In Reverse mode, it is necessary to configure firewall and router on the local system, in order to allow incoming connections on proxy port.

Local Port 1:
Use this port to connect your applications to the Remcos SOCKS proxy.
Port is opened on local machine.

Local Port 2:
This is the port where the remote Remcos proxy agent will connect.
Port is opened on local machine.

CHAPTER 5
-
Uninstallation

You have multiple ways to uninstall Remcos agents:

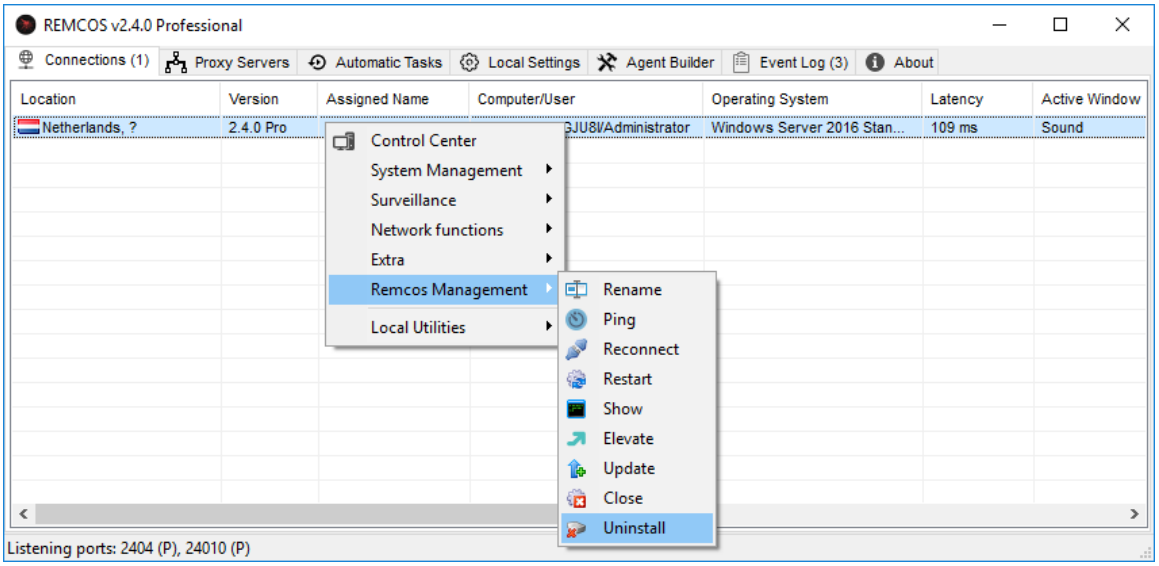
- Using Remcos Controller
- Using the stand-alone Remcos Uninstaller.

Uninstallation command will remove Remcos completely, including:

- Close Remcos process
- Delete Remcos Agent executable file
- Delete any file and registry data created by the Agent.

UNINSTALL AGENT USING CONTROLLER

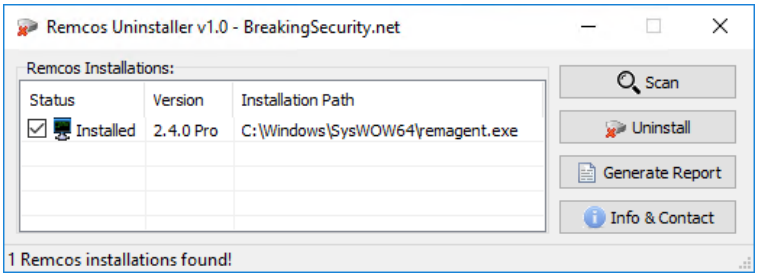
To uninstall one, multiple or all the connected agents, you can use the Uninstall command.



Uninstalling Agent using Controller

UNINSTALL AGENT USING UNINSTALLER

With the stand-alone Remcos Uninstaller you can remove any Remcos agent installation which is active on your system.



Uninstalling Agent using Uninstaller

Remcos Uninstaller is free and does not require a license to be downloaded and used.

You can find it at the link below:
https://breakingsecurity.net/remcos/uninstaller