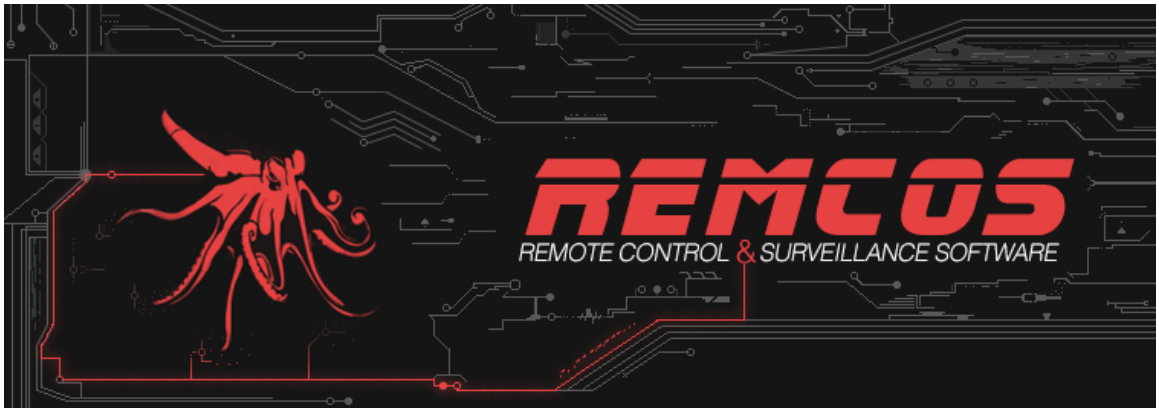



# REMCOS
# INSTRUCTION MANUAL

Revision 24
Remcos v5.3



# TABLE OF CONTENTS

# Chapter 1:
# Introduction to Remcos

## USAGE CASES

Remcos is a powerful and versatile 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;
- Security Audits, Red Teams, Penetration Testing purposes.

## USAGE AGREEMENT

To use Remcos you are obliged to comply to local and international laws
and to BreakingSecurity.net Terms of Service.

Any user shall 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 BreakingSecurity.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 BreakingSecurity.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 BreakingSecurity.net software, features which prevent or restrict use or copying of any licensed content, or features that enforce limitations on use of the BreakingSecurity.net software;
(E) intentionally interfere with or damage operation of BreakingSecurity.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 BreakingSecurity.net

## COMPATIBILITY & DEVELOPMENT

Remcos is completely native and runs without any dependencies
on **any Windows version, from WinXP to Win11**,
on both 32-bit and 64-bit platforms.

Remcos is programmed in

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

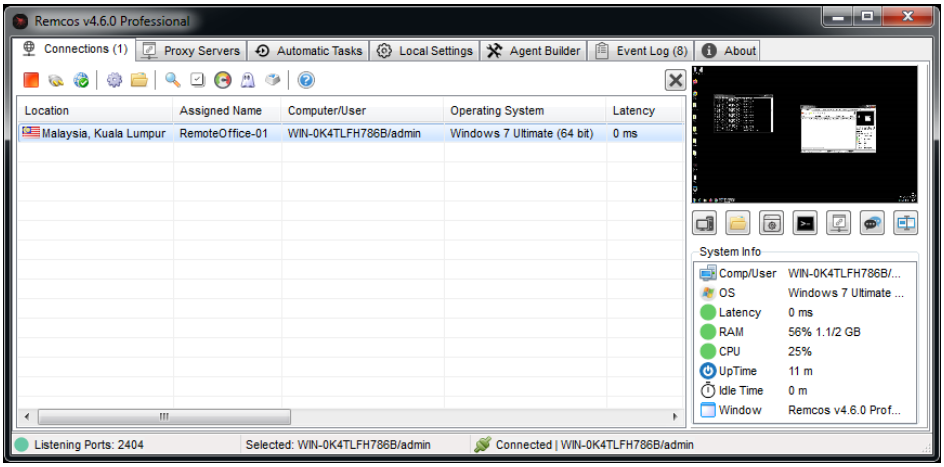
The skillful development in these programming languages provides
maximum performance, compatibility, and lightweight operation.

Remcos agent, written in C++, while it provides access to an extremely wide array of functions,
is just about 480 kb in size.
That’s just one of the many aspects of Remcos where you can view how performance,
speed and lightweight operation have always been a priority in the development.

# STRUCTURE

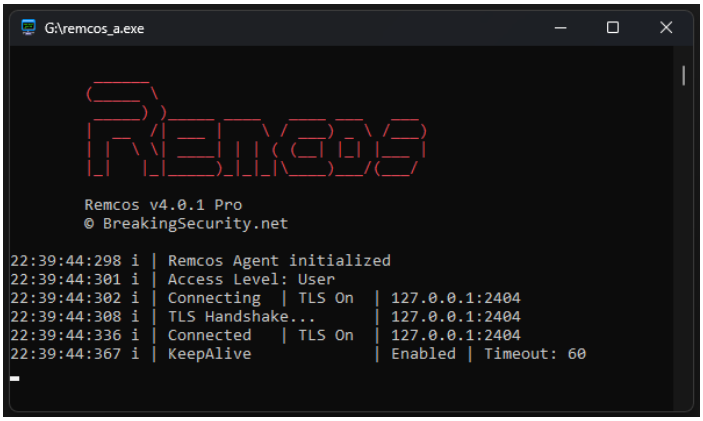
Structurally, Remcos is composed by two main parts:

- **Controller**:
  Remcos Controller is used to administrate and control the remote systems.




*Remcos Controller*

- **Agent**:
  Remcos Agent must be run on the systems which you wish to control.
  It will receive commands from the Controller and execute them.




*Remcos Agent*

# Chapter 2:
# Basic Setup

This chapter will help you configure Remcos to establish your first successful remote connection.

## CREATE A FOLDER FOR REMCOS

Remcos is a portable .exe application and does not require an installation.
Remcos saves all of its files and configuration into its current folder.

- Create a Remcos folder to save Remcos files.
  You can create this folder on your Desktop or anywhere else.

- You can download the Remcos.zip from our website and extract Remcos.zip into this folder.

## ALLOW REMCOS ON YOUR SECURITY SOFTWARE

Remcos is a surveillance and red teaming software,
therefore it may be detected as a trojan or backdoor by your security software.
Before using Remcos, make sure it is allowed by your security software.

### Windows Defender

Here is how to exclude Remcos folder from **Windows Defender**,
which is the default Windows security software:

1. **Open Windows Security**:

- Click the shield icon in the system tray (bottom-right of the taskbar).
  This directly opens **Windows Security**.

2. **Go to Virus & Threat Protection**:

- In the Windows Security window, click on **Virus & threat protection**.

3. **Open Manage Settings**:

- Go to the **Virus & threat protection settings** section.
- Click **Manage settings** under this section.

4. **Navigate to Exclusions**:

- Scroll down to the **Exclusions** section and click on **Add or remove exclusions**.

5. **Add a Folder Exclusion**:

- In the Exclusions window, click the **Add an exclusion** button.
- From the dropdown menu, select **Folder**.

6. **Choose the Folder**:

- A file explorer window will open. Navigate and select the Remcos folder.

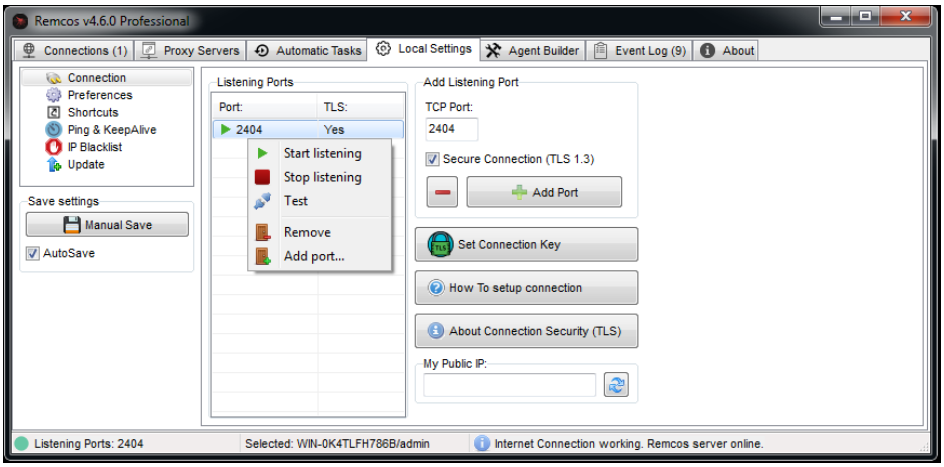
7. **Confirm the Exclusion**:

- The folder will now appear in the exclusions list.
- Windows Defender will no longer scan this folder.
- You can now copy Remcos files into this folder.

# CONFIGURE CONNECTION

Remcos uses a TLS encrypted TCP connection between Controller and Agent,
without any intermediate servers.
This provides maximum privacy, speed and security for your connections.

In Remcos, go to *Local Settings -> Connection*.




*Local Settings -> Connection*

**Add a TCP port to allow Remcos to accept incoming connections from your remote computers**.

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.

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.

# CONNECTION ENCRYPTION

## Setup Connection Encryption

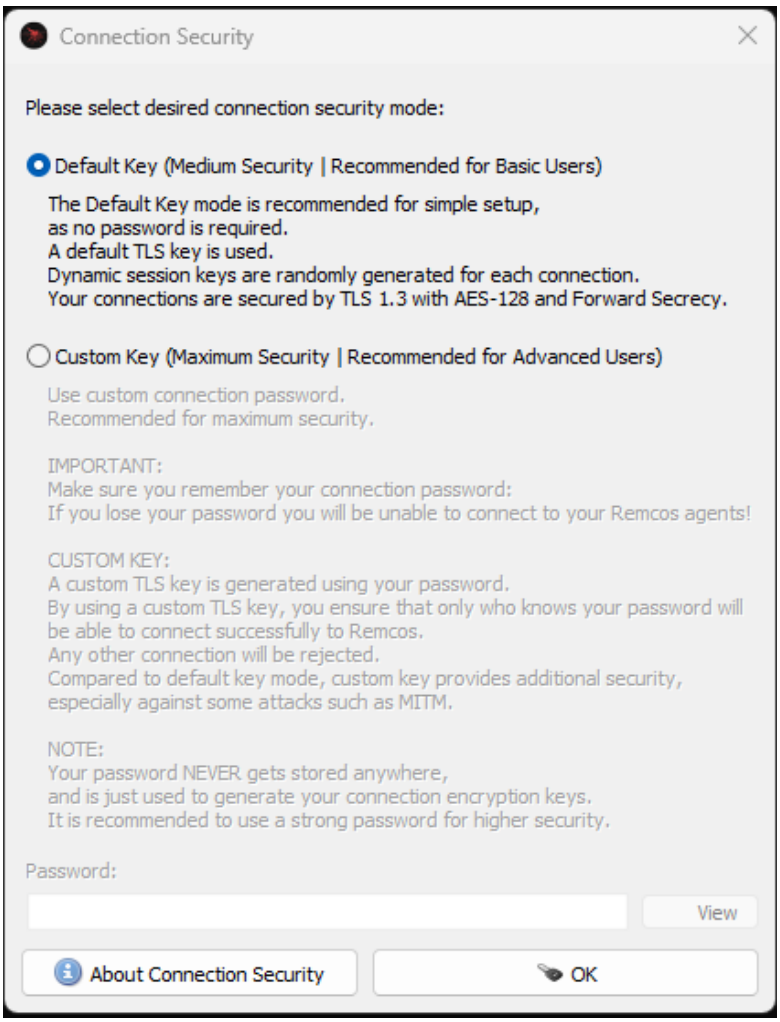
You have the option to secure your connection with TLS 1.3 (Transport Layer Security).
Our TLS v1.3 implementation secures your connection with the highest security standard, using AES-128 encryption, mutual certificate authentication, and forward secrecy.

You can choose either:

- Default TLS Key mode (Recommended for basic users and medium security)
- Custom TLS Key mode (Recommended for advanced users and maximum security).

**DEFAULT TLS KEY MODE:**

This option provides TLS encryption without the need for the user to remember a password.
It is recommended for convenient and easier setup.
Even when using the Default Key mode, random, dynamic AES-128 session keys will still be generated for each connection, which will be fully encrypted with Forward Secrecy.




**CUSTOM TLS KEY MODE:**

This option is recommended for maximum security and uses a custom password for your connection.

**Important:**
Make sure you remember your password,
you may need it if you reinstall Remcos.

Enter a **password** to setup TLS Connection.
The password will generate your custom TLS key and certificate.
Your password is just used once for the generation of the TLS certificates and keys.
It doesn't get stored anywhere.

# CONNECTION SECURITY DETAILS

**TLS** provides various security benefits:

1. **Encrypt your connection:**
   100% of data transmitted between Controller and Agent will be encrypted using AES-128.
   This will protect you from traffic sniffers, man-in-the-middle attacks,
   and anybody who is trying to monitor your traffic.

2. **Authenticate your connection:**
   Both the Controller and Agent authenticate each other identity by using TLS Certificates.
   This prevents malicious connections to your controller, as well as hijacking your Agents.

3. **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.

## TLS Mutual Authentication

In addition to AES-128 encryption, Remcos also uses **TLS Mutual Authentication**:
Both Remcos Controller and Agent authenticate each other
in the TLS handshake, using TLS Certificates:

1. The Controller makes sure that the connection is arriving from a legit Agent
   (instead of a port scanner, honeypot, or other suspicious tools).

2. The Agent makes sure it is connecting to the legitimate Controller,
   preventing the hijacking of your Agents.

## Forward Secrecy

With Forward Secrecy, if an attacker gains access to your connection password (or private key),
they will not be able to use those keys to decrypt past communication sessions.

The AES-128 encryption keys for your connection are dynamically generated on each connection,
and are valid only for a single session.
Encryption keys are discarded after each disconnection.
On each new session, new random encryption keys are generated.

# PORT FORWARDING

If you want Remcos to be able to receive connections from computers which are located outside of your home, business, or generally the Local Area Network of your Remcos Controller,
you will need to forward the ports you are using for Remcos.

A port forward is a way of making a computer accessible to computers on the internet,
even though you are behind a router.
Port forwarding is commonly used in Remote Administration Tools, gaming, surveillance cameras,
voice over IP, and file sharing.

Port Forwarding is **not** necessary if you are using Remcos only inside your Local Area Network.
This means that, in most cases, if you use Remcos only to manage a cybercafe, office, classroom,
or generally multiple computers connected to the same router, you will not need to do port forwarding.

If you want to use Remcos to control your computers abroad, outside your home or office,
or generally outside your LAN,
then you will need to forward your ports.

**If your Ports are not forwarded,**
**your Remcos Agents will NOT be able to reach your Remcos Controller.**

If you are connecting Remcos directly to your router,
then you will need to configure port forwarding on your router.

If you are connecting Remcos through a VPN,
then you will need to configure port forwarding on your VPN.
Port Forwarding steps depend on your router or VPN.

Port Forwarding references:

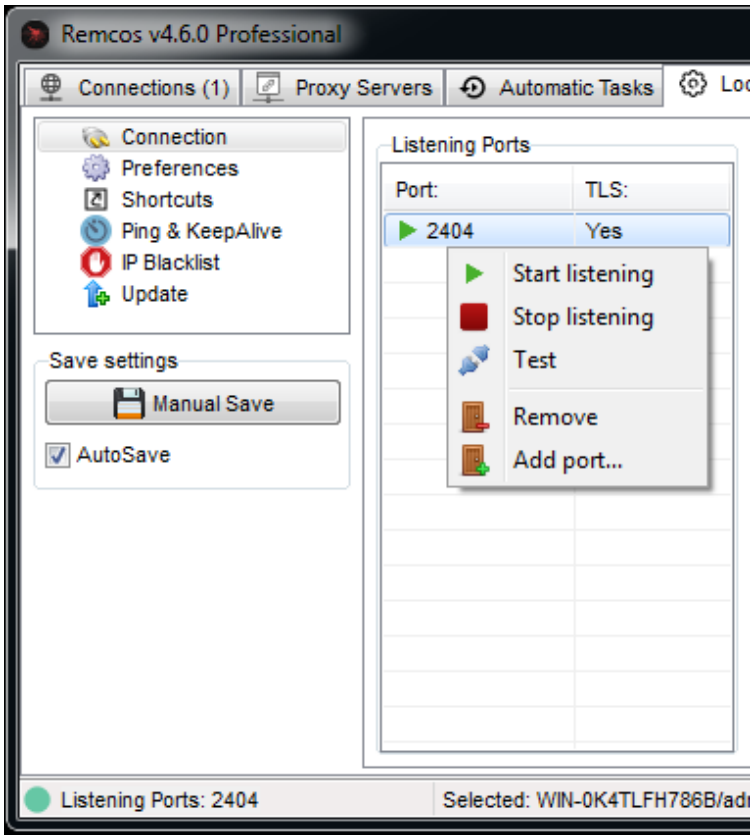
- https://youtu.be/2G1ueMDgwxw
- https://PortForward.com/
- https://en.wikipedia.org/wiki/Port_forwarding
- https://medium.com/datadriveninvestor/port-forwarding-for-beginners-11355d000867

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

## PORT TEST

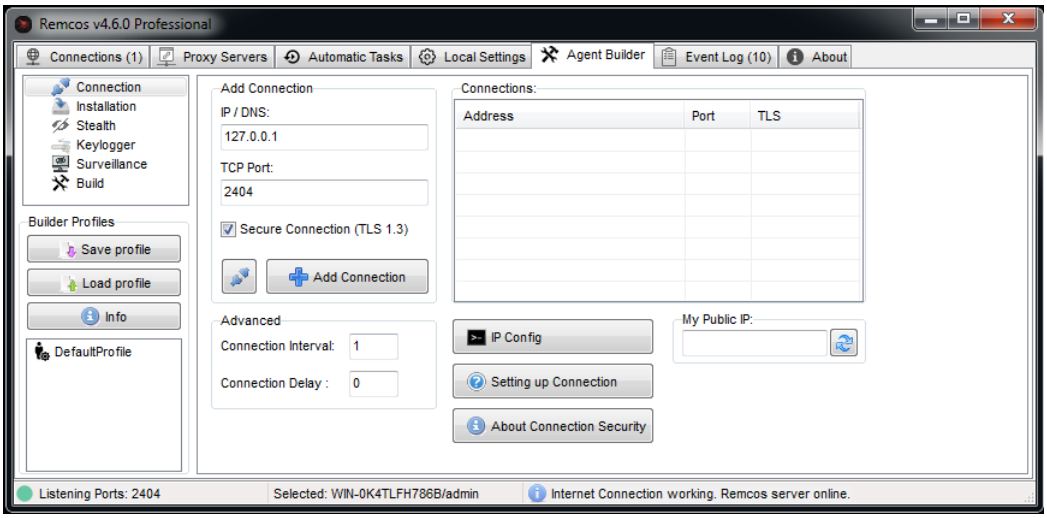
Remcos provides a useful in-built function to test if the Port is correctly open, forwarded and reachable from your remote Agents.

Right click on the port you added and click on **Test**.
A message with the test result will be displayed.



# CONFIGURE AGENT CONNECTION

In Remcos, go to *Agent Builder -> Connection*.
From here you can setup how the Remcos Agent will connect to the Controller.




**IP / DNS:**

Here you must insert the IP or DNS address of your Remcos Controller.
The Agent you create will connect to this address.

How to know the Remcos Controller IP address:

**a.** If you are connecting Remcos Agent inside a **local** network (LAN),
you will need to insert your **local IP address**.
To find your local (LAN) IP address, you can use the **ipconfig** command.
**Click on the IpConfig button to view the local IP address.**

**b.** If you are connecting Remcos from **outside of your local network**,
you must insert your **public IP address**.
**You can view your public IP address in the "Public IP" field in Remcos.**
If you are connecting Remcos through a VPN, your public IP will be the VPN server address.
You can also view your public IP by using many online services, such as

- https://www.myip.com/
- http://www.myipaddress.com

## Important Tips

**Using a DNS address:**
A DNS address can be used instead of an IP address.
If the IP address of the Controller system is variable,
you can use a Dynamic DNS service to always point to the updated IP address.
You are free to use any DNS and DDNS service you wish.

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

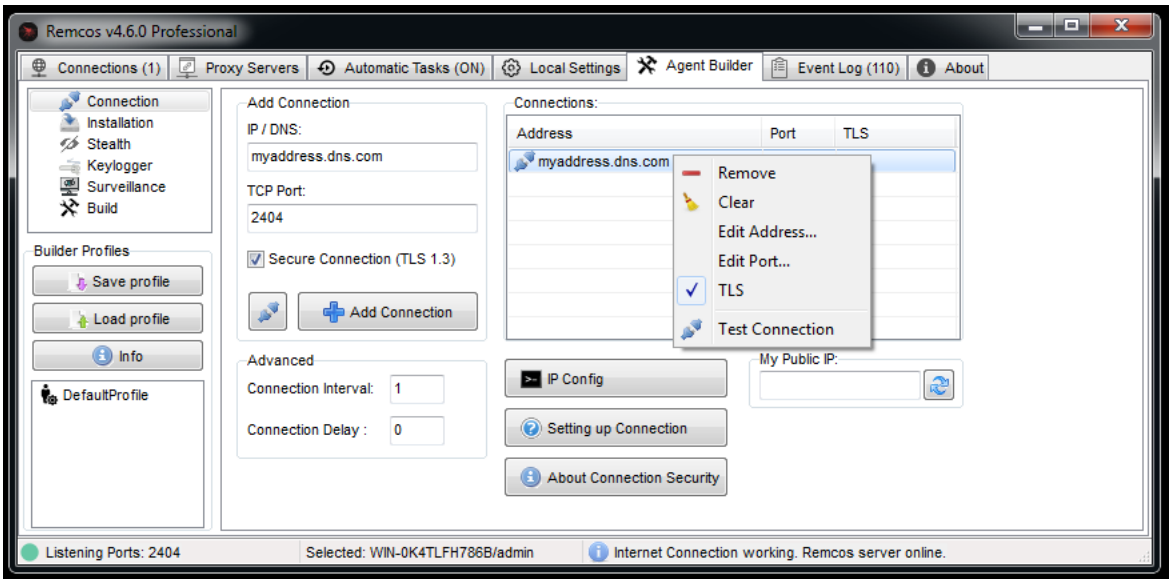
**Make sure that the TCP Ports that you use are correctly forwarded**
in case you are configuring a WAN or VPN connection.
You can read more about port forwarding later in this manual.

**TLS:**
If you selected your listening port to encrypt your connection with TLS, check this option.
Make always sure to remember the connection password that you set.

## Test Connection

Remcos provides a useful in-built function to test if the entered connection details are valid.
The test will check if your agents will be successfully able to connect to your controller.

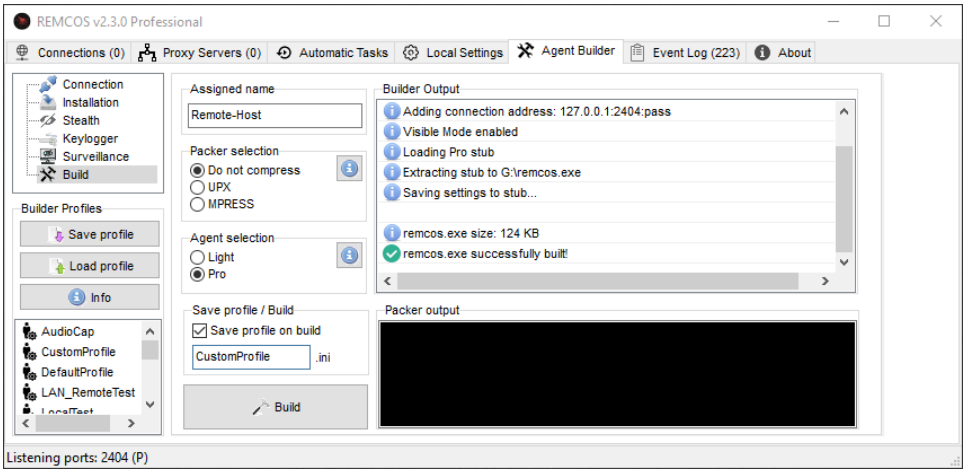
To run the test, simply click on the *Test Connection* button.
A connection test will be executed and a message with the result or the error will be displayed.



# BUILD REMCOS AGENT

After you entered your connection settings,
go to *Agent Builder -> Build*.

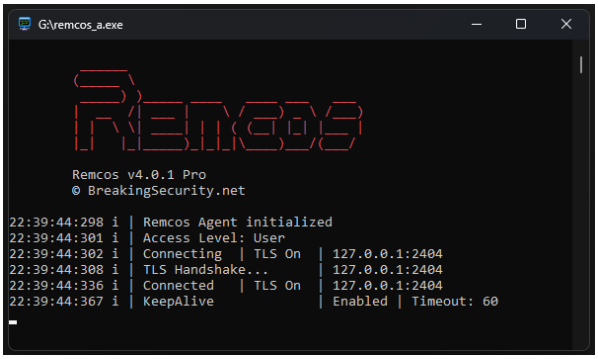
Click the *Build Agent* button to create a **Remcos Agent** file with your own configuration.




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

Deploy the Agent file on your system to be controlled and execute it.
If the connection is successful, a new connection will popup in the Controller's *Connections* tab.

The Agent should also display a window (if set in Visible mode).
From the Agent window you can also check if connection is established.




*Agent window*

# 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 Controller and Agent systems are connected to internet (if connection is via WAN), or are connected to the same Network (if connection is via LAN).
   You can check that you can reach the Controller system from the Agent system by using a ping command from the Agent system.
   Enter the address of the Controller system for the ping command.

   b. **Agent is configured with a wrong IP/DNS address or a wrong Port.**
   Check from the Agent window that the displayed connection IP/Port details are correct and match the ones of the Controller.

   c. **Controller's TCP port is not opened.**
   Check on *Local Settings -> Listening Ports* that your port is listening.

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

   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 may be subject to change,
   for example when there is a network reset or you reset your router.
   If you don't have a static IP address, you could use a Dynamic DNS.

   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 software application or webpanel 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 Security**
      Check that the listening port on Controller, and the port set on the Agent,
      are both using either Unencrypted connection, OR are both using TLS.

   b. **Mismatching Connection Password**
      Make sure that the connection password you entered for the Agent and the Controller
      is the same.
      If you change your connection passwords, existing Agents will not be able to connect.

   c. **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 TCP port only for Remcos.
      Remcos is programmed to automatically drop invalid and unauthorized connections.

   d. **An old, incompatible Remcos Agent version is trying to connect**
      Some previous version of Remcos may have a different, incompatible connection.
      You can verify this by checking the Remcos changelog.
      You can login to your previous Remcos Controller version
      and update your Agents to the latest version.

# Chapter 3:
# Advanced Setup

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.

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.

## INSTALLATION

From the Installation tab you can set whether Remcos should start automatically with Windows.
Check *Autostart on Windows startup*, if you want the Remcos Agent to 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.

# TELEGRAM BOT

The Remcos Telegram Bot allows you to interact with your computers directly from your Telegram account.
Whether you're using a **smartphone**, **tablet**, or **browser**,
you can seamlessly monitor and control your devices from anywhere in the world.

The Remcos Telegram bot is designed to provide comprehensive remote management capabilities.
Here are some of the things you can do with it:

- **Monitor Computer Activity**: Keep track of what your computers are doing, in real-time.
- **Take Screenshots**: Capture and view screenshots of your remote desktops.
- **Get Notifications**: Receive alerts and notifications for various events and activities.
- **Send Commands**: Execute commands on your remote systems with ease.
- **Run Scripts and Programs**: Trigger specific scripts or applications remotely.
- **Download Files**: Download and execute files, install programs remotely.

## Start Telegram Bot

Getting started with the Remcos Telegram bot is straightforward.
Follow these simple steps:

1. **Set Up the Telegram Bot**:
   In Telegram, start a Chat with @RemcosBot.
   The Remcos Bot will provide a Chat ID code for you.

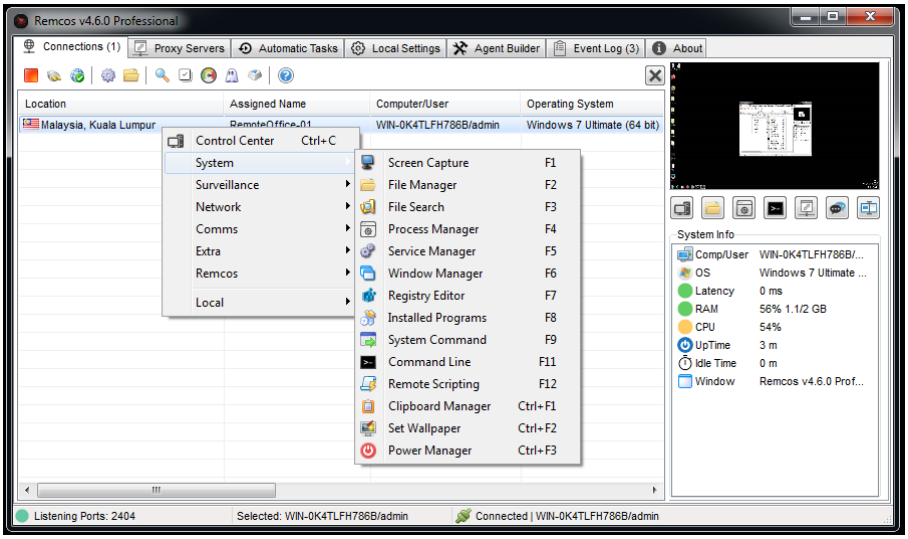
2. **Configure Remcos**:
   In Remcos Controller -> Local Settings -> Telegram Bot, insert your chat ID and press start.

3. **Start Controlling Your Computers**:
   Begin using the bot to monitor and control your devices from your Telegram app.
   Enter */help* to view the list of available commands.

# Chapter 4:
# Usage

## REMOTE ADMINISTRATION

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




You have various ways to access Remcos Functions:

1. Functions Menu
2. Keyboard Shortcut Keys (F1, F2, etc.)
3. Shortcut Keys
4. Control Center

## Functions Menu

This is the main method to access Remcos functions.
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 can run the specified function on all the selected hosts.

## Functions Menu Style

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

## Keyboard Shortcut Keys

Most of Remcos functions can be launched by using a shortcut key.

Examples:

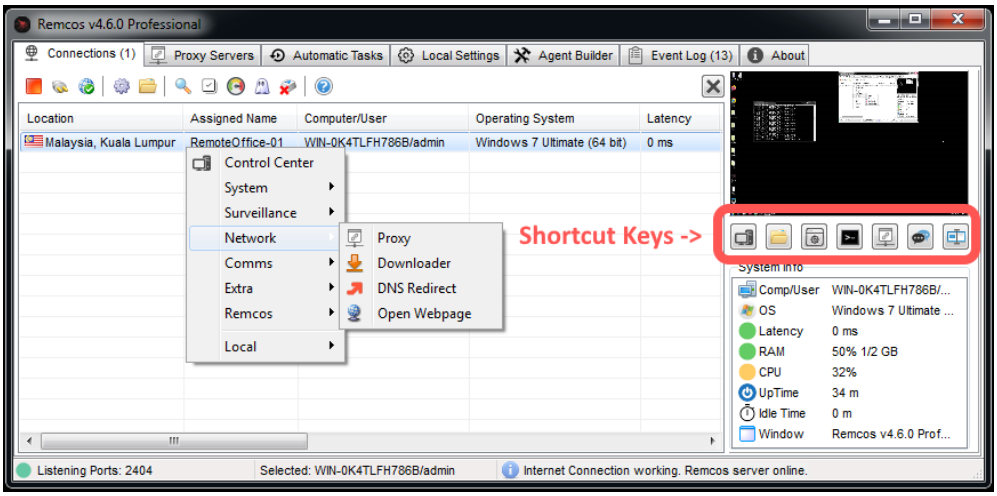
- **[Ctrl + C]** Control Center
- **[F1]** Screen Capture
- **[F2]** File Manager
- **[F3]** File Search
- **[C]** Chat

To show or hide shortcut keys from the Functions Menu, go to:
*Local Settings -> Shortcuts -> Show Shortcut Keys*.

## Panel Shortcut Keys

There are 7 shortcut keys that you can customize with any function you prefer.
These shortcut Keys are customizable from *Local Settings -> Shortcuts*.

In addition to that, you can click on the Screen Preview to open Screen Capture.



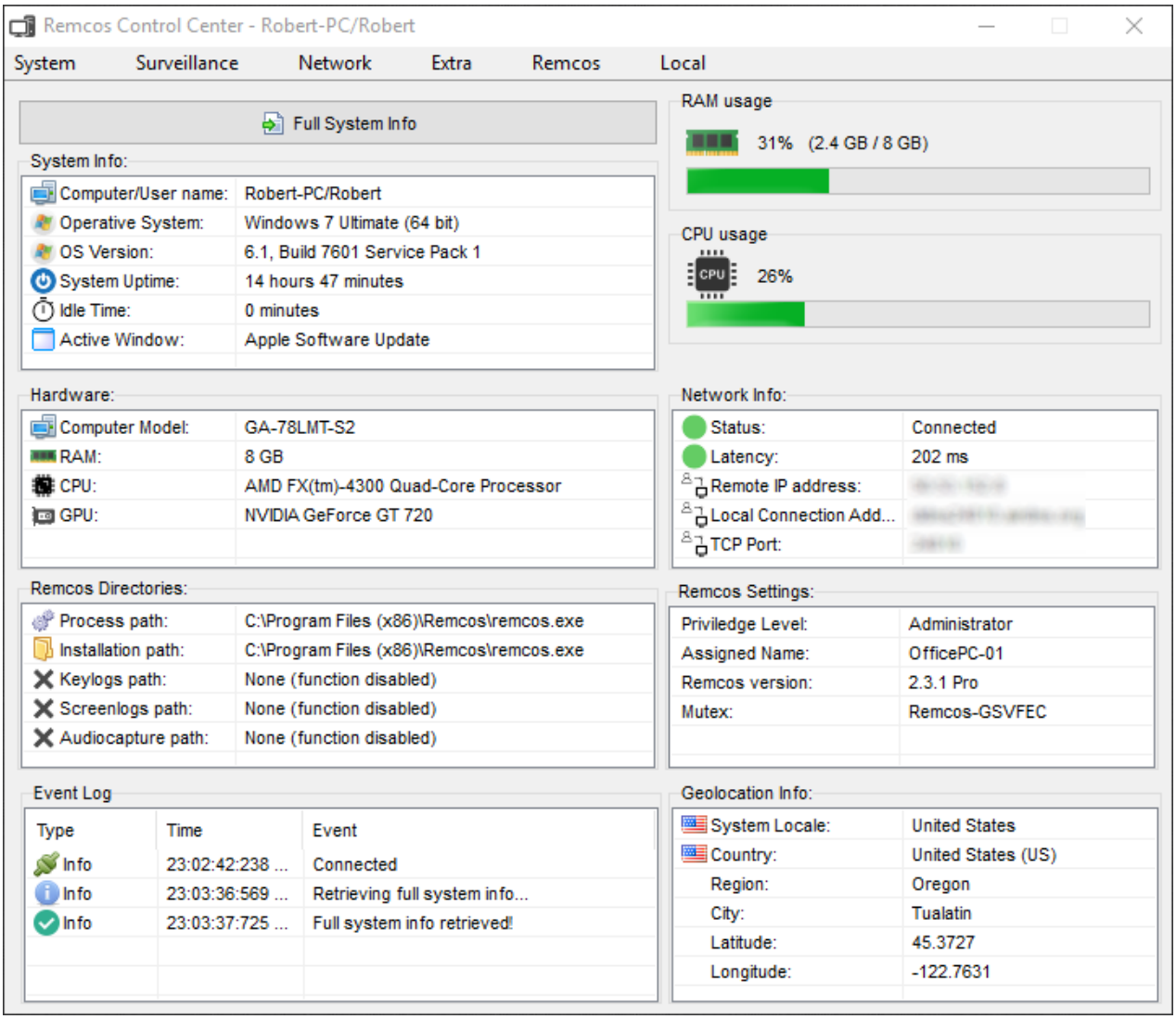

## Favorite Function

**Double-click** a remote host or press **Enter** to open the Favorite Function.
By default, Favorite Function is the Control Center.
You can change the Favorite Function from *Local Settings -> Shortcuts*.

# 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.



# FUNCTIONS OVERVIEW

**Remcos Functions** are divided into 7 categories:

## System

The System category includes all the **system management** functions.
These functions are useful to manage any part of your remote computers.

- Screen Capture
- File Manager
- Process Manager
- Service Manager
- Registry Editor
- Remote Command-Line
-…

## Surveillance

The Surveillance category contains functions useful to monitor your remote systems and their surroundings.

## Network

The Network category includes various network related functions.

- SOCKS Proxy
- DNS Redirect
- Downloader
- Open Webpage

## Comms

The Comms category contains communications related functions.
Useful to chat and transmit text and audio messages to the remote users.

- Chat
- MessageBox
- Audio Player

## Extra

This category includes miscellaneous functions which didn’t fit into the others.

- DLL Loader
- Logins Cleaner

## Remcos

Functions used to manage the Remcos Agent

- Rename
- Highlight
- Reconnect
- Restart
- Uninstall
- …

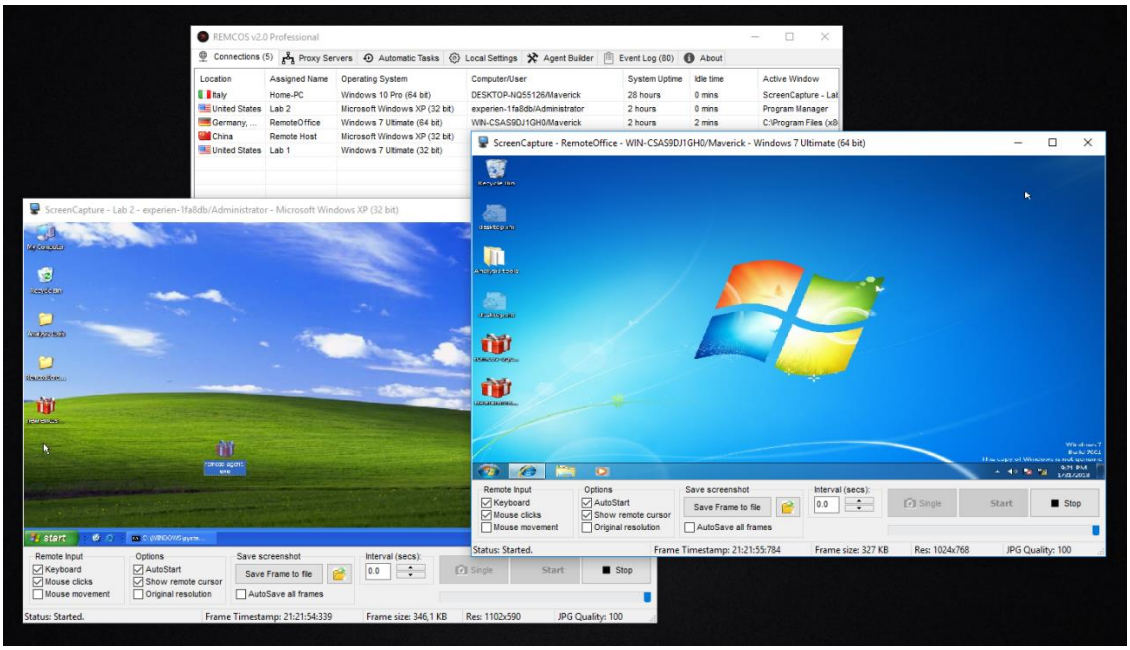
## Local

The Local category includes various Local Utilities which do not send any command to the remote host.

- Browse local Downloads folder
- BlackList IP
- Copy IP address
- Copy Computer/Username

# 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.

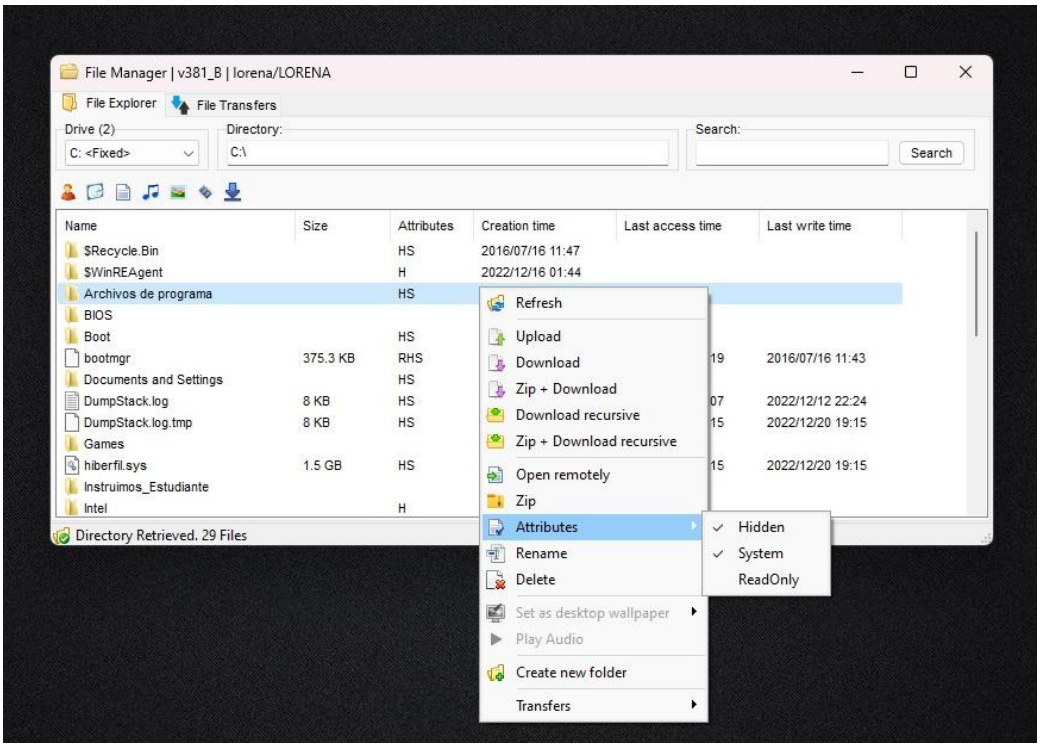
**Quality:**

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**)

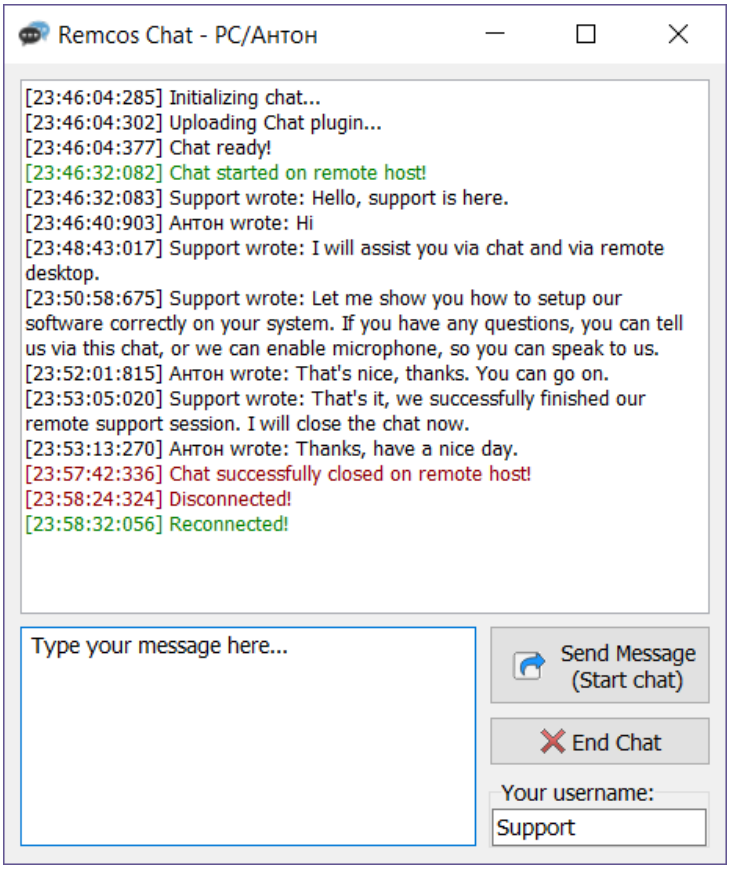
With the File Manager you can manage and transfer files between the systems.



# CHAT

**Remcos Chat** (key: **C**)

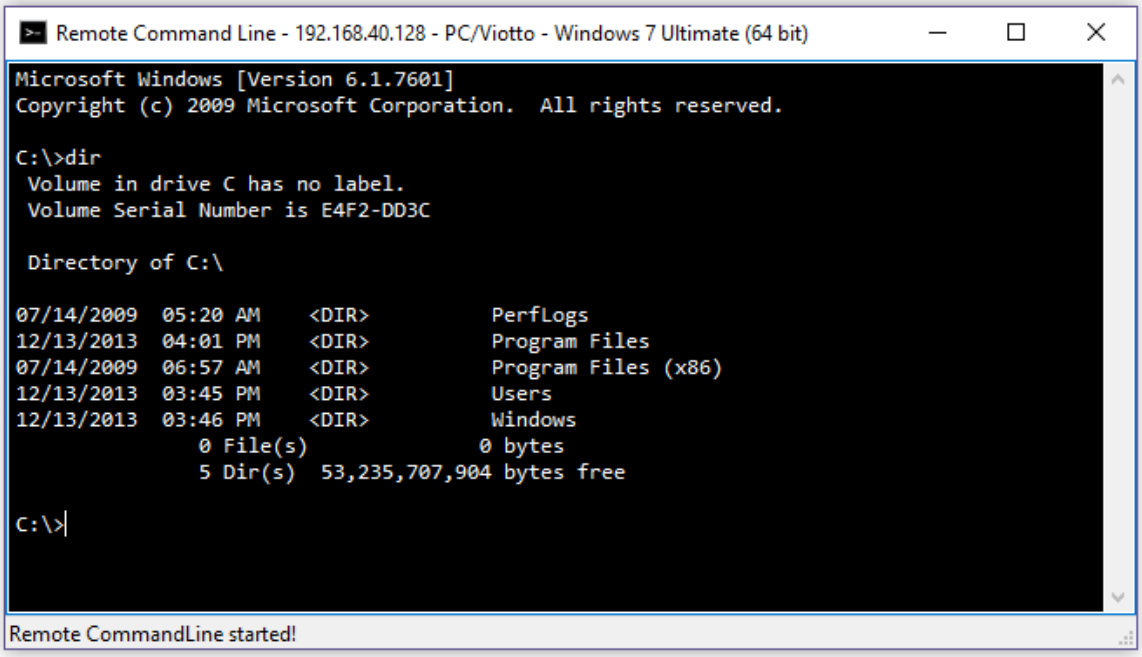
Provides you an efficient channel of communication when performing **Remote Support** sessions.



# REMOTE COMMAND LINE

**Remote Command Line** (Shortcut key: **F11**)

Opens a Remote Shell on the system,
letting you use its command line remotely.



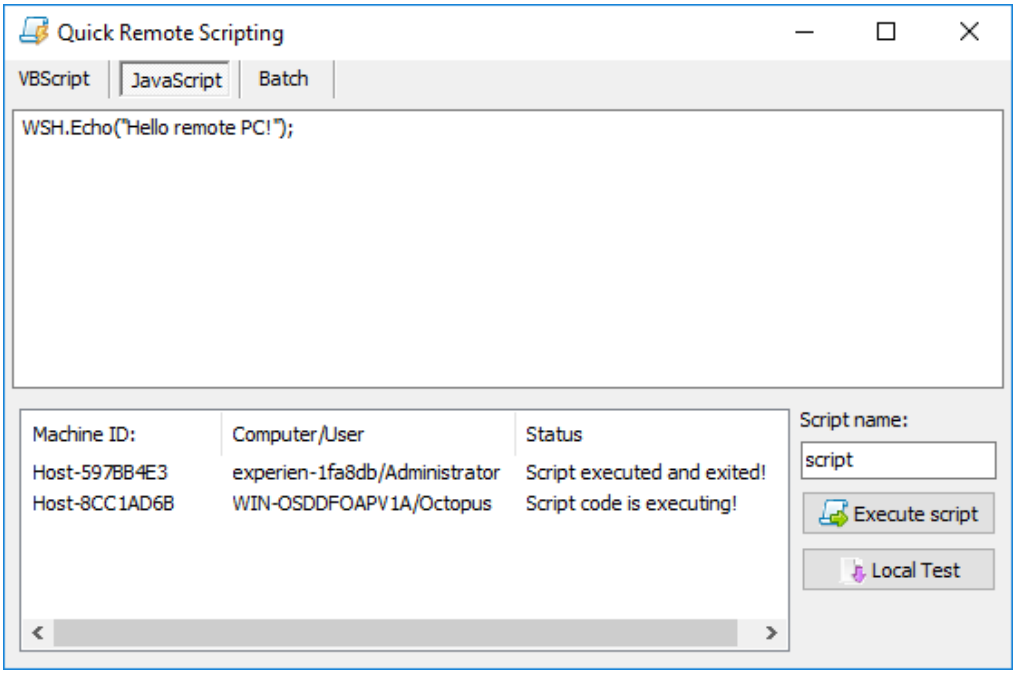
# REMOTE SCRIPTING

**Remote Scripting** (Shortcut key: **F12**)
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.

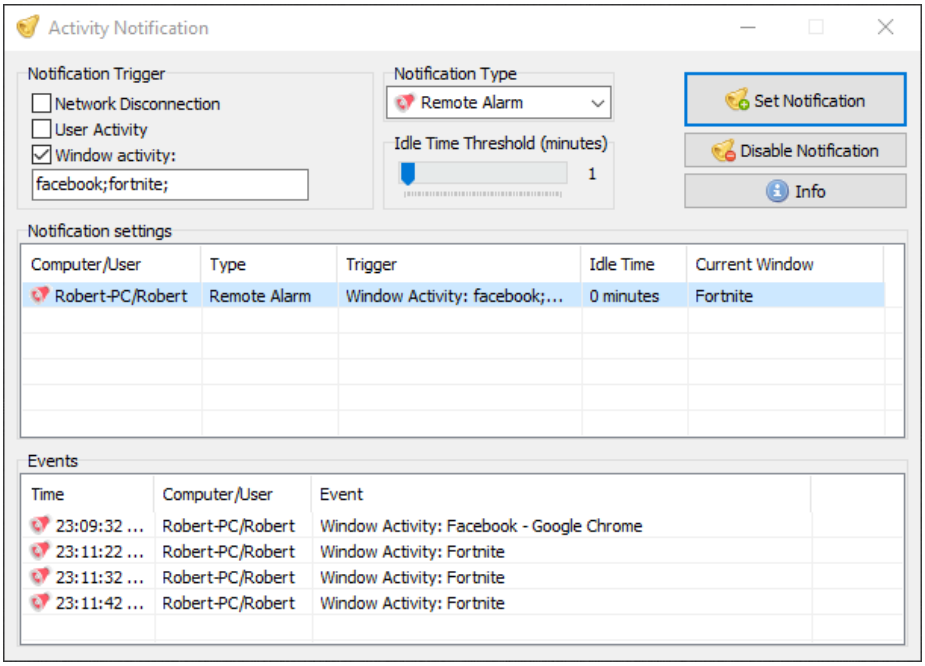
# ACTIVITY NOTIFICATION

With the Activity Notification function, you can setup remote notifications or alarms as soon as certain actions happen on your remote systems.
For example, you can set up alerts if the users enters specific webpages or is using specific programs.
You can also setup a loud alarm on the remote PC itself or the Controller PC.

**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.

If the Remcos Telegram Bot is running,
you will also receive a **telegram notification**.



**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.

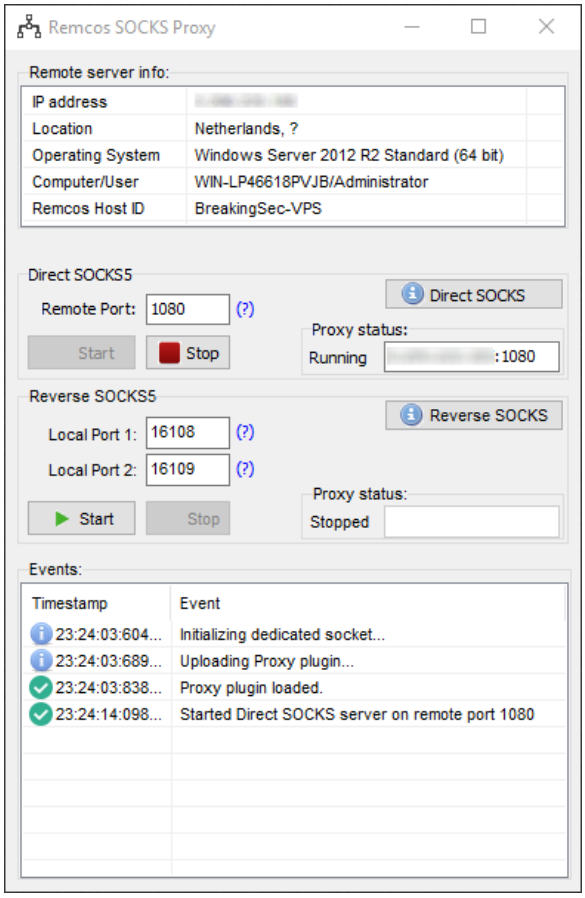
**Idle Time Threshold:**
User Activity notification will be triggered only if idle time exceeds threshold.
Example: A 5 minutes Threshold will trigger User Activity Notification only if user comes back after 5 minutes or more.
This is useful if you plan to active the notification only after a certain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

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

# 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:

Client Application -> Proxy Server (Remcos Agent)

**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.

# INTERNET QUALITY CHECKER

In the Remcos toolbar you can find a useful tool which constantly measures the quality of your internet connection.
If you are experiencing slow or lagging connection with your remote clients, this tool will show you in a blink of an eye if your network connection is the culprit.
The icon of the tool gets updated automatically, but you can manually click on it to get an immediate network quality and latency test.

**Green Icon:**
Your connection is good and fast.

**Yellow Icon:**
Your connection is slow.
Maybe your wireless connection signal is not strong enough.

**Red Icon:**
Your connection is offline.
There is an error connecting to the internet.

# Chapter 5:
# Uninstallation

You have multiple ways to uninstall Remcos agents:

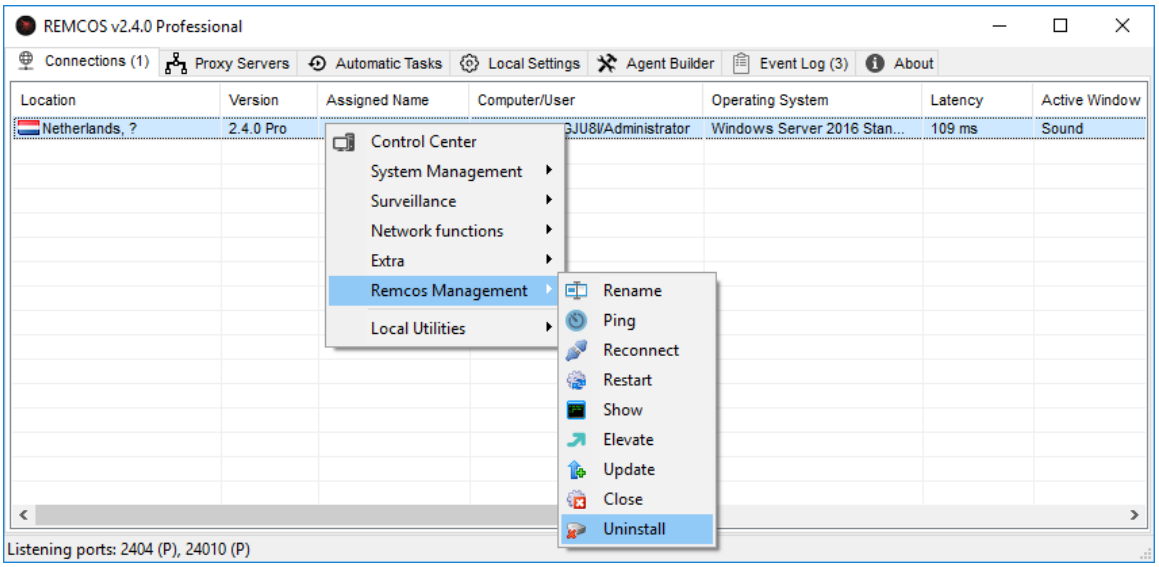
- Using Remcos Controller
- Using the stand-alone Remcos Uninstaller.

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

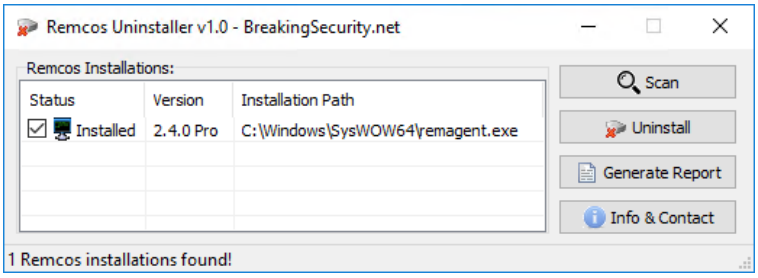
To uninstall one, multiple or all the connected agents, you can use the Uninstall command.




*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