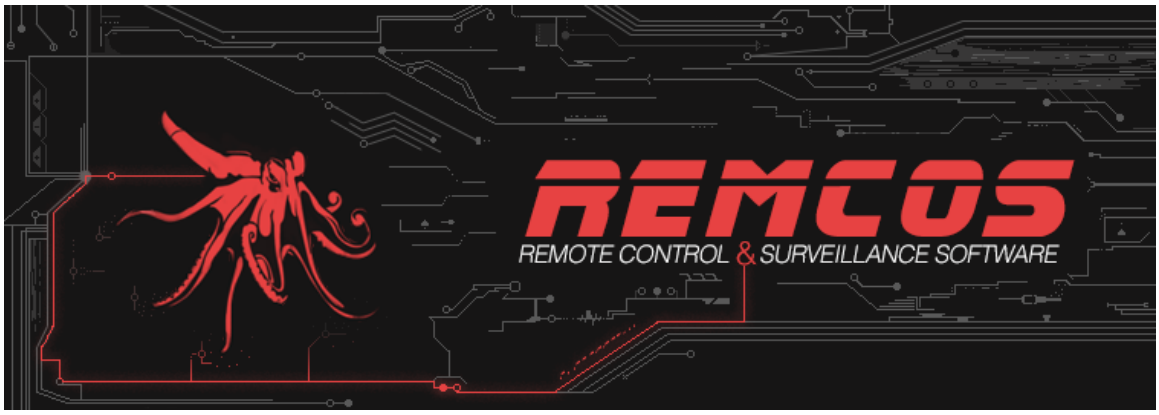


INSTRUCTION MANUAL

Revision 5

--
Remcos v2.0.9

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.

Remcos is programmed in

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

Remcos is completely native and works without any dependencies (except the default Windows ones), on any Windows version, from WinXP to Win10.

In order to use Remcos you are obliged to comply to the local laws and to BreakingSecurity.net Terms of Service.

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.

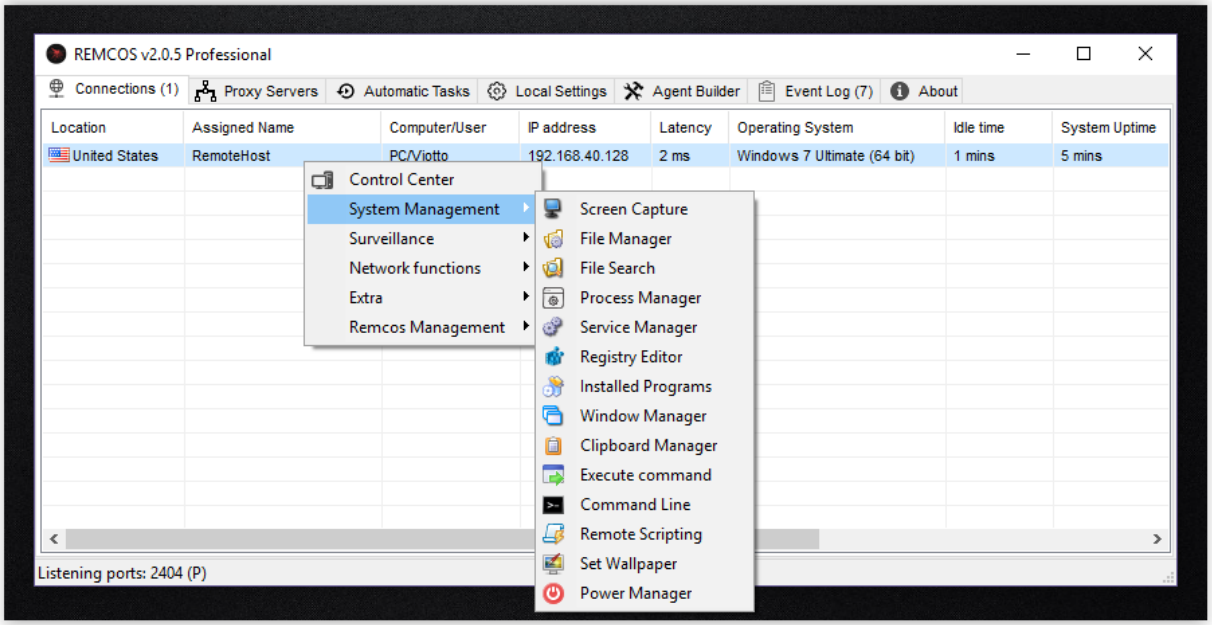


Figure 1: Remcos Controller

- **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.

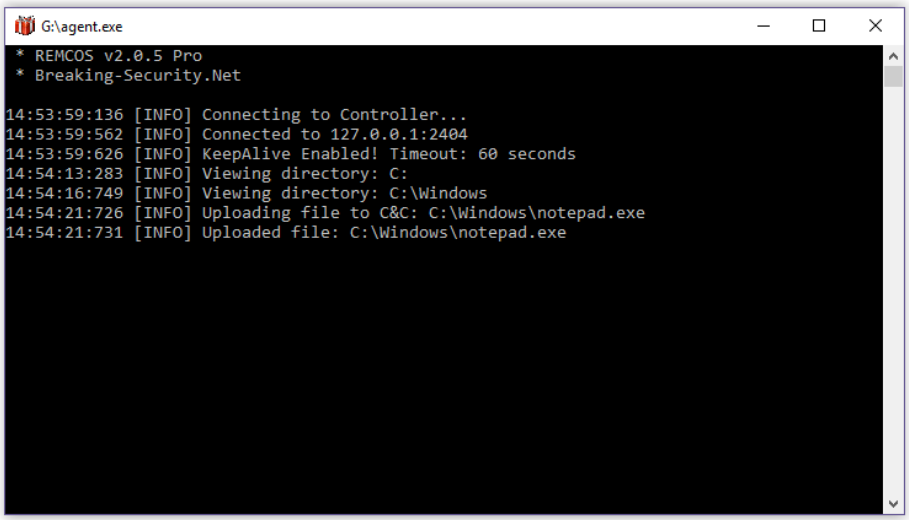


Figure 2: Remcos Agent

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.

CONFIGURE CONTROLLER CONNECTION

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

From here you can add a TCP port.
Port numbers range from 0 to 65535.
You can use the default Remcos port, which is 2404, or any other.
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.

Be sure 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.

After you successfully add a port, the Controller will be waiting on that port for incoming connections by the Remote agents.

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

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.

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
-
Usage

REMOTE ADMINISTRATION

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

Right Click on a host to open the **Functions Menu**.
From the Functions Menu you can open any function.

You can also **select multiple hosts** and use the Functions Menu, to use the specified function on all of them.

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

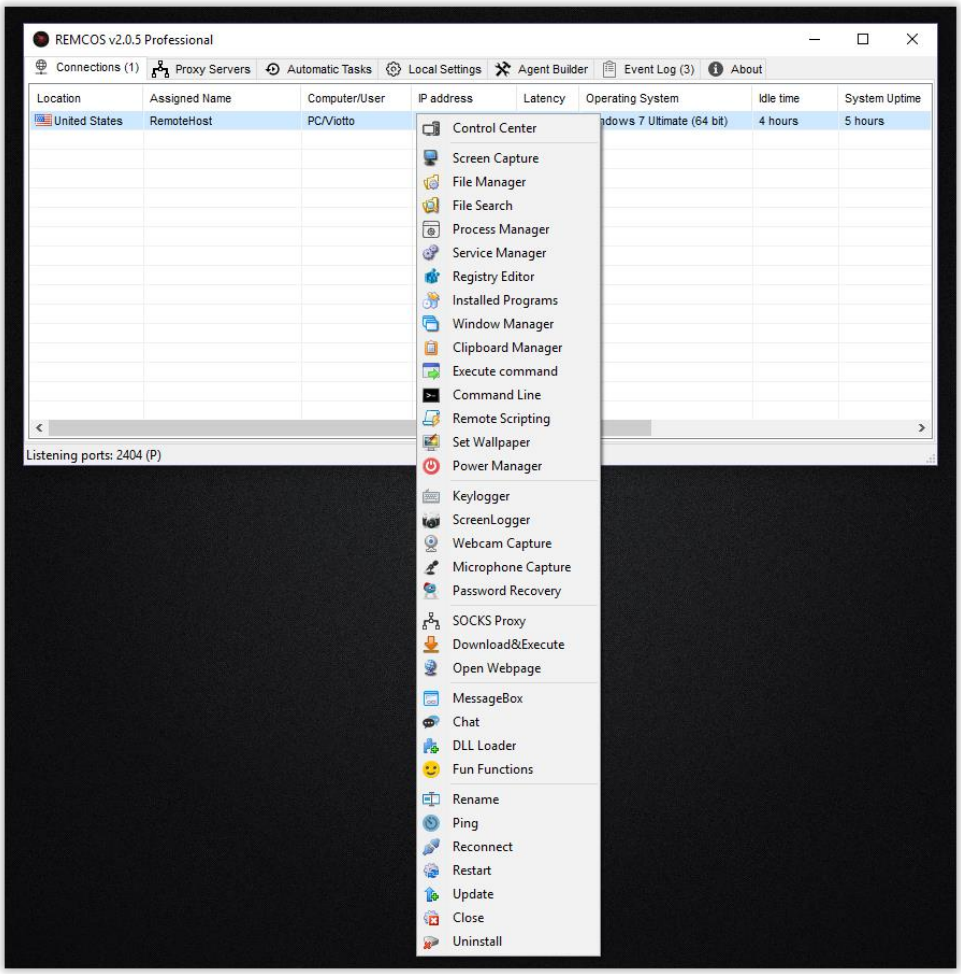
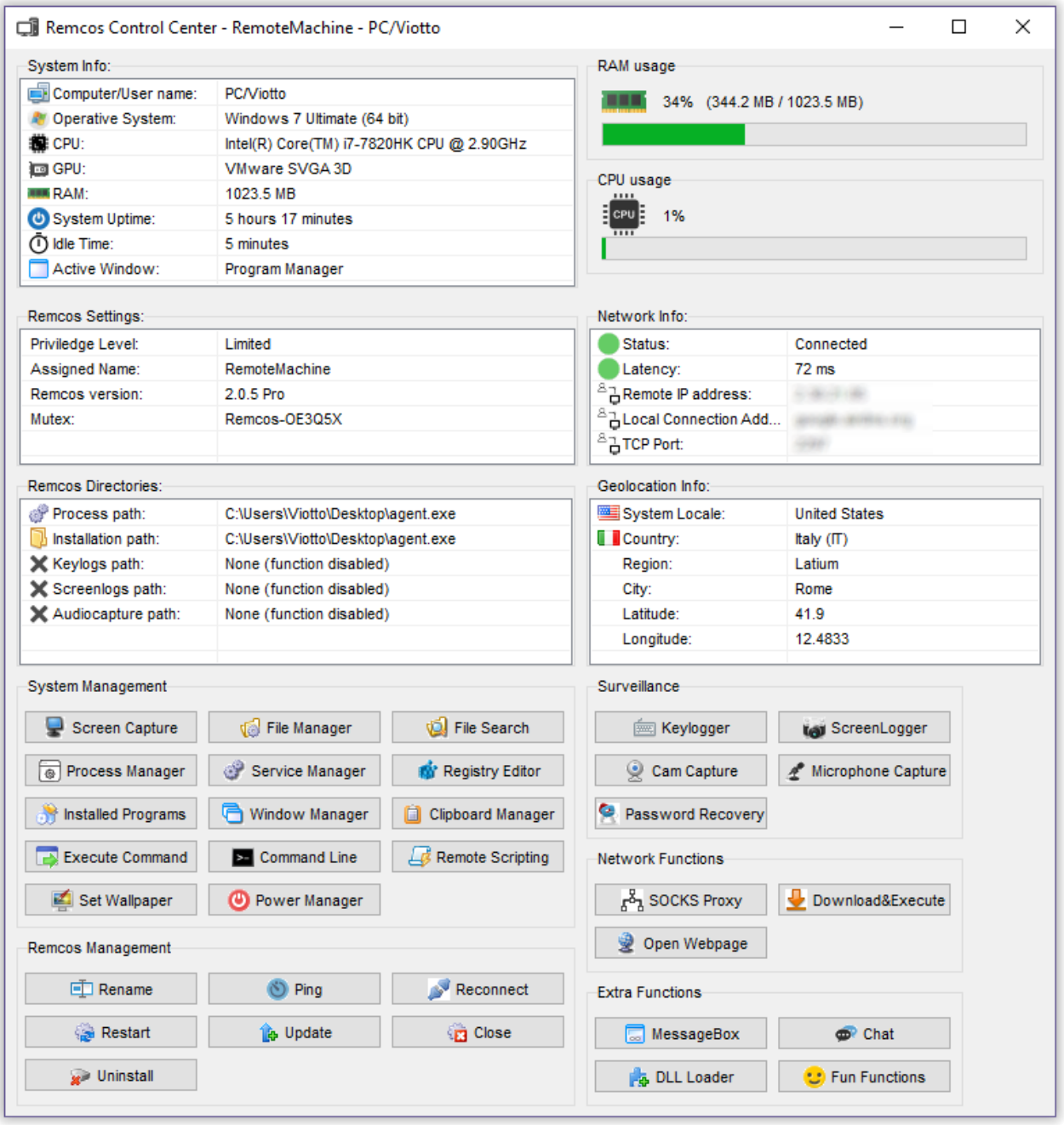


Figure 3: Functions Menu in Expanded Mode

CONTROL CENTER

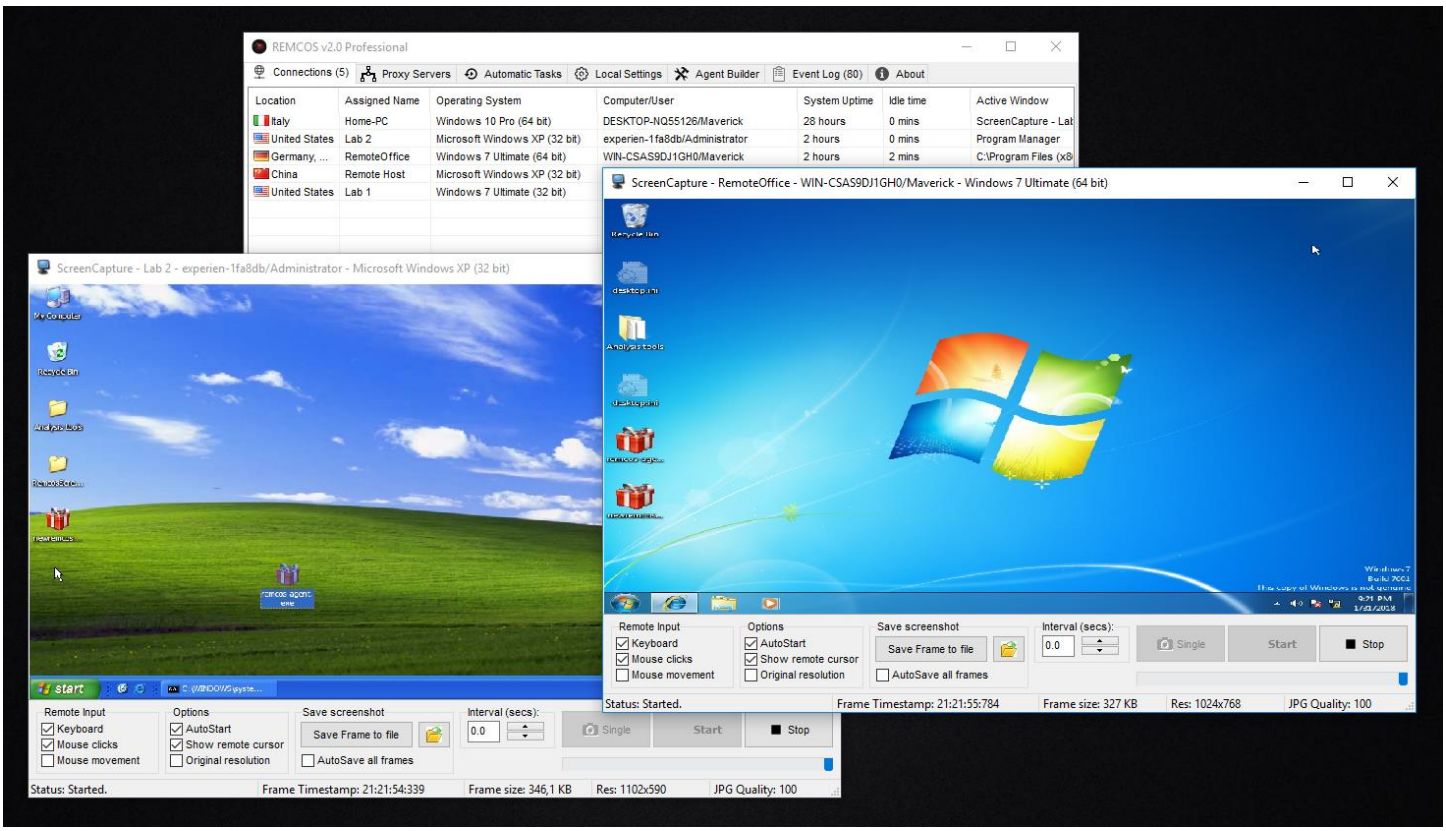
Double Click on a host, or press the **C** key to open the **Control Center**.
You can change the **Double Click Function** from **Local Settings -> Preferences**.

The **Control Center** is a convenient method to administrate your remote machine, since you have all the info and functions available at one click and all in one place.



SCREEN CAPTURE

Screen Capture let's you view and control the remote screen(s).
It is probably the most important function for most of the Remote Administration needs.

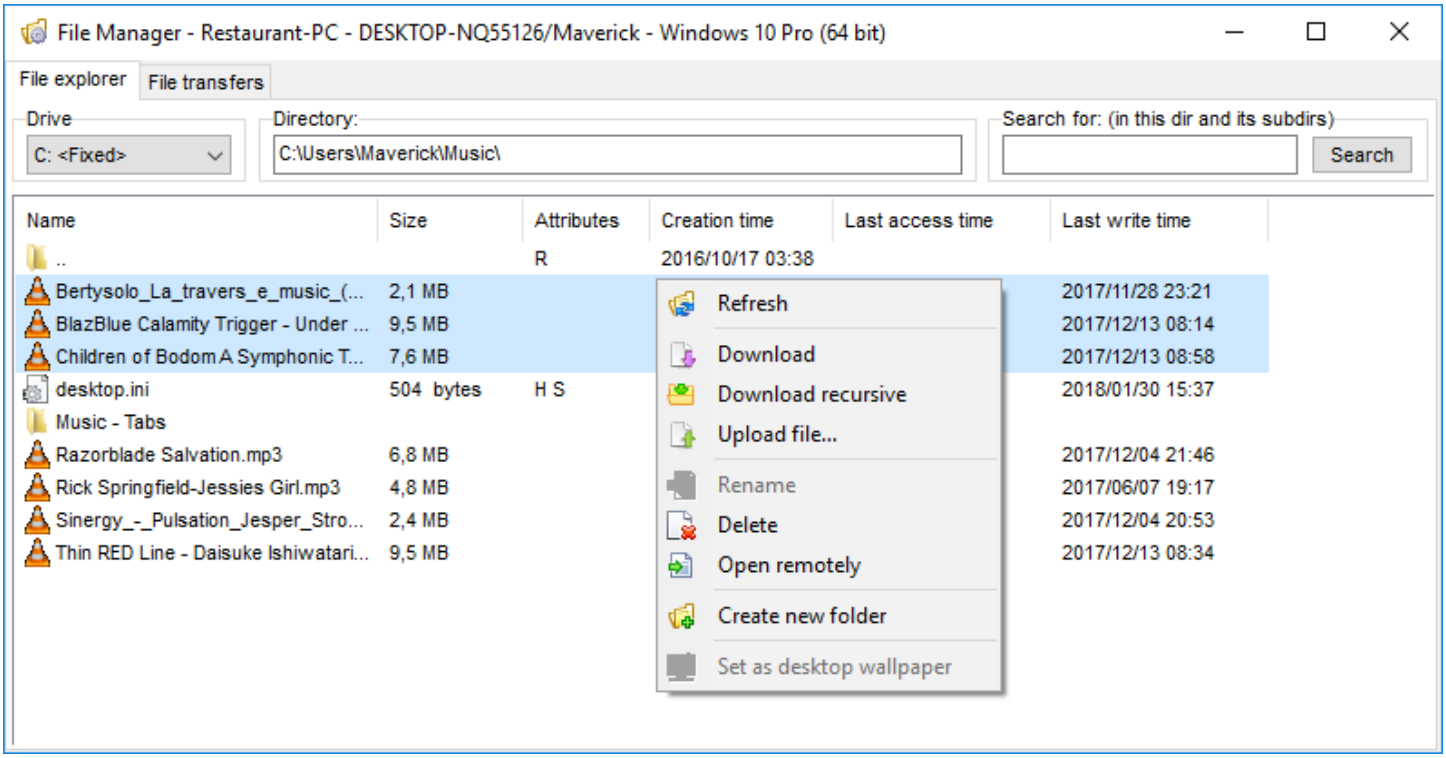


As with any other function, you can open **Screen Capture** from the **Functions Menu** or the **Control Center**.

You can also use the key **F1** to open Screen Capture on selected hosts.

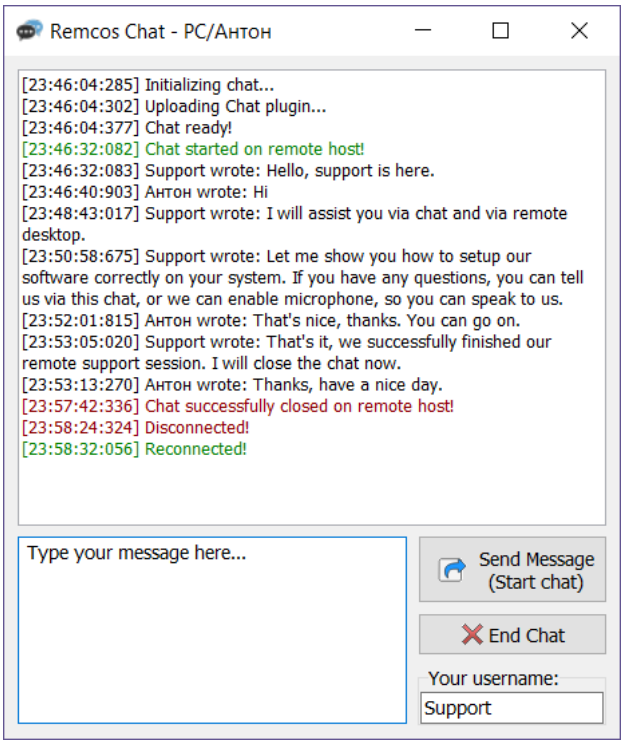
FILE MANAGER

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



CHAT

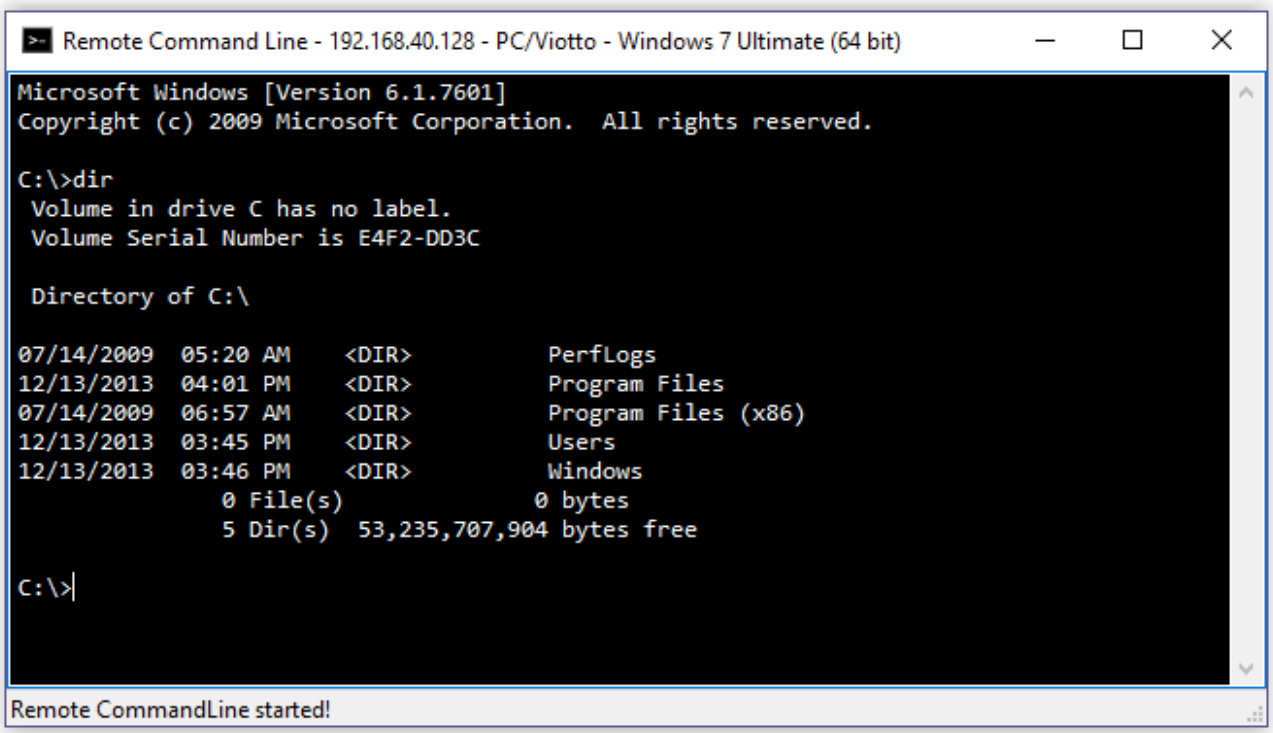
Remcos Chat (key: **H**) provides you an efficient channel of communication when performing **Remote Support** sessions.



REMOTE COMMAND LINE

Remote CommandLine (key: **F12**) open a Remote Shell on the system and let's you use it's command line remotely.

This function is very useful to users that are used to the command prompt and like to administrate systems via text commands.

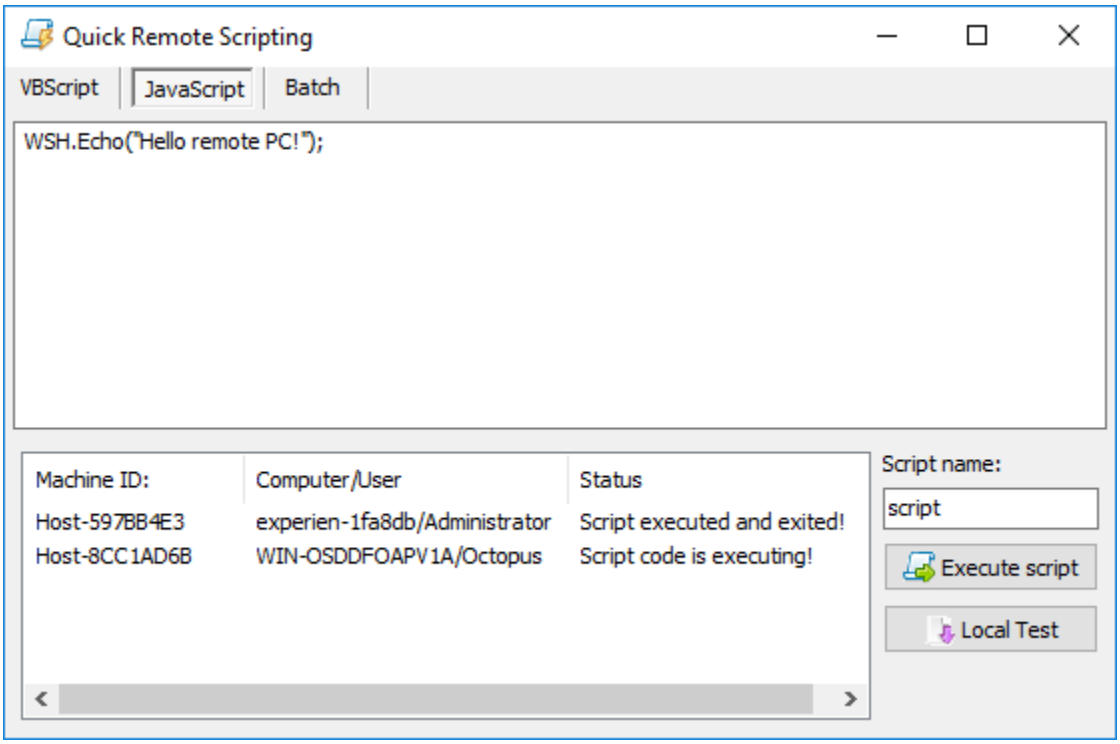


REMOTE SCRIPTING

Remote Scripting (key: **Shift + 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 into 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 security, and must be accessed only by authorized personnel to perform controlled actions.

- Be sure to comply to your local laws and our Terms of Service.
- **Keylogger**: use the Keylogger to see what has been typed on the keyboard.
- **Screen Logger**: Saves screenshots at intervals or when inside specified applications.
- **Webcam Capture**: use your computer as an IP camera.
- **Microphone Capture**: activate the computer's microphone and listen to it remotely.
- **Password Recovery:** recovers stored passwords.

REMOTE PROXY

Remcos can let you tunnel your connection through a remote host using the SOCKS protocol.
SOCKS proxy allows you to route your internet traffic via your remote machine, and also bypass internet censorships, blocks and restrictions.

Remcos supports SOCKS5 in both Direct and Reverse modes.

Direct SOCKS:

A SOCKS5 proxy server will be opened on the remote machine.
The remote proxy server will open a port and wait for connections, listening for them on specified port.
In Direct SOCKS mode, client applications (such as your browser) will connect directly to the remote proxy server.
In Direct mode, it is necessary to configure firewall and router on the remote machine, in order to allow incoming connections on proxy port.
If Remcos disconnects, the remote proxy server will keep running and listening, until our stop command.

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

Reverse SOCKS:

This function will launch a reverse SOCKS5 proxy tunnel.
Unlike Direct mode, no ports are opened on the remote machine.
In Reverse mode instead, the remote proxy will connect via reverse connection to the local endpoint, and proxy server and ports will be opened locally.
In Reverse SOCKS mode, client applications (such as your browser) will connect to the local proxy endpoint, and the traffic will be tunneled to the remote endpoint.
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, in order to tunnel data.
Port is opened on local machine.