Atelier Web Remote Commander Professional

USER MANUAL

Updated for AWRC Pro release 13.1

1   Program

1.1   Overview

Atelier Web Remote Commander Professional (AWRCP) lets you manage and audit servers and workstations from your local computer and provide remote helpdesk support.

At first sight, this does not seem to bring anything new to the arena, since there are tools in the market that provide remote connection capabilities with good performance.

However, the very moment you install and try AWRCP you will immediately notice that you are dealing with a completely different sort of tool.

- AWRCP does not require that you install any software on the remote machine, simply point and shoot. This turns the software particularly useful for accessing remote machines where no previous preparation has been made. There is no need to install any sort of drivers, no need to restart the computer after installation and no need to send any software by email or other means in order to access a remote machine.
- AWRCP is the only software able to remotely access Remote Desktop/Terminal Service sessions and Citrix XenApp applications launched from a Citrix XenApp server.
- AWRCP has the most powerful audio engine, It is totally controlled from the local computer.
- Unlike other remote control software, mostly concerned with viewing the remote screen, AWRCP provides lots of powerful tools for remote management and audit. With such tools you will be able to perform operations on the remote system that the remote interactive user himself could only dream about. With AWRCP you can know and do virtually anything on the remote computer!
- AWRCP is safe. A remote user, without Administrator privileges, can not gain higher privileges by controlling AWRCP operation on the remote system.
- It is inexpensive but not *cheap*. Don't assume paying more will bring you more, AWRCP is by far the most powerful tool you can find. With other remote software, you need one license for each machine you want to remotely access, with AWRCP you only need licenses for the machines where you install the software, not for the machines that are remotely accessed.

1.2   Features

These are the main features and capabilities of Atelier Web Remote Commander Professional:

- Access to the remote computer desktop enabling the launch of software with the mouse or keyboard.
- Supports IPv6 connections.
- Access to the remote computer logon screen, enabling connections before any user has logged on to the remote machine.
- Can remotely access, control and switch between RDP/TS sessions.
- Can remotely access, control and switch between Citrix XenApp applications launched from a Citrix XenApp server.
- Supports multiple (any number) of monitors on the remote computer, you can view and work on any one of them.
- Allows viewing and edition of the Registry (may be restricted for safety reasons) in

the same way as Regedit.
- Complete Audio engine for voice and other audio contents. Allows selection of devices and recording.
- When the remote computer has multiple monitors, you can have a simultaneous view of all of them.
- Features a powerful audio engine, fully controlled from the local computer.
- Supports User Switching sessions on Windows XP Pro and later (Vista, Windows 7, Windows 8, Windows 10, etc)
- Simulates all keystrokes on the remote keyboard computer.
- Wakes-up from screen-savers with a mouse-click or keystroke. Deals with password protected screen-savers.
- Simulates the security attention sequence (Ctrl+Alt+Del) on the remote to enable logon and on the default desktop.
- Provides access to disks, partitions, folders and files. The partitions or folders are not required to be open shares.
- Remote files or directories trees can be downloaded from the remote system.
- Local files or directory trees can be uploaded to the remote system.
- Programs can be launched on the remote with alternative credentials.
- Files can be remotely zipped or unzipped. Zip64 is fully supported. Fully compatible with all mainstream Zip software.
- New directories can be made and files and directories can be renamed.
- Remote files and directories can be deleted, copied or moved.
- Allows sending or receiving the Clipboard contents: text, pictures and other standard Windows Clipboard formats.
- Provides partition information, namely File System, Type, Number, Volume Label, Capacity and Free space.
- Allows visualization of shares.
- Allows visualization of users list and account details as well as Local and Global groups.
- Allows instant retrieval of password hashes, for audit of strong password policy enforcement across the organization.
- Allows visualization and management of services. Services can be started, stopped, paused, resumed and even unloaded.
- Allows visualization of processes, including session ID, User and Domain . Processes can be killed.
- Allows remote Shutdown, Power-Off, Reboot, Suspend and Hibernate.
- System Information (Operating System, Processor, BIOS, Memory,.Display Adapter and Logical printers).
- Lists installed programs, updates and hotfixes.
- Complete and detailed Hardware Devices list.
- Physical memory viewer.
- Wake-On-Lan facility, allows you to remotely wake up (boot) switched-off, sleeping or hibernated computers in your LAN or even across the internet.
- Ports Finder, which maps applications to open ports.
- Provides a vast number of network related information on the remote computer, namely Connections and Listening Ports, TCP statistics, UDP statistics, ICMP statistics, Routing Table, DNS Servers, Persistent Routes, IP Statistics/Settings, Installed Protocols/Protocol Details, Addressing Information Table, Net to Media Table, Interface Statistics/Settings and RDS/TS sessions.
- Chat facility for conversation with a remote interactive user.
- Provides anti-aliased scaling of remote desktop for comfortable viewing on the local computer.
- Uses Microsoft Windows authentication, which guarantees that only individuals with Administrator privileges on the remote system are able to connect (strong passwords are obviously recommended).
- Can use strong encryption to keep the information out of reach from prying eyes.
- Request authorization feature for obtaining approval from remote user before

initiating operations.
- The program can be prevented from launching until the correct password is entered.
- The remote keyboard and mouse can be disabled during a connection, for the remote interactive user not interfere with the work in progress.
- Allows View-Only mode for monitoring without interfering with the remote operations.
- Can Hide Wallpaper and Aero Composition on the remote computer.
- Transparent to Firewalls.
- Works within the company's Microsoft Networks LANs and across the Internet.
- Does not open any ports - it is absolutely transparent to any firewall, providing the Microsoft Networks operation is not blocked by the firewall.
- You can launch multiple instances of AWRCP and remotely access different computers at the same time. The maximum number of simultaneous connections is limited by available memory and CPU speed. Due to its low footprint, AWRCP will handle 5 to 10 (or more) simultaneous connections without problems on most PCs. No configuration is necessary.
- A remote computer can be simultaneously connected by multiple AWRCP clients.
- Full Unicode supported in most features.
- Can record movies of connection with optional audio comments. Movies can be recorded on motion detection.
- Remote Console feature.
- Runs on the remote as either 32-bit or 64-bit (Runs native, no .Net Framework) according to the installed operating system.
- High-end Ping tool.
- LAN Computers Enumerator.
- Microsoft Networks Sweeper.
- Unlocks without password all operating systems from Windows XP onwards.
- Unlocks without passwords, the logon screen on resume from screen saver.
- Forensics - Retrieves information from Credential Store vaults, unless those vaults are password protected.
- Forensics - Retrieves passwords from all popular browsers, when they are using the default settings.
- Forensics - Queries windows login hashes from Online Database of more than 5 GB password/hash duets.
- Forensics - Calculates NTLM and LM hashes from passwords. Adds to Online database. Calculates LM hashes with non US code page (ex: 850).

1.3   AWRCP versus AWRC

AWRCP (Atelier Web Remote Commander Professional) builds on the mature AWRC and introduces a number of new capabilities and features.

In summary, these are AWRCP specific capabilities:

- Can record a .WMV movie of the connection. It is possible to pause and resume the recording as many times as needed. The frame rate and quality can be adjusted. You can set the maximum recording file size and maximum recording time. You can insert audio comments if desired, and you can take fast snapshots in either JPEG or BMP format.
- Movies can be recorded on motion detection, i.e, recording is performed when screen changes over a threshold. This is ideal for surveillance.
- Remote Console. You can launch an application from the remote machine command line as if you were there. Runs command line utilities, cmd.exe commands, batch

files, windowed applications and documents through file association.
- Remotely access, control and switch between RDP/TS sessions (AWRCP 10 or above).
- Allows viewing and edition of the Registry (may be restricted for safety reasons) in the same way as Regedit.
- Complete Audio engine for voice and other audio contents. Allows selection of devices and recording.
- Remotely access, control and switch between Citrix XenApp applications launched from a Citrix XenApp server (AWRCP 10 or above)
- Lists all installed programs, updates and hotfixes on the remote computer. Does it both for programs installed for "Everyone" and installed just for a specific user (even if not logged in). Does better than Microsoft here, is much faster and provides more information than the Control Panel's "Add and Remove Programs".
- Connects and runs natively on the remote computer, i.e launches either a 32-bit or a 64-bit remote agent depending on the remote operating system. Running native on a 64-bit OS allows collecting the Password Hashes (not possible with AWRC, which always runs as 32-bit). Overall performance is improved by running natively.
- Comprehensive Unicode support, namely in file system manipulation, system information and almost every other feature. Zipping/Unzipping support Unicode as well in file and folder names and is fully compatible with recent Winzip and Winrar.
- High-end Ping tool. Pinging is the fastest way to assert if a remote machine is online (but that does not mean it is connectable).
- Tool that detects all reachable LAN Computers.
- Ports 445 and 139 Sweeper over any LAN or Internet.
- Unlike AWRC, AWRCP does not have 3 different releases (i.e, Classic, Standard and PB). Instead, a helper program configures AWRCP to the appropriate degree to comply with the organization policy. The Administrator of the software in the organization will have the password for that.
- Can view multiple monitor from the remote computer at the same time.
- Advanced Forensics tools (AWRCP 12 or above).
- Unlocks remote computers without passwords (AWRCP 12 or above).
- Unlocks without passwords, the logon screen on resume from screen saver (AWRCP 12 or above).

1.4   Requirements

You must have the following to use this product:

- PC compatible on local and remote systems with Pentium IV or higher.
- Works in systems with the minimum RAM recommended for the Operating System.
- **On the Local System:**
     Windows 10, 8.x, Server 2016, Server 2012/2012R2, 7, Server 2008/2008R2, Vista, XP, Server 2003/2003R2, Server/Workstation 2000. Works both in 32-bit and 64-bit operating system versions.
 On the Remote System:
     Windows 10, 8.x, Server 2016, Server 2012/2012R2, 7, Server 2008/2008R2, Vista, XP (only Professional, Home edition not supported), Server 2003/2003R2 and Server/Workstation 2000. Works both in 32-bit and 64-bit operating system versions. Runs native (no .Net Framework is required) as 64-bit on a 64-bit Operating System.
- If the remote computer platform is Windows XP Professional, the access is only possible within the classical sharing and security model for local accounts. This is enabled from Control Panel / Administrative Tools / Local Security Policy / Network access: Classic - local users authenticate as themselves. You can

obtain the same result from Windows Explorer / Tools / Folder Options / View and uncheck *Use Simple File Sharing*. In Windows Vista and later uncheck *Use Sharing Wizard (Recommended)*. This will revert you to the classical model as well

- Your log-in credentials must have Administrator's privileges on the remote machine or, alternatively, you must be able to supply a User Name/Password of an account in the Administrator's group of the remote machine. In Windows Vista and later, you need to set a Registry value to allow Filtered Administrators to connect across the network (see the FAQ).
- Microsoft Networks, i.e, Client for Microsoft Networks installed on both local and remote machines and File and Printer sharing enabled at least on the remote machine. Note: You don't need to share any folders.

1.5   Getting started

It is amazingly simple to get started with AWRCP.

Enter the name or IP address of the remote machine inside the box labeled Remote Host.
If necessary, enter the user name and password in the boxes User Name/Password.

If you want to use the keyboard on the remote computer, press down the Remote Keyboard button, if it is up.

Press the Connect button.

If you want to request authorization from the remote before starting operations on it, check the box *Request Authorization* before pressing the Connect button. If you want to keep the remote computer aware of the connection while it lasts, check the box *Connection Notification Frame*.

If you feel problems in connecting or believe that the software falls short of what is expected, proceed as follows:

1. Read *carefully* the Requirements and make sure your system and the remote system comply with them.
2. Read the FAQ.
3. If still unsuccessful, contact us through a form at http://www.atelierweb.com/index.php/contact-support/. Do not contact us before performing steps 1 and 2, while it is a pleasure to receive your contact, odds are that the answer is already provided either in the Requirements or in the FAQ.

1.6   Saving, Copying to Clipboard and Printing

Right clicking on grids then selecting Save or Save As... (Save Grid or Save Grid As... in the File System page) saves the respective contents to a file.
Note: The information is saved in unformatted ASCII, all columns perfectly aligned with the required number of spaces (no tabs).

Right clicking on grids and selecting Copy to Clipboard copies the respective contents in text format to the clipboard.

You can also print any grid by right clicking on it and selecting Print This.
Note: Fixed Pitch fonts like Courier New (usually) keep the existing alignment, so only these are presented in the Font Settings of the preview.

1.7 Adjusting the Viewing Area

You can increase or decrease the viewing area by pulling up or down a light green splitter placed between the upper bevelled panel and the lower control panel.

When you are connected, you can press the button to enter into Full-Screen mode. In Full-Screen mode, the image of the remote desktop completely covers the screen area of the local computer. To leave Full-Screen press Ctrl+Alt+Z (or the hotkey you have defined under Preferences).

In Full-Screen mode, when the remote screen resolution aspect ratio differs from the local screen resolution aspect ratio, the local image of the remote screen may become distorted. While in general this is not an issue, you can obviate it by selecting 'Maintain Full-Screen aspect ratio' under Preferences. In this case, the remote width and height receive the same amount of stretch and when the aspect ratio of the local screen differs from the remote screen an area to the bottom or to the right of the screen is left black to compensate for the different ratios.

1.8 Adjusting Fonts

The fonts of every grid can be resized by clicking the right mouse button over it and selecting Increase Font or Decrease Font.
The font sizes are maintained across sessions.

1.9 Image Scaling

The remote desktop screen can be scaled from 25% to 200% of the original size. There is also a "Fit" option where the remote screen is completely inserted, keeping the aspect ratio, inside the image display area.
Scaling is passed through a high quality anti-aliasing filter, so that most of the original details are kept.
The user can select a default scaling under Preferences.
In Full-Screen mode the scaling is done automatically but using the same anti-aliasing filter for maximum visual comfort.

1.10 Clipboard Transfers

The local Clipboard contents can be sent to the remote computer and the remote Clipboard contents can be retrieved.

This is accomplished by using the and buttons on the Desktop tab.
AWRCP can send and retrieve most standard clipboards formats including pictures and sounds.
Of course, private clipboard formats and OLE-aware formats are not directly transferable from system to system.

1.11   Encryption

AWRCP may connect either with encryption disabled or encryption enabled. Connections without encryption are good enough for many LAN environment where maintaining data confidentiality is not critical.

However, for connections across potential hostile networks, such as the Internet, AWRCP provides very strong encryption, unbreakable either by current cryptography science or by brute force attacks with current hardware.

Encryption preparation is done in only 1 communication cycle as follows:

AWRCP produces a pair of keys, Public and Private, using the Diffie-Hellman algorithm (with a 300 digits prime and a cyclic group generator previously agreed) and random data produced by Microsoft Crypto-Api. The Public key is sent to the remote computer. The remote produces as well a pair of keys, Public and Private, then computes a Shared Secret using its Private key and the Public key received from the client. The remote sends its Public key to the client which computes the same shared secret using its Private key and the Public key received from the remote. Due to the nature of this algorithm, previous knowledge by any attackers of either the prime number or the cyclic group generator can be freely assumed, only the generated Private Keys are critical but these are not disclosed. Man-in-the-middle attacks are not possible here because the connection was already authenticated by Microsoft Networks.

After that, all data exchange is Blowfish CBC encrypted with the 352-bit key length Session Key (obtained from the Shared Secret), no way to decrypt it.
Since AWRCP encryption and decryption are very fast, you may keep Strong Encryption always on without significant performance penalty.

AWRCP encryption does not cover the Microsoft Networks negotiation and protocol itself. Shares and Services information are not encrypted as well, since they are retrieved locally using the Microsoft Networks mechanism. Other than these, everything else, from the remote screen to chat conversations are strongly encrypted and kept away from anyone watching the network traffic.

1.12   Logging Connections

You can keep a complete record of all your remote access activity, which includes:

- Date and time started and ended in the format yyyy-nn-dd hh:mm:ss, where yyyy stand for year, nn for month, etc.
- Remote Host. The format is xxxx (nnnn/ip). *xxxx* is what you type in the Remote Host box, *nnnnn* is the machine name provided by the remote machine and *ip* is the IP address (IPv4 or IPv6) used for the connection.
- Local User/Connected As. Local User is the account under which you are logged in locally, Connected As is the Account under which you connected to the remote machine.
- Remote Interactive User. If available, provides the account under which the console of the remote machine is attached,and should correspond to the user that is physically logged at the machine unless AWRCP logged in first.

1.13 Multiple Monitors

Multiple monitors is one of the best ways to increase personal productivity and more and more people is using such setups. All recent versions of Windows support multiple monitors and AWRCP allows you to access any number of active monitors attached to the remote machine in a very straightforward way.
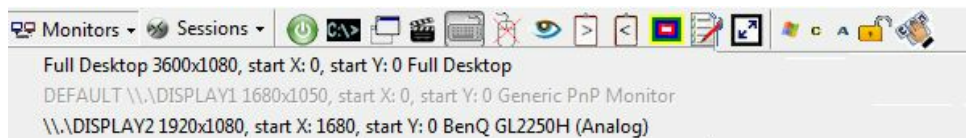
Once a connection is established you have access to the list of active monitors on the remote machine. The monitor you are currently viewing is grayed out, you can select another one clicking on its reference in the drop down list.

1.14 Sessions

Starting with its release 10, AWRCP can remotely access RDS/TS (Remote Desktop Services/Terminal Services) and Citrix sessions and interact with them the same way it interacts with a console session (i.e, the session the interactive user works with when seated in front of its computer).
No other software can do this, at most they can take snapshots of a RDS/TS and that's all.

What you need to do to access a RDS/TS session?

You don't need to do anything, when AWRCP accesses a remote computer it enumerates the RDS/TS sessions on the computer and lists the ones that can be remotely accessed. The list is similar to the following image:
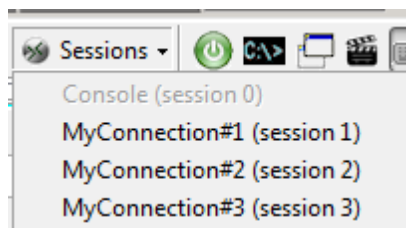
Which RDS/TS sessions can be remotely accessed?

Active sessions (and sometimes Connected sessions) are the ones that can be accessed.
If you want to know more details about a given session before connecting to it, look into the RDS/TS tab of the NetworkInfo Section.

Minimized RDS/Clients

To save resources and bandwidth, when the Microsoft RDS/TS client is minimized to the taskbar it signals the condition to the remote RDS/TS server which reduces

the GUI on the respective session to a dormant state. For such reasons, if AWRCP is remotely accessing that session it finds all graphics freeze when the GUI becomes dormant, so it drops a curtain and alerts the user. When the GUI is back to live, AWRCP detects the change, alerts the users and restarts updating the screen.

There is a setting under Preferences/Advanced that prevents the dormant state for any RDS/TS session launched from the computer where AWRCP is running.

2 Function Tabs

2.1 Desktop

Here you will see screen updates from the remote computer and will be able to interact with the remote desktop.

Mouse clicks and double clicks are replicated on the remote computer on the same screen point you press the mouse buttons on the AWRCP captured image. Mouse moves are replicated as well.

When you press down the *Remote Keyboard* button, all keys you press on the local system will be simulated on the remote system. This includes key combinations of International keyboards, though both sides must have compatible keyboard layouts for every key combination to replicate correctly. The *Remote Keyboard* button is down by default, but you can change this setting from the *Preferences* menu.

In case you just want to watch what is happening on the remote computer without passing neither key presses nor mouse activity, press down the *View-Only Mode* button. *View-Only Mode* can be set to default from the *Preferences* menu.

Screen updating can range from Fastest (almost in real time) to Paused (no screen updating).

From the Preferences/Desktop tab you can select the color model that best fits your requirements:

- **256 Colors (8 bit)**
- **65536 Color (16 bit)**
- **True Color (24 bit)**
- **True Color (32 bit)**

The first (256 Colors) is suited for problematic traffic conditions, the second (65536 Colors) is the default.. AWRCP supports palette-based screen desktops as well as 16-bit, 24-bit and 32-bit true-color either on remote or on local computer.

2.2 File System

From here you can perform most maintenance tasks you got used to do with Windows Explorer and a few others tasks Windows Explorer does not allow you (and when the remote system does not open shares to visitors you simply can not use Windows Explorer across the network, though you can still use AWRCP!).

- **Download Files**: First you select the files and folders trees with the left mouse button (press Shift or Ctrl keys, if more than one file). Then press the right mouse button to recall the popup menu and select Download Files/Compressed or Download Files/Uncompressed. When Compressed is selected, the amount of

network traffic and download time can be drastically reduced when the files to download were not already compressed. Since the compression itself takes a long time on large files, on a fast LAN it may be preferable to use the Uncompressed option. Then you are requested to select where the file or files to be downloaded are going to. After that the download will start. The operation is done asynchronously and parallelized (when the number of CPU cores allow), so you can do other tasks with AWRCP while it proceeds (you will be informed of its progress in the Progress Report box).

- **Upload Files**: First, you press the right mouse button to recall the popup menu and select Upload Files/Compressed or Upload Files/Uncompressed. Then you choose which files and folder trees you want to upload to the remote system and press OK. The uploading will start and the files and folder trees will be transferred to the directory that was selected on the remote system when you started the operation. When Compressed is selected, the amount of network traffic and upload time can be drastically reduced when the files to upload were not already compressed. Since the compression itself takes a long time on large files, on a fast LAN it may be preferable to use the Uncompressed option. The operation is done asynchronously and parallelized (when the number of CPU cores allow), so you can do other tasks with AWRCP while it proceeds (you will be informed of its progress in the Progress Report box).

- **Launch File**: Remote files can be launched (taking into account the File Association on the remote system) by right-clicking on the File System grid and selecting Launch File.
  You can launch files as:

Remote Interactive User:	Uses the credentials of the user that is logged on the remote computer.
You:	Uses the credentials you have used to log on the remote computer
System Account:	Files are launched as if you were the operating system.
Other (UserName/ Password):	This works much like the RunAs command

  Launching files from a user account provides access to the HKEY_CURRENT_USER hive of the Registry for that account.

- **Zip selected Files**: Zip64 (files and archives larger than 4 GB) is fully supported. You can zip files on the remote system as easily as on the local system. You can even use a password to restrict access to the contents of the newly created zip file. The password string should be large (8 or more characters. The more the better.) and with a mixture of alpha characters (lower and upper case) and numbers to provide a comfortable degree of protection. Small passwords are easily recovered by some specialized software. The password is compatible with other Zip utilities. Note that, if the given Zip file name already exists the files will be added to it - the Zip file will not be recreated. You must enter a valid path for the Zip file, directories will not be created, if they don't already exist. Zip supports Unicode file and folder names, and is fully compatible with major titles, like Winzip and Winrar. The operation is done asynchronously and parallelized (when the number of CPU cores allow), so you can do other tasks with AWRCP while it proceeds (you will be informed of its progress in the Progress Report box).

- **Unzip selected Files**: Zip64 (files and archives larger than 4 GB) is fully supported. To unzip a file on the remote system, first you select it with the left mouse button then right-click and select Unzip selected File. The file does not need to have a ZIP extension, but has to be a real and uncorrupted zip file. AWRCP only can confirm it on the remote system. If the unzip fails this is a possible cause. Following options are available for unzipping:

* Directory where the files will be extracted: You may enter a non-existing directory, which will be created, if possible.
* Overwrite mode: Always - Files with same name are always overwritten; Never - The file will not be extracted if it would overwrite another file; If is newer in ZIP - The file will only overwrite the existing one if the archived file is newer than the existing one; If is older in ZIP - The file will only overwrite the existing one if the archived file is older than the existing one.
* Replace Read-Only: Allows files with the read-only attribute to be replaced during the unzip operation.
* Recreate Directories: Check, if you want to use directory information in the zipfile when extracting files. The directories will be created relative to the destination directory. If unchecked, all files will be extracted to the destination directory, which could possibly result in files of the same name overwriting each other if the Overwrite mode property is set to Always.
* Password: Enter here the password to extract the file. The password is compatible with Zip archives created by other utilities.
The operation is done asynchronously and parallelized (when the number of CPU cores allow), so you can do other tasks with AWRCP while it proceeds (you will be informed of its progress in the Progress Report box).

- **Make Directory**: It will create a directory, unless it already existed.

- **Rename File or Directory**: The rename will be effected unless the new name already existed. Sometimes, it is not possible to rename when the File or Directory is in use by some process.

- **Delete selected Files and Directories**: Take care, if you uncheck the Recycle Bin box, the selection will be zapped. Chances are that nobody will be able to help you recover what you have just deleted. Even when checked, the Recycle Bin may not always be available to receive what you delete. Conclusion: Think twice before deleting anything.

- **Copy selected Files or Directories**: Copying is made in 2 stages. First, you select with the mouse what you want to copy, press the right-mouse button and select Copy selected Files or Directories. AWRCP will silently store what files you want to copy. The copy proper only happens when you right-click and select Paste Files and Directories. Make sure, you are positioned in the folder you want to copy the files to before selecting Paste Files and Directories.

- **Move selected Files or Directories**: Moving is made in 2 stages. First, you select with the mouse what you want to move, press the right-mouse button and select Move selected Files or Directories. AWRCP will silently store what files you want to move. The move proper only happens when you right-click and select Paste Files and Directories. Make sure, you are positioned in the folder you want to move the files to before selecting Paste Files and Directories.

Note 1: These options are only visible on the popup menu when a connection is established.
Note 2: All file operations support Unicode.

The File System Tab provides also some useful details about the current Logical Drive, namely: File System, Type, Capacity, Serial Number, Label and Free space.

2.3   SysInfo

2.3.1   General

A comprehensive set of useful information whose purpose is providing a general picture of the remote system characteristics.

- **Operating System**: Full description, including service packs installed, Registered User and Organization, Product ID, Partial Product Key, Local Time, Last Boot Time, Uptime, Antivirus/AntiSpyware/Firewall, Last Installed Date for Automatic Updates . The Product Key is limited to the last 5 characters, complying with Microsoft policy.
- **Processor Information**: Manufacturer, Vendor ID, CPU name, Family, Model, Stepping, Raw frequency, Norm frequency and various other intrinsic characteristics.
- **BIOS**: Comprehensive SMBIOS ROM information, if available (most recent BIOS do have it available). SMBIOS ROM is instantly read from ROM - because the software does no use the slow (and deprecated) APIs we were accustomed. In the rare occasions that SMBIOS ROM information is not available, AWRCP will dig to get some BIOS details from other sources.
- **Memory details**: This includes Total Physical Memory, Free Physical Memory, Total Page File, Page File Free and other.
- **Display Adapter**: Model, Chipset, DAC, Memory, BIOS, Screen Metrics, Font Resolution and Available Video Modes.
- **Monitors:** Follow this link for details.
- **Logical Local Printers**.

2.3.1.1   Monitor(s) Info

1- Monitor ID:

Represents the identifying information about a video monitor. The data in this class correspond to data in the Vendor/Product Identification block of Video Input Definition of the Video Electronics Standard Association (VESA) Enhanced Extended Display Identification Data (E-EDID) standard

Commercial Name: The friendly name of the monitor.
Manufacturer Name Code: These IDs are assigned by Microsoft.
Product Code ID: Code assigned by manufacturer.
Serial Number ID: 32-bit Serial Number.
Week of Manufacture: Week of manufacture by week number. The range is from 1 through 53. Zero (0) is undefined.
Year of Manufacture: ditto.

2. Basic Display Parameters:

Represents the basic display features of a computer monitor. Data in this class corresponds to data in the Basic Display Parameters/Features block of Video Electronics Standard Association (VESA) Enhanced Extended Display Identification Data (E-EDID) standard.

Display Transfer Characteristic: Display transfer characteristic (100*Gamma-100).
Max Horizontal Image Size (cm): Maximum horizontal image size in centimeters. represent the maximum image dimensions that the monitor can correctly display for the entire set of supported timing and format combinations.

The maximum image dimension is defined by VESA Video Image Area Definition (VIAD) Standard and is rounded to the nearest centimeter. The host computer system can use this data to select the image size and aspect ratio that will allow properly scaled text. Be aware that, if either or both of these fields are zero, then the system makes no assumptions about the display size. For example, the size of a projection display may be undetermined.

Max Vertical Image Size (cm): Maximum vertical image size in centimeters. represent the maximum image dimensions that the monitor can correctly display for the entire set of supported timing and format combinations. The maximum image dimension is defined by VESA Video Image Area Definition (VIAD) Standard and is rounded to the nearest centimeter. The host computer system can use this data to select the image size and aspect ratio that will allow properly scaled text. Be aware that, if either or both of these fields are zero, then the system makes no assumptions about the display size. For example, the size of a projection display may be undetermined.

Video Input Type: Can be Analog or Digital.

Supported Display Features:

- **Active Off Supported:** Support for active off and very low power. The display consumes less power when it receives a timing signal that is outside the declared active operating range. The display will revert to normal operation if the timing signal returns to the normal operating range. Examples of timing signals outside the normal operating range are no sync signals or no DE signal.
- **Display Type:** Can be Monochrome/grayscale display, RGB color display, Non-RGB multicolor display.
- **GTF Support:** Indicates whether the display has GTF support. If True, the display supports timings based on the GTF standard using default GTF parameter values.
- **Has Preferred Timing Mode:** Indicates whether the display has has a preferred timing mode. If True, the first detailed timing block contains the preferred timing mode of the monitor. Use of preferred timing mode is required by EDID v.1.3 and higher.
- **sRGB Supported:** If True, the display supports sRGB.
- **Standby Supported (VESA DPMS):** Indicates whether the display supports VESA Display Power Management Signaling (DPMS) standby. If True, DPMS standby is supported.
- **Suspend Supported (VESA DPMS):** Indicates whether the display supports VESA Display Power Management Signaling (DPMS) suspend. If True, DPMS suspend is supported.

3. Video Connector Type:

Contains the connection type of the monitor.

Technology: Video output technology connection type.

4. Analog Video Input Parameters:

Represents the analog video input parameters of a computer monitor. The data in this class corresponds to data in the Video Input Definition of Video Electronics Standard Association (VESA) Enhanced Extended Display Identification Data (E-EDID) standard.

Composite Sync Supported: Indicates whether composite sync is supported.
Separate Syncs Supported: Indicates whether separate syncs are supported,
Serration of Vsync Required: Indicates whether vertical sync pulse serration is required.
Setup Expected: Indicates whether setup is expected.
Signal Level Standard: Signal level standard for Enhanced video connector (EVC) connections.

Sync on Green Video Supported: Indicates whether sync on green is supported.

5. Digital Video Input Parameters:

Represents input parameters for digital video. The data in this class corresponds to data in the Video Input Definition of Video Electronics Standard Association (VESA) Enhanced Extended Display Identification Data (E-EDID) standard.

Is DFP 1.x Compatible: VESA DFP 1.x or compatible. If set, interface is signal compatible with VESA Digital Flat Panel (DFP) 1.x Transition Minimized Differential Signaling (TMDS) CRGB, 1 pixel/clock, up to 8 bits/color most significant bit (MSB) aligned, DE active high.

6. Color Characteristics:

Represents the International Commission on Illumination (CIE) color characteristics of a computer monitor. The data corresponds to data in the Color Characteristics block of the Video Electronics Standard Association (VESA) Enhanced Extended Display Identification Data (E-EDID) structure.

Blue: CIE coordinates for blue. To calculate the Z coordinate, based on the X and Y values, use the relation $\|(X,Y,Z)\| = 1$.
Default White: Default white CIE coordinates. To calculate the Z coordinate, based on the X and Y values, use the relation $\|(X,Y,Z)\| = 1$.
Green: CIE coordinates for green. To calculate the Z coordinate, based on the X and Y values, use the relation $\|(X,Y,Z)\| = 1$.
Red: CIE coordinates for red. To calculate the Z coordinate, based on the X and Y values, use the relation $\|(X,Y,Z)\| = 1$.

2.3.2   Registry

By default, you will be able to "view" the Registry on the remote machine in a very similar fashion you do using Regedit on the local computer.
"Viewing" the Registry of the Remote computer is a safe operation.

You can access the Registry of every Built-In account on the remote computer without need to enter credentials for that account. You can also access the Registry of the user on the physical console even if that account is not a Built-in account (i.e, it is a Domain account).
If no user is logged on at the physical console, AWRCP will default to show the Registry for the user that established the AWRCP connection.

Editing

Providing you are authorized by the Policy (accessible though File/Administration), you will be able to "edit" some parts of the Registry. By edition, we mean that you will be able to create new keys or values, change, rename or delete them.
Unless you are in GodMode, only subhives of HKEY_CURRENT_USER are editable. And while AWRCP is in trial mode, edition is not allowed.

IMPORTANT: *Editing the Registry is a dangerous operation as Microsoft adverts! Editing the Registry across a network is even more dangerous! We will never be able to guarantee that you will not be in trouble after editing the Registry, so you are aware of the risks and take the whole responsibility.*

Caution:

When editing the Registry of the remote computer, make sure no other software (such as Regedit) is doing edition at the same time. This is risky, namely when working with the same Registry keys or values.

2.3.3   Programs and Prerequisites

2.3.3.1   Programs and Updates

Retrieves the programs, updates and hotfixes installed on the remote machine, providing more details than the corresponding Control Panel applet. The process is blazingly fast, except when you tick the checkbox to retrieve the Component Based Servicing Updates (available with Windows Vista and above), where it can take up to one minute.

You can retrieve either programs installed for all users of the computer (<Everyone>) or just for a specific user (<Just me>). The information provided allows you to know which installations are based on Windows Installer, if they are 32-bit programs on a 64-bit system, the installation date (beware that may not be accurate or be just an estimate), if they are updates or hotfixes, and a few other details.

2.3.3.2   Frameworks and Redistributables

Information about installed .Net Frameworks and Visual Studio C++ Redistributables on the remote computer. Nowadays, many programs do not run without the proper . Net Framework and/or VS Redistributable already installed.

2.3.4   Hardware Devices

You know the sort of information you get from your local machine when you run the System applet from Control Panel. This is a similar list, but with a few extra details, taken directly from the remote machine.

2.3.5   Processes

A process is a container and comprises a private address space, an executable program which is mapped into a virtual address space and a list of open handles to various system resources, such as semaphores, pipes, communications ports, and files, that are accessible to all threads in the process. A process features a security context called an access token that identifies the user, security groups and privileges associated with the process, a unique identifier called a Process ID (PID) and at least one thread of execution.

The following information is provided for each running process:

Main *Tableau the Bord:*

- **PID**: This is the Process ID, i.e, the number that identifies the process throughout the system.
- **Image Name**: Normally, the same name as the executable that created the process.
- **Process Path**: Normally, the local drive or UNC path to the executable that created the process. (It is shown as a tooltip when the mouse is over).
- **CPU Usage**: The percentage of the overall CPU time taken by the process (when the last sample taken).
- **Session ID**: In Windows Vista and later (and XP with Fast User Switching), users

are allocated sessions to run their applications (starting at 1), session 0 is reserved for services. The idea was taken from Terminal Services and the mechanism is much the same.

- **User**: The user account under which the process is running
- **Domain**: The name of the domain in the security database where the account name was found. The meaning depends on whether the machine is a server or a workstation.

Other General details:

- **Command Line**: Shows the phe path and any arguments used to launch the process.
- **Inherited From Pid**: The process that directly or indirectly started this one.
- **Creation Time**: The date and time the process was created.
- **Kernel Time**: The sum of the time spent executing in kernel mode by the threads of the process.
- **User Time**: The sum of the time spent executing in user mode by the threads of the process.
- **Handle Count**: The number of handles opened by the process.
- **Thread Count**: The number of threads in the process.
- **Base Priority**: the default priority of the threads in the process.

Virtual Memory Counters (vmCounters) - Statistics of virtual memory usage for the process:

- **Virtual Size**: Current size of the virtual address space that a process is using, not the physical or virtual memory actually used by the process. Using virtual address space does not necessarily imply corresponding use of either disk or main memory pages.
- **Peak Virtual Size**: Maximum virtual address space a process uses at any one time.
- **Page Fault Count**: Number of times data has to be retrieved from disk for a process because it was not found in memory. The page fault value accumulates from the time the process started.
- **Private Page Count**: Number of memory pages allocated for the use of this process.
- **Working Set Size**: Amount of memory, private and shared with others, used by the process.
- **Peek Working Set Size**: Maximum amount of working set memory used by the process.
- **Quota Paged Pool Usage**: Means memory paged to disk.
- **Quota Peek Paged Pool Usage**: Maximum memory paged to disk.
- **Page File Usage**: Represents a commit total, not actual page file usage. It is how much page file space would be used if all private committed virtual memory had to be paged to disk.
- **Peak Page File Usage**: The maximum of Page File Usage (see above).
- **Quota Non Paged Pool Usage**: Memory that is never paged to disk.
- **Quota Peak Non Paged Pool Usage**: Maximum memory never paged to disk.

In/Out Counters (IOCounters) - Statistics of I/O operations for the process:

- **Read Operation (Count)**: The number of read input/output operations generated by the process, including file, network, and device I/Os. I/O Reads directed to CONSOLE (console input object) handles are not counted.
- **Write Operation (Count)**: The number of write input/output operations generated by the process, including file, network, and device I/Os. I/O Writes directed to CONSOLE (console input object) handles are not counted.

- **Other Operation (Count)**: The number of input/output operations generated by the process that are neither a read nor a write, including file, network, and device I/Os. An example of this type of operation is a control function. I/O Other operations directed to CONSOLE (console input object) handles are not counted.
- **Read Transfer (Bytes)**: The number of bytes read in input/output operations generated by the process, including file, network, and device I/Os. I/O Read Bytes directed to CONSOLE (console input object) handles are not counted.
- **Write Transfer (Bytes)**: The number of bytes written in input/output operations generated by the process, including file, network, and device I/Os. I/O Write Bytes directed to CONSOLE (console input object) handles are not counted.
- **Other Transfer (Bytes)**: The number of bytes transferred in input/output operations generated by the process that are neither a read nor a write, including file, network, and device I/Os. An example of this type of operation is a control function. I/O Other Bytes directed to CONSOLE (console input object) handles are not counted.

The following operations can be performed from the right-click popup menu of the Processes grid:

- **Kill process**: This is should kill even the more sticky process on the remote system. Be aware that killing some processes may cause serious instability on the remote machine. Use with caution. Both 64-bit and 32-bit processes can be killed by selecting this option, unless you selected *Runs as 32-bit on a 64-bit Remote Operating System* in Preferences/Advanced (in this case only 32-bit processes can be killed).
- **Remote shutdown**: Shuts down the computer to a point where it is safe to turn off the power. It will attempt to flush all file buffers to disk and wait a while for running processes to stop. Forcibly terminates processes that do not respond to the shut down request.
- **Remote Power-Off**: Shuts down the computer as per the previous option, then turns off the power in systems with a power-off feature.
- **Remote Reboot**: Shuts down, then restarts the remote computer.
- **Remote Standby:** The remote machine is forced into standby or sleep mode.
- **Remote Hibernate:** The remote machine is forced into hibernation.

The above operations can also be performed from the Tools/Shutdown menu.

Note:
These options are only visible on the popup menu when a connection is established.

2.3.6   Services

Enumerates and manages services in the remote Control Manager Database.

The following types of services are enumerated:
- Kernel Device Drivers.
- File System Drivers.
- Services that run in their own process.
- Services that share a process with other processes.

The following operations can be performed on remote services, by right clicking on the Services grid and selecting from the Popup menu:
Stop Service, Start Service, Pause Service, Resume Service or Unload Service.
These facilities are very powerful, the software will comply with your request, so

make sure you know what you are doing. Particularly, take special care with UNLOADING services - Some services are deeply needed for the correct operation of the remote system.

Note: These options are only visible when a connection is established.

2.3.7 Physical Memory Viewer

Typically, the operating system maps linear addresses to physical addresses in order to execute code. This mapping is made by setting up page-tables. Whenever a task switch occurs, a process receives a new set of pages which map to areas in the physical address space (when such pages are in disk they are loaded from there into the physical space). Although a process is never concerned or aware of physical addresses it is possible and interesting to have a look at them.

While some physical memory areas are fairly stable over time, most areas keep changing all the time. Either way, searching through the physical memory is a good exercise and provides useful insight.

Note: On Windows® Server 2003 SP1, Windows® Server 2003 x64 64-Bit, Windows® XP Pro x64 64-Bit SP1 and Windows® Vista and later you can only retrieve physical memory within the range 0x000C0000 - 0x000FFFFF.

2.3.8 Users and Groups

2.3.8.1 Users

Most User account details are provided:

- **User Account**: The name of the User Account.

- **Password Age**: Indicates the elapsed time since the password was last changed.

- **Privilege Level**: The level of privilege assigned to the User Account. This can be Administrator, User or Guest.

- **Comment**: Comment associated with the user account.

- **Flags**: Determine several features.

- **Full Name**: Contains the full name of the user.

- **Workstations can log from**: Contains the names of workstations from which the user can log on. As many as eight workstations can be specified; the names must be separated by commas. If no workstation is specified there are no restrictions.

- **Last Logon**: This value may not be the same when taken from different backup domain controllers (BDC) in the domain. To obtain an accurate value, you must query each BDC in the domain. The last logon occurred at the time indicated by the largest retrieved value.

- **Last Logoff**: This value may not be the same when taken from different backup domain controllers (BDC) in the domain. To obtain an accurate value, you must query each BDC in the domain. The last logon occurred at the time indicated by the largest retrieved value.

- **Account expires**: May contain either a date/time or "Never expires".

- **User ID (RID)**: Contains the relative ID (RID) of the user. The RID is determined by the Security Account Manager (SAM) when the user is created. It uniquely defines the user account to SAM within the domain.

- **Primary Global Group (RID)**: Contains the relative ID (RID) of the Primary Global Group for the user.

- **SID**: Each user and group is associated with it a security identifier (SID). The individual parts of a SID are as follows:
  - **Revision**: This value indicates the version of the SID structure used in a particular SID. The structure used in all SIDs created by Windows NT, Windows 2000 and Windows XP is revision level 1.
  - **Identifier authority**: This value identifies the highest level of authority that can issue SIDs for this particular type of security principal. For example, the identifier authority value in the SID for the group Everyone is 1 (World Authority). The identifier authority value in the SID for a specific Windows NT, Windows 2000 and XP account or group is 5 (NT Authority).
  - **Subauthorities**: The most important information in a SID is contained in a series of one or more subauthority values. All values up to but not including the last value in the series collectively identify a domain in an enterprise. This part of the series is the domain identifier. The last value in the series identifies a particular account or group relative to a domain. This value is the relative identifier (RID).

- **Domain**: Name of the domain where the account name is found or local machine if there is no domain.

- **No. SubAuthorities**: The count of subauthorities contained in the SID.

- **Length of SID**: The length in bytes of the SID.

- **Type of SID**: SIDs can be of type 'User', 'Group', 'Domain', 'Alias', 'Well Known Group', 'Deleted Account', 'Invalid' and 'Unknown'.

2.3.8.2   Groups

Provides information about each local and global group account on the remote server.

- **Names**: Local or Global group names.

- **SID**: Each group is associated with it a security identifier (SID). For more details on SID see Users.

- **Comment**: A remark associated with the Local or Global Group.

- **Attribute**: The following attributes of global groups are hardcoded by default:
  - **Group Mandatory**: The SID cannot have the Group Enabled attribute cleared by a call to the AdjustTokenGroups function. However, using the CreateRestrictToken function is possible to convert a mandatory SID to a deny-only SID.
  - **Group Enabled by Default**: The SID is enabled by default.
  - **Group Enabled**: The SID is enabled for access checks. When the system

performs an access check, it checks for access-allowed and access-denied ACEs that apply to the SID.

2.4 NetworkInfo

2.4.1 Shares

Shares are resources the remote computer makes available to other computers. Resources can be Drives, Print Queues, Communication devices or Interprocess Communication devices.
Shares are visible whenever the remote computer is using Client for Microsoft Networks, has File and Printer Sharing enabled and no firewall is blocking this setup.
When a resource receives a $ sign before its name, it is not visible to the outside World (by normal means).

2.4.2 RDS/TS

From here you can get information about Users and Sessions connected to the remote computer through Remote Desktop Services or Terminal Services (RDS/TS).

- **Information retrieved about Users:**

  - **User Name:** The client User Name.
  - **Client Name:** NetBIOS name of the client computer.
  - **Client Domain**: Domain of the client.
  - **Client IP Address:** The client network address.
  - **Display:** Horizontal x Vertical dimensions and color depth in bits per pixel.

- **Information retrieved about Sessions**:

  - **Session Name:** RDS/TS name.
  - **Is Console?:** Identifies if the displayed session is associated with the physical keyboard and monitor.
  - **Session ID:** The session identifier.
  - **Session Connection State:**
  This can be one of the following:
    - **Active:** A user is logged on to that session
    - **Connected:** The session is connected to the client.
    - **Connect Query:** The session is being connected to the client.
    - **Shadow:** One session is shadowing another session.
    - **Disconnected:** The session is active but the client disconnected.
    - **Idle:** The session is waiting for a client to connect.
    - **Listening:** The session is waiting for requests for new client connections.
    - **Reset:** The session is in the process of resetting.
    - **Down:** The session is down, due to an error or just because the system is shutting down.
    - **Initializing:** The session is starting up.
  - **Logon Time:** The date/time that the user logged on to the session.
  - **Connect Time:** The most recent client connection date/time.
  - **Last Input Time:** The date/time of the last user input in the session.
  - **Last Disconnect Time:** The last client disconnection time.

2.4.3   Ports Finder (IPv4 and IPv6)

Ever wonder which programs on the remote PC have ports opened to the outside world? The answer is probably yes.
This information is capital to complete your security assessment of the remote PC.

We were the first to find a way to obtain this information from the local machine in the 90s (with our award winning software AWSPS) and the first to obtain this information from a remote machine early this century.

From release 13.0 onwards, this feature supports IPv6 as well.

2.4.4   Ports Statistics (IPv4 and IPv6)

2.4.4.1   Connections and Listening Ports

This grid displays all connected or listening ports in the local system in a given moment.
The Proto column is for protocols, which can be either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). TCP connections are transient, they cease to exist when (or soon after) the connection makes the transition to the closed state.

The Local Address column shows the local IP address and local port for the TCP connection or UDP listener. For a TCP connection in the listen state or UDP listener that is willing to accept connections (datagrams for UDP listener) for any IP interface associated with the node, the value 0.0.0.0 is used for the local IP address.

The Remote Address column shows the remote IP address and remote port associated with the TCP connection or UDP listener.

The State column can take any of the following values:

synSent	Indicates active open.
synReceived	Server just received SYN from the client.
established	Client received server's SYN and session is established.
listening	Server is ready to accept connection.
finWait1	Indicates active close.
timeWait	Client enters this state after active close.
closeWait	Indicates passive close. Server just received first FIN from a client.
finWait2	Client received acknowledgment of its first FIN from the server.
lastAck	Server is in this state when it sends its own FIN.
closed	Server received ACK from client and connection is closed.

Notes:

- The client may have terminated the connection and the socket still being shown in closeWait state. This may indicate that the server still keeps the socket open.
- A connection can stay in timeWait for a maximum of four minutes.

2.4.4.2   TCP Statistics

Retransmission time-out algorithm
The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
This can be:
constant
rsre (MIL-STD 1778, appendix B)
vanj (Van Jacobson's algorithm)
other (none of the above)

Minimum retransmission time-out (msec)
The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

Maximum retransmission time-out (msec)
The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.

Maximum number of connections
If the maximum number of connections is not dynamic, this represents limit on the total number of TCP connections.

Active Opens
The number of times TCP connections have made a direct transition to the synSent state from the closed state.

Passive Opens
The number of times TCP connections have made a direct transition to the synReceived state from the listen state.

Failed connection attempts
The number of times TCP connections have made a direct transition to the closed state from either the synSent state or the synReceived state, plus the number of times TCP connections have made a direct transition to the listen state from the synReceived state.

Reset connections
The number of times TCP connections have made a direct transition to the closed state from either the established state or the closeWait state.

Current connections
The number of TCP connections for which the current state is either established or closeWait.

Segments received
The total number of segments received, including those received in error. This includes also segments received on currently established connections.

Segments sent
The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Segments retransmitted
The number of TCP segments transmitted containing one or more previously transmitted octets.

Segments received in error
The total number of segments received in error (such as, bad TCP checksums).

Segments sent with RST flag
The number of TCP segments sent containing the RST flag.

2.4.4.3 UDP Statistics

Datagrams received
The total number of UDP datagrams delivered to UDP clients.

No ports
The total number of received UDP datagrams for which there was no client application at the destination port.

Receive errors
The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Datagrams sent
The total number of UDP datagrams sent from this entity.

2.4.4.4 ICMP Statistics

Messages
Received - The total number of ICMP messages that the entity received, including those counted as ICMP Receive errors.
Sent - The total number of ICMP messages that this entity attempted to send, including those counted as ICMP Send errors.

Errors
Received - The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
Sent - The number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram.

Destination unreachable
Received - The number of ICMP Destination Unreachable messages received.
Sent - The number of ICMP Destination Unreachable messages sent.

Time exceeded
Received - The number of ICMP Time Exceeded messages received.
Sent - The number of ICMP Time Exceeded messages sent.

Parameter problems
Received - The number of ICMP Parameter Problem messages received.
Sent - The number of ICMP Parameter Problem messages sent.

Source quenches
Received - The number of ICMP Source Quench messages received.
Sent - The number of ICMP Source Quench messages sent.

Redirects

Received - The number of ICMP Redirect messages received.
Sent - The number of ICMP Redirect messages sent. For a host, this will always be zero, since hosts do not send redirects.

Echos
Received - The number of ICMP Echo Request messages received.
Sent - The number of ICMP Echo Request messages sent.

Echo replies
Received - The number of ICMP Echo Reply messages received.
Sent - The number of ICMP Echo Reply messages sent.

Timestamps
Received - The number of ICMP Timestamp Request messages received.
Sent - The number of ICMP Timestamp Request messages sent.

Timestamp replies
Received - The number of ICMP Timestamp Reply messages received.
Sent - The number of ICMP Timestamp Reply messages sent.

Address masks
Received - The number of ICMP Address Mask Request messages received.
Sent - The number of ICMP Address Mask Request messages sent.

Address mask replies
Received - The number of ICMP Address Mask Reply messages received.
Sent - The number of ICMP Address Mask Reply messages sent.

2.4.5   Routing (IPv4 and IPv6)

2.4.5.1   Routing Table IPv4

IP
The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network management protocol in use.

Interface index
The index value that uniquely identifies the local interface through which the next hop of this route should be reached.

Route metric 1 (primary)
The primary routing metric for this route. The semantics of this metric are determined by the Routing mechanism.

Route metric 2-5 (alternate)
An alternate routing metric for this route. The semantics of this metric are determined by the Routing mechanism.

Gateway address
The IP address of the next hop of this route. (In the case of a route bound to an interface that is realized via a broadcast media, the value of this field is the agent's IP address on that interface.)

Type of route
Possible values are:

direct - route to directly connected (sub-)network
indirect - route to a non-local host/network/sub-network
invalid - an invalidated route
other - none of the above.

Routing mechanism
The mechanism via which this route was learned. Possible values are:
other - none of the following
local - non-protocol information, such as manually configured entries
netmgmt - set via a network management protocol
icmp - obtained via ICMP, for example, *Redirect* and following gateway routing
protocols:
egp, ggp, hello, rip, is-is, es-is, ciscoIgrp, bbnSpfIgp, ospf, bgp

Route age (sec)
The number of seconds since this route was last updated or otherwise determined to
be correct.

IP Route mask
Indicate the mask to be logical-ANDed with the destination address before being
compared to the value in the IP field.

MIB Route info
A reference to MIB definitions specific to the particular routing protocol that is
responsible for this route, as determined by the Routing mechanism. If this information
is not present, its value is set to 0.0.

2.4.5.2   Routing Table IPv6

IPv6 Routing information is provides for Windows Vista and above.

Interface index
The local index value for the network interface associated with the IP route entry.

Route metric
The route metric offset value for this IP route entry. The semantics of this metric are
determined by the Routing mechanism.

Network Destination
The destination IP address of this route. It contains a Prefix and the Prefix Length in
bits separated by a slash.

Gateway
For a remote route, the IP address of the next system or gateway en route. If the route
is to a local loopback address or an IP address on the local link, the next hop is
represented by *On-link*.

Age
The number of seconds since the route was added or modified in the network routing
table.

Origin
The origin of the route. Possible values are:
manual - the result of manual configuration,
well-known - a well-known route.
dhcp - the result of a DHCP configuration.
router advertisement - the result of router advertisement.

6to4 - the result of 6to4 tunneling.

Protocol
The mechanism via which this route was learned. Possible values are:
other - none of the following.
local - local interface.
netmgmt - a static route set via network management.
icmp - obtained via ICMP redirect.:
egp - Exterior Gateway Protocol, a dynamic routing protocol.
ggp - *G*ateway-to.Gateway Protocol, a dynamic routing protocol.
hello - the Hellospeak protocol (no longer used).
rip - Berkeley Routing Protocol, a dynamic routing protocol.
is-is - Intermediate System-to-Intermediate System, a dynamic routing protocol.
es-is - End System-to-Intermediate System, a dynamic routing protocol.
ciscoIgrp - Cisco Interior Gateway Routing Protocol (IGRP), a dynamic routing protocol
bbnSpfIgp - Bolt, Beranek, and Newman (BBN) Interior Gateway Protocol (IGP) that used the Shortest Path First (SPF) algorithm. This was an early dynamic routing protocol.
ospf - Open Shortest Path First, a dynamic routing protocol.
bgp - Border Gateway Protocol, a dynamic routing protocol.

Loopback
A value that specifies if the route is a loopback route (i.e, the gateway is on the local host).

2.4.5.3 DNS Servers

A DNS server is a computer which stores FQDN[1]-to-IP-address mappings.
Most DNS servers are authoritative[2] for some zones[3] and perform a caching function for all other DNS information

Notes:
(1) FQDN means Fully Qualified Domain Name, i.e, a domain name that indicates w ith absolute certainty its location in the domain namespace tree.
(2) A name server is said to be an Authority or Authoritative for the parts of the name space for w hich they have complete information.
(3) Authoritative information is organized into units called ZONEs, and these zones can be automatically distributed to the name servers w hich provide redundant service for the data in a zone.
(4) The IPv6 DNS Servers List is only provided for Window s Vista and above.

2.4.5.4 Persistent Routes

By default, the routes in the routing table are not persistent, they are lost when the computer is rebooted. It is possible to make some routes permanent using the console program route.exe with the switch */p* and command *ADD.*

For example, adding a IPv4 persistent route:
route /p ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2
and an IPv6 persistent route:
route /p ADD 3ffe::/32 3ffe::1

2.4.6   IP/Transport Protocols

2.4.6.1   IP Statistics/Settings

Acting as IP router
Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams, but IP hosts do not (except those source-routed via the host).

Default TTL
The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity whenever a TTL value is not supplied by the transport layer protocol.

Packets received
The total number of input datagrams received from interfaces, including those received in error.

Received header errors
The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Received address errors
The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Datagrams forwarded
The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter will include only those packets that were Source-Routed via this entity, and the Source-Route option processing was successful.

Unknown protocols received
The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Received packets discarded
The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (for example, for lack of buffer space). Does not include any datagrams discarded while awaiting reassembly.

Received packets delivered
The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

Output requests
The total number of IP datagrams that local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Does not include any datagrams counted in Datagrams forwarded.

Discarded output packets

The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (for example, for lack of buffer space). This includes datagrams counted in Datagrams forwarded if any such packets met this (discretionary) discard criterion.

Output packet no route
The number of IP datagrams discarded because no route could be found to transmit them to their destination. This includes any packets counted in Datagrams forwarded that meet this "no-route" criterion, which includes any datagrams that a host cannot route because all of its default gateways are down.

Reassembly time-out (sec)
The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.

Reassembly required
The number of IP fragments received that needed to be reassembled at this entity.

Reassembly successful
The number of IP datagrams successfully reassembled.

Reassembly failures
The number of failures detected by the IP reassembly algorithm (for whatever reason, such as timed out or errors).

Datagrams successfully fragmented
The number of IP datagrams that have been successfully fragmented at this entity.

Datagrams failing fragmentation
The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set).

Fragments created
The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Routing discards
The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.

2.4.6.2   Installed Protocols

All information about the collection of transport protocols and protocol chains installed on the local machine.
The order of presentation in the list "Installed Protocols" coincides with the order in which the protocol entries were registered by the service provider with the Winsock DLL, or any subsequent reordering that may have occurred.

Protocol details:

1. Address Family:
These can be:

```
AF_UNSPEC          unspecified
AF_UNIX            local to host (pipes, portals)
```

AF_INET	internetwork: UDP, TCP, etc.
AF_IMPLINK	arpanet imp addresses
AF_PUP	pup protocols: e.g. BSP
AF_CHAOS	CHAOS protocols
AF_IPX	IPX and SPX
AF_NS	XEROX NS protocols
AF_ISO/AF_OSI	ISO protocols
AF_ECMA	European computer manufacturers
AF_DATAKIT	datakit protocols
AF_CCITT	CCITT protocols, X.25 etc
AF_SNA	IBM SNA
AF_DECnet	DECnet
AF_DLI	Direct data link interface
AF_LAT	LAT
AF_HYLINK	NSC Hyperchannel
AF_APPLETALK	AppleTalk
AF_NETBIOS	NetBios-style addresses
AF_VOICEVIEW	VoiceView
AF_FIREFOX	FireFox
AF_UNKNOWN1	Unknown
AF_BAN	Banyan
AF_ATM	Native ATM Services
AF_INET6	Internetwork Version 6
AF_CLUSTER	Microsoft Wolfpack
AF_12844	IEEE 1284.4 WG AF
AF_IRDA	IrDA
AF_NETDES	Network Designers OSI & gateway enabled protocols

2. Protocol:

Value of the protocol parameter which depends on the Address Family. For AF_INET/AF_INET6 this can be any of the following:

IPPROTO_IP	Dummy for IP
IPPROTO_HOPOPTS	IPv6 hop-by-hop options
IPPROTO_ICMP	Control Message Protocol
IPPROTO_IGMP	Group Management Protocol
IPPROTO_GGP	Gateway^2 (deprecated)
IPPROTO_IPV4	IPv4
IPPROTO_TCP	TCP
IPPROTO_PUP	PUP
IPPROTO_UDP	UDP
IPPROTO_IDP	XNS IDP
IPPROTO_IPV6	IPv6
IPPROTO_ROUTING	IPv6 routing header
IPPROTO_FRAGMENT	IPv6 fragmentation header
IPPROTO_ESP	IPsec ESP header
IPPROTO_AH	IPsec AH
IPPROTO_ICMPV6	ICMPv6
IPPROTO_NONE	IPv6 no next header
IPPROTO_DSTOPTS	IPv6 destination options
IPPROTO_ND	Net Disk Protocol (unofficial)
IPPROTO_RAW	Raw IP Packet

3. Socket Type:

Value of the socket type parameter. This can be any of the following:

SOCK_STREAM	Stream. This is a protocol that sends data as a stream of bytes, with no message boundaries.
SOCK_DGRAM	Datagram. This is a connectionless protocol. There is no virtual circuit setup. There are typically no reliability guarantees.
SOCK_RAW	Raw. The protocol type in the IP header may be know or not.
SOCK_RDM	Reliably-Delivered Message. This is a protocol that preserves message boundaries in data.
SOCK_SEQPACKET	Sequenced packet stream. This is a protocol that is essentially the same as SOCK_RDM.

4. Connectionless:

Specifies whether the protocol provides connectionless (datagram) service. Otherwise, the protocol supports connection-oriented data transfer.

5. Guaranteed Delivery:

Guarantees that all data sent will reach the intended destination.

6. Guaranteed Order:

Guarantees that data only arrives in the order in which it was sent and that it is not duplicated. This characteristic does not necessarily mean that the data is always delivered, but that any data that is delivered is delivered in the order in which it was sent.

7. Message Oriented:

Honors message boundaries—as opposed to a stream-oriented protocol where there is no concept of message boundaries.

8. Pseudo Stream:

A message-oriented protocol, but message boundaries are ignored for all receipts. This is convenient when an application does not desire message framing to be done by the protocol.

9. Graceful Close:

Supports two-phase (graceful) close. If not set, only abortive closes are performed.

10. Expedited Data:

Supports expedited (urgent) data.

11. Connect Data:

Supports connect data.

12. Disconnect Data:

Supports disconnect data.

13. Supports Broadcast:

Supports a broadcast mechanism.

14. Supports Multipoint:

If it supports a multipoint or multicast mechanism, control and data plane attributes are indicated and can be either rooted or non-rooted.

15. QoS Supported:

Supports quality of service requests.

16. Unidirectional Sends:

Protocol is unidirectional in the send direction.

17. Unidirectional Receives:

Protocol is unidirectional in the receive direction.

18. IFS Handles:

Socket descriptors returned by the provider are operating system Installable File System (IFS) handles.

19. Partial Messages:

The MSG_PARTIAL flag is supported in WSASend and WSASendTo.

20. Provider Flags:

Provides information about how this protocol is represented in the protocol catalog. The following flag values are possible:

PFL_MULTIPLE_PROTO_ENTRIES	Indicates that this is one of two or more entries for a single protocol (from a given provider) which is capable of implementing multiple behaviors.
PFL_RECOMMENDED_PROTO_ENTRY	Indicates that this is the recommended or most frequently used entry for a protocol that is capable of implementing multiple behaviors.
PFL_HIDDEN	Hides the protocol entry when this flag is set.
PFL_MATCHES_PROTOCOL_ZERO	A value of zero in the protocol parameter of socket or WSASocket matches this entry.

21. Provider ID:

Globally unique identifier assigned to the provider by the service provider vendor. This value is useful for instances where more than one service provider is able to implement a particular protocol.

22. Catalog Entry ID:

Unique identifier assigned by the WS2_32.DLL for each protocol structure.

23. Number of Chain Entries:

Counted list of Catalog Entry identifiers that comprise a protocol chain.

24. Version:

Protocol version identifier.

25. Max Socket Address Length:

Maximum address length.

26. Min Socket Address Length:

Minimum address length.

27. Protocol Max Offset:

Maximum value that may be added to when supplying a value for the Protocol parameter to socket and WSASocket. Not all protocols allow a range of values. When this is the case this parameter is zero.

28. Network Byte Order:

This can be either Big-Endian or Little-Endian.

29. Security Scheme:

Indicates the type of security scheme employed (if any).

30. Message Size:

Maximum message size supported by the protocol. This is the maximum size that can be sent from any of the host's local interfaces. For protocols that do not support message framing, the actual maximum that can be sent to a given address may be less. There is no standard provision to determine the maximum inbound message size. The following special values are defined:

0	The protocol is stream-oriented and hence the concept of message size is not relevant.
0x1	The maximum outbound (send) message size is dependent on the underlying network MTU (maximum sized transmission unit) and hence cannot be known until after a socket is bound.
0xFFFFF FFF	The protocol is message-oriented, but there is no maximum limit to the size of messages that may be transmitted.

2.4.6.3   Address Information Table

IP
The IP address to which this entry's addressing information pertains.

Interface index
The index value that uniquely identifies the interface to which this entry is applicable.

Sub-net mask
The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.

LSB in IP non-unicast address
The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will

be 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.

Largest IP datagram can reassemble
The size of the largest IP datagram that this entity can reassemble from incoming IP fragmented datagrams received on this interface.

2.4.6.4 Net to Media Table

The IP Address Translation table used for mapping from IP addresses to physical addresses.

Interface index
The interface on which this entry's equivalence is effective.

Media dependent physical address
The media dependent physical address.

IP address
The Ip address corresponding to the media-dependent physical address.

Type of mapping
The type of mapping. Can be any of the following:
static
dynamic
invalid
other, none of the above

2.4.7 Interfaces

Index
A unique value identifying the interface.

Description
A textual string containing information about the interface. This string may include the name of the manufacturer, the product name, and the version of the hardware interface.

Type
The type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.

MTU
The size of the largest datagram that can be sent/received on the interface, specified in octets.

Speed
An estimate of the interface's current bandwidth in bits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this should contain the nominal bandwidth.

Adapter physical address
The interface's address at the protocol layer immediately "below" the network layer in the protocol stack.

Admin status
The desired state of the interface. This can be either up, down or testing. The testing

state indicates that no operational packets can be passed.

Operational status
The current operational state of the interface. This can be either up, down or testing. The testing state indicates that no operational packets can be passed.

Bytes received
The total number of octets received on the interface, including framing characters.

Packets delivered unicast
The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Packets delivered non-unicast
The number of non-unicast (that is, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.

Inbound packets discarded
The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

Inbound packets with errors
The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Inbound packets discarded unknown protocols
The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.

Bytes transmitted
The total number of octets transmitted out of the interface, including framing characters.

Packets requested unicast
The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Packets requested non-unicast
The total number of packets that higher-level protocols requested be transmitted to a non-unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.

Outbond packets discarded
The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

Outbond packets with errors
The number of outbound packets that could not be transmitted because of errors.

Output packet queue
The length of the output packet queue in packets.

MIB specific information
A reference to MIB definitions specific to the particular media being used to realize the interface. If this information is not present, its value is set to 0.0.

2.5   Audio & Text Chat

2.5.1   Audio

You can do voice chat or exchange other audio content with a remote computer. All control remains in the local computer (in some countries, for legal reasons, you must make sure the the user at the remote computer has been previously informed that audio is being captured, and eventually recorded, from his/her computer).
The sound flow is fully duplexed with independent in and out streams.
The audio can be recorded.

To use the audio features, the order of procedures is the following:
1) Establish a connection to the remote computer.
2) Push the Initialize button in the Audio tab, then select the Local and Remote Sound Capture and Play Devices.
3) Push the Start Sound button, to start the audio streaming.
4) When done, simply push the Stop button, to shut down the audio engine.

From the Audio tab, you can:

Select the Local and Remote Sound Capture and Play Devices
As you are aware from the Windows Control Panel/Sound options, computers have various audio devices for playing and recording sound. Although Control Panel sets default devices for playback and recording, you are not restricted to use those. For example, you may have the default Recording device set in Control Panel to "Microphone SomeBrandName" but you are interested in using the "Stereo Mix" (if it exists and is enabled. Sometimes also known under other names like "What-You-Hear") during the connection (the purpose might be, capture sound played from an internet browser or other software: voice, radio, music or anything). So you will select that device in the Remote Sound Capture Device grid (or Local Sound Capture grid, depending on your purpose. Note that selecting both may cause audio feedback, unless you "Mute" one of the endpoints).
If you use over and over the same Play and Capture devices on the Local Computer, you may set them as default. This will not change the Control Panel settings. Default devices cannot be set for the Remote Computer because the list changes from computer to computer.

Use the Mute switch buttons
Any time while audio streaming is active you can prevent it from playing either on the local and/or on the remote computer. When sound is muted for the local computer and sound recording is in progress, only silence is recorded for audio arriving from the remote computer. Conversely, when sound is muted for the remote computer and sound recording is in progress, only silence is recorded for sound outgoing to the remote computer.

Record
When you push the Record button, you must select a file to save to. If you select an existing file, the recording will be added to it. Recording can be Paused and Resumed any number of times. When you are done, push the Stop Sound Recording button. Recording will stop as well, when the Sound engine is stopped. Sound is recorded in 2 channels (stereo); one of the channels is for incoming audio, the other for outgoing audio.

Adjust Sound Volume

You can adjust the sound volume level on either computer, but there are two cases:
1) If the Sound Play engine is DirectSound the adjustment is "relative" (i.e, is a fraction of it and does not change it) to the Master Volume level of the computer.
2) If the Sound Play engine is WaveOut, the sound adjustment is made to the Master Volume level of the computer. If possible, the software will reset the Master Volume level to its initial values when the audio engine shuts down. The sound volume lever will self adjust if the Master Volume level is externally adjusted by either the local or remote users or by other software.

Check Preferences for more permanent settings.

2.5.2   Text Chat

You can carry a live conversation with the interactive user on the remote computer. You should take the initiative for the Chat. AWRCP does not allow the remote computer to take any initiative, you are in absolute command. The remote interactive user may, however, end the chat by closing the Chat window.

2.6   Forensics

2.6.1   Credentials Stores

The Credentials Stores are secret store vaults used to store various type of information, including, but not limited to, network login passwords.

Credentials Stores have been around in Windows since XP/2003 although Microsoft had been calling them different names along the time. We will not spend time detailing what names have been used, the important points to retain are that:
- Microsoft wants to maintain Credential Stores, although they are not very safe.
- Internet Explorer 10 and 11 and Windows 8.xx and 10, now use exclusively the Credentials Stores to save passwords.

Note1: This AWRCP feature is not available when the remote computer is running a 64-bit operating system and you selected *Run as 32-bit on a 64-bit Remote Operating System* in Preferences.
Note2: This feature needs to be enabled under Policy/Forensics by running Configure.exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.2   Browsers

2.6.2.1   Microsoft Edge

Currently, Microsoft Edge is only available for Windows 10, and the passwords are visible under the Credentials Stores tab of AWRC Pro.

Autocomplete Passwords:
These are visible under the Credentials Stores/Other Vaults tab when you click the Get button. The Vault Name is *Web Credentials* and the resources are named *Internet Explorer* by Windows, probably because under Windows 10 the passwords for both browsers were consolidated.

HTTP Basic Authentication Passwords:
These are visible under the Credentials Stores/Windows Vault tab when you click the Get button. The target names begin with *Microsoft_Wininet_*

On Windows 10, the same passwords are valid for both Internet Explorer 11 and Microsoft Edge.

2.6.2.2   Internet Explorer

AWRC Pro is able to find passwords from release 4.0 up to at least release 11.0 of Internet Explorer.
However, the way Windows uses to conceal the passwords has varied largely along the time, so AWRC Pro uses different techniques to find them.

Internet Explorer 4 till 6:
Currently, only existing Windows 2000 machines are likely to have IE 6 or below installed. The reason is that they could not upgrade to more recent releases of IE. These release of IE store the passwords in the Registry, in a place with hidden values called Protected Storage. AWRC Pro will find easily all these passwords and will show them in the Browsers/Internet Explorer tab.

Internet Explorer 7 till 9:
IE 7 and 8 are typical for Windows XP, which never allowed an upgrade to IE 9. IE 9 was the last IE supported by Windows Vista.
For these releases of Internet Explorer, the HTTP Basic Authentication Passwords are visible under the Credentials Stores/Windows Vault tab when you click the Get button. The target names of these passwords begin with *Microsoft_Wininet_*
The Autocomplete Passwords are visible under the Browsers/Internet Explorer tab. However, due to the mechanism used by Microsoft to hide those passwords it is impossible to retrieve all of them unless the corresponding URLs exist in the history cache of IE. Still, AWRC Pro does have a supplement of common used URLs to test, even if they don't exist in the history cache. However, the bottom line is that only by luck all Autocomplete Passwords are retrievable.

Internet Explorer 10 and 11:
Under Windows 7, IE 10 and IE 11 work similarly to IE 7 to 9 as far as the passwords storage mechanism is concerned.
Windows 8, supports IE 10 but not IE 11. Windows 8.1 and Windows 10 support IE 11.
Under Windows 8.xx and 10, all passwords are visible under the Credentials Stores tab. The HTTP Basic Authentication Passwords are visible under the Credentials Stores/Windows Vault tab, and are the ones where the target names begin with *Microsoft_Wininet_*. The Autocomplete Passwords are visible under the Credentials Stores/Other Vaults tab. Web Credentials is the Vault Name and the resources are called (by Windows) *Internet Explorer*.

Note: This feature needs to be enabled under Policy/Forensics by running Configure.exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.2.3   Chrome

We performed tests in versions of Chrome from their earliest times till the most recent at the time of this writing (version 47), and the conclusion is the same:
The Chrome browser is not able to offer a minimum of security for the passwords, so collecting them is easy.

Note: This feature needs to be enabled under Policy/Forensics by running Configure.exe (or selecting File/Administration from within Awrcp.exe), and is not available in

trial mode.

2.6.2.4   Firefox

AWRC Pro is able to find passwords for all releases of Firefox. When there is a Master Password protecting the other passwords, AWRC Pro will not be able to retrieve the passwords, unless the user knows the Master Password and enters it in the box labeled *Master Password* before pressing the *Get Passwords* button.

When the remote computer is running a 64-bit Operating System, AWRC Pro can only retrieve the passwords if it run as 32-bit on the remote computer. This can be selected from *Preferences/Advanced/Runs as 32-bit on a 64-bit Remote Operating System*. The reason is that Firefox is a 32-bit application, AWRC Pro will use some DLL from Firefox and, as you know, 64-bit applications can not run code from a 32-bit DLL (at least without a surrogate application, which would be very expensive in terms of code).

Note: This feature needs to be enabled under Policy/Forensics by running Configure. exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.2.5   Opera 16+

AWRC Pro finds the passwords for releases of Opera from 16.0 and later (i.e, from middle 2013 onwards). Since the procedure is similar to the one used by Google Chrome, the collection of passwords is easy.

Note: This feature needs to be enabled under Policy/Forensics by running Configure. exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.2.6   Opera old

Releases of Opera up to 16.0 used a pretty sophisticated way of protecting the login credentials in a file named Wand.dat, which is located under the Opera subfolder of the roaming *Application Data* folder (in the user's personal folder)
When no Master Password is in place AWRC Pro is able to decrypt the content of the Wand.dat and present it in a raw format perfectly readable.

Note: This feature needs to be enabled under Policy/Forensics by running Configure. exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.3   Password Hashes

2.6.3.1   Local Hashes

We decided to include this tool to enable System Administrators to audit their systems for adequate passwords. It is not prudent to believe that your systems are safe without fully testing them. In most cases, the systems are not safe at all! Passwords are the fundamental lock on your systems, it is a good practice, provided your management approves, to regularly assess the quality of your users' passwords and provide feedback to users who select easy-to-guess passwords.

Passwords are not stored anywhere within NT technology systems, only their hashes.

AWRCP is able to instantly retrieve the password hashes from the remote, even with the default Syskey protection activated and within the Active Directory on Windows 2000 networks.

With the hashes it is always possible to retrieve the original passwords, but it can take from a few seconds to days, months, years, a life time, or the age of the Universe.

Brute force cracking is not the best approach to retrieve the original password, so we can find a whole bunch of password-cracking software using various strategies to crack in a short period of time the so-called *weak (easy to guess)* passwords. However, for such software, problem arise when the passwords are from the *strong* type.

What is a *strong* password then? Microsoft provides the following tips:

- Is at least eight characters long.
- Does not contain your user name, real name, or company name.
- Does not contain a complete word.
- Is significantly different from previous passwords.
- Contains characters from at least three of the following five categories:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /
Unicode characters	€, Γ, , and λ

Under Windows XP and older, passwords are stored in 2 types of hashes: LM hashes and NTLM hashes.

LM hashes made life relatively easy for password-cracking software. The storage of LM hashes could be disabled without problems through a simple Registry Key change, but almost no one did that. These were times of glory for password-cracking software like L0phtCrack.

With Windows Vista and later, LM hashes are not computed and stored anymore by the operating system, only NTLM hashes are used. Cracking NTLM is much more difficult, particularly if they contain Unicode characters.

Strong NTLM passwords resist to dictionary attacks and Rainbow table cracking.

AWRCP uses a third technique to attempt to retrieve passwords from NTLM hashes, a mammoth online Database.

Pressing the **Resolve NTLM Hashes** button, opens the *Query NTLM Hashes in Database* window with the collected hashes ready to be queried.

Also, AWRCP has an option for saving the hashes in pwdump* format, so they can be imported by L0phtCrack, OphCrack and others.

(*) PWDUMP is a command line utility w hich captures hashes from remote computers by loading a special DLL into lsass.exe address space, storing the captured hashes into the Registry then attempting a connection to the remote Registry to retrieve them.

Note1: This feature is not available when the remote computer is running a 64-bit operating system and you selected *Run as 32-bit on a 64-bit Remote Operating System* in Preferences.

Note2: This feature needs to be enabled under Policy/Forensics by running Configure.exe (or selecting File/Administration from within Awrcp.exe), and is not available in trial mode.

2.6.3.2   Query NTLM Hashes in Online Database

AWRCP makes use of a special battery of online databases (for simplicity, will be called in here just *Online Database*) of more than 5 billion NTLM *partial hash to password* duets.
This 205 GB Online Database contains every password from published lists of easy passwords, common passwords, internet leaked passwords, English and foreign language dictionary words, foreign language common passwords, and also a compilation of short passwords built according to various strategies.

Why are the Online Database queries so fast?
Because the Online Database consists of a battery of 256 SQLite databases, each with around 20 million *partial hash to password* duets and a size of about 820 MB.
Each database is suffixed with the first 2 characters of the hash.
For example if the hash is F30AD41CD0B5AC9C3D76F6F177501CAB, the hash will be looked for in the database file DBF3.db


```
12-Sep-15   04:02  PM        860,622,848 DBF0.db
12-Sep-15   04:02  PM        860,827,648 DBF1.db
12-Sep-15   04:02  PM        860,925,952 DBF2.db
12-Sep-15   04:06  PM        860,205,056 DBF3.db
12-Sep-15   04:06  PM        860,745,728 DBF4.db
12-Sep-15   04:06  PM        860,491,776 DBF5.db
12-Sep-15   04:06  PM        860,565,504 DBF6.db
12-Sep-15   04:06  PM        860,770,304 DBF7.db
12-Sep-15   04:07  PM        860,581,888 DBF8.db
12-Sep-15   04:12  PM        860,667,904 DBF9.db
12-Sep-15   04:12  PM        860,798,976 DBFA.db
12-Sep-15   04:12  PM        860,688,384 DBFB.db
12-Sep-15   04:12  PM        860,360,704 DBFC.db
12-Sep-15   04:12  PM        860,766,208 DBFD.db
12-Sep-15   04:12  PM        860,549,120 DBFE.db
12-Sep-15   04:15  PM        860,925,952 DBFF.db
            256 File(s) 220,331,409,408 bytes
              2 Dir(s)   736,780,095,488 bytes free
```

Partial view of the Online Database Battery

In order to save space, the databases do not store the full hash, only store the first 8 characters of it. So all passwords with the same first 8 characters in the hash are collected, later the full hash is calculated for each of the passwords in order to compare with the queried hash.
All simple and straightforward,

Another feature of this project is that new password/hashes can be added by users, making the Online Database grow dynamically. By default, each time users calculate Hashes from passwords, those new duets will be added to a special database file and become immediately available for new queries.

2.6.3.3 Calculate Hashes

Users can calculate hashes for various purposes, one of them is to investigate if some password is already in our Online Database.
Beware that, by default, hashes and passwords are automatically added to the Online Database, this means that unless you uncheck "*Add NTLM Hash to Online Database, if not there*", the duets will start making part of the Online Database after you check if they are there.

Although not of much use for modern operating systems, but of forensics interest for sure, LM hashes are also calculated. Most people is not aware, but LM hashes are code page dependent and no other software (except the Windows operating system) does this calculation in a proper way. Moreover, not every character is acceptable in every code page, for instance the password: *abcdã* contains invalid characters in code page 437 (so the LM hash is not calculated) but not in code page 850 (and the LM hash is calculated).

3 Tools

3.1 Unlock Remote

3.1.1 How it Works

AWRCP is able to *unlock* the computer without entering any password. The feature works as well with Screen Savers that display the logon screen on resume.

Note1: This feature works in all versions of Windows released so far (tested with Windows 10), except Windows 2000.

3.1.2 Using the Unlock Remote command

Just select Tools/Unlock Remote on the main menu or click the 🔓 icon on the Desktop page to unlock the remote computer.

Important: *If the Unlock Remote command does not work, issue Control-Alt-Del first and then the Unlock Remote command again.*

3.2 Wake-on-LAN

3.2.1 How it Works

Wake-on-LAN (WOL) allows a computer to be turned on by sending a message called a Magic Packet over an Ethernet based network. Since the computer is powered off, an IP address may not be anymore assigned to it by a router and it appears there is no way to find the computer on the network. However, the magic can work because the network card itself may not be completely switched off (if you see a small light flashing in there, that means it is not).

Each network card has a unique hard-coded identification called MAC (Media

Access Control) Address. The Magic Packet containing the MAC address of the PC to be waked up is broadcasted to every PC on a subnet.
When the powered off PC detects a Magic Packet with its MAC address it switches on.
This is as simple as that.

3.2.2   Conditions to Work

Wake-on-Lan (WOL) is not a new technology, it has been around for well over 10 years. Most recent motherboards, if not all, do indeed support WOL, although the name WOL is not always mentioned in the motherboard manual. For WOL to become available you may need to set it in the BIOS by running the BIOS Setup at power on. If is not clear how to set it up in your specific computer motherboard try to perform a web search for the answer, I am sure you will find it this way.
Another way, is to set it from Power Management on the LAN Adapter of the computer (see image below):
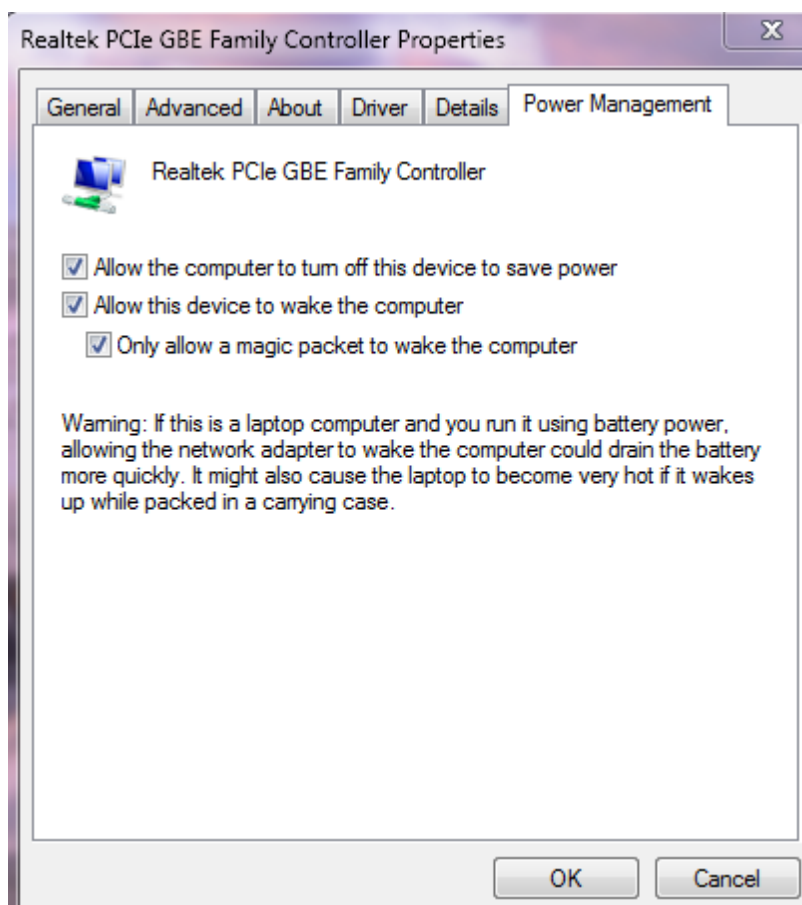
Once this is done, you should be aware that not all machines wake up from all power off states. Some don't wake up from Hibernation, other don't from Stand-By and others don't from a Shutdown. Of course, most modern ones will wake up from most, if not all, states.

3.2.3 WOL over the Internet

You can wake up a computer over the Internet, but this depends somewhat on the capabilities of the router that receives the Magic Packet.
Before you start wondering why it does not work for you, beware that most routers (actually, almost all) don't broadcast from WAN (Wide Area Network, or the internet). In other words, they don't support forwarding to an IP address like 192.168.0.255 (if Subnet Mask is 255.255.255.0 and LAN IP is 192.168.0.1, this is a broadcast address) in you LAN . The alternatives are various, but none of them is straightforward and require some sort of geek mentality, so we will not endorse or even refer any of them. Obviously, the purchase of a suitable router would fix, but since suitable routers are rare in the market, some people flash popular routers with alternate open source firmware like Tomato or DD-WRT to get what they want.

In short, let's reduce it to 2 cases. If the the router supports broadcast from WAN, forward the selected port to the broadcast address (for example, 192.168.0.255, as seen above). If the router does not support broadcast from WAN and you forward the port to the IP address of the switched off machine (instead of the broadcast address), this may work if the router arp cache has not been refreshed in the meantime.

3.2.4 WOL over Wireless Networks

Wake-on-LAN does not work on wireless networks.
A technology called WoWLAN exists but is not widespread.

3.2.5 Using the WOL tool
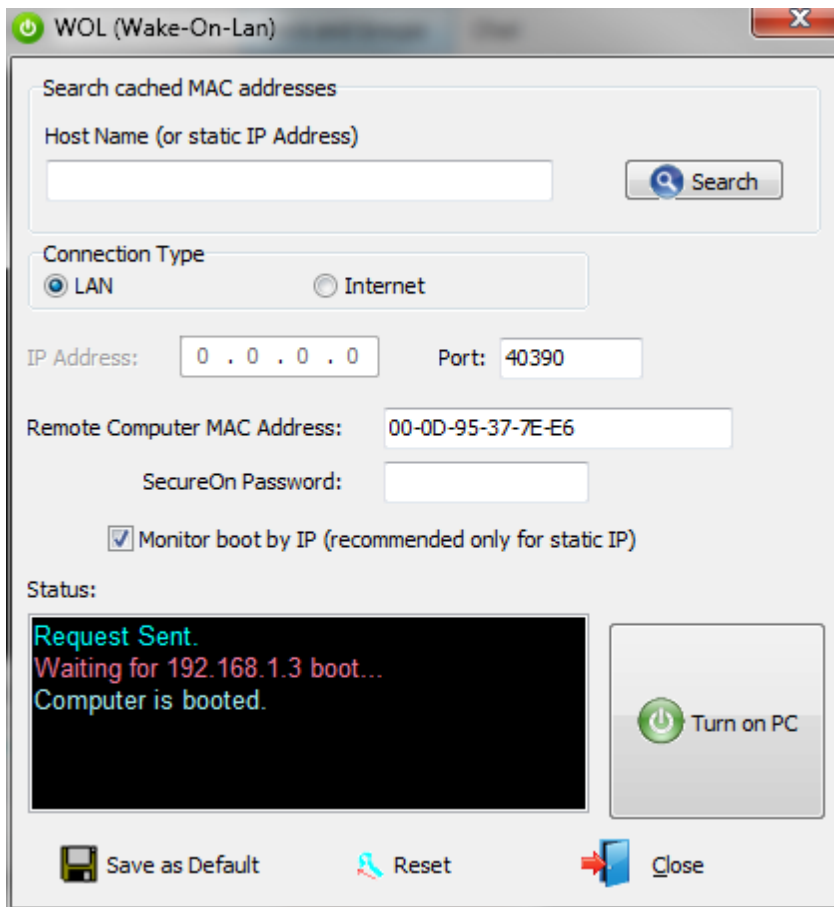
To wake up a computer on a LAN the only information you need is the MAC Address of the computer you want to power on. To wake a computer over the internet you also need the public IP address of the router, but since WOL over the internet is not straightforward we are going to restrict our explanation to WOL over a LAN.

If you don't know the MAC Address you can enter the Computer Name or IP (if static) into the box near the top and press the Search button. This part works if you have ever connected to that computer with AWRCP, because AWRCP automatically retrieves and caches the MAC Address of a connected machine. If the MAC Address is not cached but is available through ARP (only when you search by IP) you can still get it by pressing the Search button.

The Port number should not be important when doing WOL over a LAN, leave it as is or change if you wish.

SecureOn Password is normally left blank, unless the remote computer BIOS has this feature and it is active. The SecureOn password has 6 characters when not left blank.

After you press the *Turn on PC* button, AWRCP will attempt to detect when the boot is completed. This is done by *pinging* the remote computer at regular intervals. Of course, if the MAC was not retrieved from the cache there is no information about the remote computer and Ping can not be done. It is preferable to monitor the boot by IP, so you should check the corresponding box if the IP is static. The reason is that the name resolution does not always work reliably. The boot is not monitored for Internet WOL operations.

If you wake up the same computer over and over you can save the settings by pressing the *Save as Default* button. This can always be removed by pressing the *Reset* button.

3.3 Ping

3.3.1 Using Ping

The original Unix PING has been produced in 1983 by Mike Muuss, a developer deeply involved in modeling of sonar and radar systems. The term PING is after the sound that a sonar makes, inspired by the whole principle of echo-location. Some time later, PING became an acronym for the expression Packet InterNet Grouper. Anyway, Pings are no more than ICMP echo packets, which are an excellent tool for troubleshooting IP-level connectivity.

To perform a Ping:

First, you enter the host name or IP address of the target host in the **Host Name/IP Address box**.
```
The packets are always sent to an IP address. If you enter a host
name, this is resolved to an IP address using your default DNS server
.
```

Then you set the Options, if necessary (normally, no need), and click the Ping button.

3.3.2 Ping Options

Timeout: Specifies the length of the time-out interval, in milliseconds. Default is 5000.

Delay: Specifies the length of time between packets, in miliseconds. Default is 1000.
```
Note: AWRCP Ping sends each packet as a separate thread without waiting for previous packets
```

Packets: Specifies the number of packets to send. Default is 4.

Packet Size: Specifies the size, in bytes, of the payload part of the ICMP Echo Request packet. Default is 56.
```
The total message size will be the sum of this value with the ICMP header (8 bytes) and the
```

TTL: Specifies the maximum number of hops that the packet is allowed to pass through. Default is 128.

Resolve IP address: Resolves addresses to host names. Default is unchecked.

Don't fragment: If checked packets that exceed the PMTU (see RFC 1191) will not be delivered. If unchecked, those packets will be fragmented and reassembled at the target. Default is unchecked.

Record in IP Header Timestamp for x hops:
Timestamps are 32-bit numbers in milliseconds which show elapsed time since midnight UTC. If the time is not available in milliseconds or cannot be provided with respect to midnight UTC then it will be reported as non-standard time format. The

maximum number of timestamps that fit in the IP header is 4. Timestamps are normally used for debugging purposes not performance measurements.

Record in IP Header Route for x hops:
A recorded route is composed of a series of internet addresses. As datagrams traverse routers, they check to see if the recorded route option is present. If a router sees it is, it inserts its own internet address into the Options area of the IP header after the previous router. The maximum number of routes that fit in the IP header is 9.

Loose Source and Record Route (LSRR):
This provides a means for the source of an internet datagram to supply routing information to be used by the gateways in forwarding the datagram to the destination and to record the route information. It is called *loose* because the gateway or host IP is allowed to use any route of any number of other intermediate gateways to reach the next address in the route.
`Nowadays, quite a few ISPs, Internet nodes and backbone routers do not support LSRR. This see`
To use LSRR, you push the button LSRR and enter all intermediate nodes in the presented box. The final destination you enter in the Host Name/IP Address box.

Strict Source and Record Route (SSRR):
This provides a means for the source of an internet datagram to supply routing information to be used by the gateways in forwarding the datagram to the destination, and to record the route information. It is called *strict* because the gateway or host IP must send the datagram directly to the next address in the source route through only the directly connected network indicated in the next address to reach the next gateway or host specified in the route.
Most ISPs, Internet nodes and backbones routers do not support SSRR.
To use SSRR, you push the button SSRR and enter all intermediate nodes in the presented box. The final destination is entered in the **Host Name/IP Address** box.

3.3.3   Troubleshooting with Ping

- **The remote is up but Ping fails:**
  Some remote hosts filter ICMP Echo messages at their router or use a personal firewall with such rules configured.

- **Ping succeeds but some services, like Microsoft Networks, fail:**
  This suggests you are facing a software configuration issue, as opposed to a hardware problem. Confirm that File and Printer Sharing is enabled (File and Printer sharing being enabled does not mean you will have to share disk drives!)

- **High round-trip times:**
  The reply is measured in milliseconds. As a rule of thumb, across the Internet, it's best if round-trip times are under 200 milliseconds. The time it takes a packet to reach its destination is called *latency*. A large variance in the round-trip times (which is called *jitter*), implies poor performance talking to the host. However, a couple of laggards in a large sample (50 to 100) is no cause for worries.

- **Detecting changes in routes:**
  When you know the TTL of the remote, you can use it to determine how many router hops the packet has gone through. If the TTL field varies in successive pings to the same remote, it could indicate that the successive reply packets are going via different routes, which could be a reason for further analysis.

- **Path Maximum Transmission Unit (PMTU) Discovery:**
  The PMTU (see RFC 1191) between two hosts can be discovered manually with

Ping, varying the Packet Size with the Don't Fragment bit set.
Note that the Ping's packet size specifies just the size of the ICMP Echo Request data to send, not including the IP and ICMP Echo Request headers. The ICMP Echo Request header is 8 bytes, and the IP header is normally 20 bytes (but can go up to 60 with IP options). In a typical Ethernet link layer MTU is 1500 and the maximum allowed packet size will be 1472 (considering 8 bytes for the ICMP header plus 20 bytes for the IP header).

- **High packet losses:**
If Ping indicates a high packet loss or slow round-trip response on a LAN, your network might have a hardware problem. On a WAN, these results may be normal, and TCP/IP is designed to handle the variability. On a LAN, round-trip time is very low, and you see little or no packet loss. If this isn't the case, test your cables, cable terminations, hubs, switches, and transceivers.

- **Ping by name fails:**
If pinging by address succeeds but pinging by name fails, the problem usually lies in name resolution, not in network connectivity. There are two type of names in the Windows world. The first type is called DNS (Domain Name Resolution) and would use a DNS server (either in the organization or in the internet) or Hosts file. The second type is Netbios names and are resolved either by a LMHosts file, by a WINS server or just by broadcasting the request. This second type is legacy and slowly being phased out, while Microsoft is standardizing in resolving every name through DNS Server or Hosts file.

3.4   LAN Computers

3.4.1   Network Shared Resources

In a Microsoft Network you have a number of shared resources namely, local printers, media devices, urls and computers that can be accessed from your computer under certain conditions. Microsoft has always provided a facility to list such resources in the form of a folder with names like Network Neighborhood, My Network Places or just Network.

Of course, here we are only interested in accessing other computers, most notably those that are online. The facility provided by Microsoft lists computers on the LAN even when they are offline since long. The issue is related to the way the Browser Service works, which machine is the Master Browser and the frequency the Browser List is built. Sometimes. machines are hanging dead in the Browser List for hours, as you probably noticed.

3.4.2   Enumerate LAN Computers

The LAN Computers facility lists all online computers on the Local Area Network. Since it works on the same principle used by My Network Places, the complete enumeration may take long on a large LAN, but you are getting results all the time during the process.
The alternative is to use the Microsoft Network Scanner.

3.5 Microsoft Networks Sweeper

3.5.1 Microsoft Networks

Microsoft Networks are based on an application-layer network protocol used for shared access to files, printers and other resources on a network. This protocol is known as SMB (Server Message Block). Since Windows 2000, SMB is hosted on TCP port 445, i.e., while Windows NT used NetBT (NetBIOS over TCP port 139) for SMB, later operating systems do not (but can fall back to it in the unlikely event that port 445 does not respond in a timely fashion).

AWRCP does not support Windows NT (only supports Windows 2000 and later), so you can disable NetBT and rely only on port 445 for your Microsoft Networks connection needs.

Did you notice that I appear to be recommending to disable NetBT? Yes, I do because it is pretty much useless nowadays. Some people defend (with a dose of paranoia) that NetBT is also a security risk, name tables are visible and some vulnerabilities have been found. Actually, NetBT (and other NetBIOS variations) is just 30 years old and performs bad according to today's standards. However, hundreds of millions of computers, mostly in corporate environments do support NetBT. So, our scanner looks for both ports, 445 and 139.

3.5.2 Using the Sweeper

The Microsoft Networks Sweeper searches a range of IPs for open TCP ports 445 and 139 (see Microsoft Networks).

Enter the Start IP and End P, decide if you want the hostname to be resolved (resolving slows down a bit) and press the Search button.

Note that Windows XP SP2 and SP3, Windows Vista RTM and SP1 and Windows 2008 RTM and SP1 limit the number of simultaneous outbound connections. So you must keep checked the box near the bottom and perform the slow sweep, otherwise data will be lost. Other operating system, namely Windows 7 and Windows 2008 R2 don't have this restriction, so you can scan at full speed.

The image below shows the result of a sweep across the internet, we omitted resolving and disguised some data for privacy reasons.
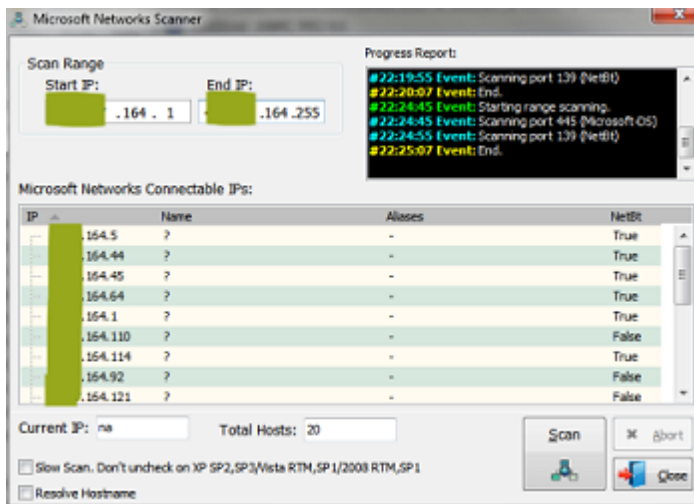
All these machines are connectable by AWRCP, provided you are an Administrator on them.

Machines that have a mention of True in the NetBT column have port 139 open. If you double click any of them you will see the respective NetBIOS Names Table and Mac Address (below).
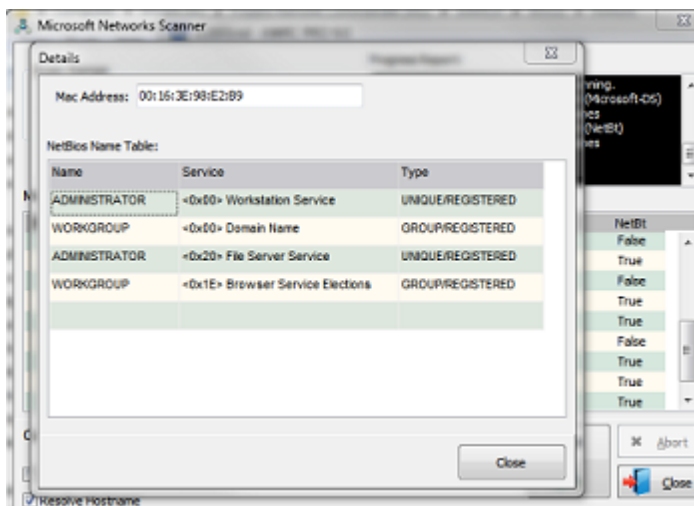
3.6   Remote Console

3.6.1   What is it?

The concept of opening a console window to a remote computer is not new, a utility developed by Mark Russinovitch in the late 90's, psexec.exe, became famous for doing just that.However, psexec.exe is flagged as virus or trojan by a number of antivirus programs, because some viruses use it to propagate. This is unfair, but antivirus is big business.

Anyway, having command line remote access is particularly useful for running console applications and cmd.exe commands on the remote machine.
Our Remote Console does just that, it is more convenient to use than psexec.exe

and is impossible to be flagged as a virus. You can run Remote Console and do any other tasks at the same time inside AWRCP.

For safety reasons, you can not copy files to the remote machine with the Remote Console (but you can do it with AWRCP's File System tools).

3.6.2 Using Remote Console

You can use the Remote Console during an ongoing connection with another computer.
Select Tools/Remote Console on the main menu or click the ![icon] icon on the Desktop page to open the Remote Console Launcher (see below).
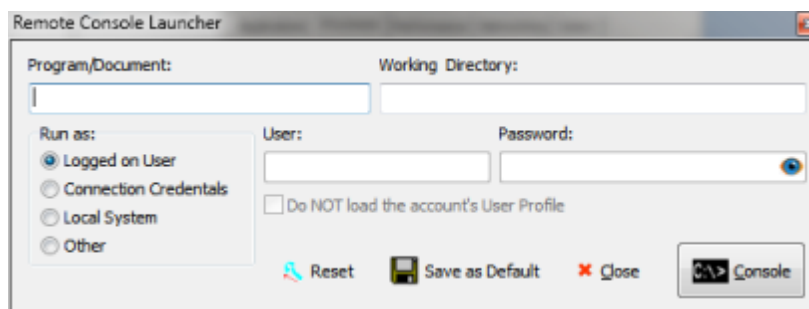
As you can see, we have various options on the Remote Console Launcher, but if you press now the Console button, it will open a console window, like the one below.
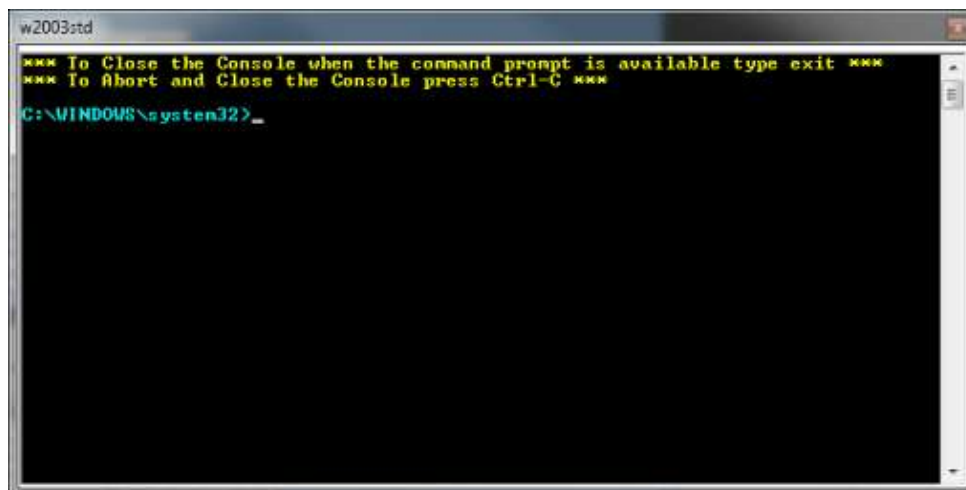
As mentioned, you can set a few options on the Remote Console Launcher (and even save them if such options are recurring).

On the Program\Document box you can enter a program to be executed or a document (if there is a file association for it). The program to be run must be found through the Path environment variable, otherwise enter the respective directory on the Working Directory box.

You can run the program under any account that can log in to the remote machine or under the Local System account. If you check *Do NOT load the account's User Profile*, you will not be able to access the Registry hive of that user, however this is

sometimes a necessity.

To close the Remote Console type *exit* on the prompt followed by *<enter>.* If for some reason, you don't have access to the prompt, namely because you launched a windowed application, press *Control-C.*

As you saw, there is not really a difference between what you can do when you open a console to your local machine and what you do when you open a console to the remote system.

3.6.3   Policy Restrictions

By running Configure.exe, directly or through the menu File/Administration, it is possible to deny the use of Remote Console on the local machine in order to comply with the organization's policies.
The setting is found in the Policy tab.

3.7   Recorder

3.7.1   What you can do

The Recorder allows you to produce compact, small sized .WMV movies.
You can Pause and Resume the video recordings, adjust the frame rate or the quality and insert audio comments.
You can also capture fast snapshots in either JPEG or BMP formats. If you press Ctrl while clicking the JPEG or BMP buttons, the full remote screen will be captured, even if not visible.

With the Recorder you can record on Motion Detection as well, this is ideal for unattended monitoring.

3.7.2   Launching the Recorder

The Recorder can be launched either from the Tools menu or by clicking the 🎬 icon on the central toolbar of the Desktop tab.
After launching the Recorder, AWRCP will lock its size, i.e, you can't resize, maximize or minimize the window, but you can move it
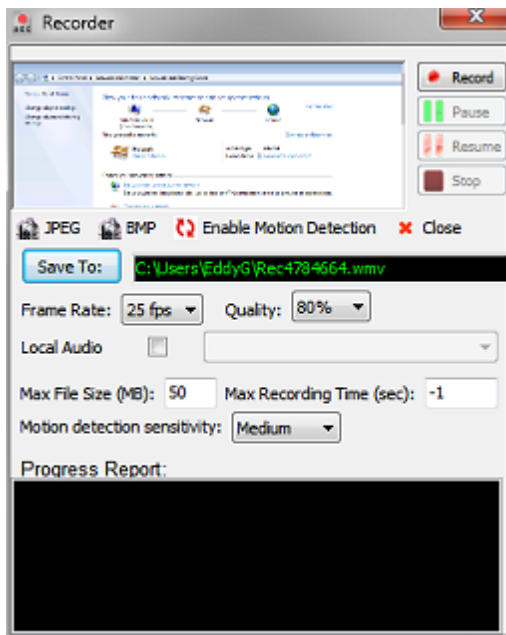
3.7.3   Preparation

- **Select the folder to Save the movies and snapshots**
  The Recorder proposes a file path to save the movie but you can change it by pressing the *Save To* button or by entering directly the value. The new folder becomes the new default folder for future sessions. Image snapshots will use the same folder and file name (appending *Cap* before and a number after).

- **Frame Rate**
  Normally, 25 fps is good for most purposes. For very lengthy recordings where not much action is expected you may want to reduce the frame rate to prevent the building of very large files.

- **Quality**
  Normally, a value of 80% or above is desired when you want to capture every detail. More quality implies larger files, so you will have to decide.

- **Local Audio**
  You can insert voice or other sort of audio in the movie. After you check the Local Audio box, select the input device from the dropdown list.

- **Max File Size (MB)**
  Setting a limit may be important, although the WMV format is very compact, the movie may grow in size far beyond what you expect and want.

- **Max Recording Time (sec)**
  You may need to set a limit in recording time when you are not sure to be present to stop the recording yourself.

3.7.4   Motion Detection

Recording on Motion Detection is particularly suited to unattended surveillance. The software starts recording when a certain level of activity is detected and pauses the recording after a few seconds of inactivity. The cycle is repeated as many times as

the situation occurs. There are 3 levels of sensitivity, a lower level requires more activity to wake up the engine and start the recording process.

3.8 Save Remote Screen

The full remote desktop can be saved in .JPG or .BMP formats. Before saving you can select the file name.
The full remote desktop can also be saved from the Recorder Dialog (but from there, file names are automatically chosen).

4 Preferences

4.1 Desktop

- **Refresh rate**:
  This can range from Fastest to Paused. When you select Fastest, updates are processed almost in real time while in Paused updates are freezed.

- **Default scale**:
  When you connect always to the same machine or have found an ideal scaling you may set it here to be used on every connection.

- **Desktop Colors**:
  You can select 256 Colors (8-bit), 65536 Colors (16-bit), 24-bit True Color or 32-bit True Color.
  True Color and 16-bit Color provide the best user experience, but 256 Colors and 16 Colors improve the throughput and are suitable for problematic traffic conditions.

- **View Layered Windows:**
  When checked you will be able to see the small tooltips on the remote desktop. However, the mouse will have a noticeable flicker effect on the remote desktop on most computers. When unchecked, the flicker will disappear. Most users seem to prefer the flicker free mouse, so the default for this option is unchecked.
  Note: On Windows 7 with Aero-Glass enabled, it appears that layered windows are visible even without checking this checkbox. This is not documented by Microsoft.

- **See remote mouse activity**:
  Remote mouse activity can be optionally monitored (monitoring is selected by default).

- **Permanent mouse pointer**:
  If checked, when the mouse is disconnected or does not exist on the remote computer, the local user can still see an arrow mouse cursor for easier navigation on the remote desktop.

- **Maintain Full-Screen aspect ratio**:
  In Full-Screen mode, when the remote screen resolution aspect ratio differs from the local screen resolution aspect ratio, the local image of the remote screen may become distorted unless you keep this box checked. Some local screen area is left black when the aspect ratio are different.

- **View-Only Mode:** By selecting this mode, local mouse movements and

keystrokes are not passed to the remote computer. This is useful for users that use the software mostly for passive monitoring.

4.2   General

- **Compression level**:
  Within a fast LAN it may be faster to use Light compression, while across the internet you may try the Strong compression. The default is Normal, which is a tentative compromise between both.

- **Connection timeout**:
  This is the maximum allowed amount of time without any exchange between machines. The default is 20 seconds, which sometimes is too short in low bandwidth environments or stressed and overload systems. If you are experiencing spontaneous disconnects, try setting a higher value, up to 120 seconds. The minimum value is 10 seconds

- **Reset all font sizes**:
  Clears the user-defined font sizes for every grid or table and re-establish the original values.

- **Clear Remote Host history**:
  Pressing this button, clears all past entries from the dropdown Remote Host list.

- **Clear grids on disconnect**:
  You can either clear all grids on disconnect or leave them untouched. Leaving them untouched is useful for post-mortem analysis.

- **Request authorization from remote**:
  If you check this box, the default action is: whenever you connect to a remote computer a request for authorization window will pop on the remote computer if someone is logged on. If no one is logged on, the connection will abort. This setting can be overridden by Policy under the File/Administration menu.
  You can configure some aspects of the Request for Authorization by pressing the Configure Request button, namely:
  - You can change the default message that will be seen by the remote computer.
  - You can set a different background color for the remote alert window (the default is red).
  - You can opt to have this same dialog appear every time you connect.

- **Connection Notification Frame on Remote**
  When selected, a small window, hereinwith called Frame, is placed on the remote computer, by default on top of the taskbar on its right side, to inform any remote user that there is an AWRCP connection underway. This Frame provides a hint identifying who made the connection and it can't be closed either locally or remotely while the connection takes place.

- **Remote keyboard active**:
  Keep this option checked if you want keystrokes to be passed to the remote

computer.

- **Autofill User Name and Password**:
  If checked, the User Name and Password used to connect are saved in the Registry and will autofill the respective boxes when the program launches. Selecting this option is a security risk when people not supposed to know your password may have access to the local computer. If selected, the User Name and Password boxes change color and by default a warning is shown each time the program closes.

- **Use Strong Encryption**
  When connecting through unknown networks, it is advisable to secure against eavesdropping and check this box. There is no significant performance penalty either.

- **Log connections**
  When checked all connections are logged and details retrieved by pressing the Connections Log button on the Desktop tab.

- **Connects with <ENTER>**
  When checked you can press the <ENTER> key, instead of pushing the Connect button, to establish a connection.

- **Full Screen hotkey**:
  This hotkey returns from full screen into normal mode (to enter into full screen mode from normal mode, press the button).
  The default is Ctrl+Alt+Z, but alternatively you can select any other suitable key sequence.
  Suitable sequences must have at least 2 each of Ctrl, Alt or Shift followed by a letter, number or function key. If you just press a letter, number or function key, the software will prefix those with Ctrl+Alt. Before accepting a new shortcut the software, will attempt to validate it. When validated you must press the Apply button to save and start using the new shortcut.
  Examples are: Ctrl+Alt+F9, Shift+Alt+1 or Ctrl+Shift+Alt+Z

- **Zebra colors**
  Let's you select one from the three sets of alternate colors to use in the grids.

4.3   Audio

All audio settings only become in force when the audio is initialized from the Audio & Text Chat tab.

- **Codecs**
  The user can suggest the compression codec (called here Priority Codec) to be used for the streaming between local and remote computers. However, it is not guaranteed that the Priority Codec is actuality present in either end of the connection. So, a negotiation will take place between local and remote computers, in order to decide which codec to use. If the Priority Codec cannot be used, the second choice will always be GSM 6.10 (see below).

  GSM 6.10
  This codec comes with every version of Windows and is good for voice and not too bad for music. Probably, you will stick with it in most situations.

The bit rate is 13kbs (about 102 KB/min)

MP3 Fraunhofer Layer-3 Professional
This codec comes with Windows XP and 2000. In Windows Vista and 7, the Professional edition (the one that can decode and encode) exists, but is not enabled, by default. Although, it is easy to enable it, in some countries, it may not be legal. For our implementation, the bit rate is either 8kps (60 KB/min) or 16kps (about 120 KB/min), depending on the negotiation between end points. This codec is good for music.

DSP Group TrueSpeech
This codec comes with Windows XP and 2000. It can also be downloaded from the internet for more recent Windows distributions. The bit rate is 8.5kps (about 62 KB/min). The quality of voice is not as good as with GSM 6.10, but it can be an option in extremely low bandwidth conditions.

- **Maximum Recorded File Size**
  To prevent recordings grow beyond what you expect, you can set a limit for the file size. The default is 10 MB, which gives approximately 5 minutes of decompressed, dual channel, recorded sound.

- **Sound Buffering**
  Slow computers or inconstant network conditions may require additional buffering to keep the sound flow as regular as possible. Although the default is set to Medium, you have to experiment by yourself and set according to your particular conditions. Note that for any buffer setting DirectSound latency is double the WaveOut latency.

4.4   Remote Service

Upon connection, AWRCP launches a service process on the remote computer. This service is the workhorse that receives, prepares and dispatches the instructions received from the local computer. The service will be either 32-bit or 64-bit (but can be changed to be always 32-bit) depending on the remote computer operating system.

Some users, have been requesting facilities for hiding even more the whereabouts of this service and we have done it.

- **File Name (32-Bit)**:
  You can change the 32-Bit binary name, which defaults to awrexec32P.exe. Any file name with the correct syntax is acceptable, even a file name without extension, something like My File Name is acceptable.

- **File Name (64-Bit)**:
  You can change the 64-Bit binary name, which defaults to awrexec64P.exe. Any file name with the correct syntax is acceptable, even a file name without extension, something like My File Name is acceptable.

- **Service Name (32-Bit):**
  Specifies the name of the 32-Bit service to install (up to a maximum of 256 characters). Forward-slash (/) and back-slash (\) are invalid service name characters.

- **Service Name (64-Bit):**
  Specifies the name of the 64-Bit service to install (up to a maximum of 256 characters). Forward-slash (/) and back-slash (\) are invalid service name characters.

- **Display Name (32-Bit):**
  Specifies the display name to be used by user interface programs to identify the 32-Bit service. The string has a maximum length of 256 characters. If the Display Name is blank, user interface programs may display the Service Name instead.

- **Display Name (64-Bit):**
  Specifies the display name to be used by user interface programs to identify the 64-Bit service. The string has a maximum length of 256 characters. If the Display Name is blank, user interface programs may display the Service Name instead.

- **Don't use random suffix**
  By default, in AWRCP, File Name (32-Bit), File Name (64-Bit), Service Name (32-Bit), Service Name (64-Bit), Display Name (32-Bit) and Display Name (64-Bit) add some random extra information to make them unique and allow a given remote machine to support simultaneous connections. You can disable this behaviour if the remote machine is not going to receive simultaneous connections. The local machine can still perform simultaneous connections to different machines if you check this option.

4.5   Updates

AWRCP supports manual and automatic updates (the default). When an update exists, and the user accepts to proceed with it, the new software is installed directly from the web with no need to run any setup or install program. Some updates may be installed only from here and not be available for download in our website in the traditional way through an install program, so you are recommended to check for updates regularly.

4.6   Advanced

- **Runs as 32-Bit on a 64-Bit Remote Operating System**
  This option should be left unchecked unless you have any particular reason to proceed otherwise.

- **Pings remote before attempting to connect**
  Leave it checked, unless the remote system can not be pinged for some reason.

- **Use IPv6 whenever possible**
  If checked AWRCP will attempt to connect with IPv6 if it finds an IPv6 on the Remote Host box or if it can resolve a name to an IPv6 address.

- **Check IPv4 and IPv6 internet availability at launch**
  Leave it unchecked if you know beforehand they are not available or you don't want to connect across the internet. The reason is that it may delay the launch a little bit if no internet is found immediately.

- **Local RDS/TS Client keeps GUI active when Minimized**
  Leave it checked if you plan to use AWRCP and a RDS/TS client at the same time. When unchecked, the RDS/TS client behaves as Gui-Less when minimized. This setting has effect only on the local computer (not the remote computer you are accessing).

5 Policy

5.1 Why Policy settings?

AWRCP is such a powerful software that some organizations don't feel comfortable allowing employees to use some of its features, connecting without identification and/or authorization or when no one is logged in.

For such reasons, someone in charge of software in the organization, namely the Network Administrator or other IT officer, has the capability to force AWRCP to comply with the organization's rules.
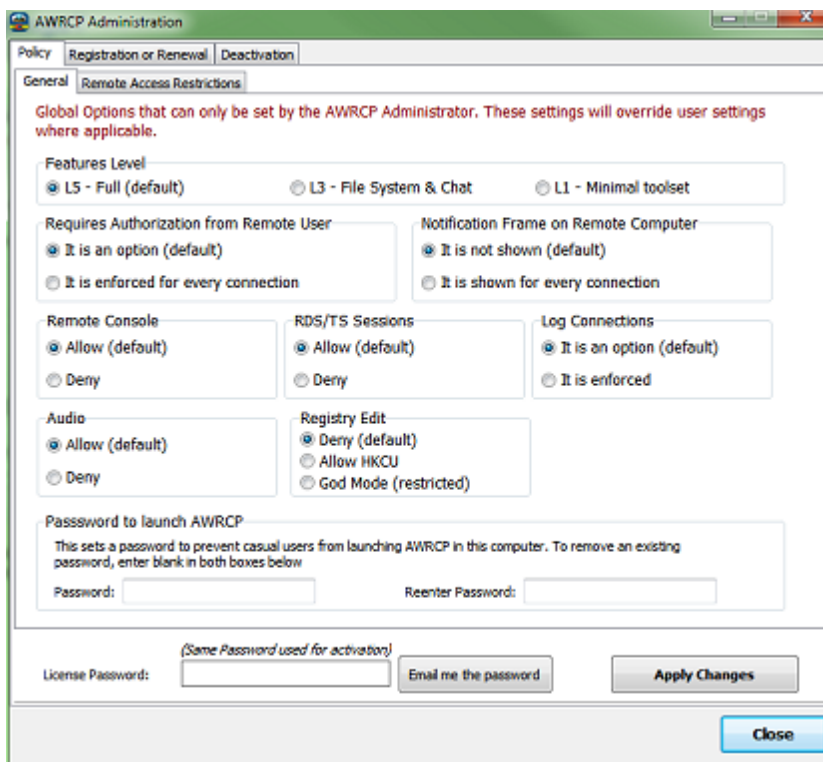
It is possible as well to deny remote access to some computers or, conversely, to allow remote access only to some computers.
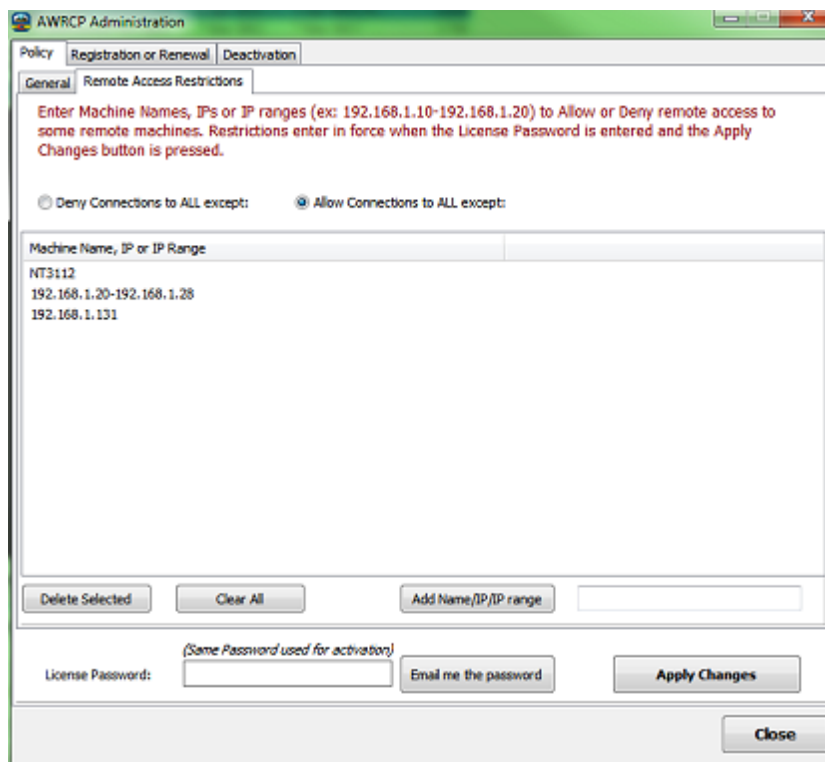
5.2   General Policy Settings

There are only 9 settings that can be changed but every combination is possible. We believe there is no need to add more settings, but we are all the time open to suggestions.
After you change the settings, enter the License Password you received from us (unless changed in the meantime from your web control panel) and press the Apply Changes button.

- **Features Level**
  AWRCP is so powerful that, within an organization, may not be desirable to allow everyone to use it to its full power. You can select from 3 Features Levels. Level L5 allows every feature and is the default.
  Level L3 hides or disables Installed Programs and Updates, Ports Finder, User and Groups, Hashes, Shutdown tools, Network Sweeper and Remote Console.
  Level L1, removes, hides or disables most other features, including File System manipulation facilities.
  Level L2 and L4 are reserved for future use..

- **Connection requires Authorization from Remote User**
  When enforced, the connection does not proceed without an explicit Authorization being received from the remote user. If no user is logged in, the connection aborts.

- **Connection shows a Notification Frame on Remote Computer**
  When connected to the remote computer a small frame is placed over the taskbar (defaults to the lower right corner of the screen for the usual bottom laid taskbar). This frame provides a tooltip identifying who made the connection. The frame can't be closed either locally or remotely while the connection lasts.

- **Remote Console**
  The use of the Remote Console may be denied from here.

- **RDS/TS Sessions**
  If company policy requires, you may disable remote access to Remote Desktop/ Terminal Service sessions as well as to Citrix XenApp applications launched from a Citrix XenApp server.

- **Log Connections**
  In order to comply with organizations' policies logging of connections can be enforced. The Log File integrity is monitored to prevent forging.

- **Audio**
  If company policy requires, you may disable the Audio facilities.

- **Registry Edit**
  Registry edition (create new keys or values, change, rename or delete them) is disable by default. By selecting "Allow HKCU" you will be able to edit subhives of HKEY_CURRENT_USER\Software (with the exception of Classes and Wow6432, when this one exists). Edition of other parts of the Registry (God Mode) is possible but the user must request from Atelier Web a special code to enable this feature.

- **Password to launch AWRCP**
  Do not confuse this password with the License Password. This password prevents casual users from launching AWRCP, the License Password is required to set the Policy and to Activate the software. Like most things in computing, the password will not deter a determined hacker, it is just good enough for the occasional lurker.
  The AWRCP Password feature is disabled in the Evaluation release, and after registration must be used only after the trial period has expired.

5.3   Remote Access Restrictions

Although Administrators are supposed to have unrestricted access permission to the computers they administer, even across the network, it is a fact of life that organizations do not always consider this acceptable.
There are 2 cases to consider:
- The most frequent is to restrict access by AWRC Pro to a limited number of machines, for example the notebooks of the members of the Board of Directors.
- The other case is to deny access to every computer in the organization, except to a limited number. This happens, for example when an AWRC Pro Seat can be used by different people (even no Administrators, namely using the Autofill User Name and Password option) to connect to a restricted number of computers in the organization.

To solve these problems, you can either "Deny Connections to ALL except" or

"Allow Connections to ALL except" a List of remote computers.
The List can be filled with Machine Names, IPs or IP ranges. IP ranges consists of 2 IPs separated by a dash (other characters are also accepted).

When the List is filled according to your requirements, enter the License Password you received from us (unless changed in the meantime from your web control panel). and press the Apply Changes button.

Notes:
1) Filling the list with many Machine Names will delay the start of the connection process to a remote computer, because the software may need to resolve Names to IPs to find matches. Even more serious is when the Machines Names simply do not exist in the network, here the DHCP server may take a long time to conclude just that.
2) When there are Access Restrictions in place, no version of AWRC Pro older than 11.3 will be able to run after the trial period has expired. What this means is that it will not be possible to make a temporary install of a previous version to circumvent the restriction (at least, without knowing the unlocking code). This makes the feature very solid in terms of security. Setting "Allow Connections to ALL", without machines on the List removes the restrictions and it is again possible to install older AWRC Pro versions.

6 FAQ

6.1 All Windows Releases

Q: How can I produce Ctrl+Alt+Del on the remote computer?
A: You can produce Ctrl+Alt+Del (the security attention sequence) by pressing

the CAD button ⌨.

Q: Why am I unable to connect to other remote computers?
A: Either within a local area network or across the Internet, AWRCP requires Microsoft Networks to be operative - Client for Microsoft Networks installed on both local and remote machines and File and Printer sharing enabled at least on the remote machine.
If the remote computer platform is Windows XP Professional, the access is only possible within the classical sharing and security model for local accounts. This is enabled from Control Panel / Administrative Tools / Local Security Policy / Network access: Classic - local users authenticate as themselves. You can obtain the same result from Windows Explorer / Tools / Folder Options / View and uncheck Use Simple File Sharing. (In Windows Vista and Windows 7 uncheck Use Sharing Wizard (Recommended). This will revert you to the classical model as well).

Q: How can a Domain Administrator connect to a workstation within Active Directory?
A: Enter the user name in the form User@Domain or Domain\User. Note: Sometimes it is necessary to launch (runAs) AWRCP.EXE as a Domain Administrator to connect to some machines.

Q: Which ports are used by AWRC?
A: AWRCP does not open any ports, it simply requires Microsoft Networks. Microsoft Networks use TCP port 445 (if a connection is not possible to TCP port 445, the system will try to connect to TCP port 139).

Q: You say that AWRCP is transparent to firewalls but I can't get it to work within my Company LAN!?
A: The firewall is blocking the use of Microsoft Networks, in particular TCP port 445. See the question above..

Q: How safe is AWRCP for use across the Internet?
A: Microsoft Networks, in particular port 445 is safe when you have a good password. Since all security is based on the password, all exploits are just password-guess dictionary attacks. A good password will take millions of years to be guessed. Additionally, AWRCP may use strong encryption which makes virtually unbreakable the data exchange between both end-points.

Q: Do I need to share any folders on the remote computer
A: No, you need File and Printer Sharing enabled but that does not mean you have to share any resources at all, and in general you must not do it.

Q: Can I use AWRCP across a VPN?
A: Yes, AWRCP works very well with the VPN products we are aware of. An advantage of VPNs, not always stressed, is that you don't have to be concerned with perimeter firewalls blocking port 445.

Q: How fast is AWRCP?
A: AWRCP was tested to be faster than every other remote access software we are aware off, including all VNC variants. It is not faster than software that use display mirror drivers (they need reboot to install drivers and reboot to uninstall).

Q: Why does the mouse flicker on the remote machine?
A: The mouse only flickers when View Layered Windows is selected in the Preferences (this is not the default). Due to hardware and OS implementation reasons, in most cases there is no way around it unless we used a display mirror driver. *Only in Windows XP and 2008/2008R2 you need to select View Layered Windows to view the layered windows. So, keep it deselected for Windows Vista and Windows 7 (unless DWM is disabled). For Windows 8 and later and for Windows Server 2012 and later keep it always deselected.*

Q: Does AWRCP work in Windows 64-bit Operating Systems?
A: The AWRCP remote agent runs natively as 64-bit on a 64-bit OS and runs natively as 32-bit on a 32 bit OS.

Q: How does AWRCP compare with other remote access software?
A: AWRCP is different, it is by far and large the most feature rich remote access software you can find (others say the same, please make yourself a favor and confirm who tells you the truth before taking a decision). AWRCP has an amazing performance and stability, great security features, you can instantly connect to any PC without installing any software on it, and since you do not pay per remotely accessed PC (like other softwares do) it is best deal you can close.

Q: How can I connect to another computer across the Internet?
A: The same rules apply, see the previous questions. If the local and remote computers are behind routers and personal firewalls you must make sure that:
- The local computer personal firewall allows outgoing connections on TCP port 445.
- The router on the remote network forwards TCP port 445 to the private IP address of the target machine.
- The personal firewall of the remote machine allows incoming connections on TCP port 445.

Q: When trying to connect, I get the error "The Network Path was not found"?
A: The connection is made by Microsoft Networks not by AWRCP. This is not an AWRCP error, it is a Windows error. Usually, it means that the remote machine is not connected to the network or has just been booted and the network is not yet aware of its existence. Wait a couple of minutes then retry.

Q: I have been trying and can not connect to my XP Home Edition laptop!?
A: You can not, have another look at the Requirements. XP Home Edition machines are severely crippled and can not be connected to with AWRCP.

Q: I have downloaded AWRCP from a third-party site and the program produces some strange errors.
A: You must download AWRCP from http://www.atelierweb.com/products/ AWRCP/awrc-pro-download/ or from sites that point to http://evalsoftware. atelierweb.com. Reverse-engineered warez releases of this software can not work as expected and have probably a trojan attached..

Q: How can I block connections from AWRCP?
A: AWRCBL, included in the distribution can block connection attempts from AWRCP and AWRC. Note that AWRCBL is not part of the AWRCP product, it requires registration.

Q: Is it possible to launch AWRCP from the command line and make a connection?
A: yes, it is possible. The syntax is:
Path\AWRCP.exe /r=<Remote Host> /u=<User> /p=<Password> /f (Full Screen)
For example:
"C:\Program Files\Remote Commander\AWRCP.exe" /r=192.168.1.100 / u=Administrator /p=Mypassword /f

6.2   Vista and later FAQ

In this page, when we mention Windows Vista the some answers still apply in full to Windows 7, Windows Server 2008/2008R2, Windows 8.x, Windows Server 2012/2012R2, Windows 10, (and will probably apply to all forthcoming releases).

Q: What versions of Vista are supported by AWRCP?
A: You can install AWRCP on any edition of Windows Vista and later, and you can connect to computers running any edition of these operating systems.

Q: Does AWRCP require Administrator privileges?
A: You do not need Administrator privileges on the machine where you install AWRCP - you can launch and run the software as a Standard User.
However, "by default", you need to be a Real Administrator on the remote Vista machine for the connection to succeed because, "by default", Vista does not allow Filtered Administrators to connect through the Administrative shares (C$, ADMIN$, etc.). You can connect as a Filtered Administrator by changing a single Registry key (see below).
```
Note: In Vista there are 2 classes of Administrators: Filtered
Administrators and Real Administrators. The built-in Administrator
account is set to be a Real Administrator account. Within a domain,
Domain Administrators are as well set to be Real Administrators. In
Vista, Real Administrators, behave like traditional Administrators
did in previous Windows versions.
```

Q: How do I enable the Real Administrator Account on a Vista machine?
A: Proceed as follows (see also next question):
1- Click Start, then type secpol.msc in the Search box and <enter>.
2- In the left pane, choose Local Policies/Security Options
3- Set Accounts: Administrator account status to Enabled.
4- Set User Account Control: Admin Approval Mode for the Built-in Administrator account to Disabled.

Q: How do I enable the Real Administrator Account on Vista Home Premium and Starter editions?
A: Proceed as follows:
1. Click Start, and then type cmd in the Start Search box.
2. In the search results list, right-click Command Prompt, and then click Run as Administrator.
3. When you are prompted by User Account Control, click Continue.
4. At the command prompt, type net user administrator /active:yes, and then press <enter>.
5. Type net user administrator <Password>, and then press <enter>.
Note: Please replace the <Password> tag with the password which you want to set to administrator account.
6. Type exit, and then press <enter>.

Q: Is it possible for Filtered Administrators to connect without disabling UAC (User Account Control) on the remote machine?
A: Yes, all you need is change (or add, if is not there, then change) a single key value in the Registry of the remote computer:
1- Click Start, then type regedit.exe in the Search box and <enter>.
2- Browse to HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Policies\ System
3- If it is not there, enter a new DWORD Value named LocalAccountTokenFilterPolicy
4- Set Value data of LocalAccountTokenFilterPolicy to 1
That's all.

Q: Why am I unable to connect to other remote computers?
A: Either within a local area network or across the Internet, AWRCP requires Microsoft Networks to be operative - Client for Microsoft Networks installed on both local and remote machines and File and Printer sharing enabled at least on the remote machine.
Also access is only possible within the classical sharing and security model for local accounts. This is enabled from Control Panel / Administrative Tools / Local Security Policy / Local Policies / Security Options / Network access: Classic - local users authenticate as themselves. You can obtain the same result from Windows Explorer / Tools / Folder Options / View and uncheck Use Sharing Wizard (Recommended). This will revert you to the classical model as well.

Q: Why am I unable to connect to some Vista and later computers?
A: If, within Active Directory, you can't connect to a remote workstation in the Domain, despite complying with all other requirements, there are several possibilities:
1- If you are logged into the workstation with a *built-in* account (i.e, either a local User or local Administrator account), we have not found issues connecting to any workstation in the domain.
2- If you are logged into the workstation as a Domain User or Domain Administrator, enter in the User Name box
RemoteWorkstationName\Administrator. Another alternative is to enter

Domain\DomainAdministratorAccount or simply *DomainAdministratorAccount* in the User Name box.

3- In a small number of cases, for no clear reason, it is necessary to launch Remote Commander elevated or *runAs* with a Domain Administrator account.

If you are in a Workgroup and want to connect to a computer within Active Directory that has not joined the Domain, connect by entering *RemoteWorkstationName\Administrator* in the User Name box.

If you are in a Workgroup and want to connect to a computer within Active Directory that has joined the Domain, you can connect either by entering *RemoteWorkstationName\Administrator or Domain\DomainAdministratorAccount* in the User Name box.

Q: Can DEP (Data Execution Prevention) cause connection failures?
A: We are not aware of any problems with AWRCP.

7 License and Purchasing

7.1 License

License Terms and Agreement for AWRCP (Atelier Web Remote Commander Professional)

IMPORTANT: DO NOT CLICK ON THE "Buy" BUTTON, EITHER INSIDE THE SOFTWARE OR IN THE WEBSITE, UNTIL YOU HAVE READ THIS AGREEMENT. BY CLICKING ON THE "Buy" BUTTON, YOU ACCEPT ALL OF THE TERMS OF THIS AGREEMENT. IF YOU DO NOT ACCEPT ALL OF THE TERMS OF THIS AGREEMENT DO NOT CLICK ON THE "Buy" BUTTON,

AWRCP ("Software") is licensed, not sold, to you for use only under the terms of this License Agreement ("Agreement"). Jose Pascoa ("Licensor") continues to own the Software and reserves any rights not expressly granted to you.

1. GRANT OF LICENSE.

The Licensor grants to you, subject to the terms and conditions of this Agreement and payment of all applicable license fees, a nonexclusive, non-transferable right to use the Software. This Agreement grants to you the right to install and use the Software on a number of computers up to the Seats number specified in your purchase.

The term "Licensed User" means the user to whom Licensor issues an Unlocking Code and License Password to enable the Software upon such user's acceptance of the terms of this Agreement and payment of the applicable license fee. Ownership of, and title to, the Software and any manuals, guides or any other printed material that Licensor provided to you for use with the Software ("Documentation") is and will be held by Licensor and its licensors.

2. PROTECTION OF SOFTWARE.

You acknowledge that the source code for the Software and other trade secrets embodied in the Software have not been, and are not going to be, disclosed to you. Modifications of, additions to, or deletions from the Software (including any deletion or addition of code) are strictly prohibited. Except as specifically permitted in this Agreement, you agree not to, directly or indirectly, (1) use any Confidential Information to create any software or documentation that is similar to any of the

Software or Documentation; (2) reverse engineer, disassemble or decompile the Software; (3) encumber, transfer, sublicense, rent, lease, time-share or use the Software in any service bureau arrangement; or (4) copy (except as provided herein), distribute, manufacture, adapt, create derivative works of, translate, localize, or otherwise modify Software or permit any third party to engage in any of the acts proscribed in clauses (1) through (4). You agree not to remove or alter any printed or on-screen copyright, trade secret or other legal notices contained on or in the Software or the Documentation.

3. OWNERSHIP.

Licensor retains all of its respective rights, title and interest in the Software and the Documentation, including without limitation any and all patents, patent applications, copyrights, trade secrets, trademarks and other intellectual property rights, and you agree not to take any action inconsistent with such title and ownership. YOU ACKNOWLEDGE AND AGREE THAT THE SOFTWARE MAY CONTAIN CODE OR REQUIRE DEVICES THAT DETECT OR PREVENT UNAUTHORIZED USE OF THE SOFTWARE

4. DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY.

.1 Disclaimer of Warranty.

YOU ACKNOWLEDGE THAT THE SOFTWARE AND THE DOCUMENTATION ARE BEING SUPPLIED TO YOU ON AN "AS IS" BASIS. LICENSOR HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES REGARDING THE SOFTWARE AND THE DOCUMENTATION, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT, AS WELL AS ALL WARRANTIES ARISING BY USAGE OF TRADE AND COURSE OF DEALING. LICENSOR DOES NOT WARRANT THAT (A) THE SOFTWARE WILL MEET YOUR REQUIREMENTS, (B) OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR (C) DEFECTS WILL BE CORRECTED. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU. To the extent permissible, any implied warranties are limited to ninety (90) days.

4.2 Limitation of Liability.

LICENSOR'S LIABILITY FOR DAMAGES TO LICENSEE FOR ANY CAUSES WHATSOEVER, REGARDLESS OF THE FORM OF ANY CLAIM OR ACTION, SHALL NOT EXCEED THE AGGREGATE FEES PAID BY Y0U FOR THE SOFTWARE. LICENSOR SHALL IN NO EVENT BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF DATA, INTERRUPTION OF BUSINESS, OR FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND, WHETHER UNDER THIS AGREEMENT OR OTHERWISE ARISING IN ANY WAY IN CONNECTION WITH THE SOFTWARE, THE DOCUMENTATION OR THIS AGREEMENT, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

5. USER INFORMATION.

5.1 Registration.

To register the Software you will be required to enter the unique Unlocking Code and to Activate (connection to the internet is required for this, but if you do not have an internet connection there is an alternative offline procedure) you will be required to enter the License Password. You are responsible for maintaining the confidentiality of your Unlocking Code and License Password. The same Unlocking Code will be used to register all the Seats you purchased. After purchase, you will be provided with a License Control Panel from where you will be able to change the License Password and Email Address. You will also be able to view the Seats if you have activated.

5.2 Seat Management

You can Deactivate Seats from some computers and Activate them on other computers any number of times. Deactivation must be done in place on the computer being Deactivated, not from the License Control Panel. If you do not have anymore physical access to that computer, you can contact the Licensor providing the name of the computer you need to deactivate the Seat for. There is a cooling period of 48 hours before the Deactivated Seat is returned to the pool of available Seats.

6. EVALUATION VERSION

Provided that you verify that you are distributing the Evaluation version (select the About in the main menu of the Software to check) you are hereby licensed to make as many copies of the Evaluation version of the Software and Documentation as you wish; give exact copies of the original Evaluation version to anyone; and distribute the Evaluation version of the Software and Documentation in its unmodified form via electronic means. There is no charge for any of the above.
You are specifically prohibited from charging, or requesting donations, for any such copies, however made; and from distributing the Software and/or Documentation with other products (commercial or otherwise) without prior written permission from Licensor.

7. GENERAL

In the event that any provision of this Agreement shall, in whole or in part, be determined to be invalid, unenforceable or void for any reason, such determination shall affect only the portion of such provision determined to be invalid, unenforceable or void, and shall not affect in any way the remainder of such provision or any other provision of this Agreement.

7.1 Severability.

In the event that any provision of this Agreement shall, in whole or in part, be determined to be invalid, unenforceable or void for any reason, such determination shall affect only the portion of such provision determined to be invalid, unenforceable or void, and shall not affect in any way the remainder of such provision or any other provision of this Agreement.

7.2 Waiver.

The waiver by either party of a breach or a default of any provision of this Agreement by the other party shall not be construed as a waiver of any succeeding breach of the same or any other provision, nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has, or may have hereunder, operate as a waiver of any right, power or privilege by such party.

7.3 Entire Agreement; Amendment.

This Agreement constitutes the entire agreement between the parties with regard to the subject matter hereof and supersedes all prior understandings and agreements, whether written or oral, as to such subject matter. No waiver, consent, modification or change of terms of this Agreement shall bind either party unless in writing signed by both parties, and then such waiver, consent, modification or change shall be effective only in the specific instance and for the specific purpose given.

7.4 Assignment.

This Agreement and the rights and obligations hereunder, may not be assigned, in whole or in part by Licensee, without the prior written consent of Licensor. In the case of any permitted assignment or transfer of or under this Agreement, this Agreement or the relevant provisions shall be binding upon, and inure to the benefit of, the successors, executors, heirs, representatives, administrators and assigns of the parties hereto.

7.5 Privacy.

During Activation no personal information or information about your computer configuration is transferred. It is transferred only the Computer Name, the License Password, and a one-way hash that guarantees the uniqueness of identification. On the first Activationthe Email Address you used when purchasing is also transferred. Currently, the Activation Server is not lodged in the Licensor website but with a reputable and established company with more than fifteen years in business called Softworks.

8. LAW
This agreement shall be governed by the laws of the Republic of Portugal.

9. ACKNOWLEDGMENTS
You acknowledge that (a) you have read and understand this Agreement; and (b) that this Agreement has the same force and effect as a signed agreement.

7.2   Purchase

This is not free software. Subject to the terms of the License Agreement, you are hereby licensed to use this software for evaluation purposes without charge for a period of 15 days. In order to use this software after the evaluation period you are required to register it.

Ordering Information:

For pricing information and register online, please visit: http://www.atelierweb.com/products/AWRCP/awrc-pro-order/
Any time, feel free to contact us through the contact forms at http://www.atelierweb.com/index.php/contact-support/.