

Atelier Web Remote Commander

USER MANUAL

Updated for AWRC release 14.7

1.	Program	4
1.1	Overview	4
1.2	Features	4
1.3	Requirements	6
1.4	Getting started	6
1.5	Saving, Copying to Clipboard and Printing	7
1.6	Adjusting the Viewing area	7
1.7	Adjusting Fonts	8
1.8	Image Scaling	8
1.9	Clipboard Transfers	8
1.10	Encryption	8
1.11	AWRC Password	9
1.12	Logging Connections	9
1.13	Multiple Monitors	9
2.	Function Tabs	10
2.1	Desktop	10
2.2	SysInfo	10
2.2.1	General	10
2.2.1.1	Monitor(s) Info	11
2.2.2	Hardware Devices	13
2.2.3	Processes	13
2.2.4	Services	15
2.2.5	Physical Memory Viewer	15
2.3	NetworkInfo	16
2.3.1	Shares	16
2.3.2	Ports Finder	16
2.3.3	Ports Statistics	16
2.3.3.1	Connections and Listening Ports	16
2.3.3.2	TCP Statistics	17
2.3.3.3	UDP Statistics	18
2.3.3.4	ICMP Statistics	18
2.3.4	Routing	20
2.3.4.1	Routing Table	20
2.3.4.2	DNS Servers	21
2.3.4.3	Persistent Routes	21
2.3.5	IP/Transport Protocols	21
2.3.5.1	IP Statistics/Settings	21
2.3.5.2	Installed Protocols	23
2.3.5.3	Address Information Table	27
2.3.5.4	Net to Media Table	27
2.3.6	Interfaces	27

2.4	File System	29
2.5	Users and Groups	31
2.5.1	Users	31
2.5.2	Groups	32
2.5.3	Password Hashes	33
2.6	Chat	33
3.	Tools	34
3.1	Shutdown	34
3.2	Save Remote Screen	34
4.	Preferences	34
4.1	Desktop	34
4.2	General	35
4.3	Remote Service	37
4.4	Updates	37
4.5	Advanced	37
5.	FAQ	38
5.1	All Releases FAQ	38
5.2	Vista and later FAQ	40
6.	License and Purchasing	42
6.1	License	42
6.2	Purchase	45
	Index	46

1 Program

1.1 Overview

Atelier Web Remote Commander 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 AWRC you will immediately notice that you are dealing with a completely different sort of tool.

- AWRC 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.
- Unlike other remote control software, mostly concerned with viewing the remote screen, AWRC 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 AWRC you can know and do virtually anything on the remote computer!
- AWRC is safe. A remote user, without Administrator privileges, can not gain higher privileges by controlling AWRC operation on the remote system.
- It is inexpensive but not *cheap*. Don't assume paying more will bring you more, AWRC is the most powerful tool you can find. With other remote software, you need one license for each machine you want to remotely access, with AWRC 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:

- 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.
- Supports multiple (any number) of monitors on the remote computer, you can view and work on any one of them.
- 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.
- 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, Serial 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).
- Complete and detailed Hardware Devices list.
- Physical memory viewer.
- 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 and Interface Statistics/Settings.
- 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 AWRC 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, AWRC will handle 5 to 10 (or more) simultaneous connections without problems on most PCs. No configuration is necessary.
- A remote computer can be connected simultaneously by multiple AWRC clients.
- Full Unicode supported.

1.3 Requirements

You must have the following to use this product:

- PC compatibles 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:**
Server 2019, Windows 11, 10, Server 2022, 2019, 2016, 8.1, 8.0, Server 2012/2012R2, 7, Server 2008/2008R2, Vista, XP, Server 2003/2003R2, 2000 and Server 2000. Works both in 32-bit and 64-bit operating system versions. .
- **On the Remote System:**
Server 2019, Windows 11, 10, Server 2022. 2019, 2016, 8.1, 8.0, Server 2012, 7, Server 2008/2008R2, Vista, XP (only Professional, Home edition not supported), Server 2003/2003R2, 2000 and Server 2000. Works both in 32-bit and 64-bit operating system versions.
- 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
- 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.

1.4 Getting started

It is amazingly simple to get started with AWRC.

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 tick the Remote Keyboard check box, 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 (always checked in the PB Build) 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 (always

checked in the PB and Standard Build).

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](#) or look for an updated FAQ in our website at <http://www.atelierweb.com/products/awrc/awrc-faq/> or <http://www.atelierweb.com/products/awrc/vista-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.

1.5 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).

The remote desktop can also be saved in .JPG or .BMP formats by pressing the Save button on the Desktop page or from the menu at Tools/Save Screen.


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.

1.6 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.

1.7 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.

1.8 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.

1.9 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.
AWRC 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.

1.10 Encryption

AWRC 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, AWRC 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:

AWRC 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 AWRC encryption and decryption are very fast, you may keep Strong Encryption always on without significant performance penalty.

AWRC 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.

1.11 AWRC Password

You can prevent other users from launching AWRC by setting a password under Preferences. If you forget the password you will have to reinstall the software. Since reinstalling removes the password protection, you may want to investigate why it has been done.

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.** 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 AWRC logged in first.

In the PB Build, logging is enforced and the Log File is monitored for integrity. If the Log File is deleted or modified, the software will have to be reinstalled, and you may want to investigate why it has been done..

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 AWRC 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.

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 AWRC 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).

By pressing the Save button, screen captures can be saved in BMP format for later viewing.

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

- 16 Colors (4 bit)
- 256 Colors (8 bit)
- 65536 Color (16 bit)
- True Color (24 bit)
- True Color (32 bit)

The first (16 Colors) is suited for problematic traffic conditions, the third (65536 Colors) is the default, but 256 Colors is normally a good option since it increases responsiveness. AWRC 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 SysInfo

2.2.1 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, Serial Number, Local Time, Last Boot time, Uptime, Anti-Spyware installed and Last Automatic Updates.
- **Processor Information:** Manufacturer, Vendor ID, CPU name, Family, Model, Stepping, Raw frequency and Norm frequency, Cache, SIMD and other diversified information.
- **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 not use the slow (and deprecated) APIs we were accustomed. In the rare occasions that SMBIOS ROM information is not available, AWRC 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.**

2.2.1.1 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 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 $\|(X,Y,Z)\| = 1$. Enter topic text here.

2.2.2 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 a remote machine.

2.2.3 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 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.
- **Peak 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.

2.2.4 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.

2.2.5 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 NetworkInfo

2.3.1 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).

2.3.2 Ports Finder

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.

2.3.3 Ports Statistics

2.3.3.1 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:

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

2.3.3.2 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.

2.3.3.3 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.

2.3.3.4 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.

2.3.4 Routing

2.3.4.1 Routing Table

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.

2.3.4.2 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

(1) FQDN means Fully Qualified Domain Name, i.e, a domain name that indicates with 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 which they have complete information.

(3) Authoritative information is organized into units called ZONES, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.

2.3.4.3 Persistent Routes

By default, the routes in the routing table are not permanent, they are lost when the computer is rebooted. In Windows NT, 2000, XP or 2003, it is possible to make some routes permanent using the console program route.exe with the command route -p ip_address.

2.3.5 IP/Transport Protocols

2.3.5.1 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.

2.3.5.2 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 known 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_EN
TRIES | 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_PRO | Indicates that this is the recommended or most |

TO_ENTRY	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.

0xFFFF The protocol is message-oriented, but there is no maximum limit to the size of messages that may be transmitted.

FFF

2.3.5.3 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.

2.3.5.4 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

2.3.6 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.

2.4 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 AWRC!).

- **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 AWRC 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 AWRC 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	Uses the credentials of the user that is logged on the remote computer.
User:	
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 AWRC 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. AWRC 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 AWRC 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. AWRC 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. AWRC 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 operation 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.

2.5 Users and Groups

2.5.1 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'.

2.5.2 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.

2.5.3 Password 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.

AWRC 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, it can take from a few seconds to days, months or years. Some software, like L0phtCrack, given the time can work out the hashes and come up with the original passwords.

If using L0phtCrack, select the option to import from PWDUMP, in order to enter the AWRC saved hashes into L0phtCrack.

Note: PWDUMP is a command line utility which 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.

Weak passwords are retrieved from the hashes in a matter of minutes, sometimes seconds. Always use long strong passwords in a mix of !,*,{,\$,*,#,% characters, uppercase, lowercase English characters and digits! Although all passwords are retrievable from the hashes you should make it as hard as possible.

(*) On AWRC, this feature is not available when the remote computer is running a 64-bit operating system, because AWRC runs as 32-bit on the remote computer (it is available on AWRC Pro, because by default it runs as 64-bit on 64-bit operating systems).

2.6 Chat

You can carry a live conversation with the interactive user on the remote computer. You should take the initiative for the Chat. AWRC 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.

3 Tools

3.1 Shutdown

The following operations can be performed from *Shut down* submenu:

- **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.

3.2 Save Remote Screen

From the *Save Screen* submenu, 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 by pressing the Save button on Desktop page.

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 frozen.
- **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 16 Colors (4-bit), 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 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 and boxes on disconnect:**
You can either clear all grids and boxes 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 AWRC 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 Remote Service

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

- **File Name:**
You can change the binary name, which defaults to awrexec.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:**
Specifies the name of the service to install (up to a maximum of 256 characters). Forward-slash (/) and back-slash (\) are invalid service name characters.
- **Display Name:**
Specifies the display name to be used by user interface programs to identify the 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 AWRC, File Name, Service Name and Display Name add some random extra information to make them unique and make a remote machine support simultaneous connections. You can disable this behaviour if you don't need simultaneous connections to a remote machine. The local machine can still perform simultaneous connections to different machines if you check this option.

4.4 Updates

AWRC supports manual (the default) and automatic updates. 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.


4.5 Advanced

- **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 AWRC 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.
- **Password**
To request a password when launching AWRC, check the box I want a password for AWRC.
Enter the password in the two boxes below, then press the Apply button.
To remove the password, just uncheck the box I want a password for AWRC.

5 FAQ

5.1 All Releases FAQ

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, AWRC 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) AWRC.EXE as a Domain Administrator to connect to some machines.

Q: Which ports are used by AWRC?

A: AWRC 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 AWRC 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 AWRC 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, AWRC 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 AWRC across a VPN?

A: Yes, AWRC 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 AWRC?

A: AWRC was tested to be faster than every other remote access software we are aware of, 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 AWRC work in Windows 64-bit Operating Systems?

A: AWRC can run and can connect to any 64-bit OS.

Q: How does AWRC compare with other remote access software?

A: AWRC is different, with the exception of AWRC Pro, 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). AWRC 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 AWRC. This is not an AWRC 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 AWRC.

Q: I have downloaded AWRC from a third-party site and the program produces some strange errors.

A: You must download AWRC from <http://www.atelierweb.com/products/awrc/awrc-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 AWRC?

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

Q: Is it possible to launch AWRC from the command line and make a connection?

A: yes, it is possible. The syntax is:

Path\awrc.exe /r=<Remote Host> /u=<User> /p=<Password>

For example:

"C:\Program Files\Remote Commander\awrc.exe" /r=192.168.1.100 /
u=Administrator /p=Mypassword

5.2 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, 10 (and will probably apply for all forthcoming releases).

Q: What versions of Vista are supported by AWRC?

A: You can install AWRC on any edition of Windows Vista and later, and you can connect to computers running any edition of these operating systems.

Q: Does AWRC require Administrator privileges?

A: You do not need Administrator privileges on the machine where you install AWRC - 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, AWRC 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 AWRC.

6 License and Purchasing

6.1 License

License Terms and Agreement for AWRC (Atelier Web Remote Commander) Version 10 or later

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,

AWRC ("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 YOU 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 you have activated.

5.2 Seat Management

For Single Computer Licenses (also called 1 Seat Licenses), you can transfer or reactivate your license in another computer that you own (maximum 2 times every 30 days).

For 2 or more Seats Licenses, you can Deactivate Seats in some of the 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 Activation the 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.

6.2 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/awrc/awrc-order/>

Any time, feel free to contact us through the contact forms at <http://www.atelierweb.com/index.php/contact-support/>.

- 6 -

64-bit Operating Systems 38

- A -

Active Directory 33

Address Information Table

Interface index 27

IP 27

Largest IP datagram can reassemble 27

LSB in IP non-unicast address 27

Sub-net mask 27

Administrator privileges 40

Auto 10

AWRC Password 9, 37

- B -

BIOS

SMBIOS ROM 10

Blowfish 8

- C -

CAD 38

Chat 33

Check for product Updates 38

Client for Microsoft Networks 6, 16, 38

Clipboard

local 8

remote 8

transfers 8

command handler initialization 38

Command line 38

Configure

Desktop 34

General 35

Remote Service 37

Updates 37

Connections and Listening Ports

closed 16

closeWait 16

established 16

finWait1 16

finWait2 16

lastAck 16

listening 16

synReceived 16

synSent 16

TCP 16

timeWait 16

UDP 16

Control Alt Delete 38

Copy to clipboard 7

Credential 6

Ctrl+Alt+Del 4, 7, 38

- D -

Data Execution Prevention 40

Date and time started and ended 9

DEP 40

DEP (Data Execution Prevention) 38

Desktop 10

Default Scale 34

Desktop Colors 34

Maintain Full-Screen aspect ratio 34

Permanent mouse pointer 34

Refresh rate 34

See remote mouse activity 34

View Layered Windows 34

View-Only Mode 34

Display Adapter

BIOS 10

Chipset 10

DAC 10

Font Resolution 10

Memory 10

Model 10

Screen Metrics 10

Video modes 10

Display Name 37

DNS Servers

authoritative 21

FQDN 21

Fully Qualified Domain Name 21

zones 21

Dual Monitors 9

- E -

Ease of Access Center 40

Elliptic-Curve 8

encryption 8

Enforced Logging in PB Build 9

- F -

FAQ 38

- Features 4
- File and Printer Sharing 6, 16, 38
- File Name 37
- File System 29
 - Capacity 29
 - Copy Files or Directories 29
 - Delete Files and Directories 29
 - Download Files 29
 - File System 29
 - Free space 29
 - Label 29
 - Launch File 29
 - Logical Drive 29
 - Make Directory 29
 - Move Files or Directories 29
 - Rename File or Directory 29
 - Serial Number 29
 - Type 29
 - Unzip Files 29
 - Upload Files 29
 - Zip Files 29
- Filtered Administrators 40
- firewall 38
- Fonts
 - Ajusting fonts 8
- Frequently Asked Questions 38

- G -

- General
 - Reset all font sizes 35
- General
 - Autofill User Name and Password 35
 - Clear grids on disconnect 35
 - Clear Remote Host history 35
 - Compress Image 35
 - Compression level 35
 - Connection timeout 35
 - Connects with <ENTER> 35
 - Default scale 35
 - Full Screen hotkey 35
 - Interface 35
 - Log connections 35
 - Maintain Full-Screen aspect ratio 35
 - Remote Ctrl+Alt+Del keyboard shortcut 35
 - Remote keyboard active 35
 - Request authorization from remote 35
 - See remote mouse activity 35
 - View Layered Windows 35
- Getting started 6
- Groups

- Attribute 32
- Comment 32
- Group Enabled 32
- Group Enabled by Default 32
- Group Mandatory 32
- Names 32
- SID 32

- H -

- Hardware Devices 13
- Hashes 33

- I -

- ICMP Statistics
 - Address mask replies 18
 - Address masks 18
 - Destination unreachable 18
 - Echo replies 18
 - Echos 18
 - Errors 18
 - Messages 18
 - Parameter problems 18
 - Redirects 18
 - Source quenches 18
 - Time exceeded 18
 - Timestamp replies 18
 - Timestamps 18
- Image Scaling 8
- Installed Protocols
 - Protocol details 23
- Interfaces
 - Adapter physical address 27
 - Admin status 27
 - Bytes received 27
 - Bytes transmitted 27
 - Description 27
 - Inbound packets discarded 27
 - Inbound packets discarded unknown protocols 27
 - Inbound packets with errors 27
 - Index 27
 - MIB specific information 27
 - MTU 27
 - Operational status 27
 - Outbond packets discarded 27
 - Outbond packets with errors 27
 - Output packet queue 27
 - Packets delivered non-unicast 27
 - Packets delivered unicast 27

Interfaces

- Packets requested non-unicast 27
- Packets requested unicast 27
- Speed 27
- Type 27

IP Statistics/Settings

- Acting as IP router 21
- Datagrams failing fragmentation 21
- Datagrams forwarded 21
- Datagrams successfully fragmented 21
- Default TTL 21
- Discarded output packets 21
- Fragments created 21
- Output packet no route 21
- Output requests 21
- Packets received 21
- Reassembly failures 21
- Reassembly required 21
- Reassembly successful 21
- Reassembly time-out (sec) 21
- Received address errors 21
- Received header errors 21
- Received packets delivered 21
- Received packets discarded 21
- Routing discards 21
- Unknown protocols received 21

IPv6 37

- L -

- L0phtCrack 33
- Last Boot 10
- Licence 42
- linear address 15
- Local Time 10
- Local User/Connected As 9
- Logging Connections 9
- Logical Local Printers 10
- low-bandwidth 10

- M -

- Memory 10
 - Free Physical Memory 10
 - Page File Free 10
 - Total Page File 10
 - Total Physical Memory 10
- Monitor(s) Info 11
- Multiple Monitors 9

- N -

Net to Media Table

- Interface index 27
- IP address 27
- Media dependent physical address 27
- Type of mapping 27

- O -

- Operating System 10
- Options 35
- Organization 10
- Overview 4

- P -

- Page File Free 10
- page table 15
- Password 33, 37
- Password Hashes 33
- Persistent Routes 21
- Phone home 38
- physical address 15
- Physical Memory Viewer 15
- Pings remote before attempting to connect 37
- Ports finder 16
- Ports used by AWRC 38
- Preferences
 - Advanced 37
- Print 7
- Printing 7
- Processes
 - Kill process 13
 - Remote Power-Off 13
 - Remote Reboot 13
 - Remote shutdown 13
- Processor 10
 - CPU name 10
 - Family 10
 - Manufacturer 10
 - Model 10
 - Norm frequency 10
 - Raw frequency 10
 - Stepping 10
 - Vendor ID 10
- Protocol details
 - Address Family 23
 - Catalog Entry ID 23
 - Connect Data 23

Protocol details

- Connectionless 23
- Disconnect Data 23
- Expedited Data 23
- Graceful Close 23
- Guaranteed Delivery 23
- Guaranteed Order 23
- IFS Handles 23
- Max Socket Address Length 23
- Message Oriented 23
- Message Size 23
- Min Socket Address Length 23
- Network Byte Order 23
- Number of Chain Entries 23
- Partial Messages 23
- Protocol 23
- Protocol Max Offset 23
- Provider Flags 23
- Provider ID 23
- Pseudo Stream 23
- QoS Supported 23
- Security Scheme 23
- Socket Type 23
- Supports Broadcast 23
- Supports Multipoint 23
- Unidirectional Receives 23
- Unidirectional Sends 23
- Version 23

PWDUMP 33

- R -

- Real Administrator 40
- Register 45
- Registered User 10
- Remote Host 9
- Remote Interactive User 9
- Remote keyboard 6, 10
- Remote Service
 - Display Name 37
 - File Name 37
 - Service Name 37
- Requirements 6
- Routing Table
 - Gateway address 20
 - Interface index 20
 - IP 20
 - IP Route mask 20
 - MIB Route info 20
 - Route age (sec) 20
 - Route metric 1 (primary) 20

- Route metric 2-5 (alternate) 20
- Routing mechanism 20
- Type of route 20

- S -

- Save Screen 34
- Saving 7
- Serial Number 10
- Service Name 37
- services 8
 - File System Drivers 15
 - Kernel Device Drivers 15
 - Pausing 15
 - Resuming 15
 - Starting 15
 - Stopping 15
 - Unloading 15
- Session Key 8
- Shares 8
 - Communication devices 16
 - Drives 16
 - Interprocess Communication devices 16
 - Print Queues 16
- Syskey 33

- T -

- task switch 15
- TCP Statistics
 - Active Opens 17
 - Current connections 17
 - Failed connection attempts 17
 - Maximum number of connections 17
 - Maximum retransmission time-out (msec) 17
 - Minimum retransmission time-out (msec) 17
 - Passive Opens 17
 - Reset connections 17
 - Retransmission time-out algorithm 17
 - Segments received 17
 - Segments received in error 17
 - Segments retransmitted 17
 - Segments sent 17
 - Segments sent with RST flag 17
- Terminal Services 38
- Tools
 - Remote Hibernate 34
 - Remote Power-Off 34
 - Remote Reboot 34
 - Remote shutdown 34
 - Remote Standby 34

Traditional 35

- U -

UDP Statistics

Datagrams received 18

Datagrams sent 18

No ports 18

Receive errors 18

Uptime 10

Use IPv6 whenever possible 37

Users

Account expires 31

Comment 31

Domain 31

Flags 31

Full Name 31

Identifier authority 31

Last Logoff 31

Last Logon 31

Password Age 31

Primary Global Group 31

Privilege Level 31

Revision 31

RID 31

SID 31

Subauthorities 31

User Account 31

User ID 31

Workstations can log from 31

- V -

Viewing Area

Adjusting the Viewing Area 7

aspect ratio 7

Ctrl+Alt+Z 7

Full-Screen 7

Vista Home Edition 38

VPN 38

- W -

Windows Classic 35

- X -

XP Home Edition 38