

# Table of Contents

<b>Part I Program</b>	<b>3</b>
1 Overview .....	3
2 Features .....	3
3 Requirements .....	4
4 Getting started .....	5
5 Saving, Copying to Clipboard and Printing .....	6
6 Adjusting the Viewing area .....	6
7 Adjusting Fonts .....	6
8 Image Scaling .....	6
9 Clipboard Transfers .....	7
10 Encryption .....	7
11 AWRC Password .....	7
12 Logging Connections .....	8
13 Multiple Monitors .....	8
<b>Part II Function Tabs</b>	<b>8</b>
1 Desktop .....	8
2 SysInfo .....	9
General .....	9
Hardware Devices .....	9
Processes .....	9
Services .....	10
Physical Memory Viewer .....	10
3 NetworkInfo .....	11
Shares .....	11
Ports Finder .....	11
Ports Statistics .....	11
Connections and Listening Ports .....	11
TCP Statistics .....	12
UDP Statistics .....	13
ICMP Statistics .....	13
Routing .....	14
Routing Table .....	14
DNS Servers .....	15
Persistent Routes .....	16
IP/Transport Protocols .....	16
IP Statistics/Settings .....	16
Installed Protocols .....	17
Address Information Table .....	22
Net to Media Table .....	22
Interfaces .....	22
4 File System .....	24

<b>5 Users and Groups</b> .....	<b>26</b>
Users .....	26
Groups .....	27
Password Hashes .....	28
<b>6 Chat</b> .....	<b>28</b>
<b>7 Configure</b> .....	<b>28</b>
Desktop .....	28
General .....	29
Remote Service .....	31
Updates .....	31
Password .....	31
Advanced .....	32
<b>Part III FAQ</b> .....	<b>32</b>
1 All Releases FAQ .....	32
2 Vista and later FAQ .....	35
<b>Part IV AWRC BLocker (AWRCBL)</b> .....	<b>0</b>
<b>Part V License and Purchasing</b> .....	<b>36</b>
1 License .....	36
2 Purchase .....	37
<b>Index</b> .....	<b>0</b>

# 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.
- Access to the remote computer logon screen, enabling connections before any user has logged on to the remote machine.
- Supports multiple monitors (up to 10) on the remote computer, you can view and work on any of them.
- Supports User Switching sessions on Windows XP Pro and later (Vista, Windows 7, 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. The default hotkey is Ctr+Alt+D.
- 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.

## 1.3 Requirements

**You must have the following to use this product:**

- PC compatibles on local and remote systems with Pentium II/III 600 or higher. Pentium/AMD

- 1000 or higher recommended.
- Works in systems with the minimum RAM recommended for the Operating System.
  - **On the Local System:**  
Windows 7 (all editions), Windows Server 2008/2008R2 (all editions), Windows Vista (all editions), Windows XP (all editions), Server 2003/2003R2 (all editions), Windows 2000 (all editions). Works both in 32-bit and 64-bit operating system versions.
  - **On the Remote System:**  
Windows 7 (all editions), Windows Server 2008/2008R2 (all editions), Windows Vista (all editions), Windows XP (only Professional, **Home edition not supported**), Server 2003/2003R2 (all editions), Windows 2000 (all editions) and Windows NT 4.0 Sp6a operating systems (all editions). 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.

Press the Connect button.

If you want to request authorization from the remote before starting operations on it, check the box "Request authorization" before pressing the Connect button.

If you 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/rcomm/faq.htm>.
3. If still unsuccessful, contact us through a form at <http://www.atelierweb.com/support.htm>. 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.


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 or Ctrl+Alt+Z (or the hotkey you have defined under Configure) 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.

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 Configure. 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.

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 [Configure](#).

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

If you are an Administrator on the local machine where AWRC is installed (in Windows Vista or above, launch AWRC using run as Administrator from Windows Explorer to elevate to true Administrator), you can prevent other users from launching AWRC by setting a password under [Configure](#).

Like most things in computing, the password will not deter a determined hacker, it is just good enough for the occasional lurker.

The AWRC Password feature is disabled in the Evaluation release, and after registration must be used only after the trial period has expired.

## 1.12 Logging Connections

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

- **Date and time started and ended** in the format yyyy-nn-dd hh:mm:ss, where yyyy stand for year, nn for month, etc.
- **Remote Host.** The format is xxxx (nnnn/iii.iii.iii.iii). xxx is what you type in the Remote Host box, nnnn and iii.iii.iii.iii are the machine name and IP address provided by the remote host after a successful 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.

## 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 up to 10 monitors and AWRC 7.0 and later allow you to access up to 10 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 check the Remote Keyboard checkbox, 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. Remote Keyboard is checked by default, you can change the setting from the Configure menus.

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 Configure/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 and Uptime.
- **Processor Information:** Manufacturer, Vendor ID, CPU name, Family, Model, Stepping, Raw frequency and Norm frequency.
- **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.
- **Logical Local Printers.**

### 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

Enumerates processes with respective PID, Session ID, user and Domain.

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. On a 64-bit system, only 32-bit processes can be killed by selecting this option.
- **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.

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.

No other existing software can provide you with this sort of information. We know it, we were the first to find a way to obtain this sort of information from the local machine (with our award winning software AWSPS), now we are the first to obtain this information from a remote machine.

### 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<sup>(1)</sup>-to-IP-address mappings.

Most DNS servers are authoritative<sup>(2)</sup> for some zones<sup>(3)</sup> 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_ENTRIES	Indicates that this is one of two or more entries for a single protocol (from a given provider) which is capable of implementing multiple behaviors.
PFL_RECOMMENDED_PROTOCOL_ENTRY	Indicates that this is the recommended or most frequently used entry for a protocol that is capable of implementing multiple behaviors.
PFL_HIDDEN	Hides the protocol entry when this flag is set.

PFL\_MATCHES\_PROTOCOL\_ZER A value of zero in the protocol parameter of socket or  
O WSA Socket 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 WSA Socket. 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.
0xFFFFFFFF	The protocol is message-oriented, but there is no maximum limit to the size of

F messages that may be transmitted.

### 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. When the download is completed you are requested to select were the downloaded file or files are going to.
- **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 in 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.

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

You can launch files as:

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

Launching files from a user account provides access to the HKEY\_CURRENT\_USER hive of the Registry for that account.

- **Zip selected Files:** 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 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.
- **Unzip selected Files:** 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.
- **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: These options are only visible on the popup menu when a connection is established.

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.

(\*)Not implemented for connections to Vista and later.

## 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.

(\*) This feature is not available when the remote computer is running a 64-bit operating system.

## 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.

## 2.7 Configure

By clicking the Options button on the Configure page you can set default values for most features. You can, as well, set up the Strong Encryption environment.

### 2.7.1 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 not exist on the remote computer, the local user can still see an arrow mouse cursor for easier navigation on the remote desktop.

- **Maintain Full-Screen aspect ratio:**

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

- **View-Only Mode:** By selecting this mode, local mouse movements and keystrokes are not passed to the remote computer. This is useful for users that use the software mostly for passive monitoring.

## 2.7.2 General

- **Compression level:**


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

- **Connection timeout:**

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

- **Reset all font sizes:**

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

- **Clear Remote Host history:**  
Pressing this button, clears all past entries from the dropdown Remote Host list.
- **Clear grids on disconnect:**  
You can either clear all grids on disconnect or leave them untouched. Leaving them untouched is useful for post-mortem analysis.
- **Request authorization from remote:**  
If you check this box, the default action is: whenever you connect to a remote computer a request for authorization window will pop on the remote computer if someone is logged on. If no one is logged on the connection will abort.
- **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 a warning is shown each time the program closes.
- **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.
- **Remote Ctrl+Alt+Del hotkey:**  
To issue Ctrl+Alt+Del on the remote computer, you need to select a keyboard shortcut (also known as hotkey) on the local computer. The default is Ctrl+Alt+D, 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.
- **Full Screen hotkey:**  
This hotkey returns from full screen into normal mode (to enter into full screen mode from normal mode, press the  button or the Full Screen hotkey).  
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

- **Interface**

You can select Windows Classic which fits better with modern Windows releases or Traditional which has its own personality. Windows Classic is the default.

### 2.7.3 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.

However, the AWRCBL (Atelier Web Remote Commander Blocker) software is able to detect and stop AWRC no matter how hidden you have made it. This is by design, and in most cases there is no healthy reason to ask for any AWRC special build that circumvents AWRCBL.

- **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 8 or above, 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.

### 2.7.4 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.

### 2.7.5 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.

As explained in the topic [AWRC Password](#), you need to be an Administrator to set/unset a password

## 2.7.6 Advanced

- **XP Pro Fast User Switching (FUS) Compatibility:**

When checked (the default), you can switch to another user without disconnecting the AWRC session. If Fast User Switching Services are disabled or stopped you can still connect by unchecking the box.

- **Windows Server 2003 Physical Console ID may not be 0:**

On Windows Server 2003, the Session ID that corresponds to the Physical console (i.e, the session associated with the physical mouse and keyboard) is not guaranteed to be 0, namely when there are Administrative connections through terminal services. In these cases you may need to check this box to be able to connect with AWRC.


## 3 FAQ

### 3.1 All Releases FAQ

These are true "Frequently Asked Questions" sent to our Support staff. In most cases the answer is already provided elsewhere within the documentation. For [Windows Vista and later specific questions please read here](#).

For possible updates to the FAQ, point your browser to <http://www.atelierweb.com/rcomm/faq.htm>.

**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 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

**Q: Which ports are used by AWRC?**

A: AWRC does not open any ports, it simply requires Microsoft Networks. Microsoft Networks use ports 135, 137, 138, 139 or 445. However, operations performed by AWRC run **only** through TCP port 445 (Windows 2000, XP, Server 2003, Vista and later) or TCP port 139 (Windows NT 4. Windows 2000, XP, Server 2003, Vista and later can use as well this port if port 445 is not

available). Ports 135, 137, 138 and one of 139 or 445 can be blocked by the firewall or router without interfering with AWRC operation.

**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 port 139 or port 445. See the question above..

**Q: How safe is AWRC for use across the Internet?**

A: Microsoft Networks, in particular port 445 and even port 139 are 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: Can I use AWRC across a VPN?**

A: Yes, AWRC works very well with the VPN products we are aware of. We use AWRC with the OpenVPN software to control our Web server sited in Arizona, USA (9000 Km away). An advantage of VPNs, not always stressed, is that you don't have to be concerned with perimeter firewalls blocking ports 445 or 139. With the OpenVPN all traffic flows across a single UDP or TCP port (very cute).

**Q: Can I use AWRC on a Windows Server running Terminal Services?**

A: You can without restrictions with AWRC 6.0 or later.

**Q: Does AWRC work in Windows 64-bit Operating Systems?**

A: It works at the same level with both 32-bit and 64-bit Windows Operating Systems.

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

A: AWRC is different, it is by far and large the more feature rich remote access software you can find (others say the same, even some pretty basic ones, please make yourself a favour and confirm who tells you the truth before taking a decision). AWRC has very good 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 or/and TCP port 139.
- The router on the remote network forwards TCP port 445 or/and TCP port 139 to the private IP address of the target machine.
- The personal firewall of the remote machine allows incoming connections on TCP port 445 or/and port 139.

**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 connect 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/rcomm/download.htm> or from sites that point to <http://evalsoftware.atelierweb.com>. Reverse-engineered warez releases of this software can not work as expected. Note in particular, that some warez sites have distributed at least one AWRC release with a trojan horse attached to it.

**Q: What does it mean the error 'Remote Host' failed at base command handler initialization (see Help/FAQ)?**


A: There are a few possible reasons.

- AWRC Blocker does not allow connections to that machine (normally you will receive a hint, but is not guaranteed).
- Antivirus software. We are not aware of problems with recent releases of Antivirus software, but this may happen anytime because some companies invent new pests to keep their business rolling. In such cases, enter an exception for the remote service file name (Configure/Remote Service) or give it an unusual file name extension and enter an exception for files with that extension.
- A large number of simultaneous connections to a remote server or a remote computer too busy may also give this error.

**Q: How can I improve the remote screen updating response of AWRC?**

A:

After release 7.5, AWRC is extremely fast, faster than any other no-driver assisted remote access software we are aware of, but if you are still unsatisfied (namely when connecting across the internet) the following factors contribute to an improvement of the response:

- **Number of Desktop colors** selected under Configure. Selecting 8 bit is 4 times faster than 32 bit colors.
- **Image Scaling**. The anti-aliasing filter takes time to render the images. The best response is obtained with 100% scaling factor. Higher scaling is better than lower scaling.
- **Hide Wallpaper and Aero Composition** (Vista/Windows 7) using the  button.
- **Smaller screen resolutions**. 1024x768 provide 66% better response than 1280x1024.
- Also, bear in mind that the **hardware** can make all of difference. Graphics cards and CPU model, class and frequency are important.
- Do not waste **bandwidth in other connections**, for example downloading a big file from the internet at the same time.
- When connecting across the internet, experiment with Compression Level set to Strong under Configure/General.

**Q: Does AWRC access the Internet to phone home?**

A: AWRC only tries to access the internet if **Check for Product Updates** is set to **Automatically**.

**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=Myppassword
```

## 3.2 Vista and later FAQ

**In this page, when we mention Windows Vista the some answers still apply in full to Windows 7 and to Windows Server 2008/2008R2**

**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 also 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: Can DEP (Data Execution Prevention) cause connection failures?**

A: We are not aware with recent releases of AWRC.

## 5 License and Purchasing

### 5.1 License

You should carefully read the following terms and conditions before using this software.

**LICENSE AGREEMENT FOR ATELIER WEB REMOTE COMMANDER**

Evaluation Period before registration

Unregistered use of AWRC after the evaluation period is in violation of Portuguese and International Copyright laws. The evaluation period is 15-days or 30-executions, whichever comes first.

**Governing Law**

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

**Disclaimer of Warranty**

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SOLD 'AS IS' AND WITHOUT WARRANTIES AS TO PERFORMANCE OR MERCHANTABILITY OR ANY OTHER WARRANTIES WHETHER EXPRESSED OR IMPLIED. Because of the various hardware and software environments into which AWRC may be put, NO WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE IS OFFERED.

Good data processing procedure dictates that any program be thoroughly tested with non-critical data before relying on it. The user must assume the entire risk of using the program. ANY LIABILITY OF THE SELLER WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR REFUND OF PURCHASE PRICE.

**Distribution of Evaluation Version**

Provided that you verify that you are distributing the evaluation version (select the Configure tab while running AWRC to check) you are hereby licensed to make as many copies of the evaluation version of this 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.

**Purchased Version**

One Single User/Workgroup license of AWRC allows the program to be used by a single person who uses the software personally (maximum of 2 computers used by the same person) within a Microsoft Windows Workgroup.

One Single User/Domain license of AWRC allows the program to be used by a single person who uses the software personally (maximum of 2 computers used by the same person) within a Microsoft Windows Domain or Workgroup.

One Company license of AWRC allows the program to be installed on a Local Area Network to be used within Microsoft Windows Domains or Workgroups of a Company or Site by the number computers specified in the license details.

## 5.2 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 or 30 executions. 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/rcomm/order.htm>

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

**Registration entitles you:**

- To the unrestricted full featured release.
- A Single-User license entitles to a free license for AWRCBL (Atelier Web Remote Commander Access Control). A Company License entitles to three free licenses for BL.
- Priority in technical support and advice.
- To be directly informed of new major releases.