PROSUM

WOOWEB-PRO V6

Software Router for Windows

USER'S GUIDE

Version 1.2
November 2015

Legal Notices

PROSUM reserves the right to, without notice, modify all or part of this document and/or make any changes or improvements in any program described in this manual.

PROSUM shall not be liable for any loss, cost, or damage consequential to reliance on this manual.

PROSUM has no liability to the end user or to any third party for consequential damages (including, but not limited to, cost, loss of profits, downtime, damage of equipment or programs).

PROSUM makes no warranty that its software products are error free and will work in combination with any hardware or software products provided by third parties.

Trademarks and Registered Names

Table of Contents

Introduction

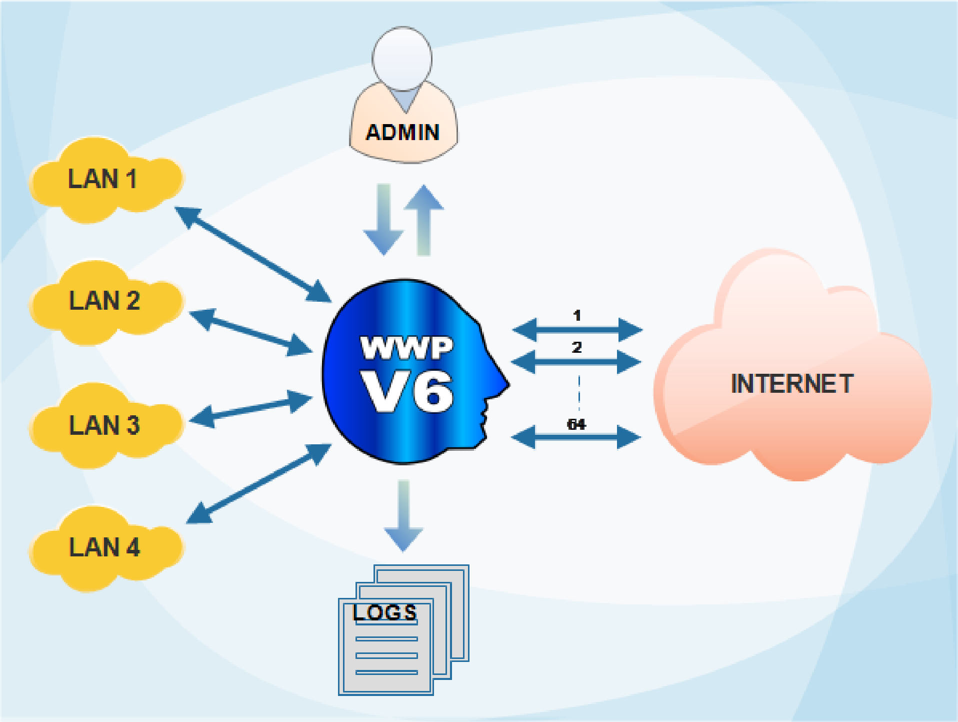
WOOWEB-PRO V6 is firewall and router software providing a solution at the corporate level for outbound and inbound Internet access. It transforms any computer into a powerful high-level multiple-port router with advanced filtering, tight management, and large log recording. It is the perfect solution to secure and control the Internet access of organizations such as companies, schools, barracks, hotels, public libraries, campsites, cybercafés, etc.

WOOWEB-PRO V6 features a web server. It can be configured and accessed locally or remotely using any web browser via a simple HTTP connection, or via an SSL HTTPS connection for those that are concerned by security.

WOOWEB-PRO V6 can manage thousands of machines and users, 4 LANs, and 64 Internet connections. The global bandwidth can be distributed evenly to all users, or shared out according to configurable per-user rules, guaranteeing a minimum or a maximum percentage of the global throughput. The firewall provides strong protection against Internet attacks. It can be configured and it gives information details about the intrusion attempts. There is no need for an extra networked firewall.

WOOWEB-PRO V6 accepts incoming connections. However, the access to your servers is tightly controlled by the rules you build. These rules permit to forward the remote Internet users to the right servers and applications, at no risk for other computers. All accesses are recorded into log files.

WOOWEB-PRO V6 runs on the 32-bit or 64-bit versions of Windows 10 / 8 / 7 / Vista / XP operating systems. It supports the most popular Internet connection types such as routers, 3G keys, cable modems, wireless cards, ADSL modems, analog or ISDN modems. The computer does not have to be dedicated to WOOWEB-PRO usage.



This manual gathers all WOOWEB-PRO V6 help pages.

Quick Setup

Click **Settings** and **Quick Setup**.

This page is the mandatory start point of WOOWEB-PRO V6. Except the Help pages, it is the only page that can be accessed at first start. It allows you to set up basic settings permitting to use WOOWEB-PRO V6 with a minimum feature set:

one ISP connection

one LAN connection

no user restrictions

no inbound connection allowed

After you filled out this page, higher level setup can be carried out in other management pages.

General Settings

Date and Time Format	Select the date and time formats that will be used in configuration forms. DD-MM-YYYY hh:mm, for example "25-08-2012 18:45" MM-DD-YYYY hh:mm:tt, for example "08-25-2012 06:45PM" (more US style) **Important Note:** All log pages display the international de-facto standard based on **ISO 8601** format, YYYY-MM-DD hh:mm:ss, which is unambiguous, easily comparable, and sortable. For example: "2012-08-25 18:45"
Language	Select the management language.
Filtering Priority	User outgoing Internet connections, as well as remote incoming accesses to your local servers can be allowed, disallowed, or limited, according to filtering rules built by the WOOWEB-PRO administrator. These filters can be combined in complex time-dependant arrangements permitting to cover all cases met by companies and organizations that are concerned by their security and their efficiency. This should not be usual, but it may happen that two filters enter in conflict, anytime, or during time periods. This option specifies which filter gets precedence in conflicting situations. Choose between the filter that grants, and the filter that denies the access.
Remote Management	Check this box to allow the remote management of WOOWEB-PRO. Only local users can manage WOOWEB-PRO when this box is not checked (default). **Note:** Remote users have a chance of losing the access to WOOWEB-PRO by doing wrong settings. For example choosing a management port that is blocked by the hardware router will forbid further accesses to the Web-based management of WOOWEB-PRO.
Management Connection Type	Specify whether the Web based management must use a standard HTTP connection, or an SSL HTTPS secure connection.
Management Port	Specify the TCP port used by the Web-based management. By default, it is 80 for HTTP and 443 for SSL.

Wan Connection Settings

Connection Name	Give a name to this ISP connection for future usage.
Connection Speed	Indicate the uplink and downlink data rates of this connection in Kbps. These values are used for balancing the load between connections and for the bandwidth management.

Connection Type	Select the way you are connected to your ISP Microsoft Dial-Up Router with DHCP Server Router without DHCP Server PPPoE Modem Note: The Dial-Up Networking is a service provided by Windows OS that allows your computer to connect to external networks such as the Internet. WOOWEB-PRO is able to use this service instead of a physical router or modem. This feature permits to extend the WOOWEB-PRO capability to any connection already supported by the OS, such as USB ADSL modems for example. Connection through the Dial-Up Networking must be selected for analog, RNIS, USB ADSL modems, and more generally, for any connection type that is not directly supported by WOOWEB-PRO.
Dial-Up Parameters	Select the Dial-Up and fill in the User ID, the Password, and if need be the Domain of the connection.
Router with DHCP Server	Select the Connection Device (most of times this is an Ethernet card) that is used for the router link.
Router Without DHCP Server	If the physical router does not provide a DHCP server, you need to select the Connection Device and to fill in Router IP Address, WOOWEB-PRO IP Address, Network Mask, and Primary and Secondary DNS. The Connection Device is the NIC card dedicated to WOOWEB-PRO for the router connection. WOOWEB-PRO transforms this card into a physical port. It does not use the network protocols and settings attached to this card by the OS. The only condition imposed is that the card IP address does not conflict with the WOOWEB-PRO IP address. Router IP Address is the address used by WOOWEB-PRO to access the router. WOOWEB-PRO IP Address is the IP address WOOWEB-PRO shows to the router. It should be the only address the router sees since all connections are supposed to pass through WOOWEB-PRO. Network Mask applies to WOOWEB-PRO and Router IP addresses. The Domain Name Servers must be specified by "hand" since the router does not provide the information.
PPPoE Modem	For those that still use a PPPoE modem, select the Connection Device and specify the User ID, the Password, and the Connection device, i.e., the Ethernet card that is used for the modem connection.

LAN Connection Settings

LAN Side Settings	We can think of WOOWEB-PRO as a two-port router, one port for the Internet connection and one port for the LAN connection. This approach is acceptable for the Quick Setup form, even if in fact WOOWEB-PRO can have 64 WAN ports and 4 LAN ports. Refer to WAN Settings and LAN Settings. Select the **Network Device** used for the connection to the LAN side, and fill in **WOOWEB-PRO IP Address** and **Network Mask** with values that are compatible with your LAN. **WOOWEB-PRO IP Address** should be set up as gateway IP address in all local machines that need to access the Internet, including the computer on which WOOWEB-PRO is running.

Setting up the LAN Connections

Click **Settings** and **LAN Connections**. This page is the place where you can configure the **four LAN interfaces** of WOOWEB-PRO V6. The purpose of four LAN interfaces is to provide the Internet access to local networks that do not use a flat addressing scheme. The purpose is not to replace a layer 3 switch because a standard computer equipped with 4 Ethernet NICs is not a hardware optimized for this task. However WOOWEB-PRO can route the traffic between the four LANs and play the role of an inefficient LAN-LAN static router.

Four tabs give access to the configuration of the four LAN interfaces. They are all similar except that the first interface cannot be disabled.

On each interface WOOWEB-PRO can provide an **independent DHCP server**.

LAN Connection

Enable	Check this box to enable this LAN interface (not applicable to the first interface)
Network Device	Select the Ethernet Network Device that is used by this interface. **Note:** The same card can be selected for more than one interface in case of different logic networks built on the same physical network.
WOOWEB-PRO IP Address	Specify the IP Address that WOOWEB-PRO will have on this interface. It should be the gateway IP address for all the machines connected to this LAN.
Network Mask	Specify the IP network mask of the LAN connected to this interface.

DHCP Server

Enable the DHCP Server	Check this box to enable the WOOWEB-PRO DHCP server on this LAN.
Pool of IP Addresses	Fill in **IP Address Pool Start** and **IP Address Pool End** to specify the range of IP addresses the DHCP server will allocate to clients. **Note:** It is still possible to exclude some IP Addresses from the Pool so that they will not be allocated by WOOWEB-PRO. Refer to DHCP.
Leases	The DHCP mechanism is simple: each client requests the use of an address for some period of time called a **lease**. The clients may ask for temporary or for permanent assignments by asking for infinite leases. However the DHCP server may be configured to give out lengthy leases to allow detection of clients that have been retired. Check **Time Limited Lease** to limit the duration of leases, and fill in **Months**, **Days** and **Minutes** to specify the maximum lease duration.

List of WAN Connections

Click **Settings** and **WAN Connections**. In this page you can see the list of WAN connections that are managed by WOOWEB-PRO.

WOOWEB-PRO can manage up to 64 WAN connections simultaneously. One of them is the default connection that is required and cannot be removed. The other ones are optional. They are called **Alternate** or **Dedicated** connections. **Dedicated** connections are reserved for specific users. **Alternate** connections, along with the **Default** Connection, form a pool available for standard users. WOOWEB-PRO tries to share out the global load evenly among all connections of the pool.

Note: See Edit WAN Connection for the meaning of WAN connection in WOOWEB-PRO terminology

Navigating in the List	To select a WAN connection, **click on its line** in the list, or use the keyboard **Up** and **Down** arrows.
List Information	Each row of the list shows a summary of the connection properties; Enabled, Default, Dedicated, Name, Type, and Device. Refer to Edit WAN Connection for detailed description.
Enabled	If enabled is set to **No**, the connection still exists, but is no longer used by WOOWEB-PRO.
Default	Main connection that cannot be removed and cannot be used for a dedicated machine.
Dedicated	A dedicated connection is not in the pool of connections shared by standard users. It can be assigned to one or several specific machines.
Alternate Connections	**Alternate** connections are all connections that are, neither the **Default** one, nor **Dedicated**. Along with the Default connection, they form a pool whose bandwidth is shared among standard users.
New, Edit, Remove	To configure a connection, click **New** or select a connection and click **Edit**. Click **Remove** to remove the selected connection from the list.

Editing a Wan Connection

Into page **WAN Connections**, click **New** or select a connection and click **Edit**. This page is the place where you can set up a new WAN connection, or change the settings of an existing WAN connection.

Important note: What is called WAN or Internet connection in WOOWEB-PRO terminology is a connection to the Internet using a **single public IP address**. Do not confound WOOWEB-PRO V6 WAN connections with ISP connections. ISP connections may include several WAN connections if the ISP provides several public IP addresses. For example you may have got one ISP connection and 16 WAN connections if you got a block of 16 public IP addresses from your ISP (/28 subnet). WOOWEB-PRO can manage up to 64 WAN connections, which does not necessarily mean 64 ISP connections.

Main Connection Settings

Connection Name	Give a name to this Internet connection for future usage.
Connection Speed	Indicate the uplink and downlink data rates of this connection in Kbps. These values are used for balancing the load between connections and for the bandwidth management.
Connection Type	Select the way you are connected to your ISP Microsoft Dial-Up Router with DHCP Server Router without DHCP Server PPPoE Modem **Note:** The Dial-Up Networking is a service provided by Windows OS that allows your computer to connect to external networks such as the Internet. WOOWEB-PRO is able to use this service instead of a physical router or modem. This feature permits to extend the WOOWEB-PRO capability to any connection already supported by the OS, such as USB ADSL modems for example. Connection through the Dial-Up Networking must be selected for analog, RNIS, USB ADSL modems, and more generally, for any connection type that is not supported directly by WOOWEB-PRO.
Dial-Up Parameters	Select the **Dial-Up** and fill in the **User ID**, the **Password**, and if need be the **Domain** of the connection.
Router with DHCP Server	Select the **Connection Device** (most of times this is an Ethernet card) that is used for the router link. In (the unlikely) case there are several DHCP servers on the network, you will need to fill in **Use a Preferred DHCP Server** to specify which one is to be used by WOOWEB-PRO.

Router Without DHCP Server	If the physical router does not provide a DHCP server, you will need to select the **Connection Device** and to fill in **Router IP Address**, **WOOWEB-PRO IP Address**, **Network Mask**, and **Primary and Secondary DNS**. The **Connection Device** is the NIC card dedicated to WOOWEB-PRO for the router connection. WOOWEB-PRO transforms this card into a physical port. It does not use the network protocols and settings attached to this card by the OS. The only condition imposed is that the card IP address does not conflict with the WOOWEB-PRO IP address. **Router IP Address** is the address used by WOOWEB-PRO to access the router. **WOOWEB-PRO IP Address** is the IP address WOOWEB-PRO shows to the router. It should be the only address the router can see since all connections are supposed to pass through WOOWEB-PRO. **Network Mask** applies to WOOWEB-PRO and Router IP addresses. The **Domain Name Servers** must be specified by "hand" since the router does not provide the information.
PPPoE Modem	For those that still use a PPPoE modem, specify the **User ID**, the **Password**, and the **Connection device**, i.e., the Ethernet card that is used for the modem connection. In the unlikely case they are not provided by the PPPoE modem, uncheck the two **"Assigned by PPPoE Server"** boxes and fill in the **WOOWEB-PRO IP Address** and the **DNS Servers**.

Connection Rules

Overview	Under this tab you can specify how and when the connection will start and close. WOOWEB-PRO can support most popular connection types. It can manage up to 64 Internet connections in parallel. These connections can be all of same type or not. For example, an xDSL connection can be used with an ISDN connection in parallel or back up. WOOWEB-PRO can dial-up when it detects a machine activity, and hang-up after a while when there is no more access request. **Note:** when connected behind a hardware router, WOOWEB-PRO does not manage the physical connection to the ISP. The hardware router manages the ISP connection and WOOWEB-PRO just makes sure it can speak with the router.
Start of Connection	Specify here how the connection is to be started. **Manually** means by clicking on the Start Connection button in Maintenance->WAN Connections. **Automatically At Start Up Time** and **Automatically Every Day at a Fixed Time** are self explaining options. **Automatically On Activity Detection** is trickier. When this option is selected, WOOWEB-PRO triggers the connection on DNS requests and when it receives packets intended for most of the usual ports that are used for the Internet traffic. **Note:** These options make little sense for always-on connections, or connections behind a router since this is the router that establishes the physical connection. In these two cases select **Automatically At Start Up Time**.

End of Connection	Select from among **Manually**, **After a Fixed Delay**, **After Delay Without Activity**. **Note:** This option makes little sense for always-on connections or for connections behind a router since this is the router that establishes the physical connection. In this case select **Manually**.
Disconnection Delay	Select the fixed or no-activity disconnection delay.
First Connection Attempts	Specify the number of retries and the delay between retries to establish the connection.
Reconnection Attempt Period	After a connection has been closed for some reason, and the backup is in use, WOOWEB-PRO checks periodically the state of the main connection to come back to it as soon as possible. Specify here the delay between connection checks.
Connection Usage	Tell which purpose this connection is for. **Default**: Main connection that cannot be removed and cannot be used for a dedicated machine. **Alternate**: This connection belongs to the pool of connections whose bandwidth is shared by standard machines. **Dedicated**: This connection is not in the pool of connections shared by standard machines. It can be assigned to one or several specific machines.
Backup Connections	**Current Backup Connection** and **Add a Backup Connection** allow you to manage the set of connections that can be used in place of this connection when it fails. **Note:** The notion of backup makes sense when using connections that are established on request, such as Dialup or Modem connections. The principle of connection backup consists in replacing a failing connection with a new one that is started just for this purpose. When using always-on connections, the default and the alternate connections form a pool. Should that connection fail, the bandwidth is automatically redistributed across the remaining ones. There is no need to specify backup connections.

Time Limitations

Overview	The **Time Limitation** tab is the place where you can specify periods or amounts of time for the use of this connection. **Note:** This may be useful if you pay for Internet access by the minute or if you don't want to allow the access to this ISP anytime. If you are using always-on connections, or if you are not interested in filtering this connection, select **No Limitation** in both fields. **Note:** Filtering the access at connection level has a global effect. Global action can also be achieved by using the Global Profile.
Connection Days	On a weekly basis you can specify here a set of days when this connection can be used.
Daily Connection Time	On a daily basis you can specify here a time period when this connection can be used.

Advanced

Maximum Transmission Unit (MTU)	Most of times the Maximum Transmission Unit that is automatically set up by WOOWEB-PRO is correct and you can leave the **Default Value** option. However, if you experience some problems with some Web sites, you can try to select the **Force to** option, and to set up the MTU manually. The usual minimum Internet standard packet size is 576 and the usual maximum is 1500. Try to diminish the MTU until it works. Do not select the **Ignore** option unless you are requested to do so by the technical support. It is a debug option.
Check Connection State by Pinging	This feature allows WOOWEB-PRO to survey the connection state by pinging an Internet address. This is useful in order to restart the connection or to switch to the backup connection in case of problem. To enable this feature, select **Ping Next Router**, or select **Ping This Address** and specify an Internet IP address. **Number of Tries Before Hanging**: This is the number of successive failing pings that triggers the disconnected state. **Delay Between Tries**. Number of seconds between pings. You should not use a too short delay unless you need a very fast response time. **Note:** If you chose **Ping This Address**, make sure that the host at the address you specified does respond to pings, otherwise the connection will be permanently set to the disconnected state. To check that you can use the **Test Host Access** tool in the **Debug** page.

Local Machines

Click **Settings** and **Local Machines**. Local Machines are the computers, servers and any sort of devices that are connected to the LAN and that access to the Internet, or are accessed from the Internet, through WOOWEB-PRO. Local machines must have a unique IP address on the LAN, a unique MAC address, and a unique name.

One machine, **Default**, exists by default in the list of the machines and cannot be removed or renamed. Its content, except the IP Address and the MAC Address can be modified. Default is the template for new machines, that are not yet in the list and that try to connect to the Internet. Its content is also used by the new machines discovered on the local network (see Discover section).

This page not only allows you to configure the machines. It also shows the current state of each machine with a small icon:

🟢	Connected machine that can access to the Internet
🔴	Connected machine that is blocked by WOOWEB-PRO and thus cannot access to the Internet
○	Unconnected Machine

List of Local Machines

Navigating into the List and Editing Machines	To select a machine, **click on its line** in the list, or use the keyboard **Up** and **Down** arrows. The list can be sorted in several ways by clicking the heading name at the top of a column. When a machine is selected, its settings are copied into the **Machine Properties** panel. You can do any modification in this panel. By clicking **Set Machine,** the modifications are applied to the selected machine. By clicking **Add Machine**, a new line reflecting the machine Properties panel is created at the end of the list. Thus it is easy to create new machines from existing ones.
Machine Name	The Machine Name must be unique in the database. All machines must have a name.
IP Address	Use the dotted-decimal notation, e.g., 192.168.1.102
MAC Address	Sometime also called "Ethernet Address". Use IEEE 802 format, e.g., 00:C0:FD:0A:B5:78
Profile	The profile is not mandatory. It is combined with the **Global Profile** and may be with the three user profiles to establish the rules that apply to this machine.

User Authentication	Specify whether users that use this machine should authenticate themselves. In this case, each user trying to access the Internet from this machine must first login with a name and a password. Therefore, the machine user is identified and user profiles and filters can apply. Concerning the way to perform the authentication, WOOWEB-PRO always starts by trying to find the user in its local database. If the local research fails, then WOOWEB-PRO may send an LDAP request to a remote directory server if this option is selected. (See Auxiliary Settings for LDAP server settings). **Thus local authentication has precedence over remote authentication**. When doing a remote authentication, WOOWEB-PRO starts by trying to connect to the LDAP server with the common name (CN) and the password provided by the user at login. If the LDAP server is not found or if the connection is not accepted, the user login fails. If the connection is accepted, then WOOWEB-PRO sends a request to get the user attributes. If the server response contains the attributes "profile1" and/or "profile2" and/or "profile3", and if their values match some existing profile names, these profiles are applied. Otherwise only the Global and the Machine profiles are applied. **Note:** The method for adding the profile attributes to users in the directory is beyond the scope of this help. You can contact Prosum for technical support about this subject: support@prosum.net.
Enabled	You can block a machine with a simple click. This change is immediately transmitted to WOOWEB-PRO.
Will be Disabled on	You can give a temporary access until a certain date and time. This change is immediately transmitted to WOOWEB-PRO.
Dedicated Connection	A machine can use the common pool of WAN connections or a dedicated WAN connection.
Bandwidth Rule	Select the bandwidth rule attached to this machine. **Note:** Each machine can be bound with a bandwidth rule. Refer to bandwidth rules. WOOWEB-PRO tries to provide a certain amount of bandwidth to this machine, according to the type of bandwidth management selected, and the properties of the rule attached here.
Add Machine	Creates a new machine based on the content of the **Machine Properties** panel, and adds it at the end of the list.
Set Machine	Updates the selected machine with the content of the **Machine Properties** panel.
Remove	Removes the selected machine.
Enable All, Disable All	Enables or disables all machines in the list.
Reload	Reload the page. **Note:** All modifications are made in real time, so **Reload** does not cancel the modifications. It just reloads the table not sorted with its current values.
Discover	Run the machine discovering process to find all alive machines on the local network. **Note:** WOOWEB-PRO tries periodically to discover the machines
Import	Imports a machine list from a database. Import settings are set up under the **Advanced** tab.

Advanced

Database Import	The machine list can be imported from a database file or server. The table name must be **LocalMachines** and each machine record must contain the following fields: **Name**: character string **Enabled**: 0 or 1 **DateToDisable**: a date based on ISO 8601 format YYYY-MM-DD hh:mm **IPAddress**: character string (dotted decimal) **MACAddress**: character string (IEEE 802 format, e.g., 00:C0:FD:0A:B5:78) **Profile**: character string **UserAuth**: 0, 1 or 2 **Connection**: character string **Bandwidth**: character string
Machine List Database Import	Specify whether you want to import the machine list from a database file or from a database server. **Note:** the machine list is imported each time you click **Import** at the bottom of the machine list, and/or periodically if you checked **machine List Synchronization.**
ODBC Driver	Select the type of interface corresponding to your database.

Database Access Parameters	Fill in the parameters that will be provided to the ODBC driver to open the database. They may be simply the path to a database file, or more complex information allowing opening a database on a remote or local server. For example:
	Server=db1.database.com;
	Port=3306;
	Option=131072;
	Stmt=;
	Database=mydb;
	Uid=myUsername;
	Pwd=myPassword;

Database Server	IP address or name of the database server.
Database User Name and Password	User authentication permitting to access to the database server.
Machine List Synchronization	Check this box if the machine list must be reloaded periodically by WOOWEB-PRO from the database file or server.
Synchronization Period	Select the period time between refresh accesses.

List of Local Users

Click **Settings** and **Local Users.** Local users are the persons that use the machines connected to the LAN. Local users can be managed, provided they are authenticated. Without authentication, only machines can be managed.

User List

User Authentication	For each local machine, it is possible to specify whether users that use this machine should authenticate themselves (refer to Local Machines). In this case, each user trying to access the Internet from this machine must login with a name and a password. Therefore, the machine user is identified and user profiles and filters can apply.
Navigating in the List and Editing Users	To select a user, **click on his line** in the list, or use the keyboard **Up** and **Down** arrows. The list can be sorted in several ways by clicking the heading name at the top of a column. When a user is selected, his settings are copied into the **User Properties** panel. You can do any modification in this panel. By clicking **Set User,** the modifications are applied to the selected user. By clicking **Add User**, a new line reflecting the User Properties panel is created at the end of the list. Thus it is easy to create new users from existing ones.
User Name	The User Name must be unique in the database.
Password	For the sake of security, user passwords are not sent by the server, so, they cannot be seen by looking at the page source. If you don't touch this field, WOOWEB-PRO keeps the current password.
Profiles	The three profiles have same weight. They are not mandatory. They are combined with the **Global Profile** and the **Machine Profile** to establish the rules that apply to this user.
Enabled	You can block a user with a simple click. This change is immediately transmitted to WOOWEB-PRO.
Will be Disabled on	You can give a temporary access until a certain date and time. This change is immediately transmitted to WOOWEB-PRO.
Add User	Creates a new user based on the content of the **User Properties** panel and adds it at the end of the list.
Set User	Updates the selected User with the content of the **User Properties** panel.
Remove	Removes the selected user.
Enable All, Disable All	Enables or disables all users in the list.
Reload	Reload the page. **Note:** All modifications are made in real time, so **Reload** does not cancel the modifications. It just reloads the table not sorted with its current values.
Import	Imports a user list from a database. Import settings are set up under the **Advanced** tab.

Advanced

Database Import	The user list can be imported from a database file or server. The table name must be LocalUsers and each user record must contain the following fields: Name: character string Password: character string Enabled: 0 or 1 DateToDisable: a date based on ISO 8601 format YYYY-MM-DD hh:mm Profile1: character string Profile2: character string Profile3: character string
User List Database Import	Specify whether you want to import the user list from a database file or from a database server. Note: the user list is imported each time you click Import at the bottom of the machine list, and/or periodically if you checked machine List Synchronization.
ODBC Driver	Select the type of interface corresponding to your database.

Database Access Parameters	Fill in the parameters that will be provided to the ODBC driver to open the database. They may be simply the path to a database file, or more complex information allowing opening a database on a remote or local server. For example:
	Server=db1.database.com;
	Port=3306;
	Option=131072;
	Stmt=;
	Database=mydb;
	Uid=myUsername;
	Pwd=myPassword;

Database Server	IP address or name of the database server.
Database User Name and Password	User authentication permitting to access to the database server.
User List Synchronization	Check this box if the user list must be reloaded periodically by WOOWEB-PRO from the database file or server.
Synchronization Period	Select the period time between refresh accesses.

List of Inbound Connection Rules

Click **Settings** and **Inbound Connections**. This page shows the list of Inbound Connections Rules.

Inbound connections are connections to your local servers from remote clients. By default WOOWEB-PRO rejects all inbound connection attempts. These rejected attempts are recorded into the Inbound Firewall. However to make your server accessible from remote users without jeopardizing your local network, it is possible to tell WOOWEB-PRO under which conditions, when, and by whom, your servers can be accessed.

A set of filters governing the access to one of your servers is called an **Inbound Connection Rule**. Thus you must set up as many Inbound Connection Rules as servers are living on your LAN.

Note: Each incoming packet is analyzed and the ruled are scanned to find if the packet can be forwarded to a local machine. In order to prevent any ambiguity concerning the target server, Inbound Connection Rules should be mutual exclusive, i.e. an incoming packet should not be able to satisfy two different rules. Most of time this is achieved by specifying different TCP ports to servers. However, to escape this unlikely situation, the rules are tried in the order of the list, and the scan stops as soon as a rule allows the access. The incoming packet is then forwarded to the machine specified by the matching rule. Thus, be aware that if one rule is too wide, it may capture some packets that were intended for machines whose rules were following it in the list. Those captured packets will not reach the right machine.

Inbound Firewall

Firewall Behavior	If you have no server, you should select **Block ALL Remote Accesses**, otherwise select **Allow Remote Accesses According to the Connection Rules**, and click **Submit**.

Connection Rules

Overview	Click the **Connection Rules** tab to set up the Inbound Connection Rules that will give access to your servers. Each rule is a set of filters concerning a single server. There must be exactly as many rules as servers that must be accessible from the Internet.
Navigating in the List	To select a rule, **click on its line** in the list, or use the keyboard **Up** and **Down** arrows. **Edit** and **Remove** buttons affect the selected rule. The action of the **New Rule** button partially depends on the selected rule.
Rule Information	Each row of the list shows a summary of the rule information: the enabled or disabled state or the rule the rule name the targeted local computer the dedicated WAN connection, if any which filter types are active Select the rule and click **Edit** if you need detailed rule information (Inbound Connection). You can enable and disable a rule simply by clicking on its check box into the list. Other attributes must be changed by selecting the rule and then clicking on the **Edit** button.
Up, Down	Even if it is not recommended, a rule action may depend on its location in the list. See note above. These buttons permit to change the location of a rule in the list.
New Rule	Click this button to create a new rule. If a rule is selected, the new rule is based on it. Otherwise, the new rule gets default settings.
Edit	Click this button to open the Inbound Connection Rule configuration page related to the selected rule.

Remove	Click this button to remove the selected rule.

Editing an Inbound Connection Rule

Into page Inbound Connections Rules, under tab **Connection Rules**, click **New Rule** or select one rule and click **Edit**.

This page is the place where you can modify or create an inbound connection rule that will enable remote access to one of your local servers. In case of new rule, the page is initialized with default settings. In case of modification of an existing rule, the page is initialized with the rule settings.

General

Rule Name	Each **Inbound Connection Rule** must be given a unique name. By typing a new name, you can create a new rule based on an existing one. The rules cannot be suppressed from this page. Open the List of rules for this operation (Settings->Inbound Connections).
Target Machine	Fill in the local IP address of your server directly, or select it in the machine list.

Time Filtering

Outline	Under this tab you can specify when your server can be accessed.
Enable Time Filtering	Select **The Target can be Accessed at ANY Time** if you don't plan to use time limitations, otherwise select **The Target can be Accessed ONLY During Time Periods** and set up the accessibility **Day Time Periods**.
Add Period to Selected Days	Time periods are built on a weekly basis. Here you can add the same time period to several days of the week in a single operation. Check day boxes as needed, specify the time period by setting **Start** and **End**, and click **Add to Selected Days**. You should see below the new time period added to the lists of selected days.
Day Time Periods	Seven tabs give access to the time periods lists of the seven days of the week. Use the **Start** and **End** select fields, and the **Change**, **Insert**, and **Delete** buttons to set up the list under each day tab. **Note:** Click on the list to select a time period. Modifications apply to the selected time period.

Host Filtering

Outline	Host Filtering makes it possible to allow or deny the access to your servers by remote hosts according to their name or IP address.
Enable	When this feature is enabled, the rule uses its Black and White lists to reject or not reject remote hosts accesses, otherwise there is no host name or IP address limitation.
Black and White Lists	The **Black** and **White** lists contain sets of hosts names, or single IP addresses, or IP address ranges. All hosts that match no name or IP address in any of these lists are not rejected by this filter. The hosts that match a name or IP address in the Black list are rejected, unless they match also a name or IP address in the White list. **Note:** Instead of allowing all hosts except a few that are blocked, you can do the opposite, i.e. block everyone except a defined list. To do that, write "0.0.0.0 to 255.255.255.255" into the Black list, and place the set of allowed hosts into the White list.

Port Filtering

Port Filtering (Mapping)	Internet Services such as Web, Email, FTP, etc., are associated with port numbers. The port is a number transmitted in each TCP/IP packet that identifies the service for which the package is intended. Using the port number to target a local machine behind a NAT router is also called **Port Mapping**. Specify here the port corresponding to the service provided by the server. For example, if the target machine is running a Web server using the standard port, set **Port Name** to WEB and **Port Number** to 80. Note that the Port Number 80 is mandatory, but the Port Name could be anything else such as "HTTP", or "My Web Server". **Note:** While other filters can be seen as access restrictions for security purpose, the **Port Number** associated with the **Target Machine** IP address is most often the main setting that permits to route the inbound traffic to the appropriate machine. The WAN Connection can also play this role by mapping public IP addresses instead of ports to machines.
List of Ports	Use the **Port Name** and **Port Range** text fields, and the **Change**, **Insert**, and **Delete** buttons to set up the list of ports used by the target machine. If **Local Port** is different from the base of **Port Range**, the incoming requests matching **Port Range** are translated and forwarded to the local port range whose base number is **Local Port** and size is same as Port Range. For example, if **Port Range** is set to 6000-6001 and **Local Port** is set to 20, then all incoming requests addressed to 6000-6001 by remote users are forwarded to ports 20-21 of the local machine. **Note:** If you have several servers of same type that must be accessed by remote hosts, either set up your servers so that they use different ports, or use different public IP addresses. WOOWEB-PRO V6 can support up to 64 public IP addresses. See Wan Connection Filtering. You can also use any combination of both methods. **Note:** Click in the list or use the up and down arrows of your keyboard to select a line. All modifications apply to the selected line.

Protocol Filtering

Protocol Filtering	In IPv4, the Protocol Number identifies the upper layer protocol that an IP packet should be sent to. The protocol number can be found in the Protocol field of the IP header of packets. Note that the IP protocol number is not the same as the Port Number, which refers to a higher level, such as the application layer. This filter can block incoming IP packets based on their protocol number, for example ICMP, GRE, TCP, or UDP. **Example:** By blocking ICMP you can prevent your server from responding to ping messages.
Forbidden Protocols	Use the **Protocol Name** and **Protocol Number** text fields, and the **Change**, **Insert**, and **Delete** buttons to set up the list of blocked protocols. **Note:** Click in the list or use the up and down arrows of your keyboard to select a line. Modifications apply to the selected line.

WAN Connection Filtering

Outline	WOOWEB-PRO V6 can manage up to 64 WAN connections. These connections can be any combination from a single ISP connection providing 64 IP addresses, up to 64 different ISP connections, each of them providing a single IP address. If you have got several IP addresses, specify here whether the target machine can be accessed from all, or from only one of them. By selecting **The Target can be Accessed ONLY from this WAN Connection** and selecting the WAN connection (public IP address), you can map the public IP address to the target machine of this rule. **Example:** By setting up 64 rules, you can host 64 Web servers on your LAN, all working with port 80, but appearing at 64 different IP addresses from the Internet.

List of Filtering Profiles

Click **Settings** and **Profiles**. This page shows the list of **Filtering Profiles**.

A profile is a set of filters that can be attached to users and/or machines to limit their Internet access rights:

Access Blocked
Time Filtering
Port Filtering
Protocol Filtering
Site Filtering
Content Filtering

See Filtering for filter detailed information.

You can create as many profiles as you need. Profiles are identified by their name that must be unique.

Two profiles are set up by default and cannot be removed: **Global** and **Default**. However, their content can be modified. **Global** is always attached to all machines. It is the place where you can set up limitations that will apply to your whole organization. Default is the template for new profiles when no parent profile is specified.

Machines may have one profile attached in addition to the Global profile. Users may have up to three profiles attached. Note that user accesses are also constrained by the Global profile and by the profile of the machine they are using.

When several profiles are attached to the same entity, machine or user, WOOWEB-PRO merges all profiles into a big one before deciding if an access is granted or denied. The combination rule is as following. First, WOOWEB-PRO eliminates all profiles that are not enabled. Then it eliminates all profiles that don't apply because of time limitations. Then it gathers all filters in each category. According to this rule, all profiles have same priority. If two filters in same category, or in two different categories, enter in conflict, i.e., one grants the access and the other one denies the access, as a last resort WOOWEB-PRO refers to the **Filtering** parameter.

Navigating in the List	To select a profile, **click on its line** in the list, or use the keyboard **Up** and **Down** arrows. **Edit** and **Remove** buttons affect the selected profile. The action of the **New Profile** button partially depends on the selected profile.
List Information	Each row of the list refers to a profile and provides a summary of its content. Name Access Blocked Active Filter Types Select a profile and click **Edit** if you need more detailed profile information (Edit Profile). You can enable and disable a profile simply by clicking on the corresponding check box into the list. A disabled profile is just ignored. Other attributes must be changed by selecting the profile and then clicking on the **Edit** button.
New Profile	Click this button to create a new profile. If a profile is selected, the new profile is based on it. Otherwise, the new profile gets the **Default** profile settings.
Edit	Click this button to open the **Edit Profile** page related to the selected profile.
Remove	Click this button to delete the selected profile.

Editing a Filtering Profile

Into page List of Filtering, click **New Profile** or select one profile and click **Edit**. This page is the place where you can set up new profiles, or change the filters of an existing profile.

In WOOWEB-PRO V6 terminology, a profile is a set of filters that can be attached to users and/or machines to limit their Internet access rights:

Block All Accesses switch
Time Filtering
Port Filtering
Protocol Filtering
Site Filtering
Content Filtering

Once created, profiles can be easily attached to machines or users. Profile changes have immediate repercussions on all machines and/or users that have this profile attached.

Important Note: All profile settings are done locally. They are transmitted to the router engine only when you click **Submit**.

General

Profile Name	Each profile must be given a unique name. This name is the reference that will permit to later manage the profile and to attach it to machines and users. Two profiles have a special name that cannot be changed: **Default** and **Global**. Global is a profile that applies to all machines. Default is the profile that is used as a template when creating new profiles.
Block All Accesses	This check box allows you to block all machines and users bound to this profile by a simple mouse click. When this box is checked the profile filters are no longer taken into account. All Internet accesses are blocked, unless you gave the priority to granting profiles and there is another profile granting the access. See **Filtering Priority** in Quick Setup. **Note:** Do not confound this check box with check box **Enabled** in List of Filtering. When **Enabled** is cleared, the profile is no more in use. It is neither blocking nor granting.

Time Limitations

Overview	Under this tab you can specify when filters apply and what is to be done when they don't apply. For more flexibility, you can specify that filters are active during Time Periods or outside Time Periods. You can even set up the profile as a pure go/nogo time-based filter.

Time Period Action	**During Time Periods** and **Outside Time Periods** are two selection fields allowing you to set up the profile behavior as a function of time. WOOWEB-PRO compares the current time with the set of time periods specified in the profile. According to the comparison result, it executes either the action specified in the first field, or the action specified in the second field. Both fields exhibit same four possible actions: **Block All Accesses**: The access to the Internet is forbidden whatever the filters **Disable This Profile Filters**: The filters are not taken into account **Apply This Profile Filters**: The filters are used to compute the access rule **Give Full Access**: The access to the Internet is granted whatever the filters **Note:** To disable all time periods, just select same option in both selection fields. For example, to build a profile that does not depend on time, select **Apply This Profile Filters** in both selection fields. **Note:** You can build a pure go/no-go time-based filter. For example, select **Block All Accesses** in first selection field and **Give Full Access** in second selection field. This will block all accesses during time periods, and give full access outside time periods. **Note:** Setting both selection fields to **Block All Accesses** is equivalent to checking **Access Blocked** under the **General** tab.
Add Period to Selected Days	Time periods are build on a weekly basis. Here you can add the same time period to several days of the week in a single operation. Check day boxes as needed, specify the time period by setting **Start** and **End**, and click **Add to Selected Days**. You should see below the new time period added to the lists of selected days.
Weekly Time Periods	Seven tabs give access to the time periods lists of the seven days of the week. Use the **Start** and **End** select fields, and the **Change**, **Insert**, and **Delete** buttons to set up the list under each day tab. **Note:** Click on the list to select a time period. Modifications apply to the selected time period.
Amount of Time Limitation	It is possible to allot a fixed amount of time per day, per week, or per month, during which the filters of this profile are active. After the time has expired, the profile forbids all further accesses until a new period of time starts (day, week, month). Into **Enable**, check **Limit the Amount of Time Filters are Active** and into **Amount of Time Limit** set up the maximum amount of time in **Hours** and **Minutes**. Then select the period of time from among **Day**, **Week**, and **Month**. Into **Period Start** specify when the time period starts, i.e., when the counter is reset. For example, you can start a new period the 10th of each month at 08:30AM. **Note:** WOOWEB-PRO does not check if the amount of time is smaller than the selected period. Setting up an amount of time larger than the period just disables this function, since filters are always active. **Note: Weekly Time Periods** and **Amount of Time Limitation** can both make the filters active. If both functions are enabled, filters are only active when **both** functions allow them to be so. In all other cases, the most restrictive has precedence. For example, if the amount of time has expired, the accesses are blocked even though the current time matches a period when the accesses should be granted. Similarly, if the current time matches a period when the accesses are forbidden, then all accesses are blocked even though the amount of time has not yet expired.

Port Filtering

Port Filtering	Internet Services such as Web, Email, FTP, etc., are associated with port numbers. The port is a number transmitted in each TCP/IP packet that identifies the service for which the package is intended. By forwarding or denying outbound packets containing certain port numbers, profiles make it possible to specify which Internet services are accessible by each machine and user. To allow only a set of services, select **Allow Ports**. To disallow a set of services, select **Forbid Ports**. **Note:** Disallowing some ports is easier and more common than allowing a fixed set of ports.
List of Ports	Depending on the **Port Filtering** selected option, the port list is either a list of forbidden ports (black list), or a list of allowed ports (white list). Each line specifies a port range. Use the **Port Name** and **Port Range** text fields, and the **Change**, **Insert**, and **Delete** buttons to set up the port list. **Note:** Click in the list or use the up and down arrows of your keyboard to select a line. Modifications apply to the selected line.

Protocol Filtering

Protocol Filtering	In IPv4, the Protocol Number identifies the upper layer protocol that an IP packet should be sent to. The protocol number can be found in the Protocol field of the IP header of packets. Note that the IP protocol number is not the same as the Port Number, which refers to a higher level, such as the application layer. This filter can block or allow outgoing IP packets based on the protocol used, for example ICMP, GRE, TCP, or UDP. To allow only a set of protocols, select **Allow Protocols**. To disallow a set of protocols, select **Forbid Protocols**. **Note:** Disallowing some protocols is easier and more common than allowing a fixed set of protocols.
List of Protocols	Depending on the **Protocol Filtering** selected option, the protocol list is either a list of forbidden protocols (black list), or a list of allowed protocols (white list). Each line specifies a protocol. Use the **Protocol Name** and **Protocol Number** text fields, and the **Change**, **Insert**, and **Delete** buttons to set up the protocol list. **Note:** Click in the list or use the up and down arrows of your keyboard to select a line. Modifications apply to the selected line.

Site Name Filtering

Enable	**Site Name Filtering** allows you to grant or deny access to Web sites depending on their name. To use this feature, select **Filter Web Sites by Their Name**.

White List and Black List	**Site Name Filtering** uses two set of character strings, **White List** and **Black List**. You must fill in these tables with character strings being the whole or a part of site names. Write one string per line. For example, "www.thebestsex.com" and "sex" are strings that both match www.thebestsex.com. Strings into the white list grant the accesses to sites, while strings into the black list block the accesses. **Important Note:** The white list has got the priority over the black list. If a site name matches a string in both tables, the access is granted. If a site does not match any list, this filter is not applied. The decision to grant or deny is taken by the other filters of this profile. **Note:** an undesirable string may be included into a larger harmless string. Consider for example sex and sexagenarian. To allow sexagenarian and forbid sex, you just need to add sex in the black list and sexagenarian in the white list.

Site Content Filtering

Overview	**Site Content Filtering** is optional and is dependent on a two-year subscription to the OrangeFilter service provided by IBM ISS. The ISS Company has machines and teams that continuously and dynamically crawl, rate, and categorize web sites for objectionable contents such as pornography or hate. ISS maintains one of the most important databases in the world. The visited sites are European as well as American. The rejection of objectionable material is very high while the rate of web pages blocked for incorrect classification is very low. If **Site Content Filtering** is enabled, whenever a machine tries to access a new Web site, a request is sent to the ISS servers to get the web site rating. The access is allowed or denied according to the server's response and to your setup. To speed up the process, an internal cache of already acquired and rated URLs is maintained so that surfing is not slowed down noticeably. Whenever a site is rejected, the user receives an HTML page showing "**Blocked by WOOWEB-PRO**". **Important note:** **Site Name Filtering** has higher priority than **Content Filtering**. Thus, whatever rating a web site gets from the ISS servers, your keyword filters (if any) override the OrangeFilter classification. This priority policy allows you to grant (or to block) the access to some sites that could have been blocked (or allowed) for incorrect classification, from your point of view. **Note:** The ISS classification of a site can be checked. Refer to Debug . All sites that are not yet categorized or that does not fit into any category fall into the **No OrangeFilter** category. **Note:** You can replace the HTML page showing "Blocked by WOOWEB-PRO" with a custom page. This page is standing into the **html\english\userauth** sub folder into the WOOWEB-PRO installation folder, and must be named **filter.html**.
Enable Site Content Filtering	Select either **Forbid Selected Contents (Black Filtering)**, or **Allow Selected Contents (White Filtering).**
Content Categories	**Content Categories** are available in a two-level tree. Check the boxes of selected categories or subcategories. Depending on the chosen option, this filter can use the selected categories for black or for white filtering. When **Black Filtering** is selected, this filter gives access to all Web sites except to those that match the selected categories. On the contrary, when **White Filtering** is selected, all web sites are blocked except those that match the selected categories.

Bandwidth Management

Click **Settings** and **Bandwidth Manag**.

Except the machines that have got a dedicated connection, all local machines share the global bandwidth provided by the pool of WAN connections. WOOWEB-PRO provides three options:

Leave machines compete for the Internet access (law of the jungle)
Try to give same bandwidth to all machines
Use a set of rules indicating a percentage of the global bandwidth for each machine. A bandwidth rule can be attached to each machine when setting up the machine properties.

The first and second options are self describing. The third option is more complicated. The bandwidth percentage can be, either a minimum guaranteed rate, or a maximum allowed rate. In addition, each rule can apply, either to the computers to which it is bound, or to the group of computers. See below for details.

In order to limit the complexity when you use the bandwidth rules, we recommend that all rules have the same type of action - minimum guaranteed rate, or maximum allowed rate.

When the bandwidth management is in use all computers that have no rule attached share the remaining bandwidth. However we recommend that all computers have a rule attached.

Management Type

Type of Bandwidth Management	Select from among: No Bandwidth Management: No rule apply. The fastest machines get higher bandwidth. Give Same Bandwidth to all Connected Machines. Try to allocate the same bandwidth to all machines. Enable the Following Rules to Share the Bandwidth. Use the rules to share out the bandwidth.
Submit	Click the **Submit** button to validate the new type of management.

Rule Properties

Name	This name must be unique.
Action	**Limit**: Uplink and Downlink are allowed maxima. **Grant**: Uplink and Downlink are guaranteed minima.
Uplink, Downlink	Specify here the percentages of the uplink and downlink total bandwidths to which the **Action** is applying.
Target Type	Specify whether the rule applies to the group of machines using it, or to each machine of the group. For example let's suppose the rule "Myband" applies to 5 computers, and let's suppose that Myband Uplink and Downlink are set to 5%. If you select **Group**, each computer will get 1% of the global bandwidth. If you select **Machine**, each computer will get 5%.
Insert	Create a new rule reflecting the Rule Properties panel, and insert it just before the selected rule.
Replace	Replace the selected rule with a new rule based on the Rule Properties panel.
Remove	Remove the selected rule.

List of Rules

Navigating into the List	To select a bandwidth rule, **click on its line** in the list, or use the keyboard **Up** and **Down** arrows. When a rule is selected, its settings are copied into the Rule Properties panel. You can do any modification in this panel.
Reload	Reloads the page with its last state.

Auxiliary Settings

Click **Settings** and **Auxiliary Settings**. This page gathers the settings of three features: Routing Table, Dynamic DNS, and LDAP client.

Static Routing Table

Overview	The primary use of the static routing table is to specify IP routes to specific hosts or networks via an interface. The interface can be one of the four LAN interfaces, or one of the 64 WAN interfaces.
Navigating into the Table	To select a route, **click on its line** in the table, or use the keyboard **Up** and **Down** arrows. When a route is selected, its settings are copied into the **Route Properties** panel. You can do any modification in this panel.
Destination IP, Network Mask, Gateway, Interface	The **Static Routing Table** contains a list of **Destination IP** addresses. Each destination IP address identifies a network that WOOWEB-PRO is configured to recognize. For each destination IP address, the routing table additionally stores a **Network Mask** that specifies the destination IP address range, a **Gateway** IP address, and a network **Interface**. WOOWEB-PRO extracts the destination IP address from each outgoing packet received from local machines. Starting from the first line, it compares this address to the list of destination addresses recorded in the table. If one of them matches, it forwards the packet to the corresponding gateway through the corresponding interface. The last entry always contains a null network mask so that all packets that do not match any preceding entry are finally forwarded to the default interface. **Note:** a null network mask (0.0.0.0) makes any packet match the destination IP. Following table entries are not reached. **Note:** if an entry contains a null gateway (0.0.0.0), the packets matching this entry are not forwarded.
Insert, Replace, Remove	Press these buttons to insert a new line, change the selected line, remove the selected line.
Submit the Table	As routing table modifications need a restart of the software, all modifications in this page are made **LOCALLY**. It means that nothing is transmitted to WOOWEB-PRO until you press **Submit the Table**. Be careful not to lose your settings by opening a new page without having previously clicked on **Submit the Table**.
Recharger	Reload the page with old settings. All modifications into this page are lost.

Dynamic DNS

Overview	The Dynamic DNS (DDNS) allows you to alias a dynamic IP address to a static hostname, allowing your servers to be more easily accessed from various locations on the Internet. WOOWEB-PRO is able to manage two DDNS service providers: www.dyndns.org and www.no-ip.org . You must first register yourself to one of the two providers to get a static hostname. Once configured, WOOWEB-PRO communicates with the DDNS service provider to update its DNS table. As soon as you get a new IP address from your ISP, WOOWEB-PRO transmits this address to the DDNS service provider that updates its table immediately. The switching time to the new IP address is rather short and most of time the switching is unseen by remote clients that try to get access to your servers.

Enable DDNS, DDNS Service	To use the DDNS service, check **Enable DDNS** and select the **DDNS Service**: DynDNS.org or No-IP.com
Host Name(s), User Name, Password	Fill in the information you registered with the DDNS service provider.
Status	Shows the DDNS information
Test	Press this button to check the connection with the DDNS provider.
Submit	Submit the settings to WOOWEB-PRO.

LDAP Settings

Overview	This is the place where you can setup the connection to an LDAP server for remote user authentication. See User Authentication.
LDAP Server Name or Address	Specify the server name or IP address.
Domain Name	Fill in the domain name if any, otherwise leave it empty
Port Number	Specify the port used for the connection. The default port is 389 or 636, 389 for primary TCP connections and 636 for LDAP over SSL.
Use SSL	Check this box if your LDAP server is configured for using SSL connections.
Submit	Send your changes to WOOWEB-PRO.

WAN Connection Status

Click **Maintenance** and **WAN Connections**. This page provides all information concerning the WAN connections. It also allows you to stop and start the WAN connections one by one.

WAN Connections	Select a WAN Connection into the list of available connections. The commands, as well as all information displayed in the management page relate to the selected WAN Connection. The **Stop** and **Start** buttons allow you to hang up and restart the connection. In case of a connection behind a router, WOOWEB-PRO does not manage directly the ISP connection, so clicking on **Stop** does not produce any physical hang up. However WOOWEB-PRO will stop sending and receiving packets from the router.
Connection Status	**State**: Shows the current state of the connection, ie Connecting, Connected, Releasing, or Not Connected **Time from Start**: Time elapsed since the connection passed into the Connected state **Time to Disconnect**: Time remaining before the disconnection **Downlink Speed (Kbps), Uplink Speed (Kbps)**: Real modem speed when provided by the modem, or user-provided connection speed (see Edit Wan Connection) **Receive Data Rate (Kbps), Send Data Rate (Kbps)**: Data rates as measured by WOOWEB-PRO **Opened Sockets**: Number of TCP and UDP sockets currently open **IP Address**: WOOWEB-PRO IP Address on the WAN side. Note that this is the Internet address in case of modem connection. **Primary DNS, Secondary DNS:** IP addresses of domain name servers **MTU Value**: MTU value currently in use by this connection **Outbound Accesses**: Number of local machines accessing the Internet via this connection **Inbound Accesses**: Number of remote machines accessing local servers via this connection **Daily Activity, Monthly Activity**: Activity time of this connection for the current day and the current month
Connection Traffic Counters	These counters show the volume of data received and sent since the connection has started. You can reset them to zero by clicking **Clear Counters**.

Save and Restore Settings

Click **Maintenance** and **Backup of Settings**. You can ask WOOWEB-PRO to save a copy of all current settings into a backup file. You can also restore a previous configuration from a backup file. WOOWEB-PRO uses an automatic naming of backup files based on the current date and time.

Save Settings	Click on **Save Current Settings to a File** and select the folder when asked for. A message indicates that the backup went through.
Restore Settings	First browse to select the backup file. Then click **Restore Settings from the File**. When you are asked to restart the router, click **Ye**s.

Software Updates

Click **Maintenance** and **Software Updates**. WOOWEB-PRO is able to periodically look for new versions. You can proceed to upgrades by uploading an upgrade file, or by asking WOOWEB-PRO to directly upgrade itself from the Prosum Web site.

Important Note: Starting from Vista, the installation of new versions cannot be achieved silently unless you disable the User Account Control (UAC) on the computer running WOOWEB-PRO. However we don't recommend doing so since it makes the system less secure. Thus the upgrades cannot be carried out remotely. You or someone else will have to stand close to the computer in order to provide the answers to UAC prompts.

Current Software	Displays the WOOWEB-PRO version in use.
Automatic Check	You can schedule automatic checking for WOOWEB-PRO updates at a desired frequency. Select **Never,** or the frequency to be **Weekly**, or **Monthly**.
Check for Update Now	You can manually check for an update any time by clicking on **Check Now**.
Update from Local File	Updating from a local file maybe useful in case of downgrading for example. Click **Browse...** to select the update file and then click **Upload**.

Debug

Click **Maintenance** and **Debug**. This management page gathers several debug tools that may help to work out the source of some problems.

Get Information

Debug Traces	When **Enable Trace Capture** is checked, WOOWEB-PRO continuously builds a trace file containing a capture of all packets exchanged across the LAN and the Internet connections. **Note:** You should not enable the trace capture unless requested by a technical support engineer. You should not leave the trace capture enabled for a long time because this is a very computer resource-consuming task.
Get Trace File	Click **Get Traces** to download the trace file from WOOWEB-PRO onto your computer**.** The default file name is "trace.zip".
Technical Report	The **Technical Report** is a file containing the configuration, the license information, and the logs. Click **Get Report** to save this file onto your computer. The default file name is "report.zip".

Ping

Ping Address	This tool permits to test whether a particular host is reachable from WOOWEB-PRO. Fill in **Host Name or IP Address** and click **Ping Host**. If WOOWEB-PRO is not running in your computer, please be aware that this is a ping from WOOWEB-PRO and NOT from your computer.
Ping Result	Shows the result of the ping.

Test Sites

Overview	Under this tab you can exercise the OrangeFilter service. This feature is not available if you did not acquire and register an OrangeFilter ticket. See OrangeFilter License.
Site Name or IP Address	Fill in the name or the IP address of the site to want to check and click on **Get Content Categories**.
Retrieved Categories	Read here the result of the OrangeFilter submission.
Submit Category	If you don't agree with the OrangeFilter classification, or if the site is not yet categorized and you want it to be categorized, click **Go to Category Submission Site** and fill in your request on the ISS Web page.

Manage the DHCP Server Table

Click **Maintenance** and **DHCP Table**. WOOWEB-PRO can provide a DHCP server on each of the four LANs. Refer to the LAN Setup page for getting help about the configuration of these DHCP servers.

This page is the place where you can manage the internal IP address tables of the DHCP servers. It displays the current state of all table entries and allows you to create **static addresses** and **excluded addresses**.

Static addresses are fixed IP addresses assigned to specific clients.

Excluded addresses are IP addresses that are not allocated by the DHCP server. They are holes into the pool of addresses.

Select the LAN Interface	Indicate which LAN you want to manage the DHCP server.
DHCP Server Table	The DHCP Server Table provides information about the **Excluded**, **Static**, and **Allocated** IP addresses. Free addresses of the pool are not listed into the table. To select a table entry, **click on its line**, or use the keyboard **Up** and **Down** arrows. When a line is selected, its information is copied into the **Entry Properties** panel. You can do any modification into this panel.
Make Static	To make static an allocated dynamic address, select its line into the table and click **Make Static**. To modify a static address, select its line into the table, modify **IP Address**, **Host Name**, or **MAC Address** and click **Make Static**. To create a new static address, fill in **IP Address**, **Host Name**, and **MAC Address** with new values and click **Make Static**.
Exclude	By clicking on **Exclude**, the address in **IP address** field is manually removed from the pool. **Note:** When the DHCP server is considering dynamically allocating an IP address to a client, it first sends a ping to this address. If no response is heard, it allocates the address. If a response is heard, it means the address is already in use on the network, so **the address is automatically excluded from the pool**, and the server tries with another address.
Return to Pool	Click **Return to Pool** to move an excluded or static address back to the pool. You should see the address being removed from the table.

Restart Router Engine

Click **Maintenance** and **Restart Router**. Restarts are managed by WOOWEB-PRO and most of time you don't need to restart the router engine manually. Restarts are automatically requested after important setting changes, and you just need to click **Yes**.

You can try to restart manually if you already postponed a restart asked by WOOWEB-PRO, and whenever you think that WOOWEB-PRO must be restarted from the ground up.

General Log

Click **Log** and **General Log**. This page displays the history of events concerning the operation of WOOWEB-PRO.

Log Content

Overview	The General Log content is updated dynamically in real time. Each record is composed as following: Time Stamp Type Text message **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size that the General Log file can reach. Beyond this size, older records are deleted.
Logged Events	Nine boxes allow you to select the type of internal events that must be recorded: **System** **Network** **OrangeFilter** **Remote Access** **DNS** **DHCP** **PPPoE** **NAT** **Web Server** **Note**: Even if none of the nine boxes is checked, the most important events are nevertheless recorded. **Note**: You should not leave all boxes permanently checked because it may slow down the Internet accesses.
Backup Log File	Click **Get Log File** to download the **General Log** file (zipped tabbed text file).

Outbound Access Log

Click **Log** and **Outbound Access**. This page displays the records all machine Internet accesses.

Log Content

Machine	There is one log for each machine. Select the machine whose log you want to see.
Date	As Outbound Access logs can be huge, it is possible to directly go to a date. Use the calendar to select a date.
Site	This is the site corresponding to the selected line of the log. Click on it to open the site.
Block this Site in	You can block this site by adding it into the black list of some profiles. Select which profile will get this site into its black list, and click **Block it**. **Note:** You can add this site into several profiles by repeating the black listing operation with several profiles.
Outbound Access Log	The Outbound Access Log content is updated dynamically in real time. Each record is composed as following: **Time Stamp** **User**: name of the user. Note that this field may be empty if **User Authentication** is not set for this machine. See Local Machines **Site**: IP address or name of the site that was requested **Duration** **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size all machine log files can reach. Beyond this size, older records are deleted.
Backup Log File	Click **Get Log File** to download the log file (SQLite format).

Outbound Firewall Log

Click **Log** and **Outbound Firewall**. This page displays the records concerning the Internet access requests that have been denied.

Log Content

Overview	The Outbound Firewall Log content is updated dynamically in real time. Each record is composed as following: **Time Stamp** **Machine**: name of the machine that has been blocked **User**: name of the user. Note that this field may be empty if **User Authentication** is not set for this machine. See Local Machines **Site**: IP address or name of the site that was requested **Profile**: name of the profile that denied the access **Filter**: type of filter that denied the access **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size the log file can reach. Beyond this size, older records are deleted.
Backup Log File	Click **Get Log File** to download the log file (SQLite format).

Inbound Access Log

Click **Log** and **Inbound Access**. This page displays the records concerning the inbound connections to your servers.

Log Content

Overview	The Inbound Access Log content is updated dynamically in real time. Each record is composed as following: **Time Stamp** **Rule** that allowed the connection **Remote IP Address** **Port** **WAN Connection** **Duration** **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size the log file can reach. Beyond this size, older records are deleted.
Backup Log File	Click **Get Log File** to download the log file (SQLite format).

Inbound Firewall Log

Click **Log** and **Inbound Firewall**. This page displays the records concerning the intrusion attempts that have been blocked.

Log Content

Overview	The Inbound Firewall Log content is updated dynamically in real time. Each record is composed as following: Time Stamp IP Address of the attacking computer TCP/UDP port that was targeted Protocol used WAN Connection **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size the log file can reach. Beyond this size, older records are deleted.
Backup Log File	Click **Get Log File** to download the log file (SQLite format).

WAN Connection Log

Click **Log** and **WAN Connection**. This page displays the starting date/time and the duration of all WAN connections.

Log Content

WAN Connection	There is one log for each WAN connection. Select the WAN Connection whose log you want to see.
WAN Connection Log	The WAN Connection Log content is updated dynamically in real time. Each record is composed as following: **Time Stamp** **Connection Time** **Note:** The time stamp is in ISO 8601 format, i.e. YYYY-MM-DD hh:mm:ss.
Browsing the Log	To limit the size of transmitted HTML pages, the records are displayed by blocks of 2KBytes. You can browse the log by using the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons.
Clear	Click the **Clear** button and confirm to delete all records.

Log Configuration

Log File Maximum Size	Select the maximum size all WAN Connection log files can reach. Beyond this size, older records are deleted.
Backup Log File	Click **Get Log File** to download the log file (SQLite format).

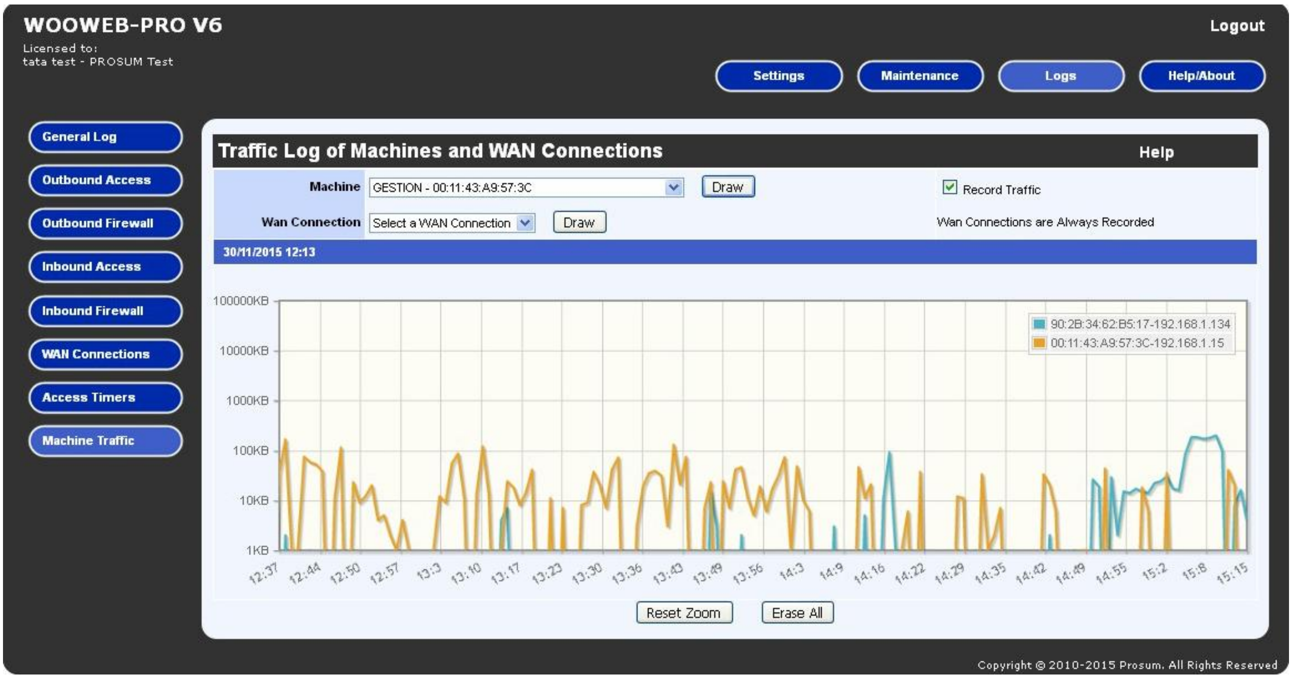
Log of Machine and Internet Connection Traffics

Click **Log** and **Machine Traffic**. This page can display a chart of the received traffic in KB/s measured for each machine and each WAN connection during the last 24 hours. The traffic of WAN connections is always recorded. In contrast, the traffic of machines is recorded only on request.

Drawing in the chart: The plotter can draw the chart of any traffic that has been recorded. On the same chart, you can draw the traffic of several machines and WAN connections. For each machine and connection you want to draw, select the machine or connection into the drop list, and click on the corresponding **Draw** button. The graph is added to the chart. Notice that you cannot remove the graph of a machine or connection that has been already drawn. You can only add new graphs or erase everything by clicking on **Erase All**.

Zooming: By selecting a zone of the chart with the mouse, you can horizontally zoom in on this portion of the graph to look at some details. To zoom out, click on the **Reset Zoom** button.

Axis: The X axis shows the time in hours and minutes. The date is not printed for the sake of clarity. However, the date of the first record is printed into the green bar above the chart. The Y axis uses logarithmic coordinates allowing to correctly seeing the low and high traffic values expressed in KB/s.



WOOWEB-PRO V6

Licensed to:
tata test - PROSUM Test

Traffic Log of Machines and WAN Connections

Machine: GESTION - 00:11:43:A9:57:3C

☑ Record Traffic

Wan Connection: Select a WAN Connection

Wan Connections are Always Recorded

30/11/2015 12:13

Copyright © 2010-2015 Prosum. All Rights Reserved

Machine and WAN Connection Drop Lists	Select a machine or Internet connection. **Note:** When you change the selected machine, the Record Traffic box is automatically updated to reflect the state of the traffic recorder concerning this machine. The traffic of the Internet connections is always recorded.
Draw	Click on one of these buttons to add the graph of the selected machine or Internet connection to the chart. If the selected machine was not under traffic surveillance, you receive a "No data" alert and nothing is plotted.
Record Traffic	This box is checked when WOOWEB-PRO is recording the traffic of the selected machine. As this box is not read-only, by clicking it you tell WOOWEB-PRO that you want to start or stop recording the traffic of the selected machine.
Reset Zoom	Click on this box to redraw everything with the default zoom value.
Erase All	Erase all graphs.

User License Management

Click **Help/About** and **User License**. This page shows the status of your user license.

By installing WOOWEB-PRO, you get a 30-day free trial. During the trial period, at start time WOOWEB-PRO opens a "Welcome" window on the computer on which it is installed. Just click on the **Try** button to start. After this 30-day trial period, a user license must be purchased and registered. After the product is registered, the "Welcome" window does not open anymore.

To buy the user license, you can either contact your reseller, or buy it on-line with a credit card. If you wish to buy the license on-line, go to the "**Purchase WOOWEB-PRO**" Web page on the PROSUM Web site, or click on **Order on Line.**

After you have got the **User License** file, store it on your computer. Then into **Register a New License**, use the **Browse** button to select the license file, and click **Register** to transfer the license to WOOWEB-PRO**.**

The license information is displayed in **Status**, **User Name**, and **Organization**. It is also displayed on top left of each page of the management.

Note: The user license gives you the right to install WOOWEB-PRO on a single personal computer. There is no limitation of users or local machines.

OrangeFilter Ticket

Click **Help/About** and **OrangeFilter** License.

The OrangeFilter service is optional. When enabled, it allows you to set up profiles with site-content filters. See Edit Profile. The purpose is to prevent users, for example children, to visit inappropriate web sites, or on the contrary to restrict them to certain categories of content.

To buy a two-year ticket for OrangeFilter service, you can either contact your reseller, or buy it on-line with a credit card. To buy on-line, go to the "Purchase WOOWEB-PRO" Web page on the PROSUM Web site, or click on the **Order on Line** button.

After you got the ticket file, store it on your computer and into **Register a New Ticket**; use the **Browse** button to select it. Then click **Activate the Ticket**.

The ticket information is displayed in **Status**, **Remaining Days**, **User Name**, and **Organization**. A warning message is displayed during the last 7 days before the ticket expiration date.

Proceed exactly the same way as above to renew your subscription.

The **Release the Ticket** button disables the ticket in the ISS servers in order to reuse the ticket on another machine for example. Any ticket must be disabled before being used again on another machine. When the ticket has been disabled, the content-filtering feature is no longer available.

Note: In case of computer crash for example, it may happen that you do not get enough time for disabling the ticket. Do not worry; the ticket will be automatically disabled within a 24-hour delay.

You can check the good working of the **OrangeFilter** service in the Debug page. For example, to check the good working of **OrangeFilter**, you can try to get the ISS classification of a site by clicking **Get Content Categories**.

Index