Columbitech Wireless VPN™

Version 1.1

User's Guide

Updated: 20 December 2001

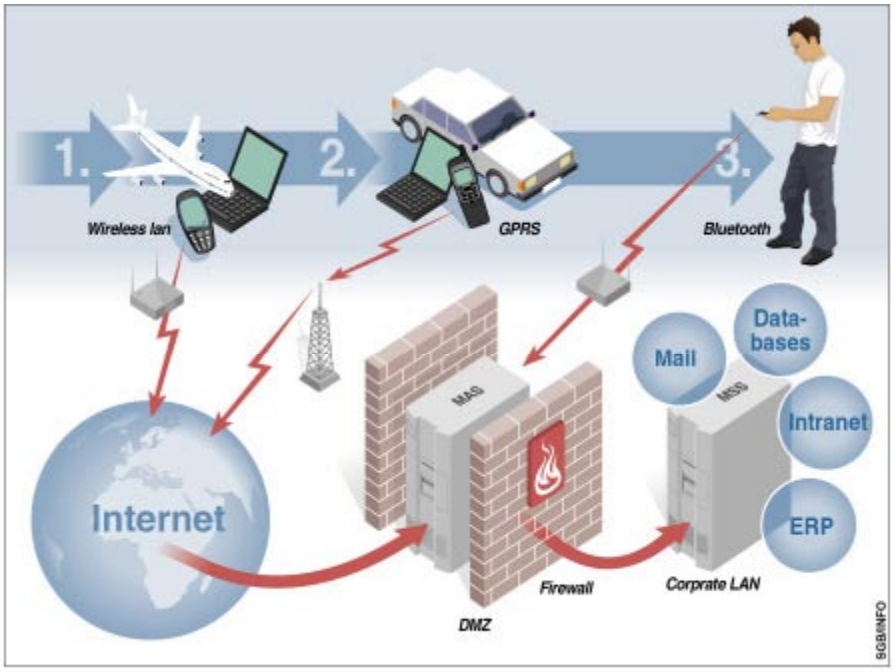
Table of contents

Columbitech Wireless VPN™

Columbitech Wireless VPN™ is a session level VPN architecture designed to eliminate the wireless weaknesses of today's VPN solutions, while at the same time creating something as unique as a roamable, wireless VPN with true end-to-end security. The solution has been designed to meet the requirements for true mobile communication, i.e. secure corporate access anywhere, anytime, and with any device.

Columbitech Wireless VPN™ includes solutions for:

- End-to-end security for remote data access.
- Automatic reconnect, session resume, transaction recovery and enables secure seamless roaming across all wireless IP-networks.
- Optimization for all networks and all major devices.



Architecture

Columbitech Wireless VPN™ is a client/server based software architecture. The client software is installed on every wireless VPN-enabled mobile terminal, and the server software is installed on a server machine on the corporate network. When the client connects to the corporate network, a secure and encrypted tunnel is established between the client and a Columbitech Mobile Session Server™ (MSS) on the corporate network. This can be done directly to the Columbitech MSS or through a Columbitech Mobile Authentication Server™ (MAS). The Columbitech MAS is usually placed in the company's DMZ (DeMilitarized Zone). Clients are authenticated using one or several of the following methods: one-time password (either by the Columbitech MSS or by the Columbitech MAS in the DMZ), client certificate and username/password.

Optimizations

The architecture implements transport optimizations that adapt messages for networks with different characteristics, and advanced data compression is applied at the session level before the data is encrypted.

Seamless interoperability

Columbitech Wireless VPN™ is designed for seamless interoperability with existing corporate solutions. A company that is already using an IP VPN solution may deploy Columbitech's wireless VPN as a wireless extension and still benefit from their existing IP VPN for wireline services. If a company is not currently operating an IP VPN, the Columbitech Wireless VPN™ is able to provide traditional wireline VPN services in addition to the wireless functionality. Many of the wireless optimizations implemented in the Columbitech architecture are just as applicable to a wireline environment.

Supports industry-standard API:s

The Columbitech architecture is a client/server software based solution built on wireless technology for optimal performance. To ensure easy wireless enabling of corporate legacy applications, the software supports industry-standard application programming interfaces on the client and server side.

The following platforms are supported:

Client side	Server side
▪ Windows 2000 Professional ▪ Windows XP ▪ Pocket PC 2002	▪ Windows 2000 Server

Connecting to Columbitech Mobile Session Server™

When the Client computer is started, immediately after you try to log on, a dialog with the following text is displayed:

"Do you wish to connect to the Wireless VPN server?"

If you click **Yes** you will connect to Columbitech Mobile Session Server™. If you click **No** you will not be connected to Columbitech Mobile Session Server™, and will only be able to work *locally* on your computer.

If you, when logging on, will connect through any kind of dial-up connection, you have to click **No** on the question above, and connect to Columbitech Mobile Session Server™ from the Monitor, after logging in, as described in the next chapter.

If you are working offline, you can at any time connect by clicking **Connect** on the Monitor, more thoroughly described in the next chapter.

Monitor icon

When the Columbitech Wireless VPN™ Client is connected to a Columbitech Mobile Session Server™, the Client Monitor icon is displayed in the system tray. The Monitor icon will be further described on the next page.

The Columbitech Wireless VPN™ Client Monitor

The Columbitech Wireless VPN™ Monitor is a tool for managing the connections used with Columbitech Wireless VPN™. The Monitor is started automatically when you start your computer, even if you work offline.

Location

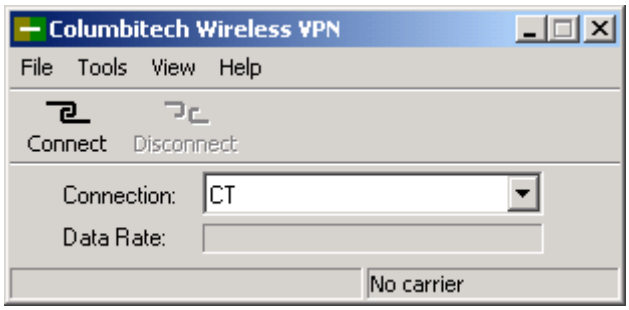
The Monitor icon is displayed in the system tray.

Monitor icon

The monitor icon displays the client's connection status, as described below:

Icon	Status	Description
	Connected	If the client is connected to a Columbitech Mobile Session Server™, the icon is green (where the blue ribbons indicate the current data rate).
	Connected, but no physical carrier	If the client is connected to the MSS, but has no physical carrier connection, the icon is yellow.
	Disconnected	If the client is disconnected, the icon is red.

Monitor window



Field descriptions

The fields and buttons in the Columbitech Wireless VPN™ Monitor are described below:

Field / button	Description
Connect	Click here to connect the Client to Columbitech Mobile Session Server™.
Disconnect	Click here to disconnect the client from Columbitech Mobile Session Server™. *Note!* When you are disconnected you will only be able to work locally on your computer.
Connection	This is where you choose what connection to use. If you choose **Automatic**, the connection with the best data rate and link quality will automatically be used.
Data Rate	The rate at which data is transferred.
(Lower left corner)	Status messages. These messages can later be viewed using the View/Logfile menu option.
(Lower right corner)	This is where the current connection name is displayed.

Menu descriptions

The menus in the Columbitech Wireless VPN™ Monitor are described below:

Menu	Description
File	The **Connect** and **Disconnect** options have the same functions as the buttons with the same names described above. When choosing **Exit**, the Monitor and the Monitor Icon in the system tray disappears. To display the Monitor and Monitor icon, select **Programs**, **Columbitech WVPN** and **WVPN Monitor** on the **Start** menu.
Tools	When pressing the **Settings** option, the Configuration applet appears. See the next section for details. The **Start** and **Stop** options are used for starting and stopping the Columbitech Wireless VPN™ service, i.e. disabling the wireless VPN and letting you connect to your network unencrypted.
View	Selecting the **Log file** option displays a text log file, if there is one. Otherwise, this option is not available.
Help	Shows which version of Columbitech Wireless VPN™ that is installed.

Deactivate Columbitech Wireless VPN

If you want to connect to your company network without using Columbitech Wireless VPN™, you have to deactivate Columbitech Wireless VPN™:

To deactivate Columbitech Wireless VPN™:

1. Select **Settings** on the **Tools** menu in the Monitor window.
   Result: The **Columbitech Wireless VPN dialog** is displayed.
2. Select the **Disable Wireless WVPN** check box.
3. Restart the computer.

Note! You might now be connected to your network unencrypted.

Diagnostic logging

Event logging

The Columbitech Wireless VPN™ client use the Windows 2000 Event Log to store messages (error, warning and information).

The Columbitech Wireless VPN™ services also have a diagnostic level that affects the amount of information logged in the event log. Four levels are available for the diagnostic logging:

1) No diagnostic logging
2) Low
3) Medium
4) High

Enable diagnostic logging

Follow the steps below to enable diagnostic logging:

1. Open the Columbitech Wireless VPN™ configuration applet from the Control Panel.
2. Select the **Logging** tab.
3. Select the level of logging that you want and click OK.

Viewing Event Log messages

The event log messages are displayed in the Windows Event Viewer.

To display the Event Viewer:

1. Select **Settings** on the **Start** menu, and then select **Control Panel**.

Click the **Administrative Tools** icon, and then click the **Event Viewer** icon.

Description of Event Log messages

For descriptions of the event log messages, see *Appendix A - Event log messages* in the *Columbitech Wireless VPN™ System Administrator's Guide*.

Status log file

A simple text log file can be displayed by selecting **Log file** on the **View** menu in the client monitor window. The file lists the status messages displayed in the status bar of the client monitor in chronological order with the most resent event at the end of the log file.

The Columbitech Wireless VPN™ Client Configuration Applet

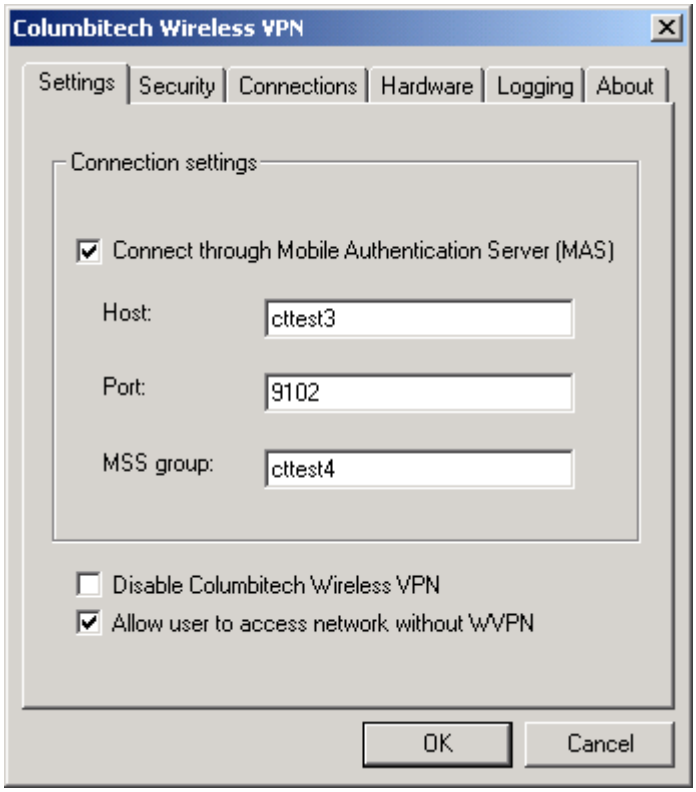
The Columbitech Wireless VPN™ configuration applet is a tool for adjusting and configuring security and connectivity settings. The only tab an ordinary user should use is the **Connections** tab.

Location

The Configuration Applet is found in three different ways:

- It is displayed on the **Start** menu under **Programs**, **Columbitech WVPN**, **Columbitech WVPN Configuration**.
- Its icon is displayed in the Control Panel.
- It can be reached by selecting Settings on the **Tools** menu in the Monitor.

The Settings tab

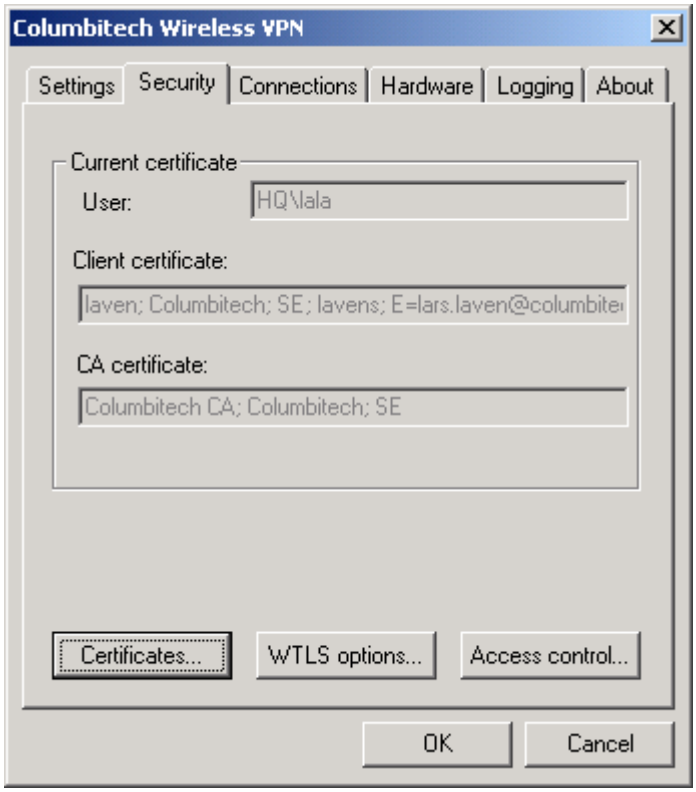


The settings under this tab should not be altered unless you are aware of what you are doing.

The Settings tab, continued…

Field	Description
Connect through Mobile Authentication Server (MAS)	If this checkbox is enabled, the client will connect through a Columbitech Mobile Authentication Server™ to reach a Columbitech Mobile Session Server™.
Host	If connecting through a Columbitech Mobile Authentication Server™, this should be the name or IP address of the Columbitech Mobile Authentication Server™, otherwise it should be the name or IP address of the Columbitech Mobile Session Server™. In case you use other Columbitech Mobile Session Servers for some connections, you can change this address individually for each connection, under the **Connections**
Port	If connecting through a Columbitech Mobile Authentication Server™, this should be the port number used on the Columbitech Mobile Authentication Server™, otherwise it should be the port number used on the Columbitech Mobile Session Server™.
MSS group	If connecting through a Columbitech Mobile Authentication Server™, this should be the logical name identifying the Columbitech Mobile Session Server™, or group of Columbitech Mobile Session Servers, that you want to connect to.
Disable Wireless VPN	If you want to connect to your company network without using Columbitech Wireless VPN™, you can deactivate the Columbitech Wireless VPN™. This is done by selecting the **Disable Wireless WVPN** check box, and then restarting the computer.
Allow users to access network without WVPN	By default, a user cannot connect to the corporate network if the wireless VPN is installed on the client but not connected to the server. Check this option if you want to be able to log on to the network without connecting to Columbitech Mobile Session Server™, i.e. if you want to be able to bypass the wireless VPN.

The Security tab

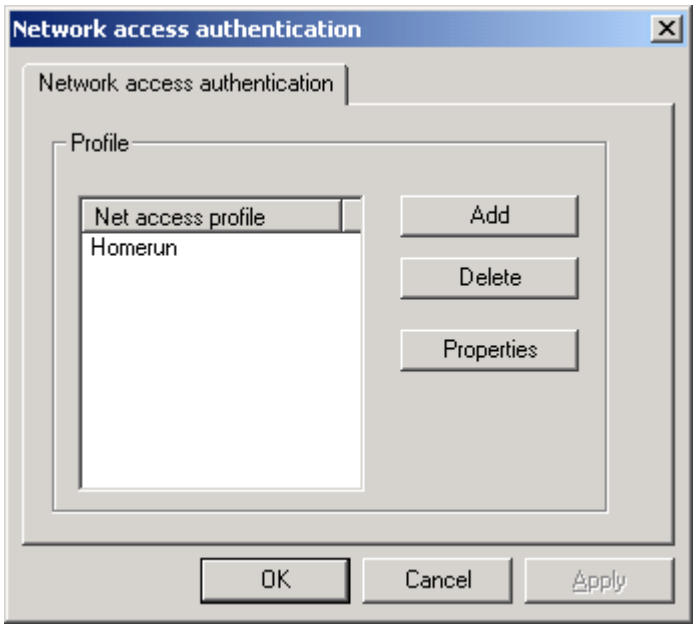


The settings under this tab should not be altered unless you are aware of what you are doing.

Button	Description
Certificates button	Click this button to display the **Certificates** dialog, where you can view, import, request, revoke and delete client and CA certificates. See the *Columbitech Wireless VPN™ Administrator's Guide*.
WTLS options button	Under the **WTLS-options** button allowed encryption algorithms, key exchange methods and hash algorithms can be viewed and chosen. You can choose any number of methods or algorithms, as long as there is at least one selected under each tab. Also, under each tab there must be at least one selection that corresponds to (is the same as) the methods or algorithms selected on the Columbitech Mobile Session Server™.
Access control button	Under the **Access control** button you configure network access profiles used when you must logon to an access network before being able to use the network to connect to your office network. This might be necessary for some hot-spot networks that require users to provide user credentials before allowing them to use the hot-spot network.

Access control button

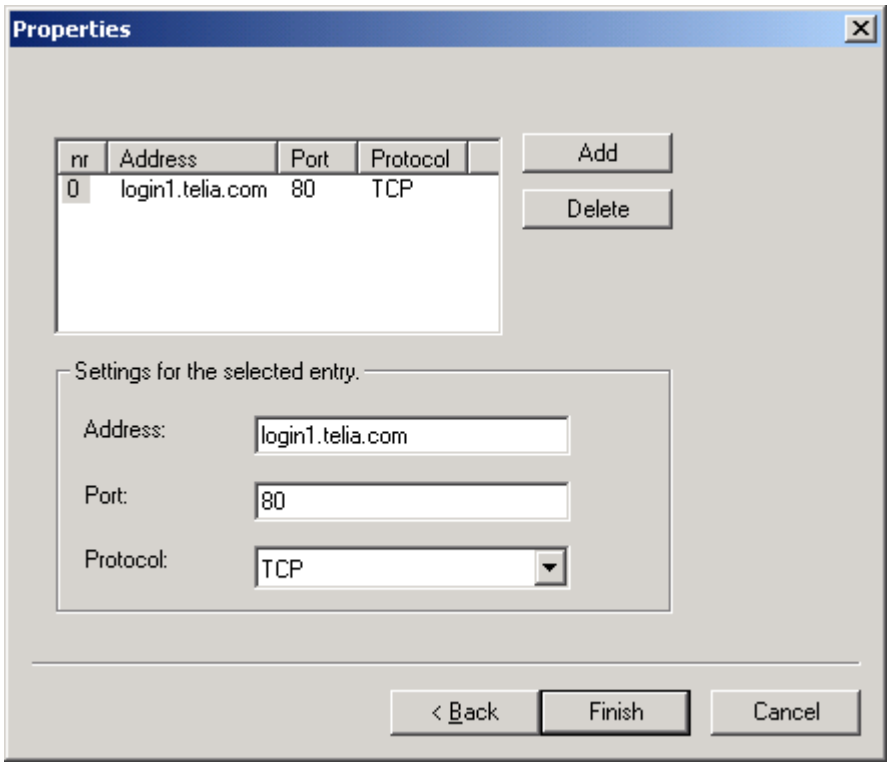
By providing an **Access network profile** you are allowed to bypass the Wireless VPN long enough to complete the initial logon transaction on the access network.



Button	Description
Add	Click this button to add a new Network access profile.
Delete	Click this button to delete the selected profile.
Properties	Click this button to view the settings for the selected profile.

Adding a profile

1. Press the **Add** button in the **Network access authentication** dialog.
2. Enter a name for the new profile.
3. Press the **Add** button in the **Properties** dialog to create a new entry.



4. In the **Address** field, enter the host name to which you want to open up a whole in the Wireless VPN.
5. In the **Port** field, enter the port that will be used.
6. In the **Protocol** field, enter the protocol type.
7. Create any additional entries if required by pressing the **Add** button again.
8. Press the **Finish** button to create the new profile.

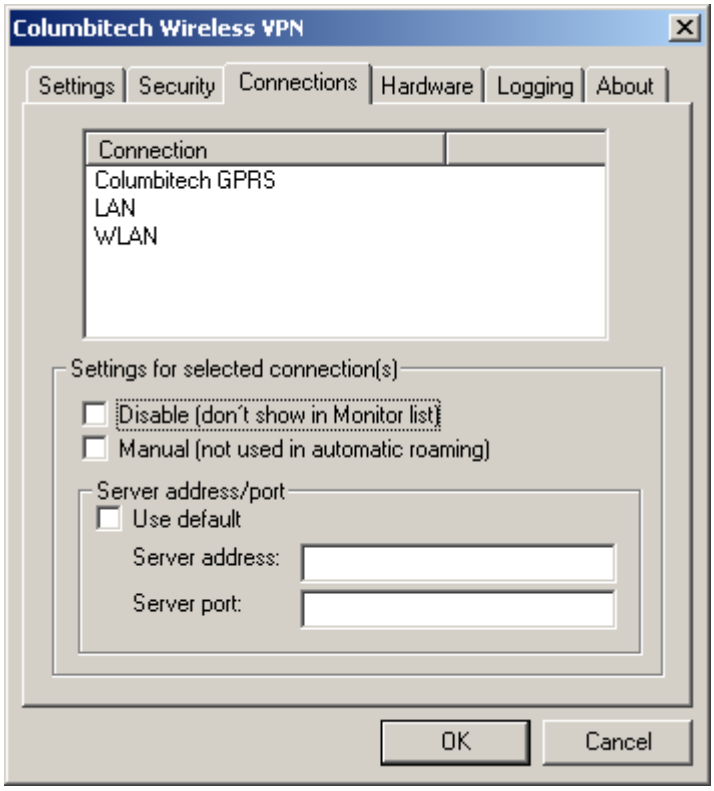
Using a profile

If a connection to your Wireless VPN server fails and you have an access network profile configured, a dialog listing all configured profiles will be shown:

1. Select the profile that you want to use.
2. Perform the required access network logon, e.g. open a browser, go to the URL for logging on to the access network, and provide your user credentials required to use the access network.
3. The initial connection to your Wireless VPN server will be completed.

The Connections tab

Under the **Connections** tab, all your available network connections are displayed. For each connection there are three possible connection-specific settings: the **Disable** check-box, the **Manual** check-box and **Server address/port** field.



Note! All dial-up connections are set to manual by default when installing Columbitech Wireless VPN™ Client, see below under **Manual** for clarifications.

Field	Description
Disable	When selecting this option, the connection will not be used by Columbitech Wireless VPN™, and the connection will not be displayed in the Columbitech Wireless VPN™ Monitor's connection list.
Manual	When selecting this option, the connection will not be used in automatic roaming. Instead you will have to select the connection manually in the **Connection** field in the Monitor. All dial-up connections are set to manual by default when installing Columbitech Wireless VPN™ Client.
Server/address port	This field enables you to enter advanced settings for every connection that overrides the default settings. For example when using GSM/CDPD/GPRS or any other public network, the Columbitech Mobile Session Server™ might have to be addressed through a NAT server. Therefore it is possible to enter different IP addresses and ports for individual connections.

Tip! If you want to, you can force Columbitech Wireless VPN™ Client to let you confirm the change to a dial-up connection: If you do not let Windows 2000 save your password for a dial-up connection, you will be able to confirm the change to this connection with your password every time the Columbitech Wireless VPN™ Client finds this connection appropriate. This might be a considerable option for your dial-up connections. For example you might not want to connect through your GSM-modem when your WLAN access-point reboots.

The Hardware tab The settings under this tab should not be altered.

The Logging tab Configure what level of diagnostic logging to use. The log messages are written to the Windows Event Log.

The About tab Shows which version of Columbitech Wireless VPN™ Client that is installed.

Manual configuration

If you want to use the client machine without Columbitech Wireless VPN™, you must make sure that the **Client for Microsoft Networks** option for the network adapter is activated.

Step-by-step To activate the **Client for Microsoft Networks** option:

1. Right-click the **My Network Places** icon and select **Properties**.
2. Right-click the first network adapter (e.g. LAN and WLAN) and select **Properties**.
   Note! Do not select the Columbitech Wireless VPN Network Adapter.
3. Select the **Client for Microsoft Networks** check box.
4. Repeat steps 2 and 3 for all LAN and WLAN adapters except the Columbitech Wireless VPN™ Network Adapter.