Columbitech Wireless VPN™

Version 1.1

Getting Started

Updated: 30 January, 2002

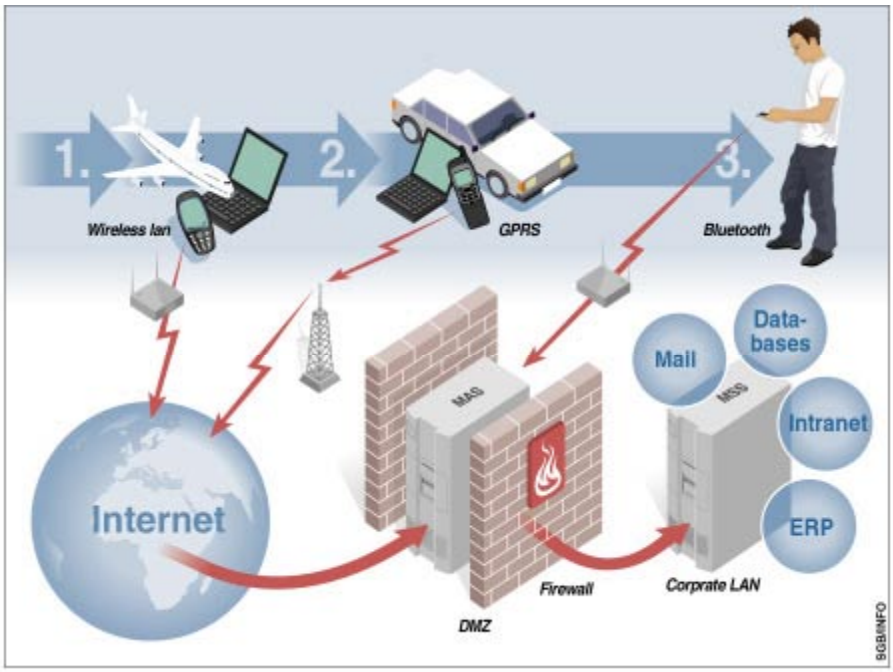
Table of contents

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.



Arcitecture

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 Professional ▪ Pocket PC 2002	▪ Windows 2000 Server

System Requirements

Server

Columbitech Mobile Session Server™ requires Windows 2000. We recommend that you use the latest service pack. The hard disk requirement is 5MB.

Columbitech Mobile Authentication Server™ requires Windows 2000. We recommend that you use the latest service pack. The hard disk requirement is 5MB.

Client

Columbitech Wireless VPN™ Client for Windows requires Windows 2000 Professional or Windows XP. We recommend that you use the latest service pack. The hard disk requirement is 5MB.

Columbitech Wireless VPN™ Client for Pocket PC requires Pocket PC 2002. The storage space required is 1MB RAM.

Server Installation

Preparations

User rights

All users of the Columbitech Wireless VPN™ must have the **Logon as a batch job** user right locally on the Columbitech Mobile Session Server™ computer.

Setting user rights

You can set the **Logon as a batch job** user right in two ways. Either:

- Create a user group for the WVPN users and give the group the user right, *or*
- Give the existing **Domain Users** group the user right.

To give a user group the **Logon as a batch job** user right:

1. Select **Programs** on the **Start** menu, and then **Administrative Tools** and **Local Security Policy**.
   Result: The **Local Security Settings** window is displayed.
2. Select **User Rights Assignment** in the left pane, and double-click **Log on as a batch job** in the right pane.
3. Add the **Domain Users** group, or the group that you have created, for example **WVPN Users**.

Before you start

Do I need to install a Mobile Authentication Server (MAS)?

Columbitech Mobile Authentication Server™ is an optional server component that you typically install on the corporate DMZ (DeMilitarized Zone) network. You install it if you want to authenticate users with single-time passwords before letting them in to the Columbitech Mobile Session Server™ on the corporate network. Another reason to install a Mobile Authentication Server is if you want all external connections to pass through a computer in the corporate DMZ.

The permanent TCP connections between the Mobile Authentication Server and the Mobile Session Server are initiated from the Mobile Session Server. This gives you the opportunity to configure your Firewall so that it only permits a TCP connection between the Mobile Authentication Server and the Mobile Session Server if it is initiated from the inside.

Local administrator

When you install Columbitech Mobile Session Server™ or Columbitech Mobile Authentication Server™ you must have **local administrator** rights on the server computer. By default, members of the **Domain Admins** group have this right on all computers in the domain.

Network information

Make sure that you have the following available:

- The IP address for the Columbitech Mobile Session Server™, Columbitech Mobile Authentication Server™, and the DCHP server.

Signing your own certificates

When you configure the Columbitech Mobile Session Server™ or Columbitech Mobile Authentication Server™ you can sign your server and client certificates using either:

- The Certificate Manager application and be your own certificate authority and sign your server and client certificates. The Certificate Manager application is included in Columbitech Mobile Session Server™ and is described in *Appendix A – Certificate Management* on page 42.
  or
- An external certificate authority (CA).

The step-by-step procedure in this document describes how you install and configure the server if you sign your own certificates.

Location of installation file

We recommend that you install Columbitech Wireless VPN™ from the CD, or that you place the WVPNServer.exe file on a local drive on the server where you will install Columbitech Mobile Session Server™.

Installing the Columbitech Mobile Session Server™ - step by step

To install and be able to use Columbitech Mobile Session Server™, you have to run the installation wizard, configure the server and import server certificates.

The step-by-step procedure in this document describes how you install and configure the server if you sign your own certificates.

The steps below are described in more detail in the following sections.

Step 1 Install the server by running the installation wizard.

Step 2 Configure the server and client settings in the configuration applet.

Step 3 Create a CA Certificate (root certificate) using the Certificate Manager.

Step 4 Import the CA certificate. This is the CA certificate that is or will be used to sign the client certificates.

Step 5 Import a server certificate.

Step 6 Start the Columbitech Mobile Session Server™ service.

Step 1 - Install the server

Step-by-step

1. Insert the installation CD in the CD drive.
   Result: The **Install Columbitech Wireless VPN™** dialog is displayed.
2. Click the **Install Mobile Session Server** button.
   If the **Install Columbitech Wireless VPN™** dialog is not displayed, double-click the **Setup.exe** file on the CD.
3. Follow the instructions in the installation wizard.
   We recommend that you select the **Typical** installation.

Note! During the installation you will see one or more dialogs with the title **Digital Signature Not Found**. This is no error, but a warning that you are about to install device drivers not signed by Microsoft. Just click **Yes** to continue the installation.

Step 2 - Configure the server

When the installation is finished, the configuration applet is started automatically, and the **Columbitech Wireless VPN dialog** is displayed.

Configuration applet location

The configuration applet, **Columbitech WVPN**, is located in the Control Panel. It can also be started from the Columbitech WVPN program group:

Step-by-step

Follow the instructions below to configure Columbitech Mobile Session Server™:

1. Verify the values under the **Settings** tab. These values were retrieved by the Installation Wizard.
2. Select the **Use DHCP server** check box and enter the default settings in the **DHCP server** field.
3. On the **Security** tab, select the following:

Select	If you want clients to authenticate using:
One-time password	A randomly generated password every time you log on to the client.
User name and password	The user name and password used to log on to your Windows 2000 domain. This option is selected by default.
Client certificate	A certificate for the client. This option is selected by default.

Leave the **Columbitech Wireless VPN dialog** open since you will come back to import the CA certificate.

Step 3 - Create and export a CA certificate

Creating a CA certificate

Continue by creating a CA certificate (root certificate). The CA certificate will be used to verify server and client certificates as well as creating new certificates and signing certificate requests. To create a CA certificate, you must start the **Certificate Manager** application. Create the certificate by following the instructions in *Creating a CA certificate* on page 42.

Exporting a CA certificate

The CA certificate must be exported to a file so that the server and the clients can import and use it for certificate verification. Export the certificate by following the instructions in *Exporting the CA certificate* on page 43 and then close the Certificate Manager. Please note that this *Getting Started* guide assumes that you create and use your own root certificates.

Step 4 - Import a CA certificate

The next step is to import the CA certificate. The server uses the CA certificate to verify the client certificates. Follow the instructions below:

Step-by-step

1. In the **Columbitech Wireless VPN dialog** (which is displayed by clicking the Columbitech WVPN icon in the Control Panel), click **Certificates** on the **Security** tab.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **CA Certificates** tab.
   Result: The **Import** dialog is displayed.
3. Point to the certificate you want to import and click **Open**.
   Result: The CA certificate is imported and displayed on the **CA Certificates** tab.

Step 5 - Import a server certificate

Finally, you have to import a server certificate. In this manual we will describe how you import a certificate that you have created in advance.

Tip! You can also request and import a new server certificate by creating a certificate signing request (CSR) and signing it yourself. This is described in *Appendix A – Certificate Management* on page 42.

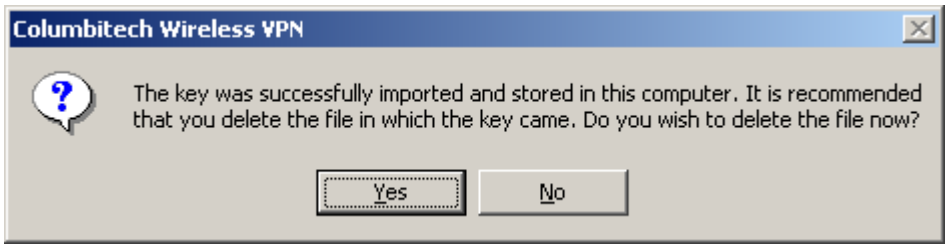
Follow the steps below to create a certificate and import it.

Step 1 - Create a certificate

To create a certificate, you have to start the Certificate Manager application and then follow the instructions in *Creating a certificate* on page 44.

Step 2 - Import an existing server certificate

1. Click the **Certificates** button on the **Security** tab in the **Columbitech Wireless VPN dialog**.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **Server Certificates** tab.
   Result: The **Import choice** dialog is displayed.
3. When importing an existing certificate, both the certificate and the private key must be imported. Select **Certificate and private key** and click **OK**.
   Result: The **Import certificate** dialog is displayed.
4. Select the certificate and click **Open**.
   Result: The **Import Private Key** dialog is displayed.
5. Select the private key and click **Open**.
   Result: The **File Password** dialog is displayed.
6. Enter the password that is used to protect the private key file and click **OK**. This is the password given in the Certificate Manager when the key was written to file. See *Creating a certificate* on page 44.
   Result: The following message is displayed:



7. For security reasons, the file containing the private key should be deleted. Click **Yes** if you want to delete the file.
   Result: A message is displayed, confirming that the certificate has been imported.
8. Click **OK**.
   Result: The **Server Certificates** tab in the **Certificates** dialog is displayed with the imported certificate.
9. Click **OK** to close the **Certificates** dialog.

Step 6 - Start Columbitech Mobile Session Server™ service

After completing the server configuration and closing the Columbitech Wireless VPN configuration applet, you are asked to start the Columbitech Mobile Session Server™ service. You are now ready to start using the server.

Tip! Verify in the Windows Event Log that no errors where detected when the Columbitech Mobile Session Server™ service was started.

Installing the Columbitech Mobile Authentication Server™ - step by step

To install and be able to use Columbitech Mobile Authentication Server™, you have to run the installation wizard, configure the server and import server certificates.

The step-by-step procedure in this document describes how you install and configure the server if you sign your own certificates.

The steps below are described in more detail in the following sections.

Step 1 Install the server by running the installation wizard.

Step 2 Configure the server and client settings in the configuration applet.

Step 3 Import the CA certificate. This is the CA certificate that is or will be used to sign the client certificates.

Step 4 Import a server certificate.

Step 5 Start the Columbitech Mobile Authentication Server™ service.

Step 1 - Install the server

Step-by-step

4. Insert the installation CD in the CD drive.
   Result: The **Install Columbitech Wireless VPN™** dialog is displayed.
5. Click the **Install Mobile Authentication Server** button.
   If the **Install Columbitech Wireless VPN™** dialog is not displayed, double-click the **Setup.exe** file on the CD.

Follow the instructions in the installation wizard.
We recommend that you select the **Typical** installation.

Step 2 - Configure the server

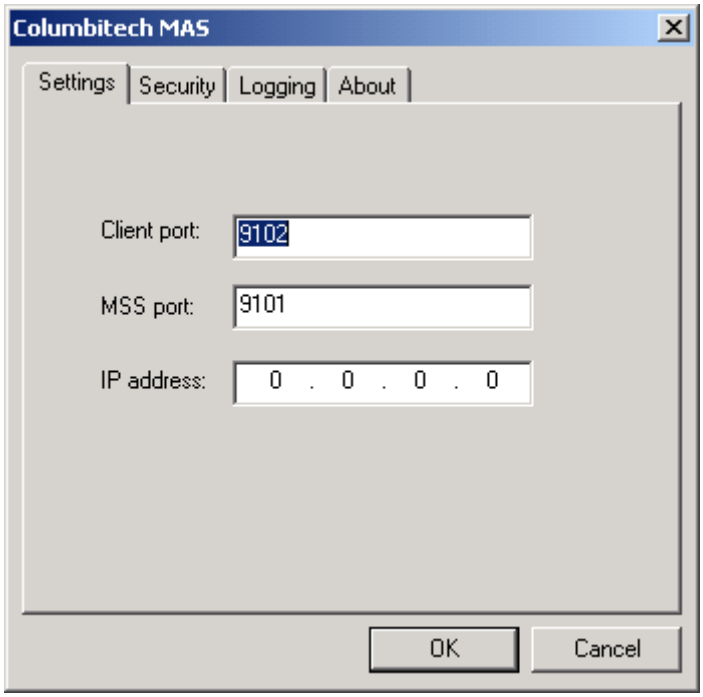
When the installation is finished, the configuration applet is started automatically, and the **Columbitech MAS dialog** is displayed.

Configuration applet location

The configuration applet, **Columbitech MAS**, is located in the Control Panel. It can also be started from the Columbitech WVPN program group:

Step-by-step

Follow the instructions below to configure Columbitech Mobile Authentication Server™:



Field	Description
Client port	The port that Wireless VPN clients connect to.
MSS port	The port that Mobile Session Servers connects to.
IP address	The IP address of the MAS. If specified, it will only listen on the specified IP Address. If left 0.0.0.0, it will listen on all available IP addresses on the MAS computer.

Step 3 - Import a CA certificate

The next step is to import the CA certificate that will be used to verify the client certificates. This is the same certificate that was imported in *Step 4 - Import a CA certificate* on page 10. Follow the instructions below to import a CA certificate:

Step-by-step

1. In the **Columbitech MAS dialog** (which is displayed by clicking the Columbitech WVPN icon in the Control Panel), click the **Certificates** button on the **Security** tab.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **CA Certificates** tab.
   Result: The **Import** dialog is displayed.
3. Point to the certificate you want to import and click **Open**.
   Result: The CA certificate is imported and displayed on the **CA Certificates** tab.

Step 4 - Import a server certificate

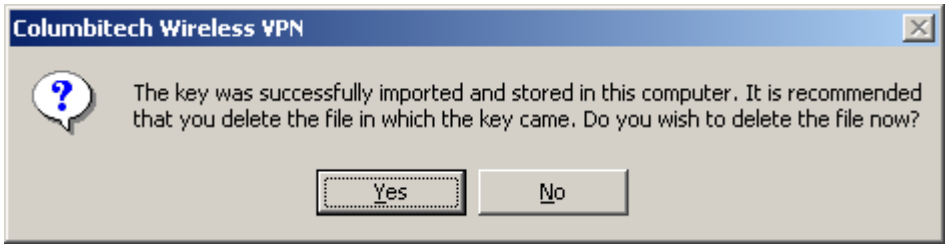
Finally, you have to import a server certificate. In this manual we will describe how you import a certificate that you have created in advance.

Step 1 - Create a certificate

To create a certificate, you have to start the Certificate Manager application and then follow the instructions in *Creating a certificate* on page 44.

Step 2 - Import an existing server certificate

1. Click **Certificates** on the **Security** tab in the **Columbitech MAS dialog**.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **Server Certificates** tab.
   Result: The **Import choice** dialog is displayed.
3. When importing an existing certificate, both the certificate and the private key must be imported. Select **Certificate and private key** and click **OK**.
   Result: The **Import certificate** dialog is displayed.
4. Select the certificate and click **Open**.
   Result: The **Import Private Key** dialog is displayed.
5. Select the private key and click **Open**.
   Result: The **File Password** dialog is displayed.
6. Enter the password that is used to protect the private key file and click **OK**. This is the password given in the Certificate Manager when the key was written to file. See *Creating a certificate* on page 44.
   Result: The following message is displayed:



7. For security reasons, the file containing the private key should be deleted. Click **Yes** if you want to delete the file.
   Result: A message is displayed, confirming that the certificate has been imported.
8. Click **OK**.
   Result: The **Server Certificates** tab in the **Certificates** dialog is displayed with the imported certificate.
9. Click **OK** to close the **Certificates** dialog.

Step 5 - Start Columbitech Mobile Authentication Server™ service

After completing the server configuration and closing the Columbitech MAS configuration applet, you are asked to start the Columbitech Mobile Authentication Server™ service. You are now ready to start using the server.

Tip! Verify in the Windows Event Log that no errors where detected when the Columbitech Mobile Authentication Server™ service was started.

Windows Client installation

Preparations

Install communication hardware

Make sure that the communication hardware (for example the WLAN card) is installed and configured on the client.

Install server first

It is recommended that you install Columbitech Mobile Session Server™ before you install the client.

Manual configuration

To achieve optimal performance and the least amount of problems, you are recommended to manually perform the changes described in *Appendix B - Manual Configuration* on page 48.

Before you start

Local administrator

When you install Columbitech Wireless VPN™ Client you must have **local administrator** rights on your computer. By default, members of the **Domain Admins** group have this right on all client computers in the domain.

Server information

Make sure that you have the following available:

- The host name or IP address used by the Columbitech Mobile Session Server™ or the Columbitech Mobile Authentication Server™, if used.
- The port number used by clients to connect to the Columbitech Mobile Session Server™ or the Columbitech Mobile Authentication Server™, if used. The default port number is 9102.

Certificate information

Make sure that the system administrator provides you with the following information:

- Where the CA (Certificate Authority) certificate and your client certificate will be located.

Simplifying the client configuration

When Columbitech Mobile Session Server™ is installed, a configuration file, **WVPNClientInstallation.ini**, is copied to the **Columbitech\MSS** folder. This configuration file can be used to simplify the configuration of Columbitech Wireless VPN™ Client when you will install many clients.

Configuration .ini file

During installation of the Columbitech Wireless VPN™ Client for Windows, the installation program searches for the **WVPNClientInstallation.ini** file on the network drive **w:** or on the drive that is specified by the **ctinipath** environment variable.

WVPNClientInstallation.ini can contain the following information:

ServerSettings	Description
Force_use = NO	If NO, the person who is installing the client can view and change the suggested values. If YES, the installation will use the predefined values.
Connect_through_MAS = YES	If NO, the client connects directly to a Columbitech Mobile Session Server™. If YES, the client connects to a Columbitech Mobile Session Server™ through a Columbitech Mobile Authentication Server™.
MSS	Description
MSS = 10.1.1.1	The MSS host name or IP address if the client connects directly to a MSS.
Port = 9102	Port to connect to on the MSS
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.
MAS	Description
MAS = 10.1.1.1	The MAS host name or IP address if the client connects to the MSS through a MAS.
Port = 9102	Port to connect to on the MAS
CACertificates	Description
CACertPath0 = w:\	The path to the CA certificate that will be imported.
CACertName0 = Cacert.cer	The name of the CA certificate that will be imported.
WPKI	Description
GenerateKeys = 0	If 0, the WPKI service will generate the clients private key and send it to the client during the first logon (this is the recommended option). If 1, the client will generate it's own private key before requesting a signed certificate from the WPKI service.
GetClientCert = 1	If 1, the client tries to get its client certificate from the WPKI service during the first logon.
WPKIPortalHost = mss	Host name for the computer running the WPKI service.
WPKIPortalPort = 5003	Port number for the WPKI service.
KeyLength = 1024	Key length to use.
Security	Description
MinimumPasswordLength = X	If X, the client certificate must be protected by a password that is at least X characters long. If 0, no password is needed.

Settings	Description
AllowDisablingOfWVPN = 1	If 1, the **Allow user to access network without WVPN** check box on the client configuration **Settings** tab is enabled. If 0, the check box is disabled.

If the settings for **ServerSettings**, **MSS**, **MAS**, **CACertificates**, **Security** and **Settings** in the table above are used during an automated client configuration, the only thing you have left to do to complete the configuration is to import the client certificate (see *Step 4 - Import a client certificate* on page 21).

The settings for **WPKI** are used only when you have used the WPKI Portal Service to create batches of client certificates. The client can then retrieve the client certificate from the server the first time that the client logs on. For more information on using the WPKI Portal service, see the *Certificate Management* section of the *Columbitech Wireless VPN™ System Administrator's Guide*.

Automating the client configuration

To automate the configuration of the Columbitech Wireless VPN™ Client for Windows during installation:

1. Create a read-only folder on a server, and copy the following files to the folder:
   - The client installation file, **WVPNClient.exe**
   - The updated **WVPNClientInstallation.ini**
   - The CA certificate that has signed the server's certificate
   - A batch file, for example **installWVPN.cmd**, with the following content:

```
net use z: \\server\wvpn
set ctinipath=z:
WVPNClient.exe
net use z: /d
```

2. Install the client by executing the **installWVPN.cmd** file.

Installing the Columbitech Wireless VPN™ for Windows client - step by step

To install and be able to use the Columbitech Wireless VPN™ client, you have to run the installation wizard, configure the client and import a client certificate.

The step-by-step procedure in this document describes how you install and configure the client if you sign your own certificates:

The steps below are described in detail in the following sections.

Step 1 Install the client by running the installation wizard.

Step 2 Configure the client and server settings in the configuration applet.

Step 3 Import a CA certificate. This is the CA certificate that will be used to verify the server certificate.

Step 4 Import a client certificate.

Step 5 Restart the computer to load the Columbitech Wireless VPN™ client properly.

Simplifying the installation of multiple clients

If you are installing multiple clients, generating a client certificate for each client can take quite a while. If you use the Columbitech WPKI Portal Service you can create batches of client certificates instead. The client can then retrieve the client certificate from the server the first time that the client logs on. For more information on using the Columbitech WPKI Portal service, see the *Certificate Management* section of the *Columbitech Wireless VPN™ System Administrator's Guide*.

Step 1 - Install the client

Step-by-step

1. Insert the installation CD in the CD drive.
   Result: The **Install Columbitech Wireless VPN™** dialog is displayed.
2. Click the **Install WVPN Client for Windows** button.
   If the Install **Columbitech Wireless VPN™** dialog is not displayed, double-click the **Setup.exe** file on the CD.

Follow the instructions in the installation wizard.

Note! During the installation you will see one or more dialogs with the title **Digital Signature Not Found**. This is no error, but a warning that you are about to install device drivers not signed by Microsoft. Just click **Yes** to continue the installation.

Step 2 - Configure the client

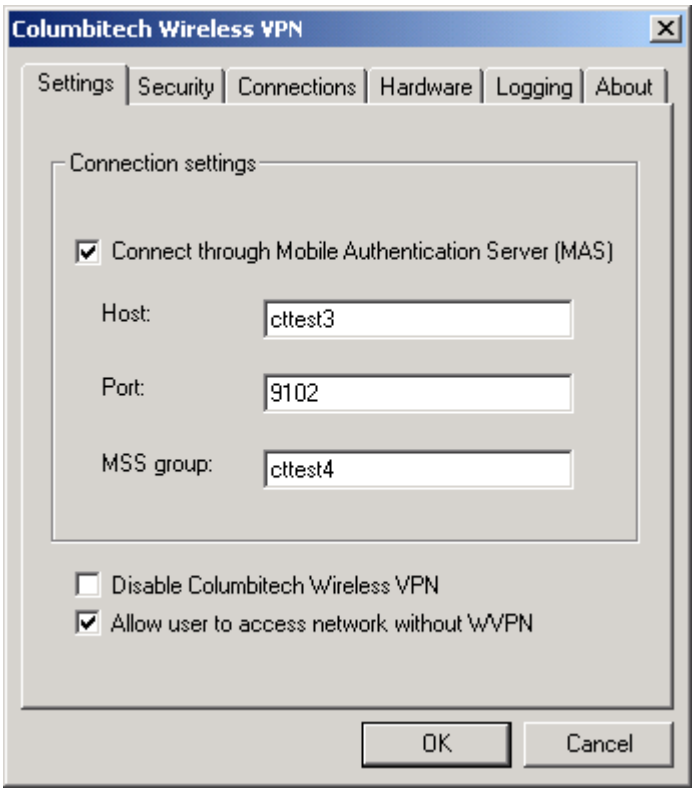
When the installation is finished, the configuration applet is started automatically, and the **Columbitech Wireless VPN dialog** is displayed.

Configuration applet location

The configuration applet, **Columbitech WVPN**, is located in the Control Panel:

Configure settings

Enter settings for the client on the **Settings** tab:

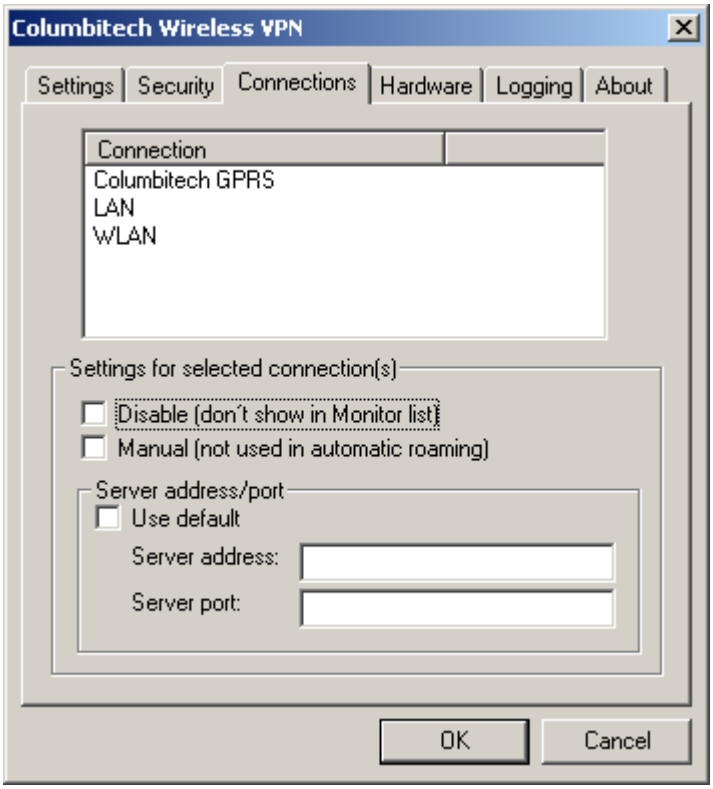


Field/checkbox	Description
Connect through Mobile Authentication Server (MAS)	If this checkbox is enabled, the client will connect through a Columbitech Mobile Authentication Server™ to reach a Columbitech Mobile Session Server™.
Host	If connecting through a Columbitech Mobile Authentication Server™, 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™.

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 Columbitech 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 user 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 the possibility to bypass the wireless VPN, that is, if you want access to the corporate network with the wireless VPN disconnected.

Configure connections

Enter information for the client connections on the **Connections** tab:



Field/Checkbox	Description
Disable connection	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.
Disable automatic roaming	By default, all dial-up connections are configured for manual roaming. The wireless VPN client will not automatically roam to a connection that is configured for manual roaming. Highlight the connection you wish to configure and check **Manual** to disable automatic roaming. Uncheck **Manual** if you wish to enable automatic roaming for the specified connection.
Server address/port	By default, all connections to the Columbitech Mobile Session Server™ are made to the IP address and port configured under the Settings tab. If the Columbitech Mobile Session Server™ is accessed through some other IP address, e.g. through a NAT server, enter that IP address and port.

Step 3 - Import a CA certificate

The next step is to import the CA certificate that will be used to verify the server certificate. This is the same certificate that was imported in *Step 4 - Import a CA certificate* on page 10. Follow the instructions below to import a CA certificate:

Step-by-step

1. In the **Columbitech Wireless VPN dialog** (which displayed by clicking the WVPN icon in the Control Panel), click **Certificates** on the **Security** tab.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **CA Certificates** tab.
   Result: The **Import** dialog is displayed.
3. Point to the CA certificate you want to import and click **Open**.
   Result: The CA certificate is imported and displayed on the **CA Certificates** tab.

Step 4 - Import a client certificate

Finally, you have to import a client certificate. In this manual we will describe how you import a certificate that you have created in advance.

Tip! You can also request and import a new server certificate by creating a certificate signing request (CSR) and signing it yourself. This is described in *Appendix A – Certificate Management* on page 42.

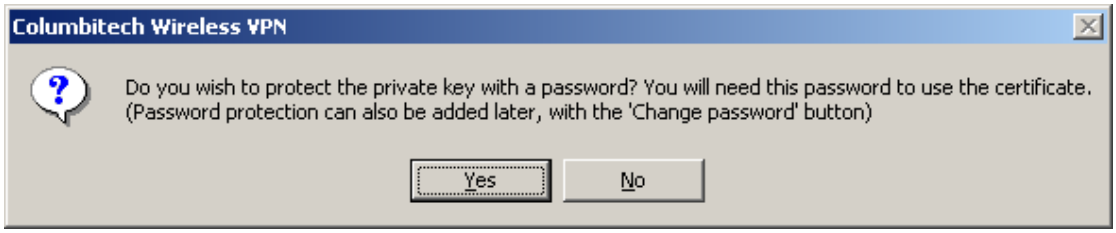
Follow the steps below to create a certificate and import it:

Step 1 - Create a certificate

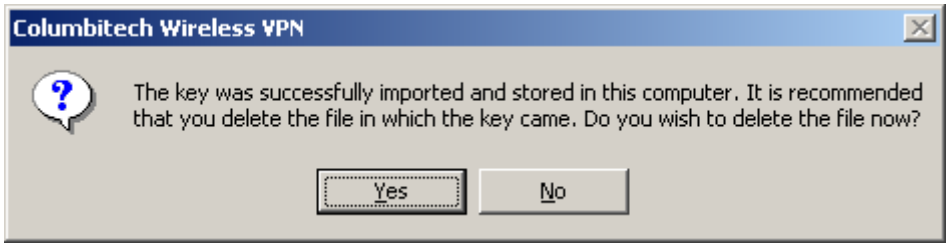
To create a certificate, you have to start the Certificate Manager application and then follow the instructions in *Creating a certificate* on page 44.

Step 2 - Import an existing client certificate

1. Click **Certificates** on the **Security** tab in the **Columbitech Wireless VPN dialog**.
   Result: The **Certificates** dialog is displayed.
2. Click **Import** on the **Client Certificates** tab.
   Result: The **Import Choice** dialog is displayed.
3. When importing an existing certificate, both the certificate and the private key must be imported. Check **Certificate and private key** and click **OK**.
   Result: The Import certificate dialog is displayed.
4. Select the certificate and click **Open**.
   Result: The **Import Private Key** dialog is displayed.
5. Select the private key and click **Open**.
   Result: The **File Password** dialog is displayed.
6. Enter the password that is used to protect the private key file and click **OK**.
   Result: The following message is displayed:



7. With a password-protected private key, an intruder will have difficulties logging on using the client certificate stored on a stolen computer. Click **Yes** if you want to use a password.
   Result: The **New password** dialog is displayed.
8. Enter and confirm the password for the private key. Click **OK**.
   Result: The following message is displayed



9. For security reasons, the file containing the private key should be deleted. Click **Yes** if you want to delete the file.
   Result: The **User name** dialog is displayed.
10. The user name for the person running the installation is displayed in the dialog. If this is not the person that will use the client, you must enter the user name of the person that will use the client, on the `domain\user` format, and click **OK**.
    Result: A message is displayed, confirming that the certificate has been imported.
11. Click **OK**.
    Result: The **Client Certificates** tab in the **Certificates** dialog is displayed with the imported certificate.
12. Click **OK** to close the **Certificates** dialog.

Step 5 - Restarting the computer

When the configuration is finished and you close the **Columbitech Wireless VPN dialog**, you have to restart the computer to load the Columbitech Wireless VPN™ client properly.

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 Client Monitor, after logging in, as described in the *Columbitech Wireless VPN™ User's Guide*.

If you are working offline, you can at any time connect by clicking **Connect** on the Monitor. This is more thoroughly described in the *The Columbitech Wireless VPN™ for Windows* Client Monitor chapter.

Monitor icon

When the Columbitech Wireless VPN™ client is connected to a Columbitech Mobile Session Server™, the client monitor icon below is displayed in the systray:

The Columbitech Wireless VPN™ for Windows 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

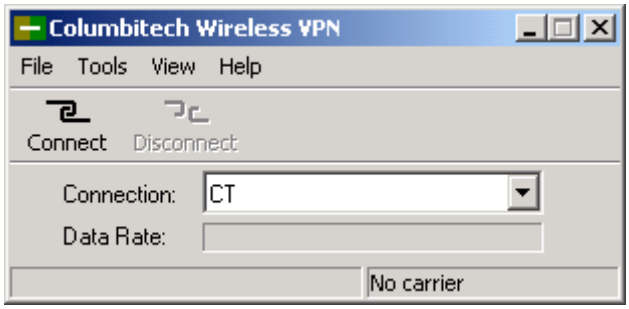
The monitor icon is displayed in the systray.

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 a Columbitech Mobile Session Server™, 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 the Columbitech Mobile Session Server™.
Disconnect	Click here to disconnect the Client from the 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

Field / button	Description
	and link quality will automatically be used.
Data Rate	The rate at which data is transferred.
(Lower left corner)	This is where status messages are displayed. These messages can later be viewed using the View/Logfile menu option.
(Lower right corner)	This is where the current connection name is displayed.

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 on the **Settings** tab.
3. Restart the computer.

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

Diagnostic logging

Event logging

Since both the WVPN client and server are implemented as Windows services, they use the Windows 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:

- No diagnostic logging
- Low
- Medium
- High

Note! Right now, only the **No diagnostic logging** and **Low** levels are used.

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.

   For more information about setting the event logging levels, see *the Columbitech Wireless VPN™ System Administrator's Guide*.

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.

Pocket PC 2002 Client installation

Preparations

Install server first

It is recommended that you install Columbitech Mobile Session Server™ before you install the client.

ActiveSync

ActiveSync must be installed on the PC that is used for installing the Columbitech Wireless VPN™ for Pocket PC client.

Before you start

Server information

Make sure that you have the following available:

- The host name or IP address used by the Columbitech Mobile Session Server™ or the Columbitech Mobile Authentication Server™, if used.
- The port number used by clients to connect to the Columbitech Mobile Session Server™ or the Columbitech Mobile Authentication Server™, if used. The default port number is 9102.

Certificate information

Make sure that the system administrator provides you with the following information:

- Where the CA (Certificate Authority) certificate and your client certificate will be located.

The step-by-step procedure in this document describes how you install and configure the Pocket PC 2002 client if you sign your own certificates.

Simplifying the client configuration

When Columbitech Mobile Session Server™ is installed, a configuration file, **AutoInstall.ini**, is copied to the **Columbitech\MSS** folder. This configuration file can be used to simplify the configuration of Columbitech Wireless VPN™ Client for Pocket PC 2002 when you will install many clients.

Configuration .ini file

During installation of the Columbitech Wireless VPN™ Client for Pocket PC 2002, the installation program searches for the **AutoInstall.ini** file in the **My Documents** folder on the Pocket PC device.

AutoInstall.ini can contain the following information:

Wireless VPN Client	Description
UseMAS = 0	If 0, the client connects directly to a Columbitech Mobile Session Server™. If 1, the client connects to a Columbitech Mobile Session Server™ through a Columbitech Mobile Authentication Server™.
host = 10.1.1.1	The host name or IP address of the Columbitech Mobile Session Server™ (if UseMAS = 0 above), or the Columbitech Mobile Authentication Server™ (if UseMAS = 1 above).
port = 9102	Port to connect to on the Columbitech Mobile Session Server™ (or the Columbitech Authentication Server™ if used).
MSSGroup =	If connecting through a Columbitech Mobile Authentication Server™, this should be the logical name identifying the Columbitech Mobile Session Server™, or a group of Columbitech Mobile Session Servers, that you want to connect to.
InstallShortcut = 0	If 1, the Columbitech Wireless VPN Client for Pocket PC 2002 will start as an icon after every reset of the Pocket PC device. If 0, the client software is not started after a reset.
PromptReset = 1	If 1, the dialog informing that you must reset your device to complete the installation is shown. If 0, no dialog is shown.

If the settings for **ServerSettings**, **MSS**, **MAS**, **CACertificates**, **Security** and **Settings** in the table above are used during an automated client configuration, the only thing you have left to do to complete the configuration is to import the client certificate (see *Step 6 - Import a client certificate* on page 34).

The settings for **WPKI** are used only when you have used the WPKI Portal Service to create batches of client certificates. The client can then retrieve the client certificate from the server the first time the client logs on. For more information on using the WPKI Portal service, see the *Certificate Management* section of the *Columbitech Wireless VPN™ System Administrator's Guide*.

Automating the client configuration

To automate the configuration of the Columbitech Wireless VPN™ Client for Pocket PC 2002:

1. Copy the **AutoInstall.ini** file to the **My Documents** folder on the Pocket PC device.
2. Run the installation program.

Installing the Columbitech Wireless VPN™ for Pocket PC 2002 client - step by step

To install and be able to use the Columbitech Wireless VPN™ Client for Pocket PC 2002, you have to run the installation wizard, configure the client and import certificates. The step-by-step procedure in this document describes how you install and configure the client if you sign your own certificates:

The steps below are described in detail in the following sections.

Step 1 Connect your Pocket PC 2002 to your desktop client PC.

Step 2 Install the client by running the installation wizard.

Step 3 Configure the client and server settings.

Step 4 Copy certificate files to your Pocket PC 2002.

Step 5 Import a CA certificate. This is the CA certificate that will be used to verify the server certificate.

Step 6 Import a client certificate.

Step 1 - Connect your Pocket PC 2002 to your desktop PC

Make sure that your Pocket PC 2002 device is connected to your desktop PC by AciveSync before installing Columbitech Wireless VPN™ for Pocket PC 2002.

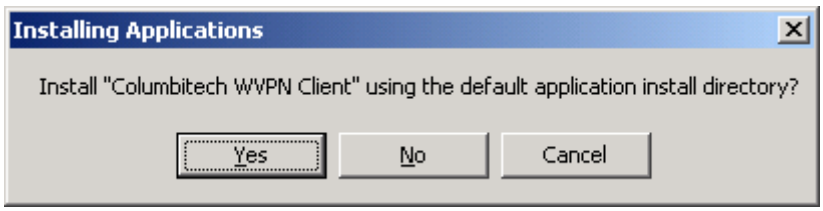
Step 2 - Install the client

Step-by-step

1. Insert the installation CD in the CD drive on your desktop PC.
   Result: The **Install Columbitech Wireless VPN™** dialog is displayed.
2. Click the **Install WVPN Client for Pocket PC** button.
   If the Install **Columbitech Wireless VPN™** dialog is not displayed, double-click the **Setup.exe** file on the CD.

Follow the instructions in the installation wizard.

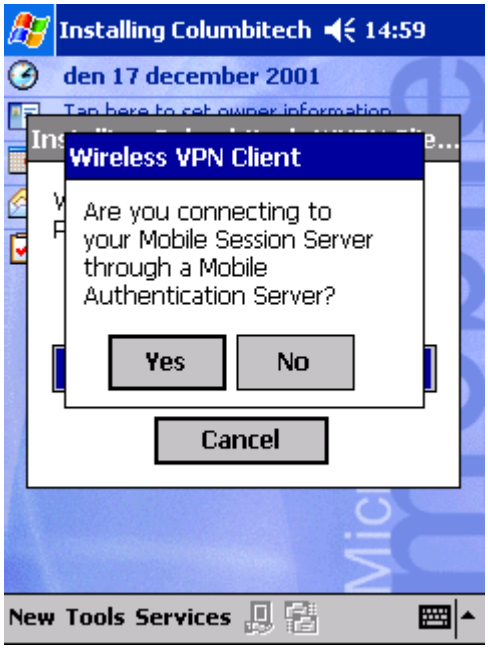
When the installation is finished ActiveSync will display the following message:



Select **Yes** to install the client onto the Pocket PC device.

Installation dialogs on your Pocket PC 2002

If you are connecting to your Columbitech Mobile Session Server™ through a Columbitech Mobile Authentication Server™ tap **Yes**, otherwise **No**.

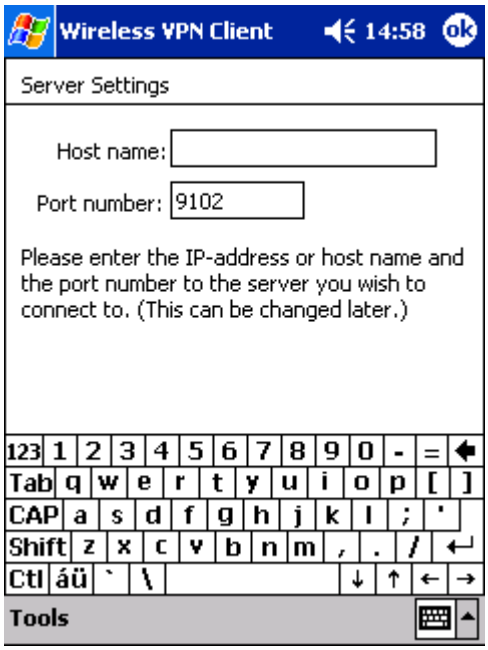


If you answered **Yes** (you connect to your Columbitech Mobile Session Server™ through a Columbitech Mobile Authentication Server™), enter the MSS Group name used to identify the Columbitech Mobile Session Server™ (or group of Columbitech Mobile Session Servers) that you want to connect to. Tap **OK** to proceed.

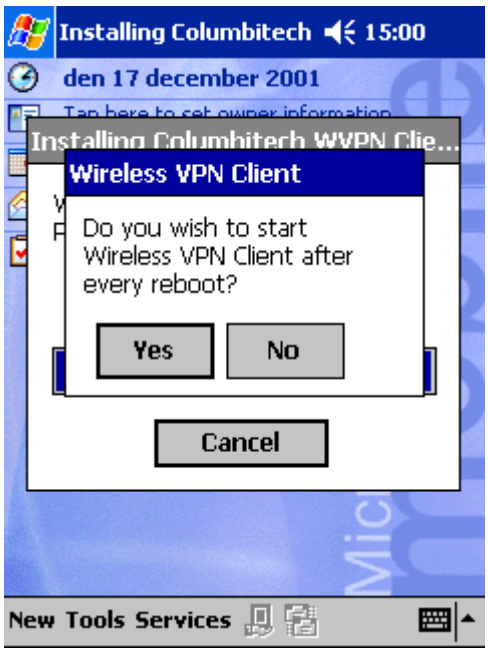
If you connect to your Columbitech Mobile Session Server™ (MSS) through a Columbitech Mobile Authentication Server™ (MAS), enter the host name or IP-address of the MAS in the host name field.

If you connect directly to your Columbitech Mobile Session Server™ (MSS), enter the host name or IP-address of the MSS in the host name field.

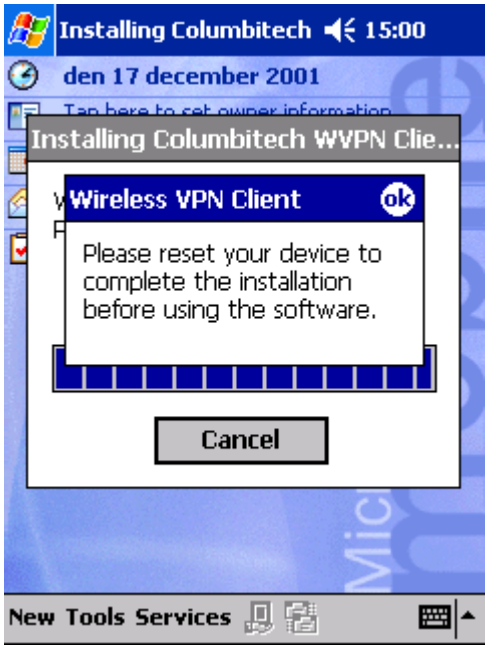
If you enter a host name, make sure to enter the fully qualified domain name, e.g. “wvpn.columbitech.com”. The default port used to connect to the MAS or MSS is 9102. Tap **OK** to proceed.



Tap **Yes** if you want to start the Columbitech Wireless VPN™ for Pocket PC 2002 client after every reset.



When the installation is finished you have to reset your Pocket PC 2002 to complete the installation.



After the Pocket PC 2002 has been reset, the client monitor icon below is displayed in the system tray (if you selected to start the Wireless VPN client after every reset):

If you tap the icon the menu Columbitech Wireless VPN™ menu is displayed:

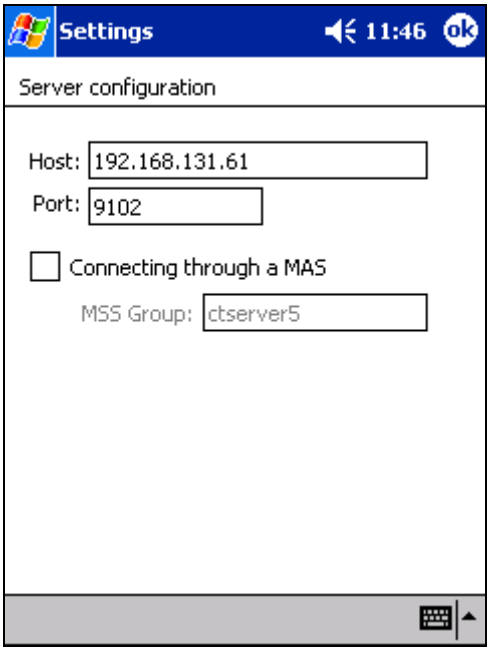
Step 3 - Verify the client configuration

Configuration program location

When the installation is completed the client should be configured and up and running. The configuration settings can be found by tapping the Columbitech Wireless VPN icon and selecting “settings”.

Configure settings

Verify the settings for the client in the **Settings** dialog:



Field/checkbox	Description
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™. If you enter a host name, make sure to enter the fully qualified domain name, e.g. “wvpn.columbitech.com”.
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™.
Connecting through a MAS	If this checkbox is enabled, the client will connect through a Columbitech Mobile Authentication Server™ to reach a 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.

Step 4 - Copy certificate files to your Pocket PC 2002.

Copy the certificate files to the **MyDocuments** folder on your Pocket PC 2002. The certificate files are:

- The CA certificate (e.g. “ca.cer”), this is the CA certificate that was exported in *Step 3 - Create and export a CA certificate* on page 9.
- The client certificate (e.g. “clientcert.cer”) and the client certificate secret key file (e.g. “clientcert.p12”). For a description how to create a client certificate see *Creating a certificate* on page 44.

Step 5 - Import a CA certificate

The next step is to import the CA certificate that will be used to verify the server certificate. Follow the instructions below to import a CA certificate:

Step-by-step

1. Tap **Certificates** on the menu of the Columbitech Wireless VPN client.
2. Tap **CA Certificates...**
   Result: The **CACertificates** dialog is displayed.
3. Tap the **Import…** button in the **CACertificates** dialog.
   Result: The **Open** dialog is displayed.
4. Tap on the CA certificate file that you want to import.
   Result: The CA certificate is imported and displayed in the **CA Certificates** dialog.

Step 6 - Import a client certificate

Finally, you have to import a client certificate. In this manual we will describe how you import a certificate that has been created in advance.

Tip! You can also request and import a new server certificate by creating a certificate signing request (CSR) and signing it yourself. This is described in *Appendix A – Certificate Management* on page 42.

Follow the steps below to import the client certificate:

Import an existing client certificate

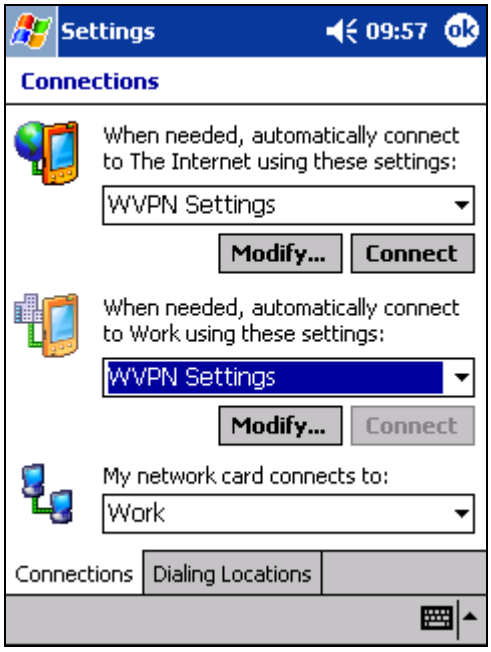
1. Tap **Certificates** on the menu of the Columbitech Wireless VPN client. Tap **Client certificates**.
   Result: The **Client certificates** dialog is displayed.
2. Tap the **Import…** button in the **Client Certificates** dialog.
   Result: The **Open** dialog is displayed.
3. Tap on the certificate file that you want to import.
   Result: You are asked if you have a personal information exchange file with the private key for the certificate.
4. Tap **Yes**.
5. Tap on the private key file that you want to import.
   Result: The **Password** dialog is displayed.
6. Enter the password that is protecting the private key file, and tap the **OK** button.
   Result: The **Certificate Password** dialog is displayed.
7. With a password-protected private key, an intruder will have difficulties logging on using the client certificate stored on a stolen computer. Enter and confirm the password that will protect the private key. Tap **OK**.
8. You must associate the imported client certificate with the user that will use the certificate. Enter the domain and user name in the format “domain\user”.
9. Tap **OK**.
   Result: The **Client Certificates** dialog is displayed with the imported certificate.
10. Tap **OK** to close the **Client Certificates** dialog.

Configuring Connections Settings

Step-by-step

Before you connect to the Wireless VPN server, you must configure the connections settings in the Pocket PC device. To configure the connections settings open the **Connections Manager**:

1. Tap the **Start** menu
2. Tap **Settings**
3. Tap the **Connections** tab
4. Tap the **Connections** icon to open the **Connections Manager**.



5. Tap the down arrow in the top selection list, “When needed, automatically connect to The Internet using these settings”, and select **New…**

6. Rename the settings to e.g. **WVPN Settings.**

7. Tap **OK.**

8. Make the new **WVPN Settings** the selected setting in the top and middle selection lists as shown in the screen image above.

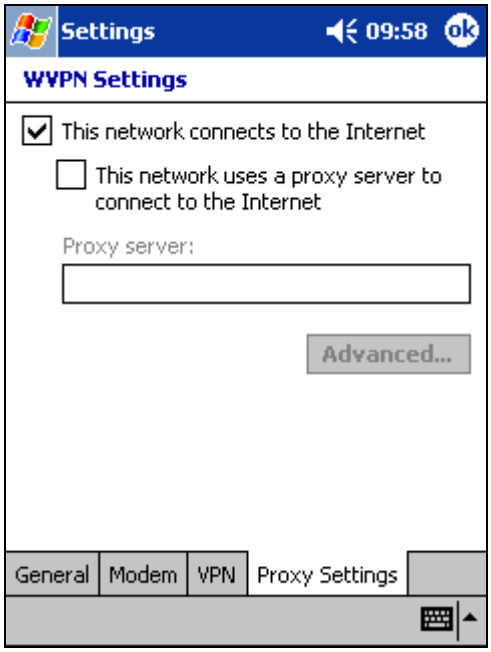
9. Make sure that the bottom selection list, “My network card connects to”, has **Work** selected.

Configure Proxy Settings

Depending on if you use a proxy server to connect to the Internet from your office network or not, you need to configure this by tapping the **Modify…** button under the selection list in the middle, “When needed, automatically connect to Work using these settings”.

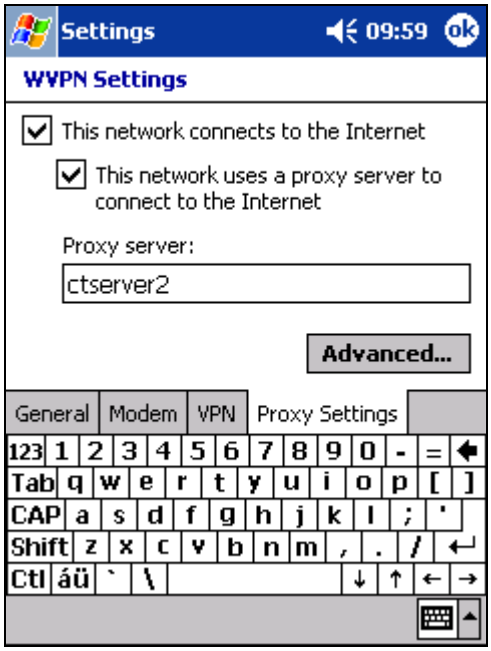
If you don't use a proxy server to connect to the Internet from your office network:

Tap the **Proxy Settings** tab and make sure to checkmark "This network connects to the Internet" as shown below.



If you use a proxy server to connect to the Internet from your office network:

Tap the **Proxy Settings** tab and make sure to checkmark "This network connects to the Internet" and "This network uses a proxy server to connect to the Internet", and enter the IP-address or host name for the proxy server. If you need to change the ports for the proxy server, tap the **Advanced…** button.



Tap **OK** to save the settings

Configure Dialing Locations

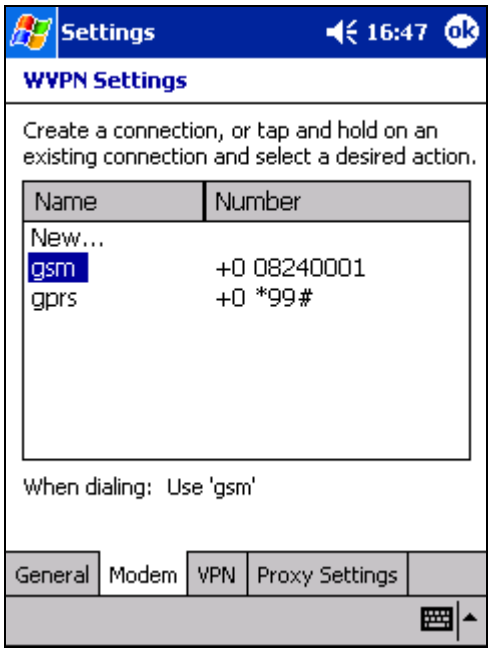
To configure Dialing Locations select the **Dialing Locations** tab at the bottom of the **Connections** dialog in the **Connection Manager**:

1. Clear the **Area code** and **Country code** fields.
2. Tap the **Dialing Patterns…** button.
3. To minimize problems, enter only “G” (without) in all three fields.
4. Tap **OK** to close the **Dialing Patterns** dialog.
5. Tap **OK** to close the **Connection Manager**.

Creating Dial-Up Connections

To create a new Dial-Up connection, open the **Connection Manager** (described above) and tap the **Modify…** button under the second combo box, “When needed, automatically connect to Work using these settings”.

The following example will configure a GPRS connection:



Step-by-step

1. Tap **New…**
2. Enter a name for the connection, e.g. GPRS.
3. Select a modem.
4. If you need to configure static IP settings or DNS settings press the **Advanced…** button, otherwise tap the **Next** button.
5. Enter the phone number, many GPRS phones use *99# as phone number.
6. Tap the **Next** button.

7. Consider lowering the value under “Cancel call if not connected within” from 120 to 20 seconds.

8. Tap the **Finish** button.

9. Tap **OK** to close the **WVPN Settings** dialog.

10. Tap **OK** to close the **Connection Manager**.

Connecting to the Wireless VPN Server

You can at any time connect to your Wireless VPN Server by tapping the WVPN Client Monitor icon in the system tray and selecting **Connect WVPN…** in the popup menu. This is more thoroughly described in the *The Columbitech Wireless VPN™ for Pocket PC Client Monitor* chapter.

The Columbitech Wireless VPN™ for Pocket PC Client Monitor

The Columbitech Wireless VPN™ Monitor is a tool for managing the connections used with Columbitech Wireless VPN™. The Monitor icon 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

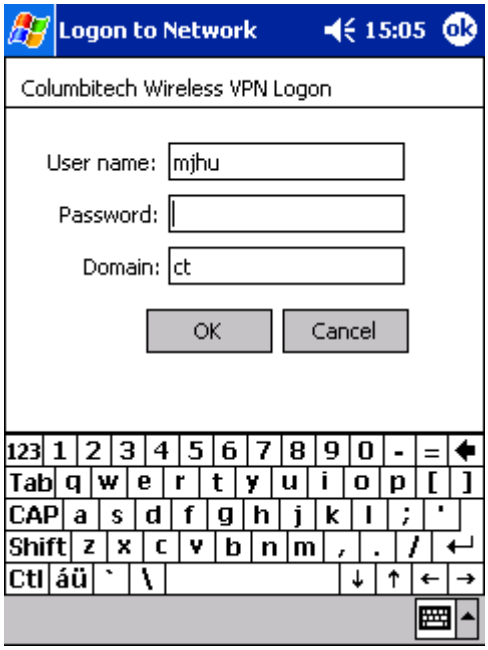
The monitor icon displays the client's connection status, as described below:

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 a Columbitech Mobile Session Server™, but has no physical carrier connection, the icon is yellow.
	Disconnected	If the client is disconnected, the icon is red.

Monitor menu

Field descriptions

The menu in the Columbitech Wireless VPN™ monitor are described below:

Field / button	Description
Connect WVPN	Tap here to connect the Client to the Columbitech Mobile Session Server™. This will result in this dialog:  Enter your user credentials to connect to the server and tap OK. Note: If you have another password on your client certificate then on your domain account, a dialog that asks for that password will be displayed before the connection to the Columbitech Mobile Session Server™ is established.
Disconnect WVPN	Tap here to disconnect the Client from the Columbitech Mobile Session Server™.
Connections	Tap here to view the connections settings.
Certificates	Tap here to view certificate information.
Settings	Tap here to view the configuration settings.
About	Tap here to view the version information.
Exit	Tap here to close down the Columbitech Wireless VPN™.

Appendix A – Certificate Management

Certificate Manager

The server installation includes the Certificate Manager application, which you use to:

- Create CA, server and client certificates.
- Sign certificate requests from clients and servers.

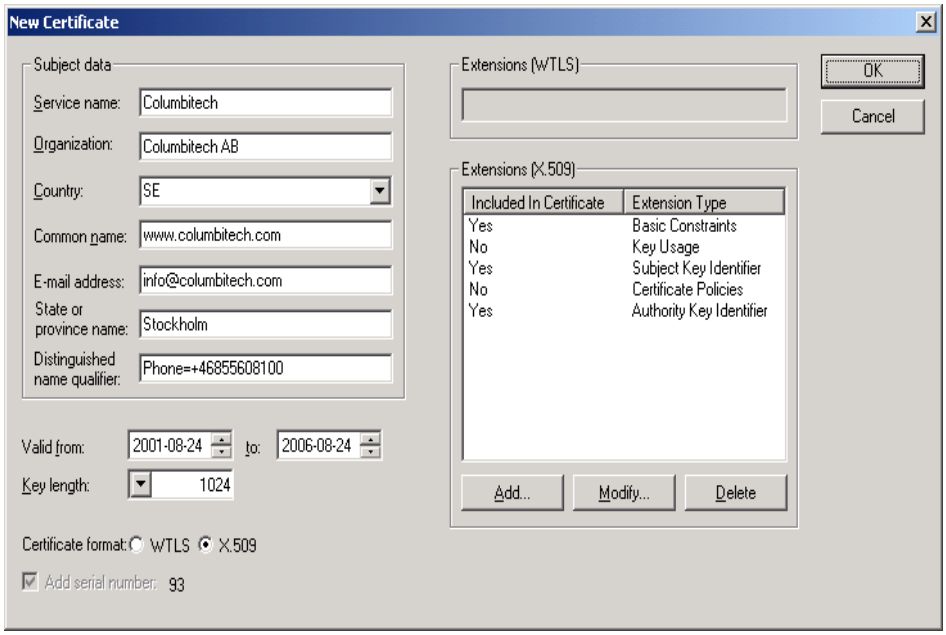
Creating a CA certificate

Note!

The CA certificate will be protected by a password that you enter when you create the certificate. You will later use this password when you sign your server and client certificate requests.

Step-by-step

1. Open the Certificate Manager application from the **Columbitech WVPN** program group.
2. Select **New** on the **File** menu, and then **CA Certificate** on the sub-menu.
   Result: The **New Certificate** dialog is displayed:



3. Enter information in the fields. Note the descriptions for the following fields:

Field	Description
Service name	Identifies a service, CA, subscriber or other entity within an organization.
Common name	URL from which the CA is available.

4. Select a **Certificate format**.
   If you select **X.509**, the available extensions are displayed in the **Extensions (X.509)** field. Select the extension(s) you want, and click **Add** to display a dialog where you can enter information about the extension.
   Note! The **Subject Key Identifier** extension must be included in a CA certificate to facilitate chain building.
5. Click OK.
   Result: The **Password for CA Certificate** dialog is displayed.
6. Enter a password and confirm it. You will use this password when you sign certificate requests. Click **OK**.
   Result: The **Certificate Log file** dialog is displayed.
7. Select a certificate log file and click OK.
   Result: The CA certificate is created and displayed in the Certificate Manager main window.

Exporting the CA certificate

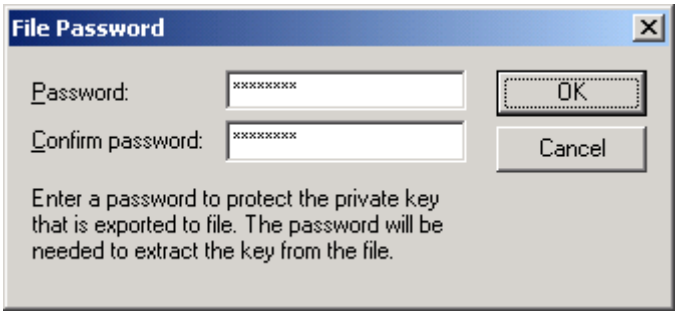
In order for clients and servers to be able to import the CA certificate used to sign your server and client certificates, you must export the CA certificate to a file accessible by both server administrators and clients during configuration.

There are two ways to export a CA certificate; if the exported CA certificate will be used to create certificates or sign certificate requests on another machine, both the CA certificate and the CA certificate's private key must be exported.

If the exported CA certificate will be used for verifying client and server certificates (the normal case), only the certificate and not the private key must be exported.

1. Open the Certificate Manager application from the **Columbitech WVPN** program group.
2. Select the CA certificate that you want to export.
3. Select **Export** on the **File** menu and then select **Certificate and private key** or **Client Certificate** on the sub-menu.
4. Save the certificate to a file located so that it is accessible when you install servers and clients, e.g. on a network drive on a file server.
   If you are exporting only the certificate, you are done here. If you are saving a private key file as well, continue with step 5.
5. Save the private key to file.
6. If the private key is exported, you have to enter the password for the CA certificate.

7. A password used to protect the private key in the file must also be given. This password is then needed to decrypt and install the private key.



Creating a certificate

In Certificate Manager, you can create client or server certificates without having a certificate signing request. When you do this, you will actually create two files:

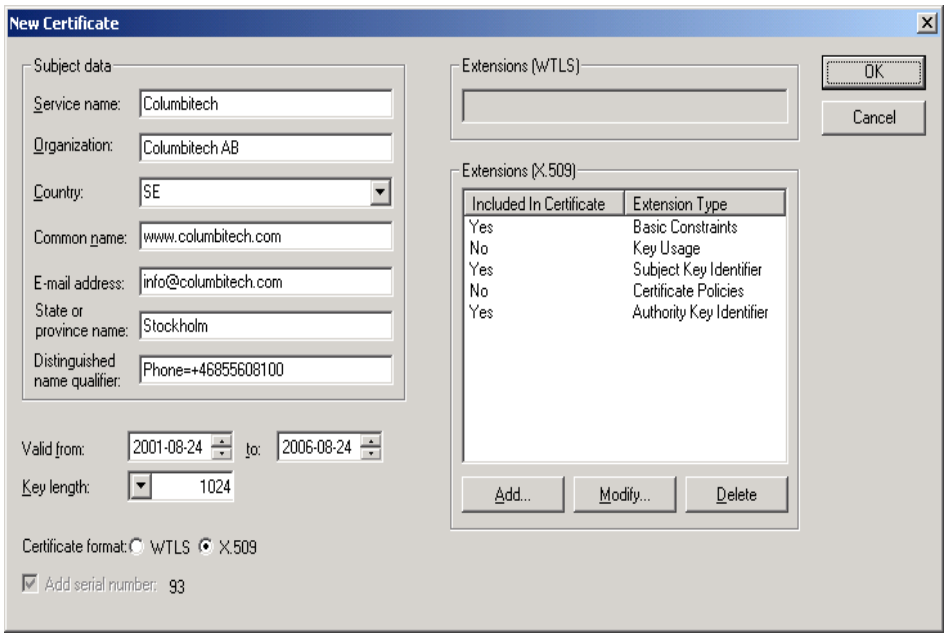
- A certificate file (*.cert/*.crt)
- A private key file (*.p12/*.pfx)

The private key file can be protected by a password that you enter when you save the file.

Note! You have to provide the private key file's password to users who import this certificate to their clients.

Step-by-step

1. Open the Certificate Manager application from the **Columbitech WVPN** program group.
2. Select **New** on the **File** menu, and then **Client Certificate** *or* **Server Certificate** on the sub-menu.
   Result: The **New Certificate** dialog is displayed:

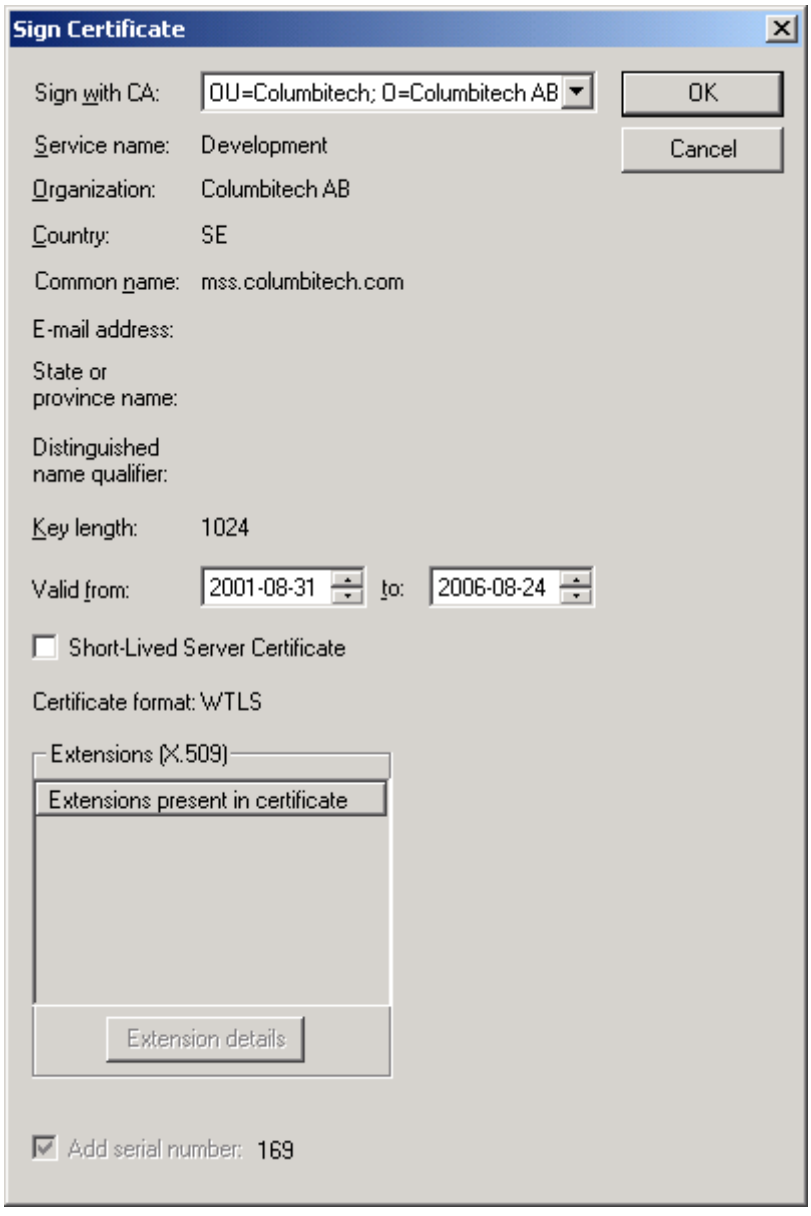


3. Enter information in the fields. Note the descriptions for the following fields:

Field	Description
Service name	Identifies an organizational unit within the organization in the **Organization** attribute.
Common name	Server certificates should here have its URL. Client certificates should have a full name, like “John Doe”.

4. Select a **Certificate Type**.
   If you select **X.509**, the available extensions are displayed in the **Extensions (X.509)** field. Select the extension(s) you want, and click **Add** to display a dialog where you can enter information about the extension.

5. Click **OK**.
   Result: The **Sign Certificate** dialog is displayed:



6. Select a CA Certificate in the **Sign with CA** field and enter a valid date range in **Valid from/to**.
   Note! You cannot enter a date range that is outside of the valid dates for the CA certificate.
7. Click **OK**, enter the password for the CA certificate in the **CA Password** dialog that is displayed, and click **OK** again.
   Result: The **Save Certificate** dialog is displayed.
8. Enter a name and location for the certificate and click **Save**.
   Result: The **Save Private Key** dialog is displayed.
9. Enter a name and location for the certificate's private key and click **Save**.
   Result: The **File Password** dialog is displayed.
10. Enter and confirm a password and click **OK**. Users who import the client or server certificate need this password to be able to use the certificate.
    Result: A message that the certificate has been created is displayed.

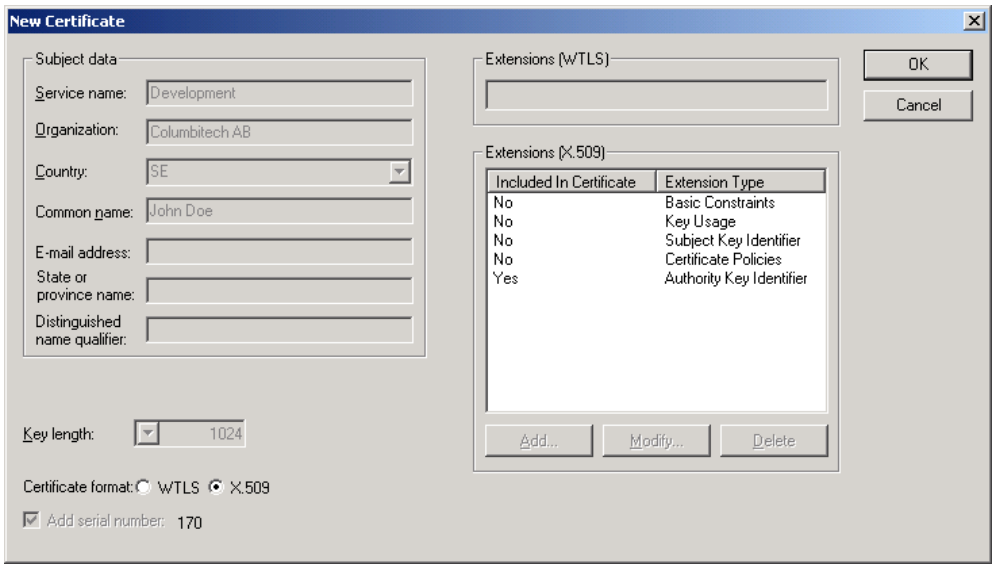
Signing a certificate request

Before you start

Make sure that you save the signed certificate in a location accessible by both server administrators and client users.

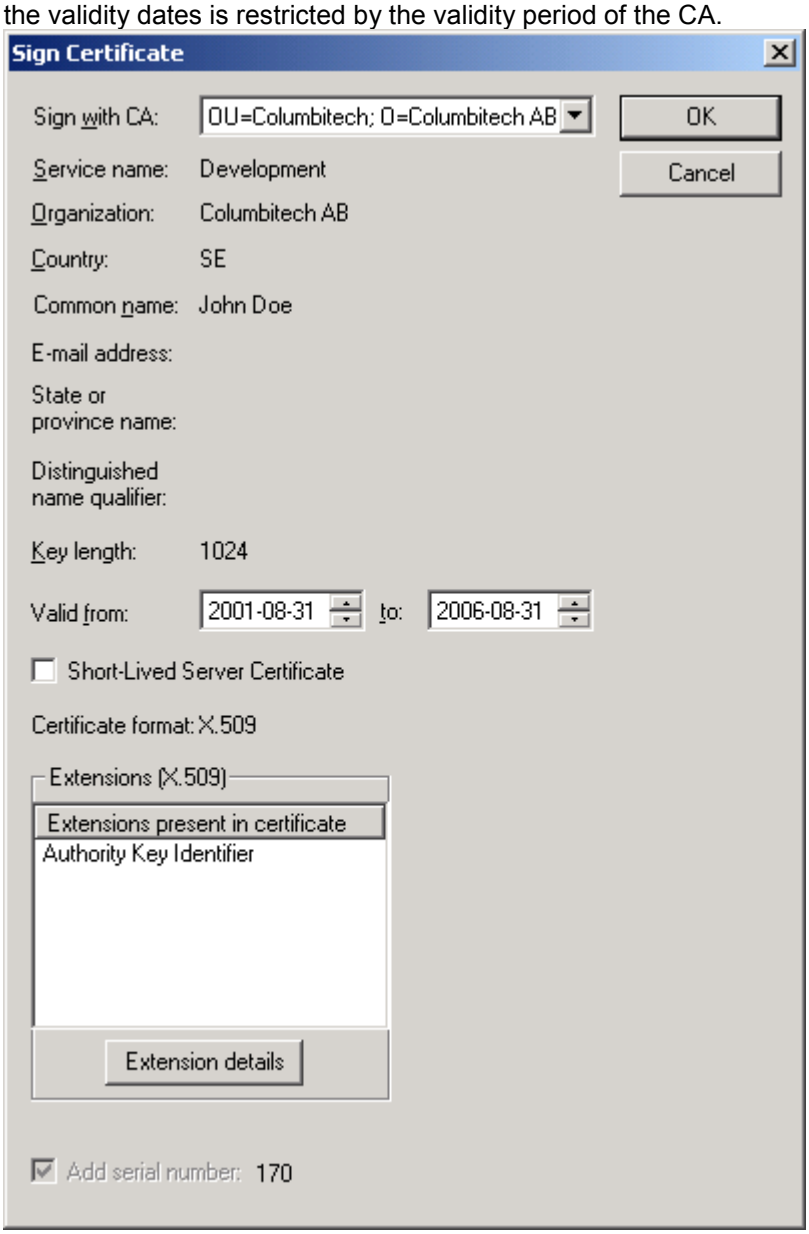
Step-by-step

1. Open the Certificate Manager application from the **Columbitech WVPN** program group.
2. Select **Open signing request** on the **File** menu.
3. Select the file from which the signing request will be imported.
   A signing request for a certificate can for example be created with the Columbitech WVPN Control Panel Applet. For more information, see the *Columbitech Wireless VPN™ System Administrator's Guide*.
4. Enter details for the certificate that you are creating from the certificate signing request.



The certificate information is the same as in *Creating a certificate* on page 44, but the information received in the CSR cannot be changed. The CA can select certificate format and extensions.

In the **Sign Certificate** dialog, select which CA certificate to use for signing the new certificate. Validity dates are also selected. The range of the validity dates is restricted by the validity period of the CA.



Note! You can only use CA certificates to issue certificates of their own format (WTLS or X.509). Therefore, the certificate format chosen for the certificate conducts which CA certificates can be used to sign it. You will only be able to choose among the CA certificates with the same format.

5. Enter the password for the CA certificate in the **CA Password** dialog. This is the password you assigned to the CA certificate in *Creating a CA certificate* on page 42.
6. Use the **Save** dialog to save. The new certificate is saved to file.

   The certificate file can now be imported via the Columbitech WVPN Control Panel Applet, in which the CSR was created.

Appendix B - Manual Configuration

On the Columbitech Wireless VPN™ for Windows Client, we recommend that you manually perform the configuration changes below to achieve optimal performance and the least amount of problems.

Adapter settings

Perform the following changes on each Windows 2000/XP client computer:

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. Disable **Client for Microsoft Networks.**
4. Disable **File and Printer Sharing for Microsoft Networks**.
5. Repeat steps 2-4 for all LAN and WLAN adapters except the Columbitech Wireless VPN™ Network Adapter.

Note!

If you later on want to use the client machine without Columbitech Wireless VPN™, you must reactivate **Client for Microsoft Networks** (which you disabled in step 3 above).