Columbitech Mobile VPN™ Client for Android

Version 3.0

User's Guide

Updated: May 2012

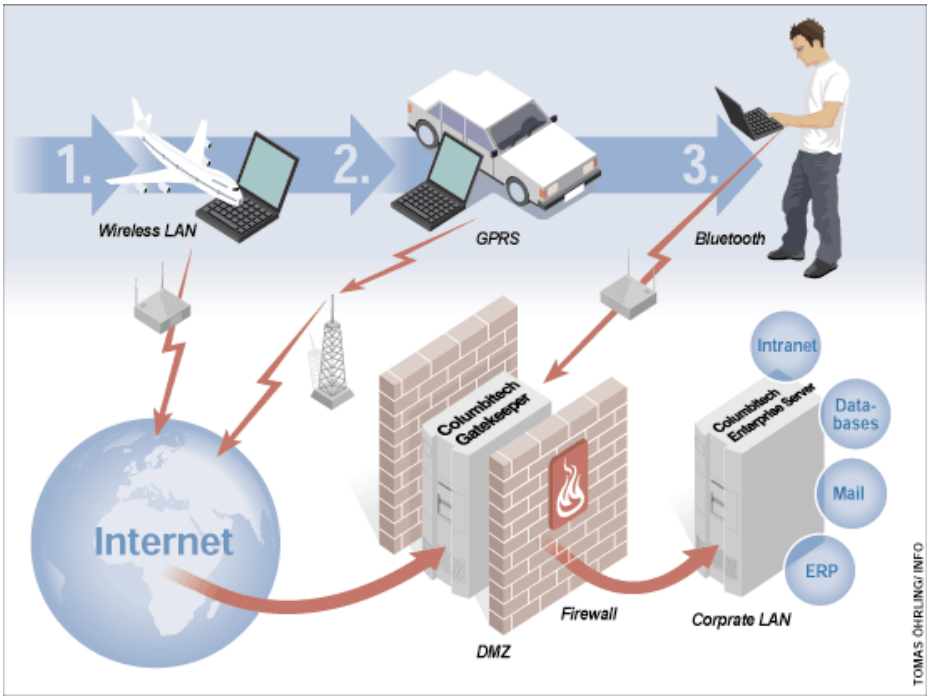
Table of contents

Columbitech Mobile VPN™ - Introduction

Columbitech Mobile VPN™ is a session level VPN architecture designed to eliminate the wireless weaknesses of traditional VPN solutions, while at the same time creating 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 Mobile 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 Mobile VPN™ is a client/server based software architecture. The client software is installed on every Columbitech Mobile VPN™-enabled mobile terminal, and the server software is installed on a server computer. When the client connects to the secure network an authenticated and encrypted tunnel is established between the client and Columbitech Mobile VPN™ Server, normally located on the corporate network behind a firewall. The connection can be done directly to Columbitech Mobile VPN™ Server or via Columbitech Gatekeeper. Columbitech Gatekeeper is usually placed in a DMZ (DeMilitarized Zone). Columbitech Mobile VPN™ Server can however also act as a firewall, a good solution when adding WLAN to a secure network without an existing firewall. Clients are authenticated using any combination of the following authentication methods: one-time password, client certificate and username/password.

Optimizations

The architecture implements transport optimizations that adapt transmitted messages for networks with wireless characteristics. Advanced data compression is applied at the session level before the data is encrypted. Flow control and retransmission mechanisms ensure optimal performance even in poor network conditions.

Seamless interoperability

Columbitech Mobile VPN™ is designed for seamless interoperability with existing corporate solutions. A company that is already using an IP VPN solution may deploy Columbitech Mobile 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, Columbitech Mobile VPN™ is able to provide traditional wireline VPN services in addition to the wireless functionality. Many of the wireless optimizations implemented in Columbitech Mobile VPN™ architecture are just as applicable to a wireline environment.

Supports industry-standard APIs

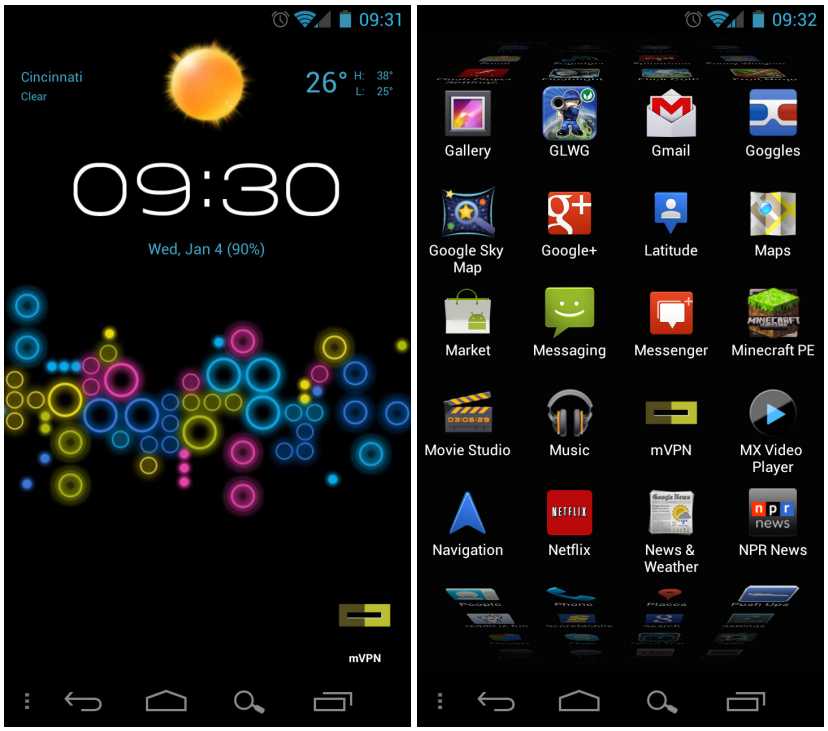
Columbitech Mobile VPN™ architecture is a client/server software based solution built on wireless technology for optimal performance. To ensure easy wireless enabling of corporate legacy applications, the software supports industry-standard application programming interfaces on the client and server side. Columbitech Mobile VPN™ is integrated into the IP communication stack and thus totally transparent to any client or server application.

The following platforms are supported:

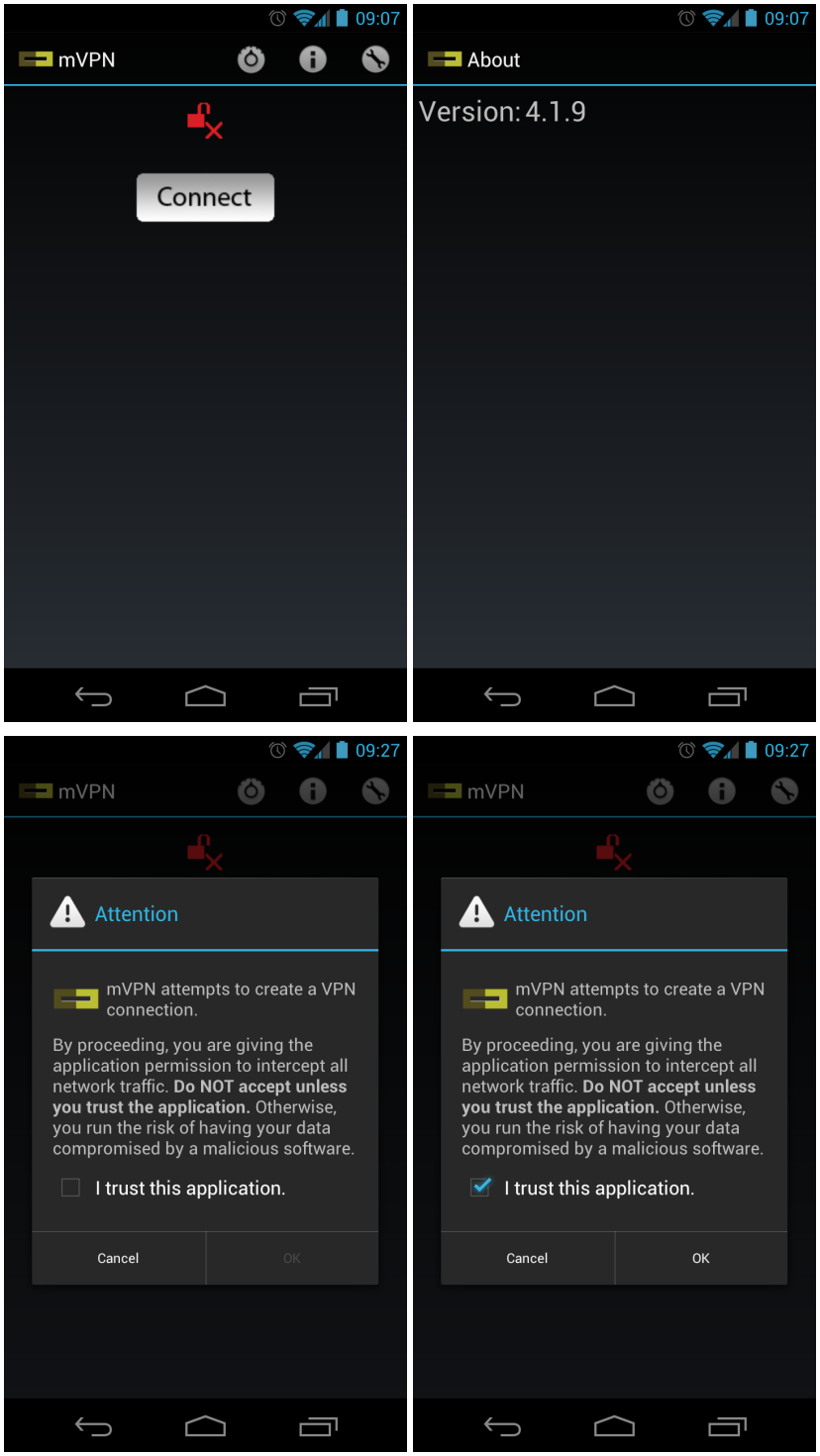
Client side	Server side
▪ Windows 2000 Professional ▪ Windows XP Professional ▪ Windows Vista ▪ Windows 7 ▪ Windows Mobile 5, Mobile 6 and Mobile 2003 ▪ IOS-based devices (Browser client) ▪ Android-based devices	▪ Windows 2000/2003/2008 Server ▪ Linux (kernel 2.6.8 or higher)

Configuring the mVPN client

Upon installing the Columbitech mVPN Android client, you will find an icon has been created: mVPN. Clicking this icon will bring you into the mVPN client monitor.



There are two buttons on the top right of the client monitor. Pressing the Settings button on the left will bring up a list of configurable options. Pressing the About button on the right will show up your mVPN version number. Upon choosing settings, you will be asked to give the client permission to intercept all network traffic. Click the box labeled 'I trust this application' and click OK to proceed.

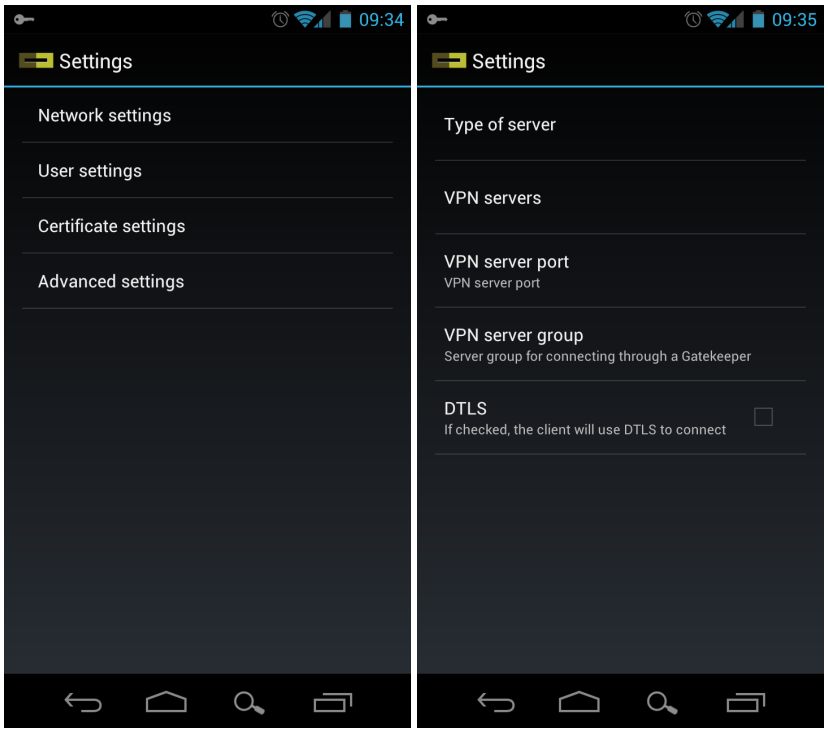


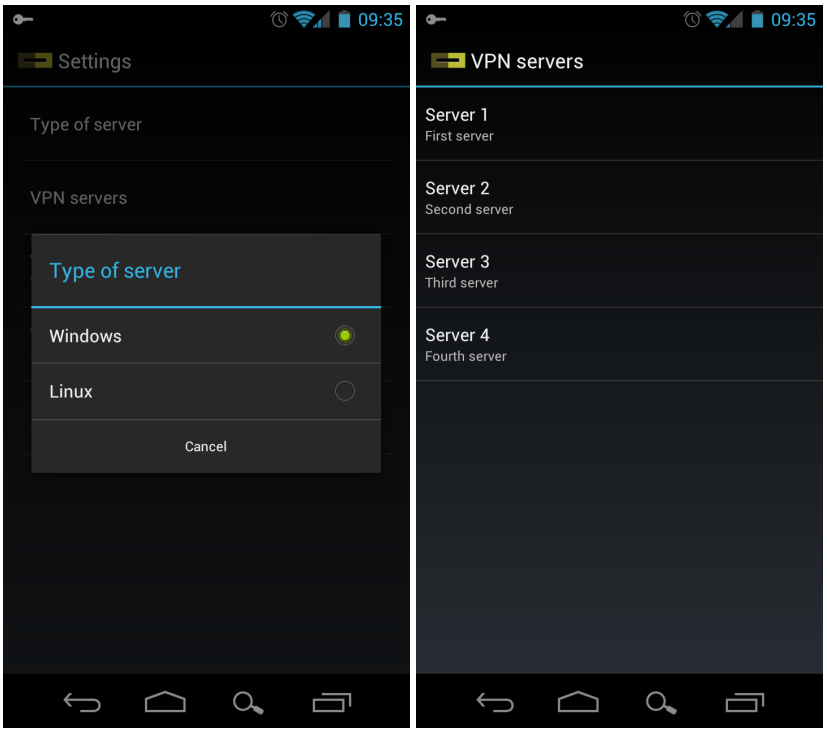
Upon clicking the 'Network settings' option, you'll have access to various client connectivity settings. When you have entered your relevant information, press the back button to save your entry and return to the Settings page.

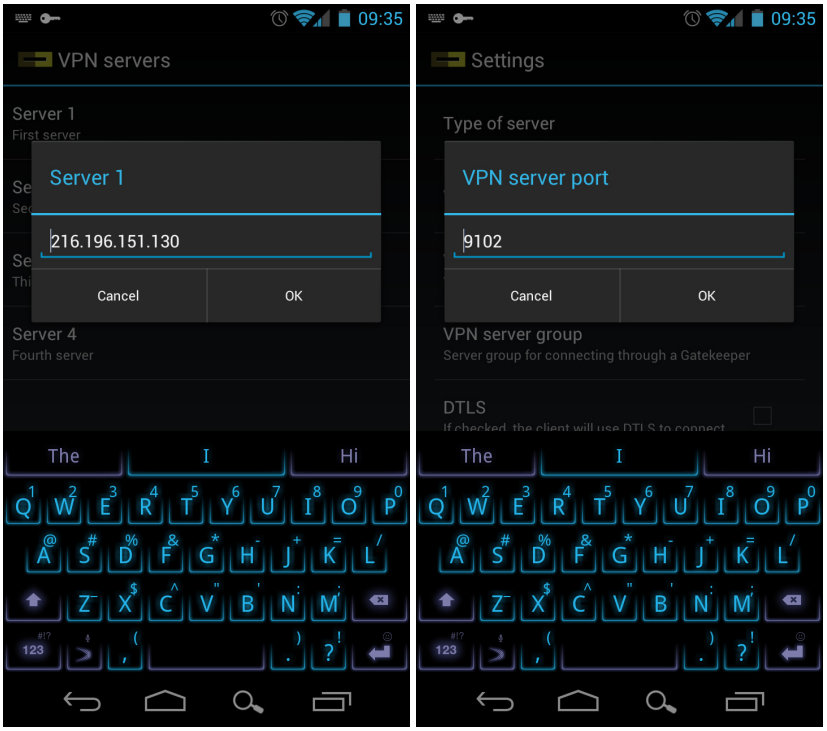
Follow these directions to enter the relevant information into the remaining fields:

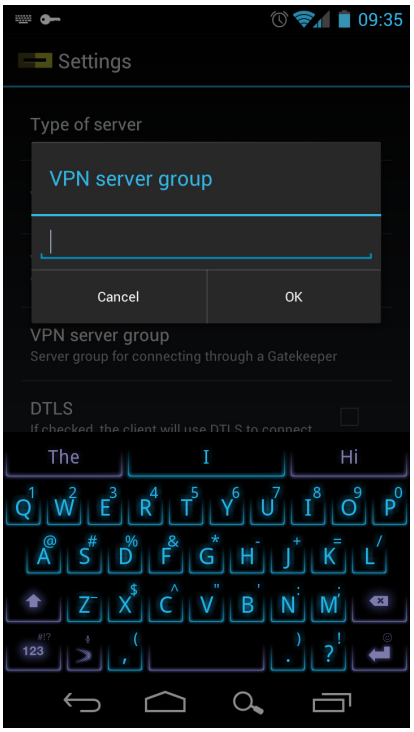
***NOTE** You do not have to enter any informaiton into the 'Cached username' and 'Cached domain' fields. If you leave these blank, the client will prompt you for them automatically.

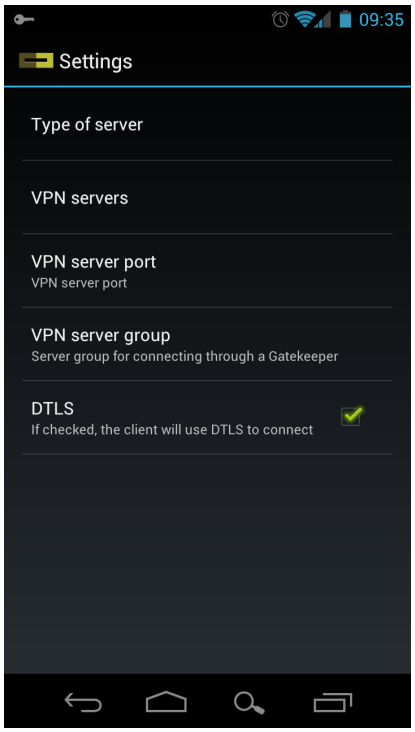
Also, only check the DTLS box if you are connecting to a Linux mVPN server.

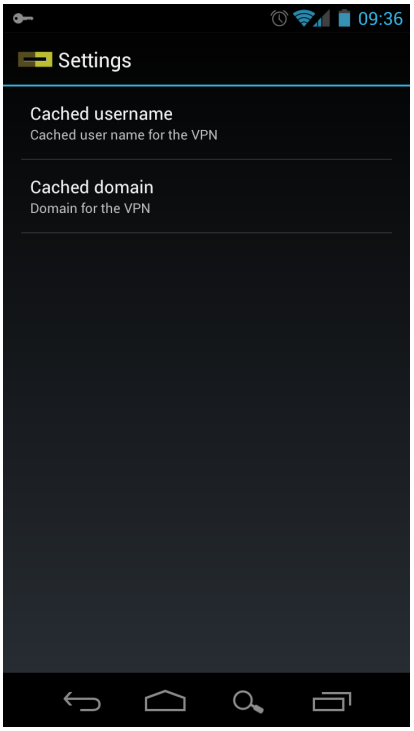


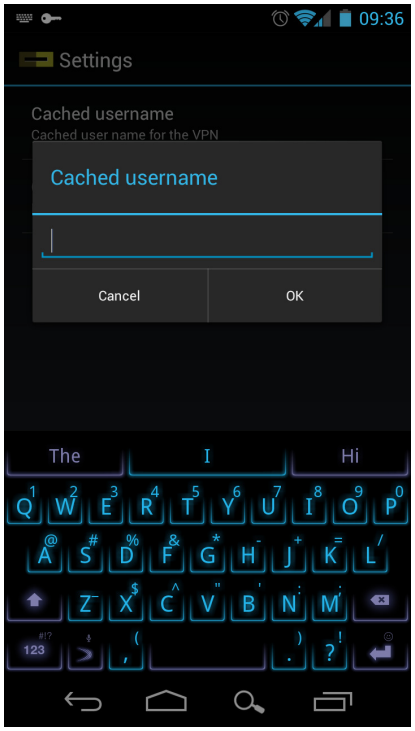


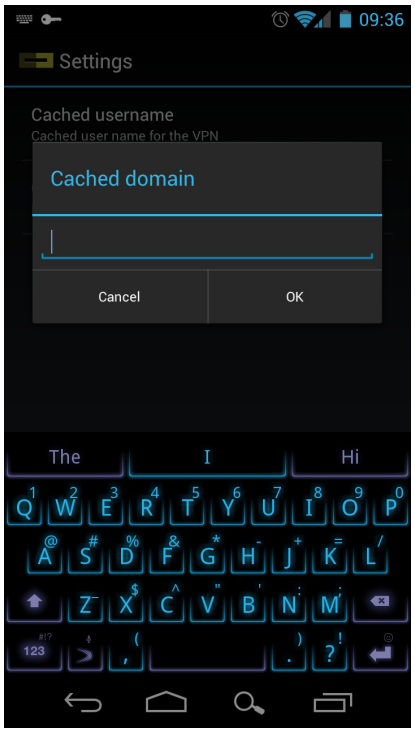






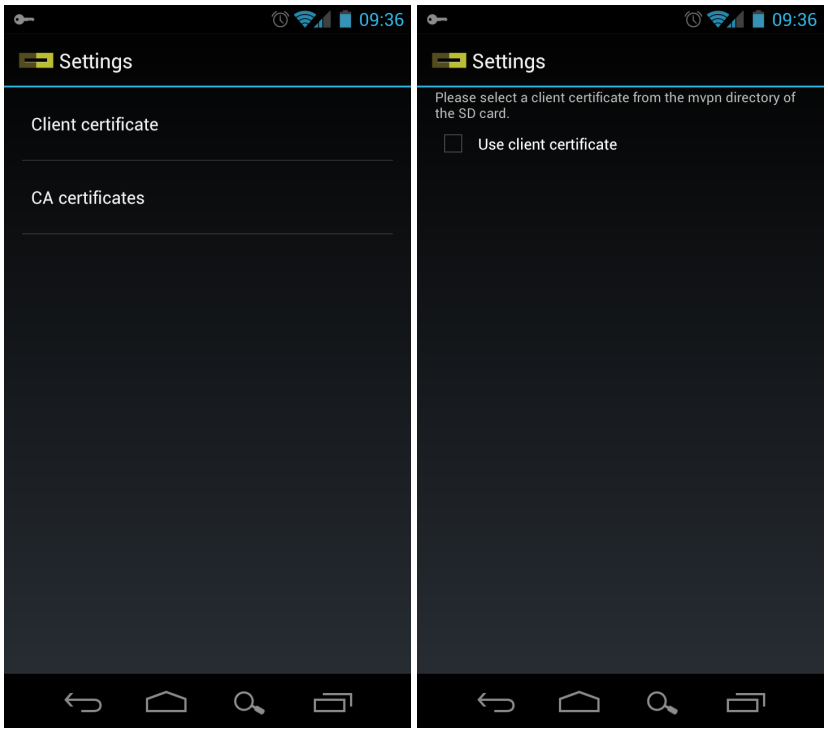


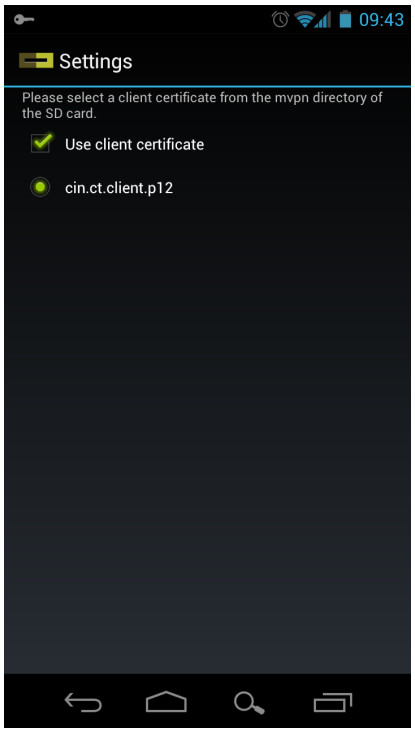


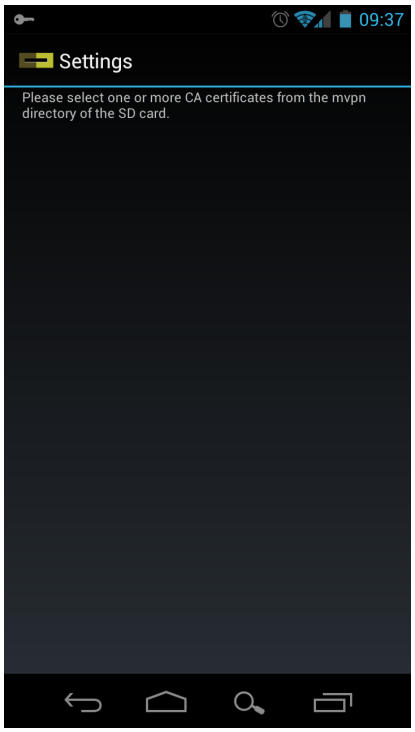


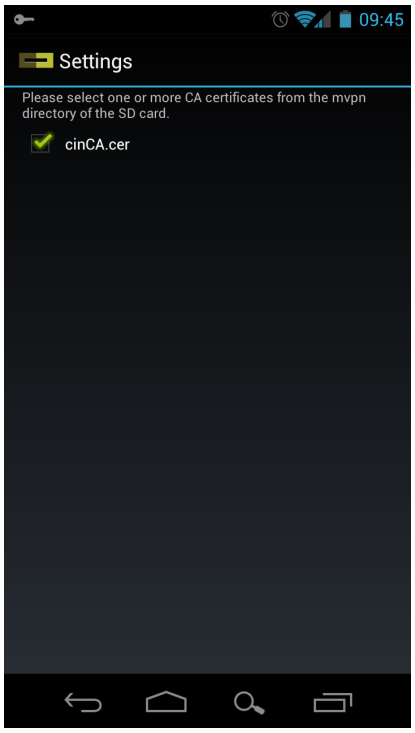
Click the Certificates option to choose client and CA certificates.

NOTE These certificates need to first reside in a mvpn folder on your SD card, or /sdcard/mvpn. If you have no certificates present, none will show on the screen. If they are already loaded onto the SD card, the name of your certificate will be shown as an available check box.

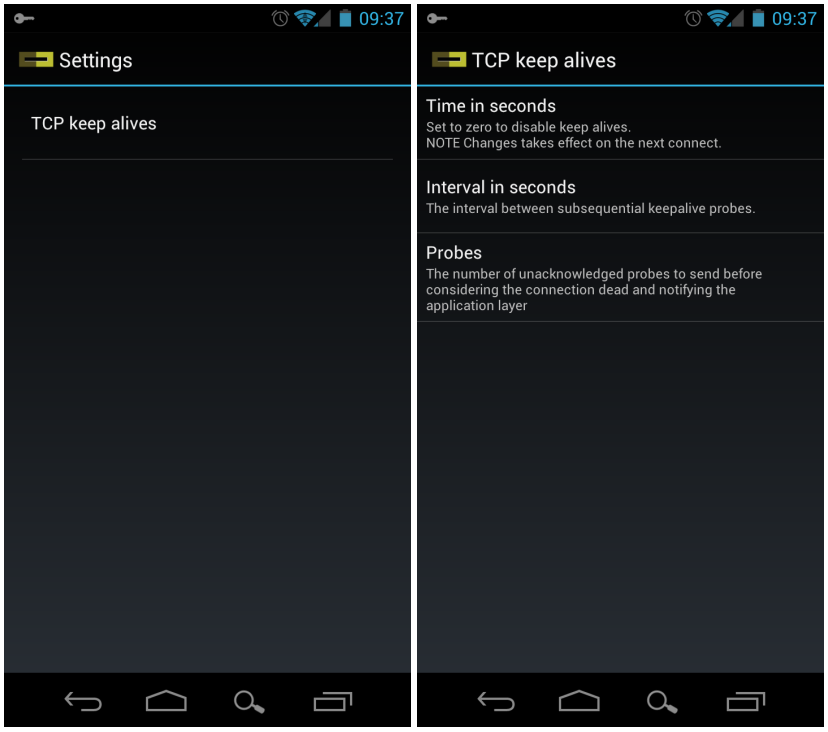


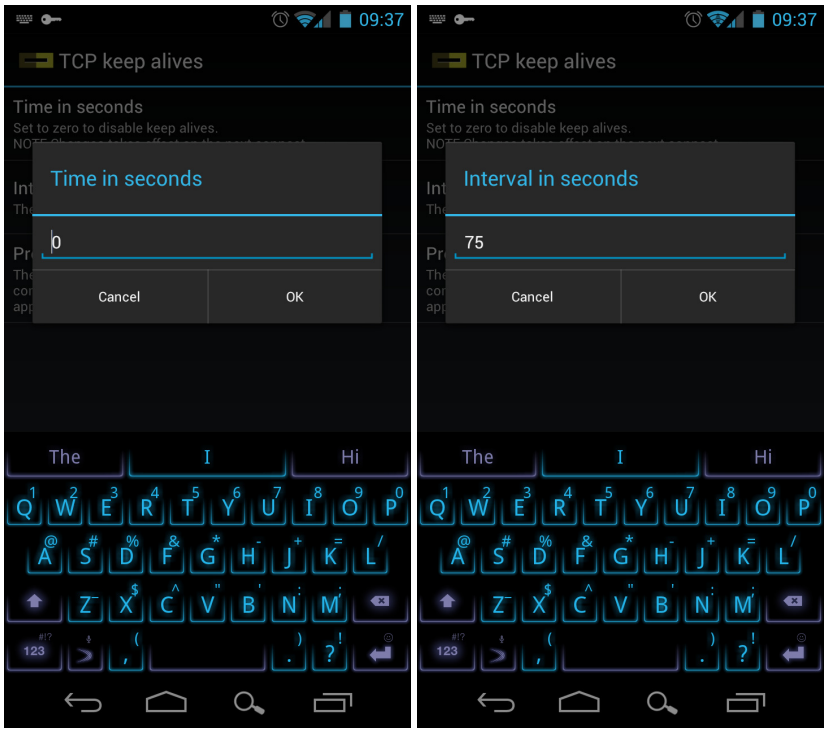


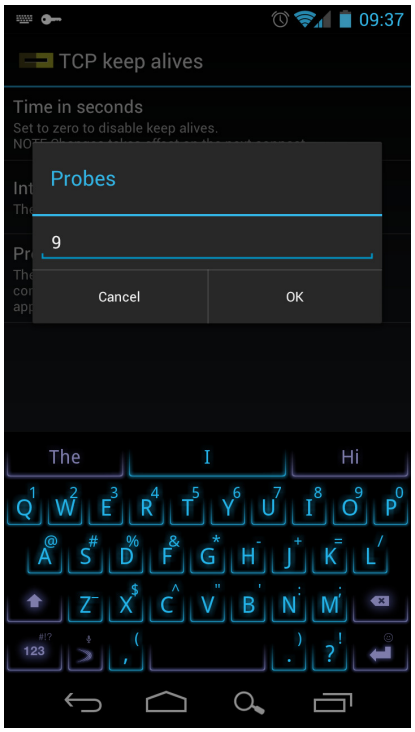




Click Advanced to access specific configuration options. 'TCP keep alives' affect how the phone responds when roaming. Below, the default values are shown.





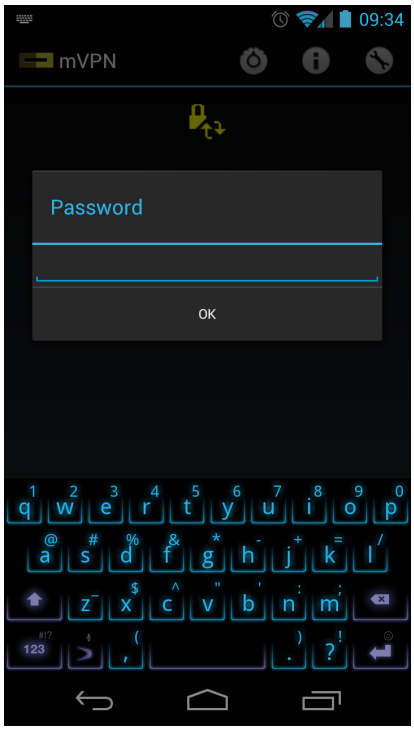


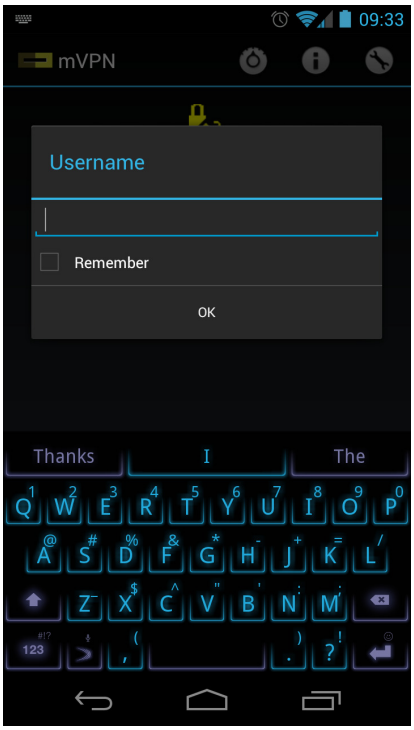
Use the back button on your phone to return to the main mVPN client screen once all of your configuration settings have been entered.

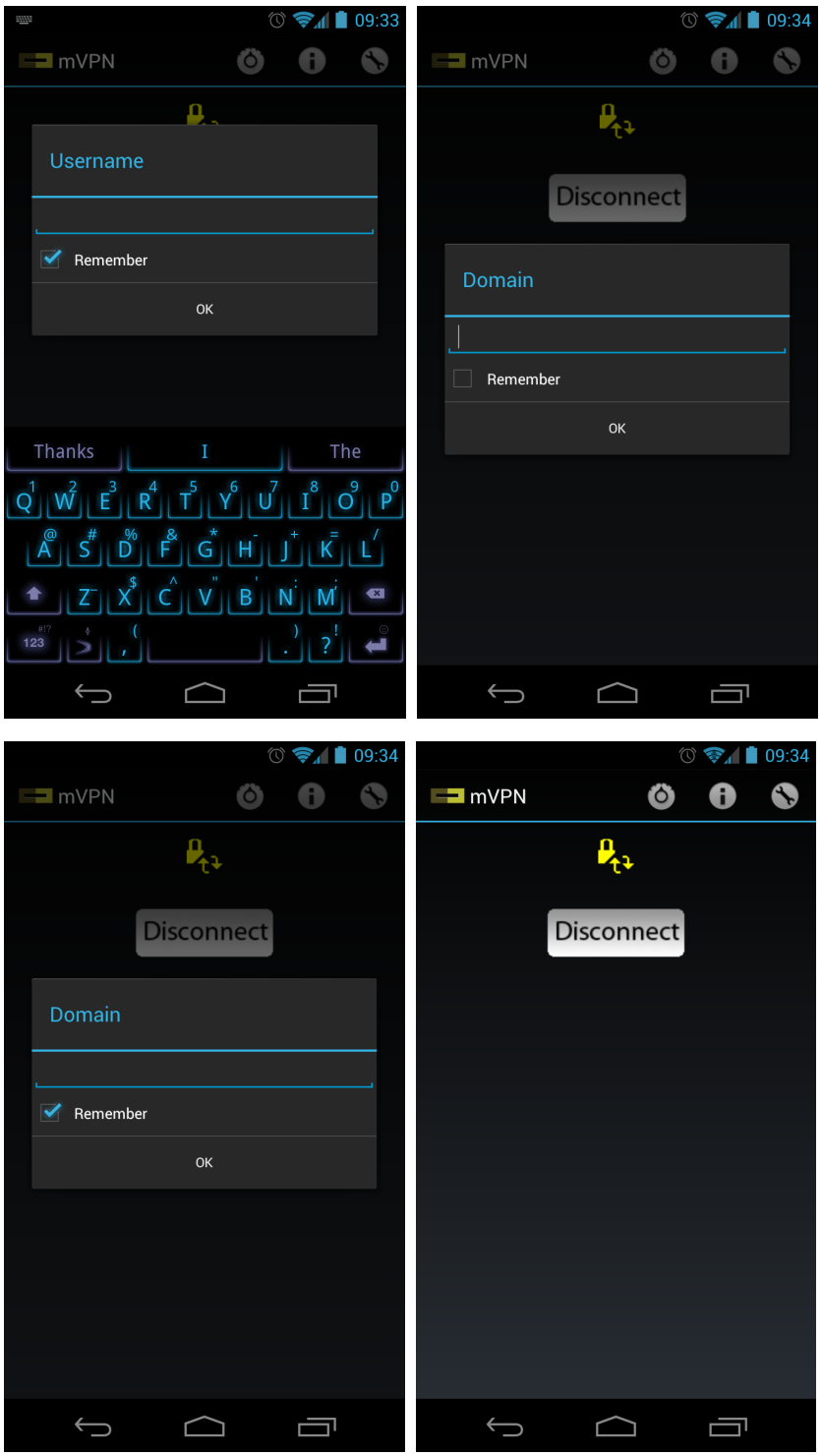
Using the mVPN Client

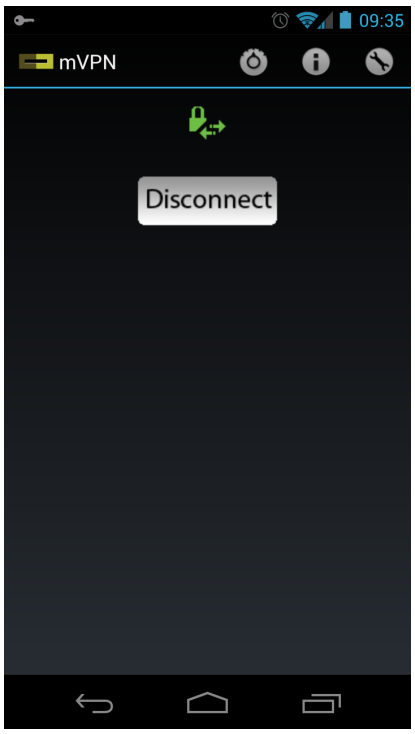
Upon clicking the green Connect button, you will be prompted for the password associated with your specific username. If your server expects a client certificate, you will be asked for that certificate's private key password. If you have not saved a username and/or domain, you may be prompted for those as well. When entering the username and/or domain, you have the option to chache or remember those credentials.

Notice below the key icon on the top left corner of the taskbar. If you see now key, it means that your client is disconnected. A key present represents that your client has previously been connected. A yellow circled arrows in the client monitor without a key in the taskbar means that your client is connecting state. A yellow circled arrows in the client monitor with a key in the taskbar means that your client is in a roaming state. Green parallel arrows mean that your client is connected. Press the Disconnect button to terminate your mVPN connection.

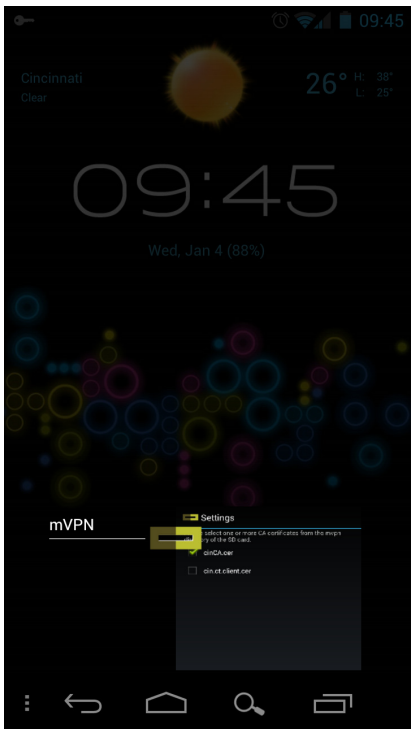


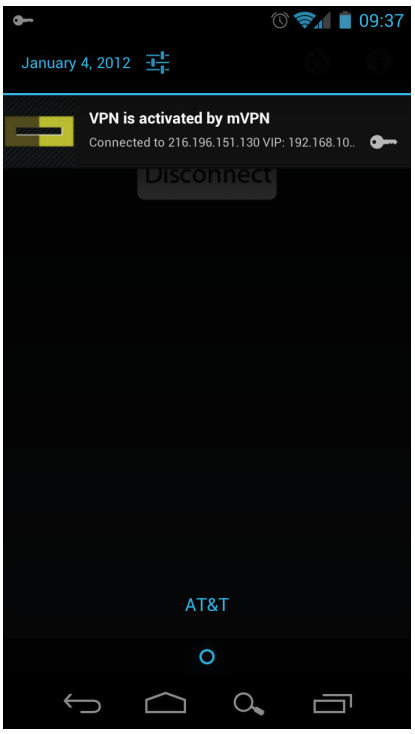


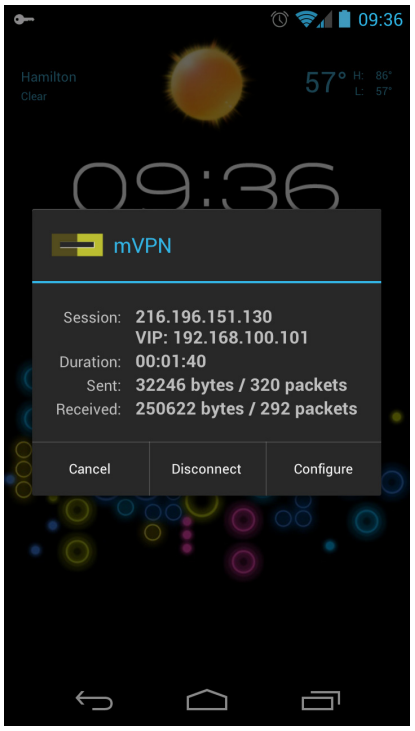




Pressing the Recent Apps button on the bottom right of your screen will allow you to quickly navigate back to the client monitor. Similarly, if you swipe downward the Notifications bar will appear. If your client is connected, you will always see here. Clicking this reference brings you back to the client monitor, but also shows a detailed status screen with various options.







Troubleshooting the mVPN Client

Upon clicking the rightmost tool button, you will be given several tools to test the connectivity of your client and your server. Test TCP will tell you if your server is listening on the appropriate port. Test Reachability will tell you what the client can reach over IP. In the example below, notice the client is connected to, and is able to reach, a private NAT address.