

# FortiClient VPN (Android) - User Guide

**VERSION 5.2**

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



February 27, 2018

FortiClient VPN (Android) 5.2 User Guide

04-520-288763-20180227

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
FortiClient VPN (Android) 5.2 features .....	5
Download FortiClient VPN (Android) 5.2 .....	5
<b>Product Integration and Support</b> .....	<b>6</b>
FortiClient VPN (Android) 5.2 support .....	6
<b>Open the Application</b> .....	<b>7</b>
<b>SSL VPN</b> .....	<b>9</b>
Create an SSL VPN connection .....	9
Connect to the VPN .....	13
Edit SSL VPN settings or delete a SSL VPN configuration .....	16
Auto start .....	16
<b>IPsec VPN</b> .....	<b>18</b>
Create an IPsec VPN connection .....	18
Connect to an IPsec VPN .....	24
Edit VPN settings or delete a VPN configuration .....	25
Auto start .....	26
<b>Endpoint Control</b> .....	<b>27</b>
FortiGate FortiClient Profile .....	27
Connect to the FortiGate .....	28
Disconnect from FortiGate .....	31

# Change Log

Date	Change Description
2014-03-05	Initial release.
2014-07-0p	Updated for 5.2.1.
2014-08-01	Updated for 5.2.2.
2014-08-20	Updated for 5.2.3.
2014-10-09	Updated for 5.2.4.
2015-08-22	Updated for 5.2.6.
2018-02-23	Release of single merged document for all 5.2 versions.

# Introduction

FortiClient VPN (Android) 5.2 includes IPsec VPN, SSL VPN, and Endpoint Control.

## FortiClient VPN (Android) 5.2 features

The following table lists and describes features supported in FortiClient VPN (Android) 5.2.

Feature	Description
IPsec VPN	<ul style="list-style-type: none"><li>• Configure IPsec VPN connections.</li><li>• IKE main mode and aggressive mode support.</li><li>• Client X.509 certificates and pre-shared key support.</li><li>• Enable always up and auto connect options.</li><li>• Disable auto start.</li></ul>
SSL VPN	<ul style="list-style-type: none"><li>• Configure tunnel mode SSL VPN connections.</li><li>• Client and server X.509 certificates support.</li><li>• Enable always up and auto connect options.</li><li>• Disable auto start.</li></ul>
Endpoint Control	<ul style="list-style-type: none"><li>• Configure and deploy a FortiOS FortiClient Profile to connected FortiClient VPN (Android)s.</li><li>• Provision VPN connections.</li><li>• Policy enforcement.</li></ul>

## Download FortiClient VPN (Android) 5.2

You can download the FortiClient VPN (Android) 5.2 application from the Google play application or at the following link, <https://play.google.com/store>.

# Product Integration and Support

## FortiClient VPN (Android) 5.2 support

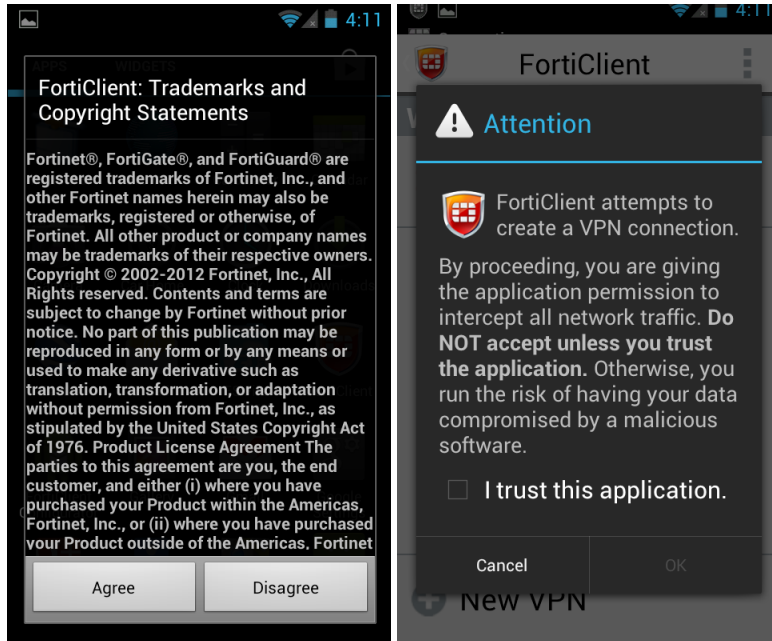
The following table lists FortiClient VPN (Android) 5.2 product integration and support information.

Android operating systems	<ul style="list-style-type: none"><li>• 4.1 Jelly Bean (API level 16)</li><li>• 4.2 Jelly Bean (API level 17)</li><li>• 4.3 Jelly Bean (API level 18)</li><li>• 4.4.3 KitKat (API level 19)</li><li>• 4.4.4 KitKat (API level 20)</li><li>• 5.0.1 Lollipop (API level 21)</li><li>• 5.1.1 Lollipop (API level 22)</li></ul>
FortiOS	<ul style="list-style-type: none"><li>• 5.0.5 and later</li><li>• 5.2.0 and later</li></ul>
FortiToken Mobile	<ul style="list-style-type: none"><li>• 2.0.3 and later</li></ul> <p>For more information, see the <a href="#">FortiToken Mobile User Guide for Android</a>.</p>

# Open the Application

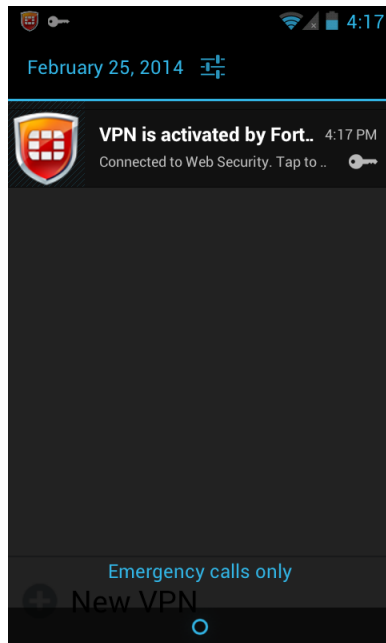
When FortiClient VPN (Android) 5.2 is installed and run for the first time, read the *Trademarks and Copyright Statement* and select the *Agree* button. Read the statement, select the *I trust this application* checkbox, and select *OK*. After that, FortiClient VPN (Android) will automatically start when Android OS starts.

## Trademarks and VPN message



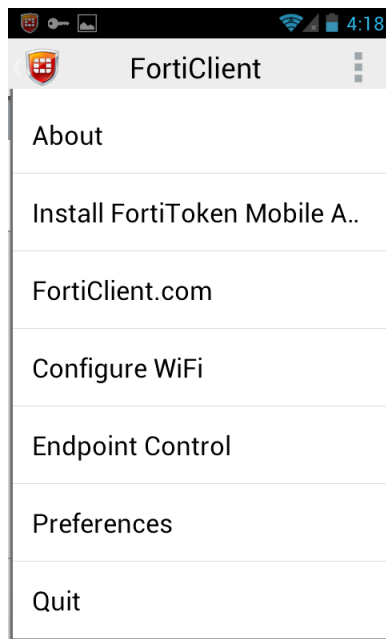
FortiClient VPN (Android) 5.2 allows you to launch the application from the notification bar.

### Launch from notification bar



You can quit the app from the menu page.

### Quit from app menu



# SSL VPN

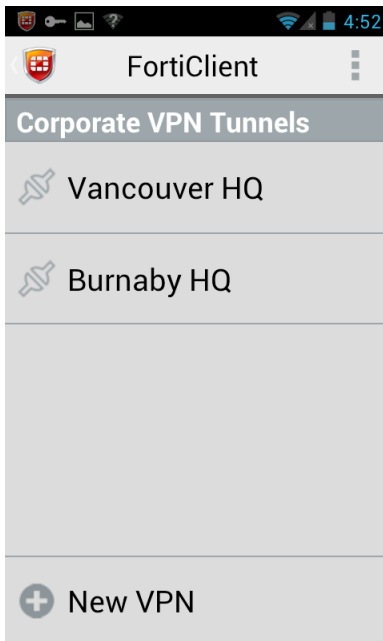
FortiClient VPN (Android) 5.2 supports tunnel mode SSL VPN connections. You can configure the SSL VPN in the FortiClient user interface or provision SSL VPN connections in the FortiGate FortiClient Profile. Provisioned SSL VPN configurations are pushed to your Android device upon successful connection with the FortiGate device for Endpoint Control. You can configure X.509 certificates, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

## Create an SSL VPN connection

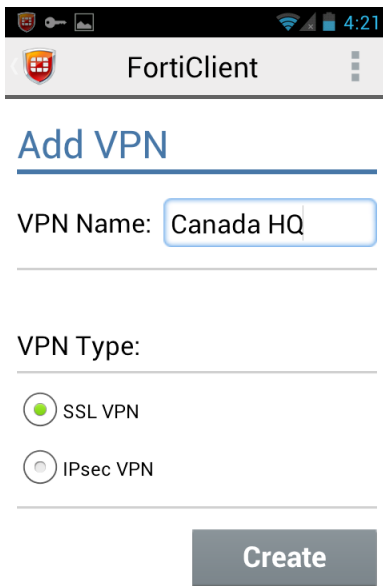
To create a new SSL VPN connection in the FortiClient VPN (Android) user interface follow the steps listed below.

**To create a new SSL VPN connection:**

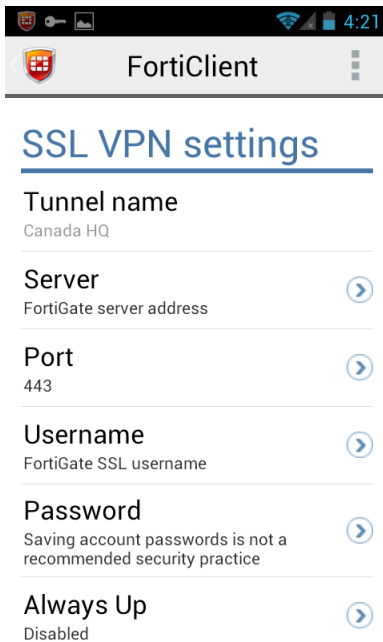
1. Select *New VPN* from the toolbar in the bottom of the page.



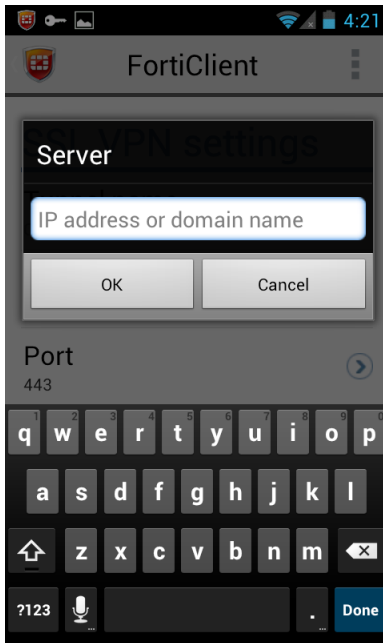
2. Enter a name for the new VPN connection, select *SSL VPN* under *VPN Type*, and select *Create*.



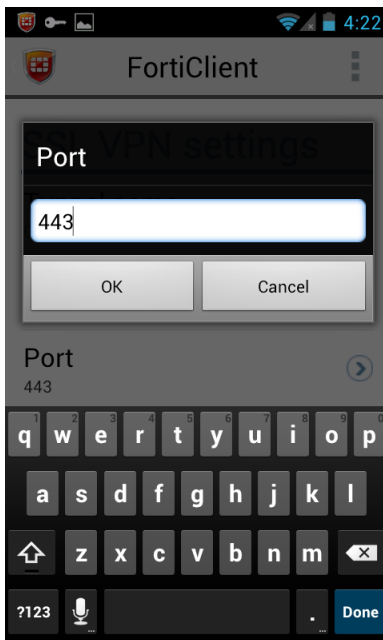
The SSL VPN settings page is displayed.



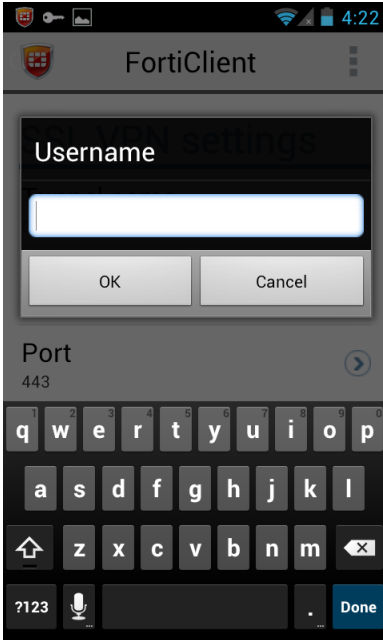
3. Select *Server*, enter the server IP address or domain name, and select *OK*.



4. Select *Port*, enter the port number, and select *OK*. The default port is 443.



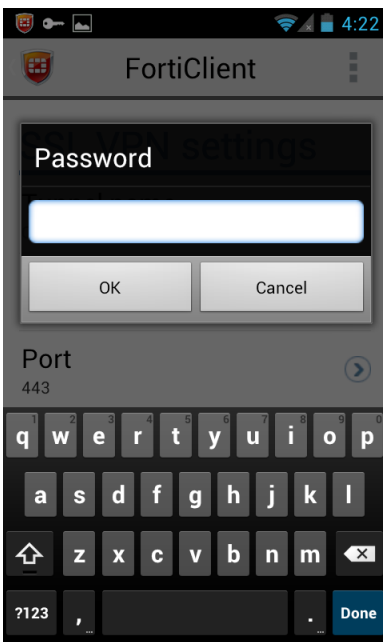
5. Select *Username*, enter a user name, and select *OK*.



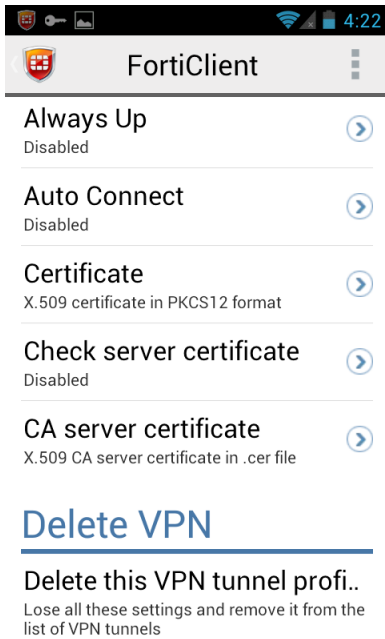
6. Select *Password*, enter a password, and select *OK*. There is no maximum value for the password length. The password can consist of alpha, numeric and special characters.



The username and password configured on the client must match the username and password configured on the FortiGate. Contact your network administrator for the correct setting.



7. You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *SSL VPN settings* page.

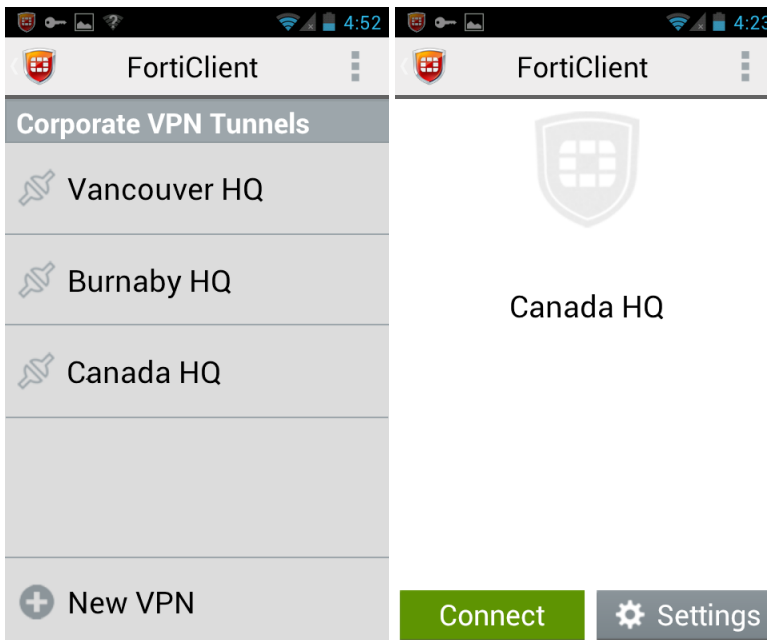


## Connect to the VPN

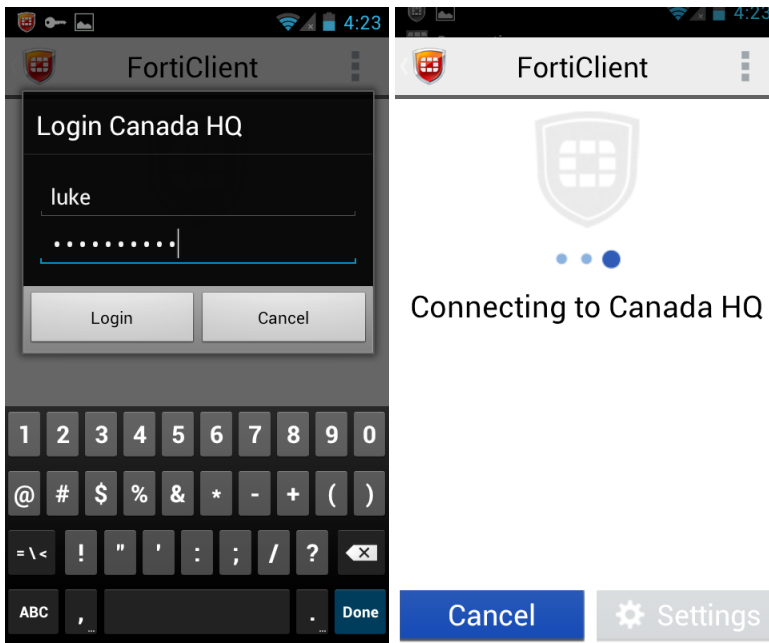
SSL VPN tunnel mode uses X.509 Certificates (PKCS12 format) for authentication. Certificate settings need to be configured if authentication requires the client certificate, otherwise leave the certificate settings as their default value.

### To connect to the SSL VPN:

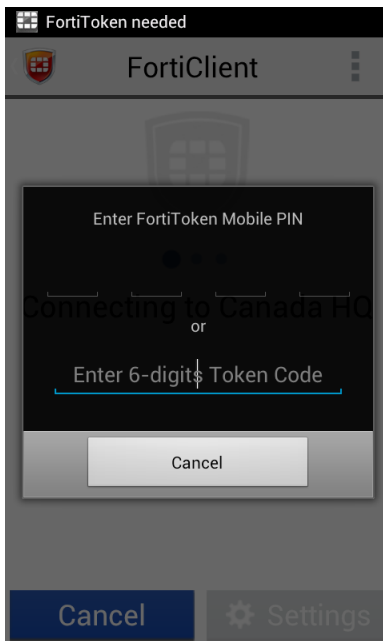
1. Select an available VPN and then select *Connect*.



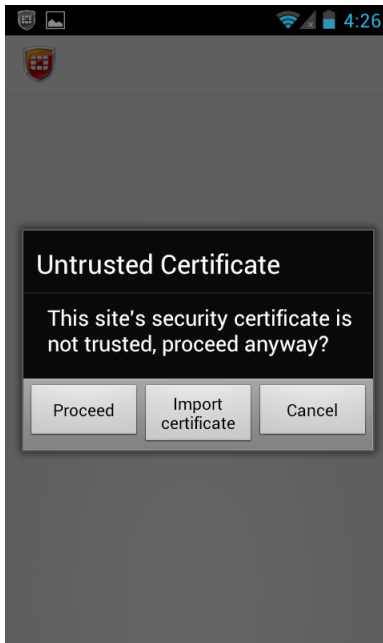
2. Enter your username and password and then select *Login*.



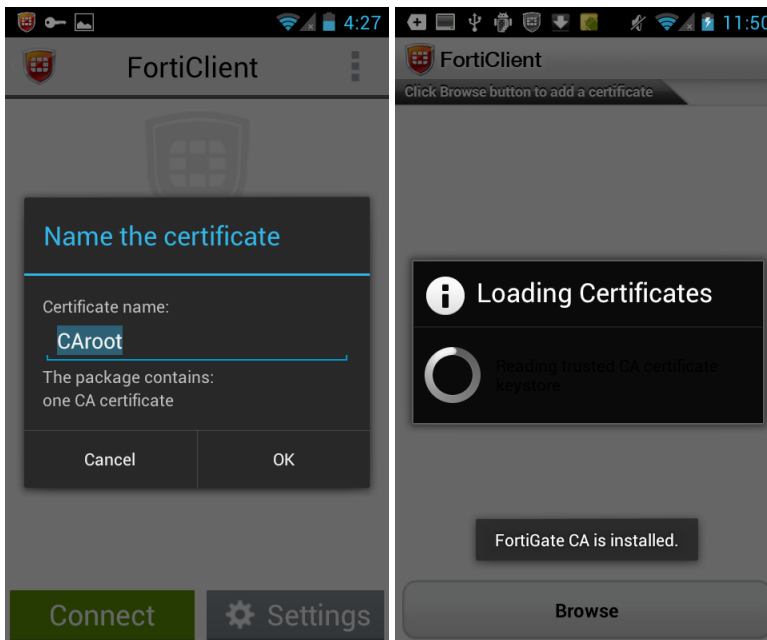
If the SSL VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token.



3. You will receive an *Untrusted Certificate* message dialog box warning message, and you will have the option to *Proceed*, *Cancel*, or *Import certificate*.



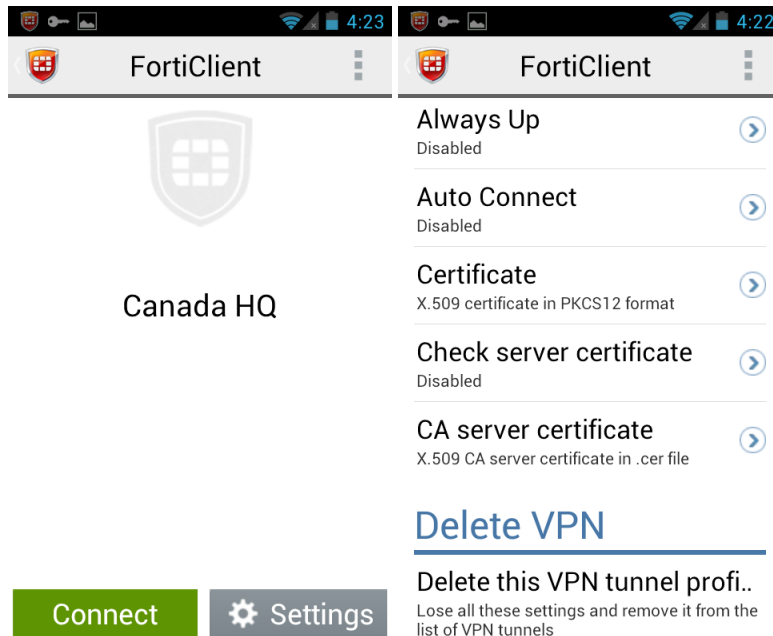
4. Select *Import certificate*, browse for the certificate file, edit the name (if required).



5. Select *OK* to load and install the certificate. The certificate is now installed on the device. Use the device back button to return to the connection screen.
6. Select an available VPN to connect.

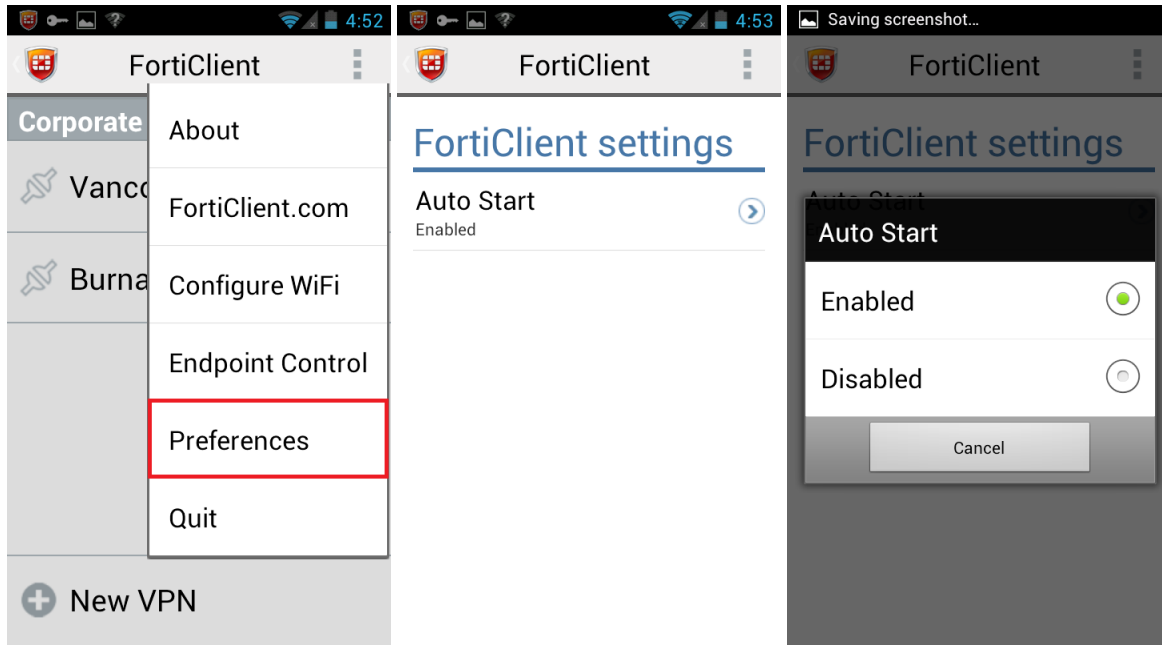
## Edit SSL VPN settings or delete a SSL VPN configuration

To edit SSL VPN settings or delete an existing SSL VPN configuration, select the SSL VPN, and select the *Settings* button.



## Auto start

In FortiClient VPN (Android) 5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start*, then select *Enabled* or *Disabled*.



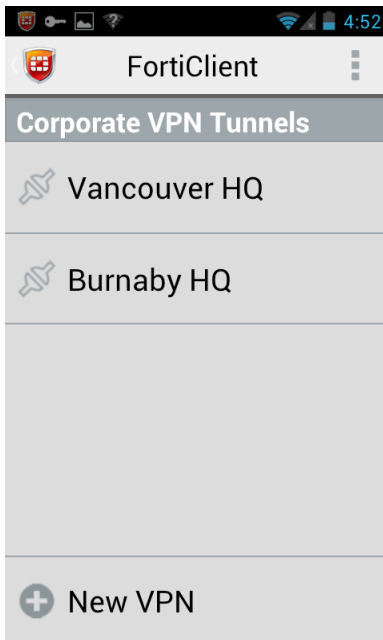
# IPsec VPN

FortiClient VPN (Android) 5.2 supports IPsec VPN connections. You can configure the IPsec VPN in the FortiClient user interface or provision IPsec VPN connections in the FortiGate FortiClient Profile. Provisioned IPsec VPN configurations are pushed to your Android device upon successful connection with the FortiGate device for Endpoint Control. You can configure server settings, phase 1, phase 2, and XAuth settings.

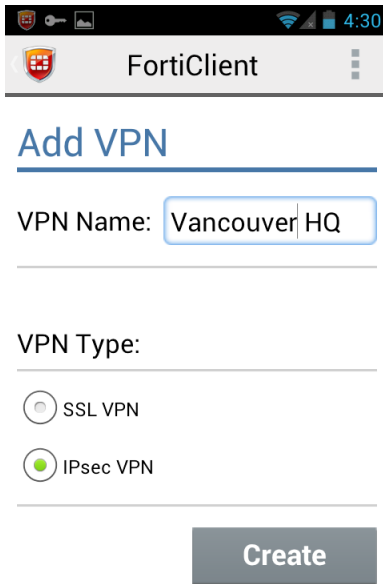
## Create an IPsec VPN connection

**Create a new IPsec VPN connection:**

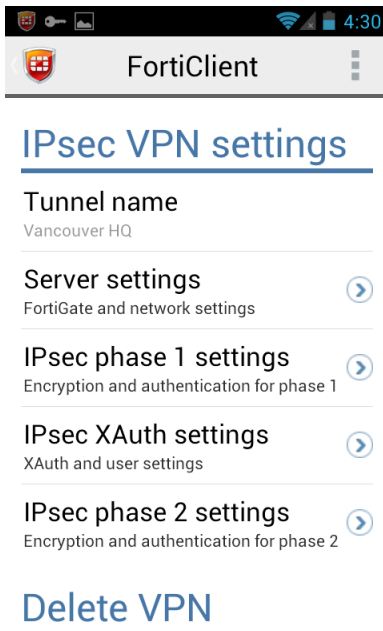
1. Select *New VPN* from the toolbar in the bottom of the page.



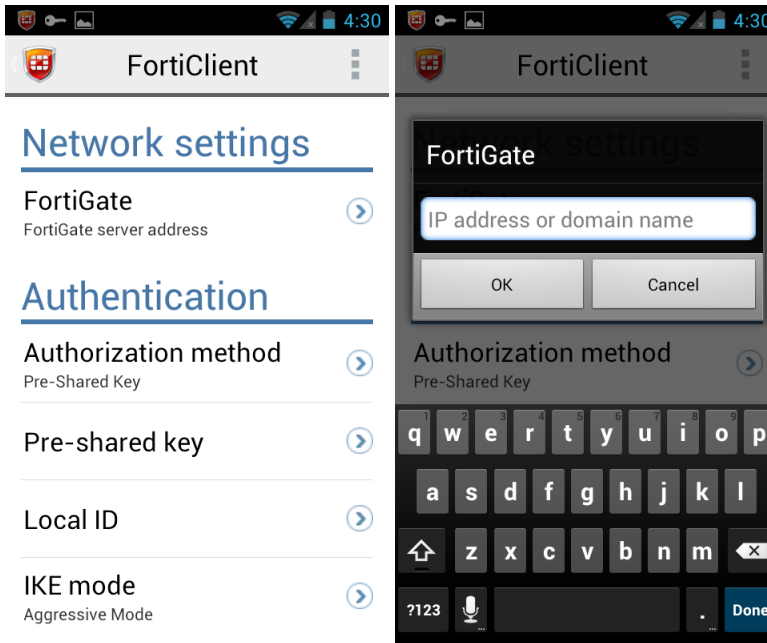
2. Enter a name for the new VPN connection, select *IPsec VPN* under *VPN Type*, and select *Create*.



The IPsec VPN settings page is displayed.



3. Select *Server settings*, under *Network settings*, select *FortiGate*, enter the server IP address or domain name, and select *OK*.



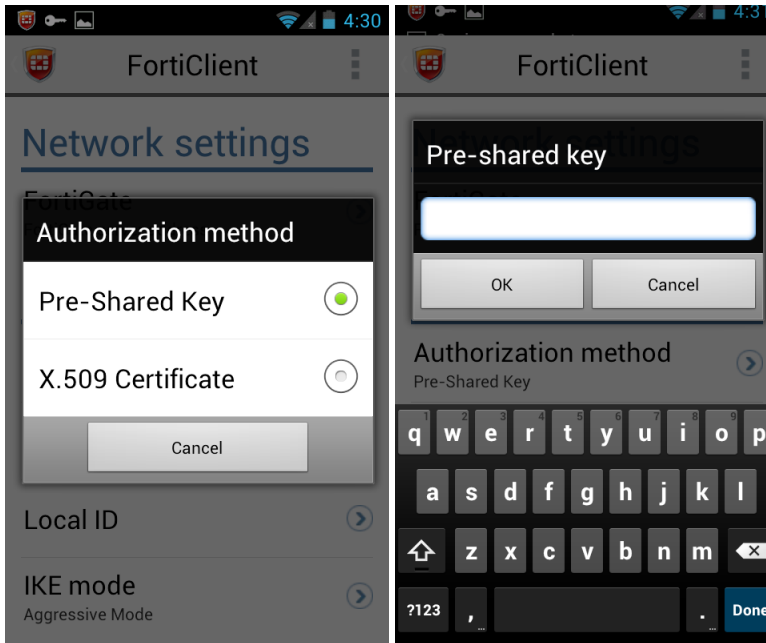
4. Under *Authentication*, select *Authorization method*, and select *Pre-Shared Key* or *X.509 Certificate*.
5. For pre-shared key, select *Pre-shared Key* to enter the pre-shared key value.

The simplest way to authenticate with the FortiGate unit is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth).

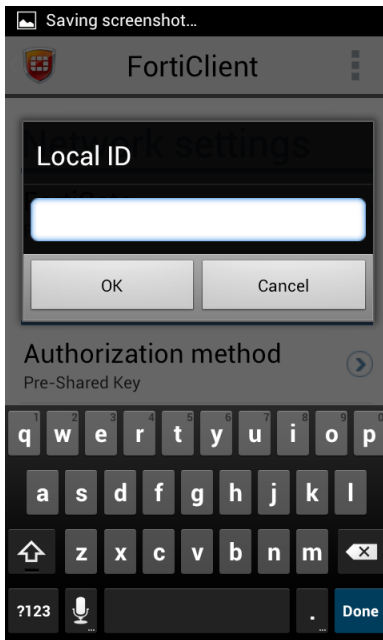
The pre-shared key must contain at least 6 characters. For optimum protection against currently known attacks, the key must consist of a minimum of 16 randomly chosen alphanumeric characters.



The pre-shared key configured on the client must match the pre-shared configured on the FortiGate. Contact your network administrator for the correct setting.



Select *Local ID*, enter the local ID, and select *OK*.

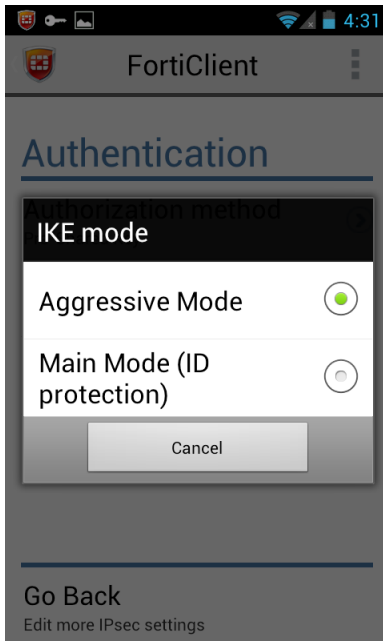


6. For X.509 certificate select *Certificate* and then browse for the certificate file on your device.  
To authenticate with the FortiGate unit using digital certificates, you must have the required certificates installed on the Android device (peer) and the FortiGate unit (server).



Contact your network administrator for the correct X.509 certificate file.

7. Select *IKE mode*, and select *Aggressive Mode* or *Main Mode (ID protection)*.



In *Aggressive Mode*, the phase 1 parameters are exchanged in single message with authentication information that is not encrypted.

In *Main Mode*, the phase 1 parameters are exchanged in multiple rounds with encrypted authentication information.



The *IKE Mode* selected on the client must match the mode selected on the server. Contact your network administrator for the correct setting.

8. Select *Go Back* to return to the *IPsec VPN settings* page.
9. Select *IPsec phase 1 settings* to view or edit the phase 1 proposal encryption and authentication settings. You can choose to use the default settings.

Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
- AES128: A 128-bit block algorithm that uses a 128-bit key.

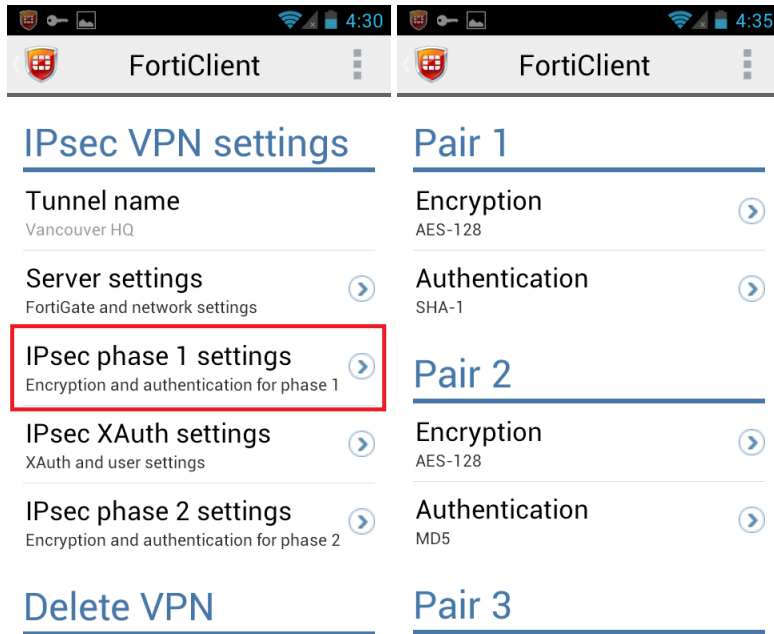
You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

Select one or more Diffie-Hellman (DH) groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.

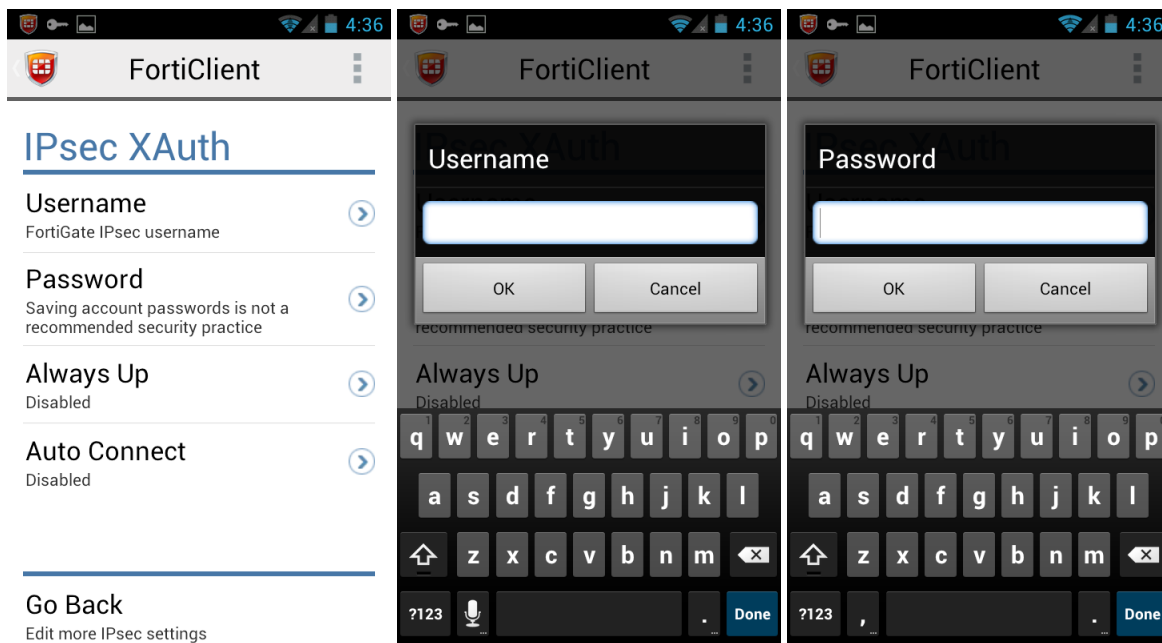


Contact your network administrator for the correct phase 1 encryption and authentication algorithms, and DH group.



10. Select *Go Back* to return to the *IPsec VPN settings* page.
11. Select *IPsec XAuth settings* to view or edit the XAuth and user settings. XAuth is enabled by default. Select *Username* to enter the FortiGate IPsec username. Select *Password* to enter the password value. To use XAuth, you must first configure the user’s credentials on your FortiGate, and external RADIUS or LDAP server. Extended authentication (XAuth) increases security by requiring the remote dialup client user to authenticate in a separate exchange at the end of phase 1. XAuth draws on existing FortiGate user group definitions and uses established authentication mechanisms such as PAP, CHAP, RADIUS and LDAP to authenticate dialup clients.

You can select to enable *Always Up*, *Auto Connect*, and *Check server certificate* in the *IPsec XAuth* page.



12. Select *Go Back* to return to the *IPsec VPN settings* page.

13. Select *IPsec phase 2 settings* to view or edit the phase 2 encryption and authentication settings. You can choose to use the default settings.

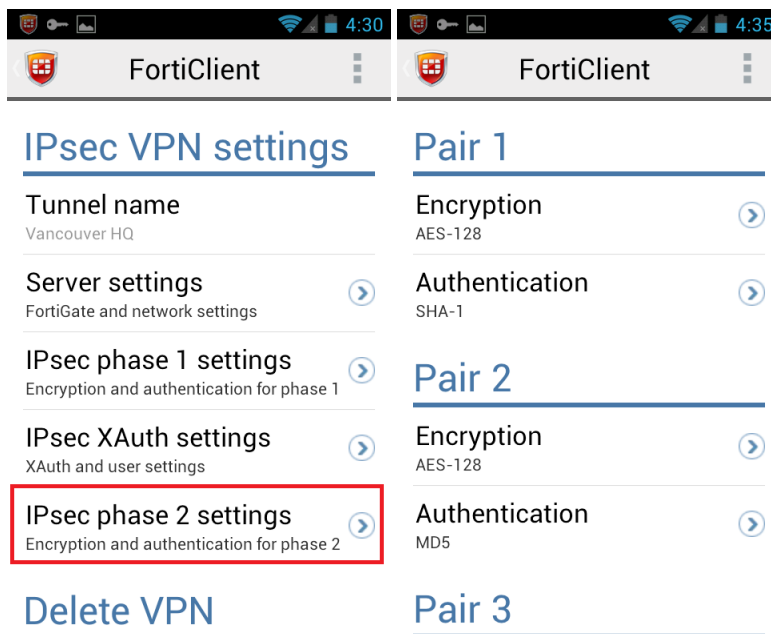
Select the encryption and authentication algorithms that will be used to generate keys for protecting negotiations. You can select any of the following symmetric-key algorithms:

- DES: Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key.
- 3DES: Triple-DES, in which plain text is encrypted three times by three keys.
- AES128: A 128-bit block algorithm that uses a 128-bit key.

You can select one of the following message digests to check the authenticity of messages during phase 1 negotiations:

- MD5: Message Digest 5, the hash algorithm developed by RSA Data Security.
- SHA-1: Secure Hash Algorithm 1, which produces a 160-bit message digest.

Select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.



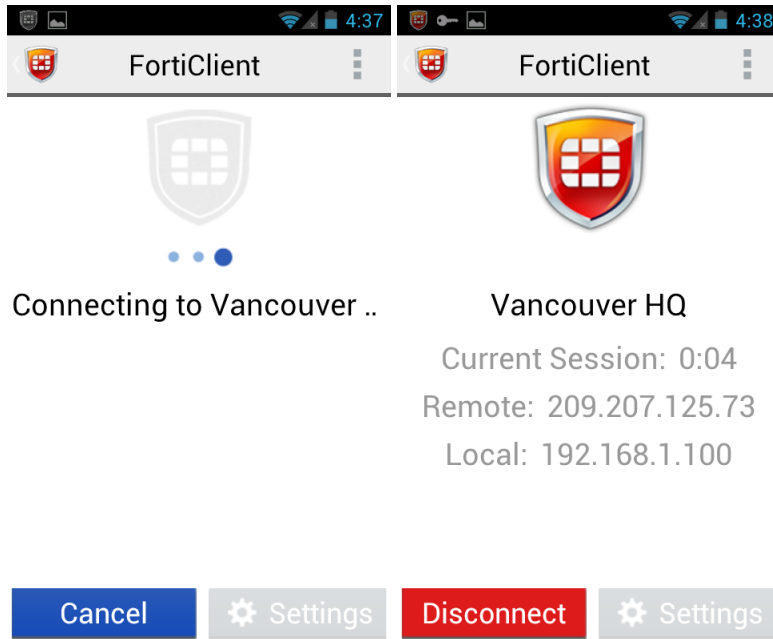
Contact your network administrator for the correct phase 2 encryption and authentication algorithms, and DH group.

14. Select *Go Back* to return to the *IPsec VPN settings* page.

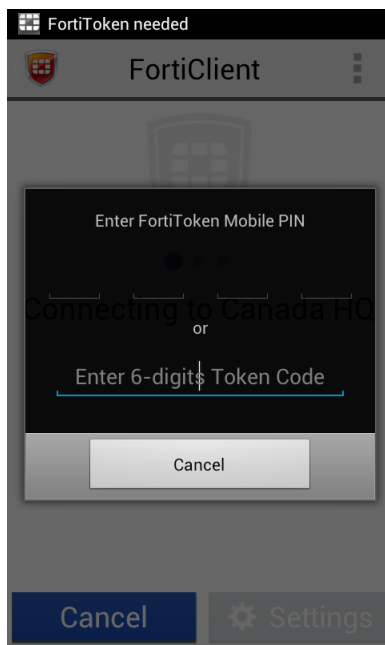
## Connect to an IPsec VPN

### Connect to an IPsec VPN:

1. Select an available IPsec VPN connection.
2. Enter the username and password, and select *Connect*.

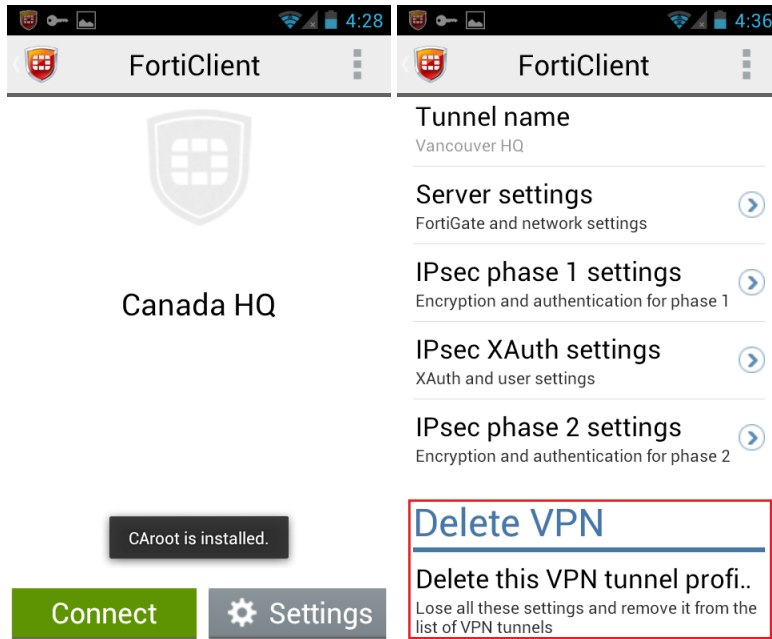


If the IPsec VPN you are connecting to requires you to enter a FortiToken Mobile token, you will be prompted to enter your FortiToken Mobile PIN or 6-digit Token code.



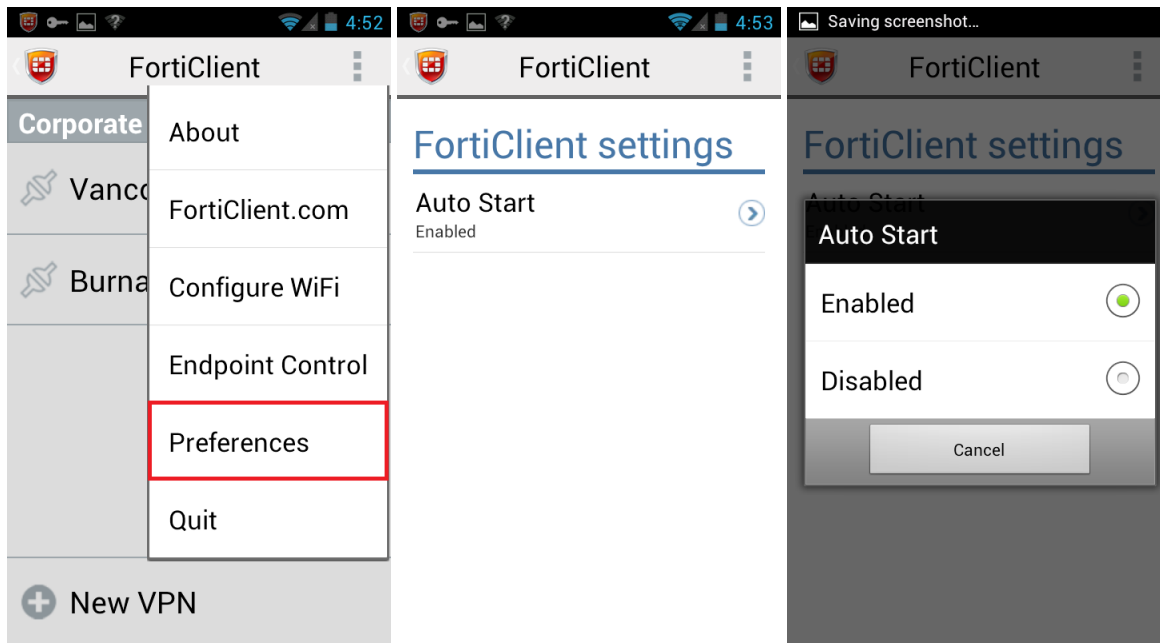
## Edit VPN settings or delete a VPN configuration

To edit IPsec VPN settings or delete an existing IPsec VPN configuration, select the IPsec VPN, and select the *Settings* button.



## Auto start

In FortiClient VPN (Android) 5.2 you can select to disable auto start. To enable or disable auto start, select the menu icon in the toolbar, and select *Preferences* in the drop-down menu. In the FortiClient settings page select *Auto Start*, then select *Enabled* or *Disabled*.



# Endpoint Control

FortiClient VPN (Android) 5.2 allows you to connect to a FortiGate device and receive a FortiClient profile for endpoint control.

## FortiGate FortiClient Profile

### Configure the FortiClient Profile:

1. On your FortiGate device, go to *User & Device > FortiClient Profiles*.
2. Select *Create New* from the toolbar. The *New FortiClient Profile* page opens.

3. In the *Android* section of the page, configure the following settings:

<b>Client VPN Provisioning</b>	Toggle the button to enable or disable client VPN provisioning. Select the add icon to add multiple VPN configurations.
<b>VPN Name</b>	Enter a name for the VPN connection.

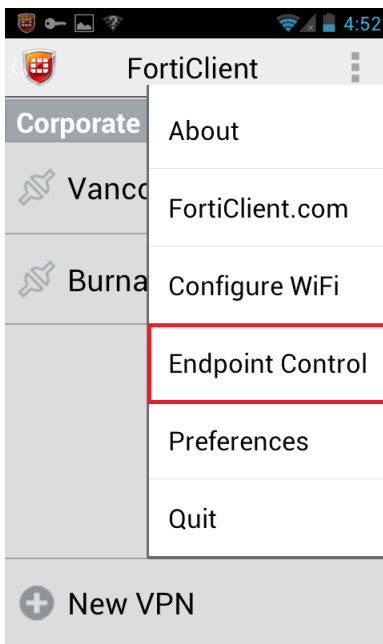
<b>Type</b>	Select IPsec VPN or SSL VPN.
<b>Remote Gateway</b>	Enter the remote gateway.
<b>Authentication Method</b>	Configure authentication settings. The options available are dependent on the type of VPN selected.

4. Select *OK* to save the settings.

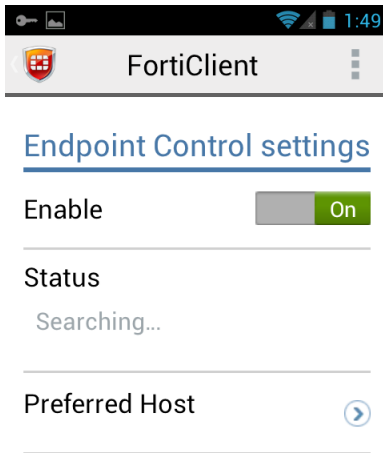
## Connect to the FortiGate

### To connect to the FortiGate:

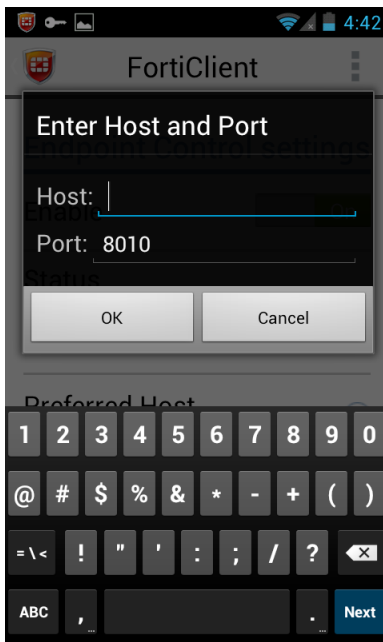
1. On your Android device, open the FortiClient application.
2. Select the menu icon in the toolbar and select *Endpoint Control*.



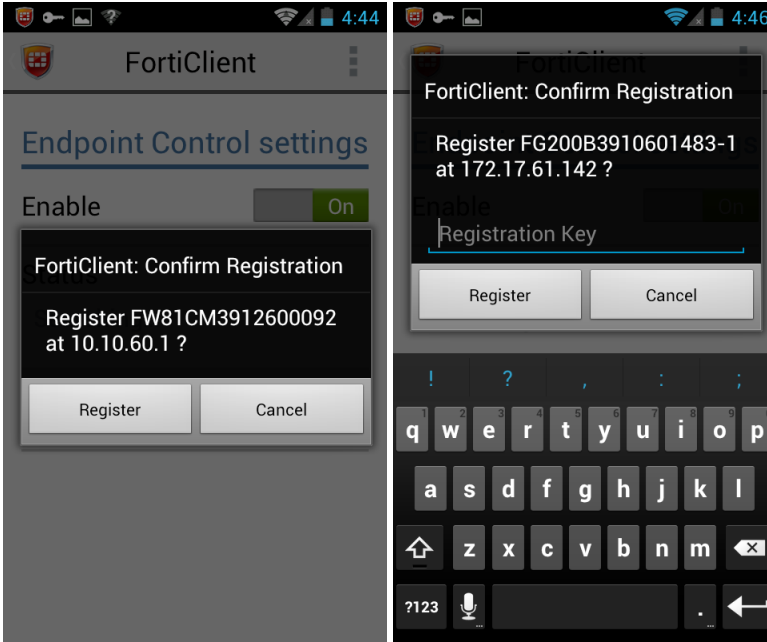
3. In *Endpoint Control settings* toggle the *Enable* switch to *On*.



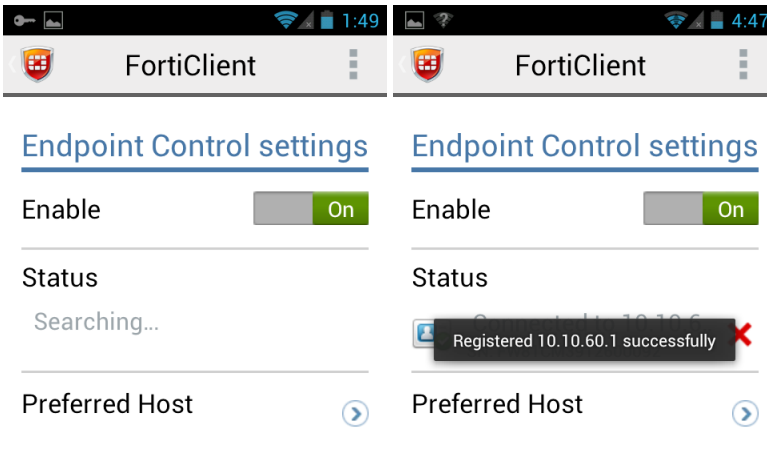
4. FortiClient will search for available FortiGate devices. Alternatively, you can select *Preferred Host* and enter the FortiGate host IP and port number.



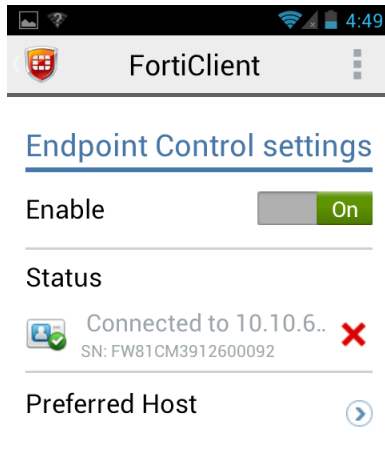
5. When a FortiGate is discovered, a confirmation dialog with the FortiGate serial number and IP address. Depending on the FortiGate configuration, you may be required to enter a FortiClient registration key.



- 6. Select the *Register* button to continue. You will receive a confirmation dialog box when connection is complete.



- 7. The *Endpoint Control settings* page will display a connected status.



8. Upon successful connection with FortiGate, FortiClient VPN (Android) will receive the FortiClient Profile.

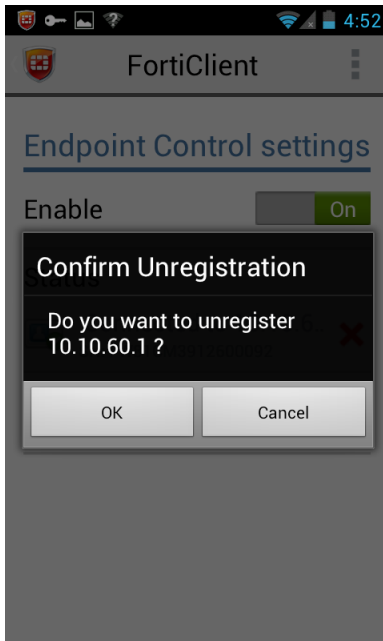


If FortiClient VPN (Android) is connected to FortiGate, it will auto start when the phone is turned on and bring up the GUI.

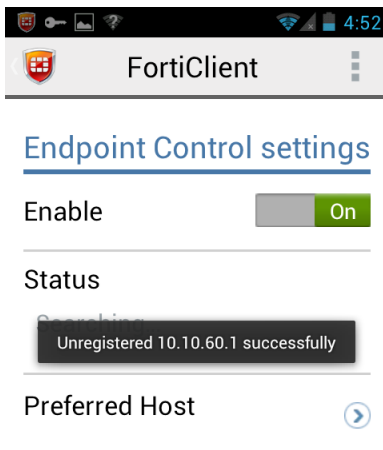
## Disconnect from FortiGate

### To disconnect from FortiGate:

1. To disconnect from FortiGate, in *Endpoint Control* settings page, in the *Status* section, select the close icon.
2. You will receive a confirmation dialog box.



3. Select *OK* to disconnect from the FortiGate. You receive a confirmation dialog box advising that you are disconnected from the FortiGate.



4. Toggle the *Endpoint Control Enable* switch to *Off*.



*High Performance Network Security*



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.