FortiClient (Android) - Administration Guide

Version 6.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

FORTINET®

January 12, 2021
FortiClient (Android) 6.4 Administration Guide
04-640-642471-20210112

TABLE OF CONTENTS

Introduction

FortiClient (Android) 6.4 includes support for IPsec VPN, SSL VPN, Web Security, Endpoint Control, and FortiClient Endpoint Management Server (EMS).

FortiClient (Android) must connect to EMS to activate its license and become provisioned by the endpoint profile that the administrator configured in EMS. You cannot use any FortiClient (Android) features until FortiClient (Android) is connected to EMS and licensed. See Launching FortiClient (Android) for the first time on page 7.

FortiClient (Android) supports integration with Microsoft Intune for enterprise mobility management. Integration with Microsoft Intune allows the administrator to configure FortiClient (Android) endpoints to connect to EMS. See Configuring Microsoft IntuneFortiClient (Android) integration on page 32.

You can also download a VPN-only FortiClient (Android) that is available on the Google Play store. The VPN-only client does not require a license or connection to EMS, but only provides the SSL and IPsec VPN features.

Features

The following table lists and describes features supported in FortiClient (Android) 6.4.

Feature	Description
IPsec VPN	• Configure IPsec VPN connections. • IKE main mode and aggressive mode support. • Client X.509 certificates and pre-shared key support. • Enable always up and auto connect options. • Disable auto start.
SSL VPN	• Configure tunnel mode SSL VPN connections. • Client and server X.509 certificates support. • Enable always up and auto connect options. • Disable auto start.
Web security	• Allow or deny web browsing based on FortiGuard groups and categories. • Monitor web browsing violations • Client Web Filtering when On-Net.
Endpoint control	• Connection to FortiClient EMS • Connection to FortiClient Cloud • Provision of web filtering profile • Provision of VPN connections • Deployment of CA certificate • Disable disconnection from FortiClient EMS • User profile picture (avatar)

Downloading FortiClient (Android) 6.4

You can download the FortiClient (Android) 6.4 application from the Google Play store or at https://play.google.com/store.

Product integration and support

The following table lists FortiClient (Android) 6.4 product integration and support information.

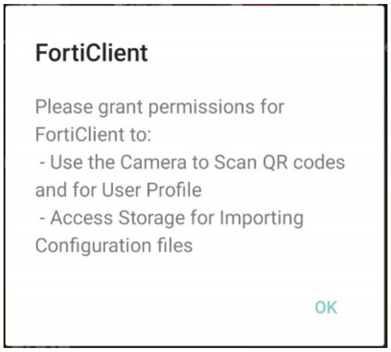
Android operating systems	- 10 (API 29) - 9 Pie (API 28) - 8.1.0 Oreo (API 27) - 8.0.0 Oreo (API 26) - 7.1 Nougat (API 25) - 7.0.0 Nougat (API 24) - 6.0.0 Marshmallow (API 23) - 5.1.1 Lollipop (API 22) - 5.0.1 Lollipop (API 21)
FortiOS	- 6.2.0 and later - 6.0.0 and later - 5.6.0 and later - 5.4.0 and later - 5.2.0 and later
FortiToken Mobile	- 4.0.0 and later See the FortiToken Mobile User Guide for Android.
FortiClient EMS	- 6.2.0 and later

Getting started

Launching FortiClient (Android) for the first time

To launch FortiClient (Android) for the first time:

1. When you launch FortiClient (Android) for the first time, FortiClient (Android) requests permissions to use the camera and access storage. Select *OK* and grant permissions as required.
   Depending on the EMS configuration, there may be additional permission requests.

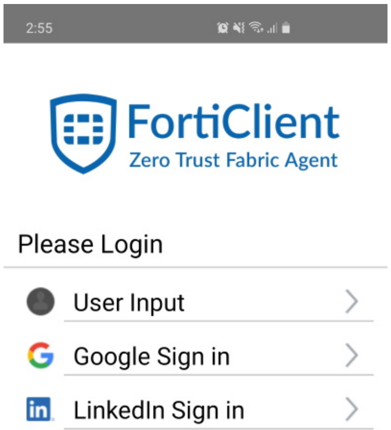


FortiClient

Please grant permissions for FortiClient to:
- Use the Camera to Scan QR codes and for User Profile
- Access Storage for Importing Configuration files

OK

2. Log in to FortiClient (Android). You can log in by manually entering your user profile (name, email address, phone number, and avatar) or by logging in to your Google or LinkedIn account.



2:55

FortiClient
Zero Trust Fabric Agent

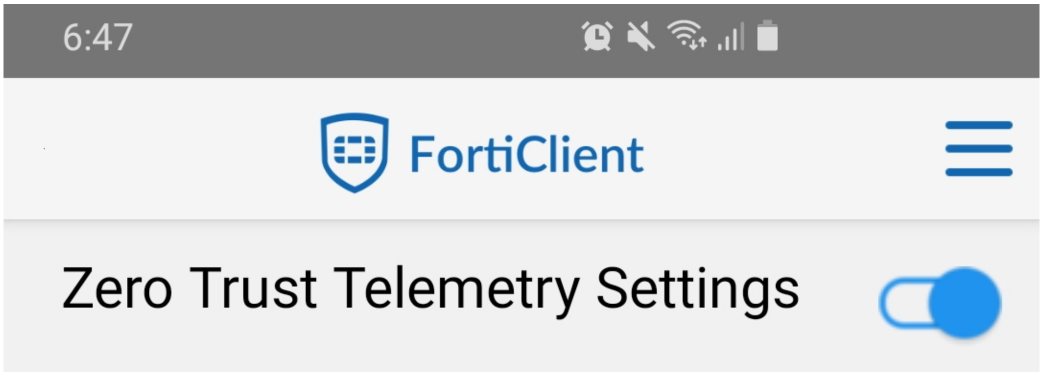
Please Login

User Input

Google Sign in

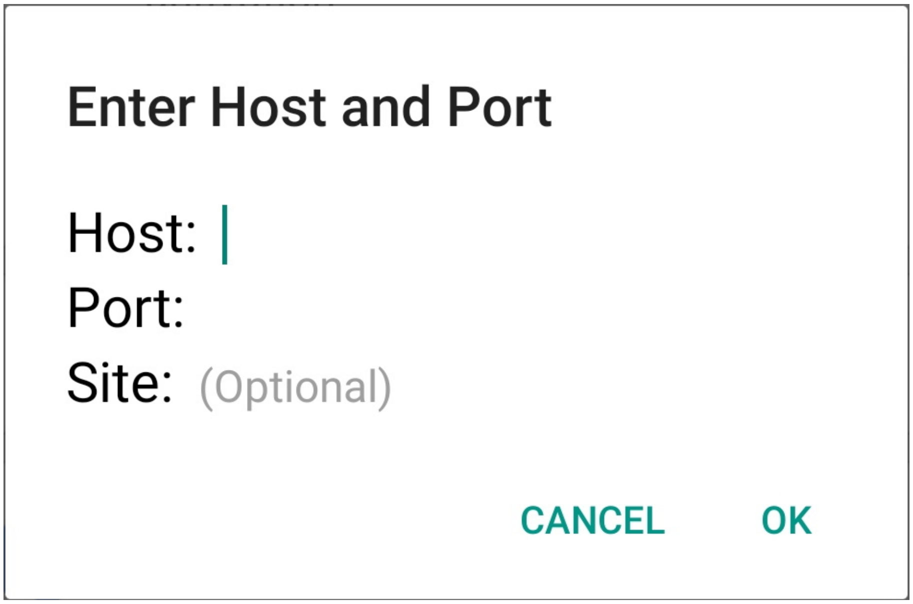
LinkedIn Sign in

3. Connect FortiClient (Android) to EMS to license FortiClient (Android) and enable features. Do one of the following:
   a. Enable *Zero Trust Telemetry Settings*. When FortiClient (Android) detects a Telemetry server, a confirmation popup appears to connect to EMS.



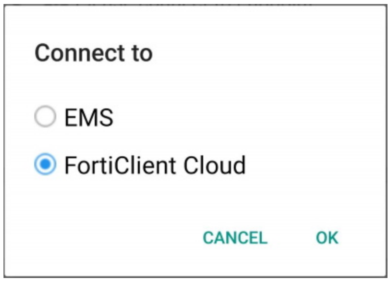
Zero Trust Telemetry Settings

b. To manually connect to an on-premise EMS instance, select *Specify EMS IP*. Enter the EMS IP address and port to manually connect to EMS. If the EMS administrator has enabled multitenancy, you can also enter the EMS site name.



c. To connect to an on-premise EMS instance or FortiClient Cloud using a QR code, select *Scan QR Code* from the right-side dropdown list. Scan the QR code with the device camera. You must allow FortiClient (Android) permissions to access the device camera. FortiClient (Android) automatically connects to the EMS server or FortiClient Cloud based on the scanned QR code.

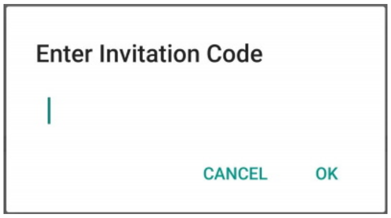
d. To manually connect to FortiClient Cloud, select *Connect to*, then select *FortiClient Cloud*. Select *OK*.



Connect to

○ EMS
● FortiClient Cloud

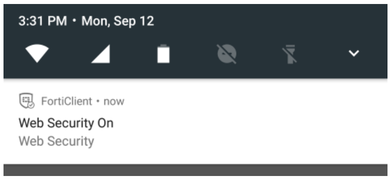
Select *Enter Invitation Code*. Enter the FortiClient Cloud invitation code, then select *OK*.



Enter Invitation Code

Launching FortiClient (Android) from the notification bar

FortiClient (Android) 6.4 allows you to launch the application from the notification bar.



3:31 PM • Mon, Sep 12

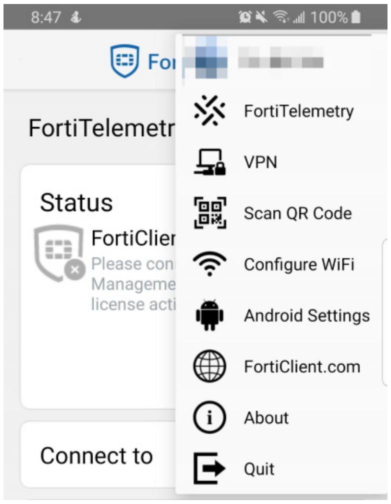
FortiClient • now

Web Security On

Web Security

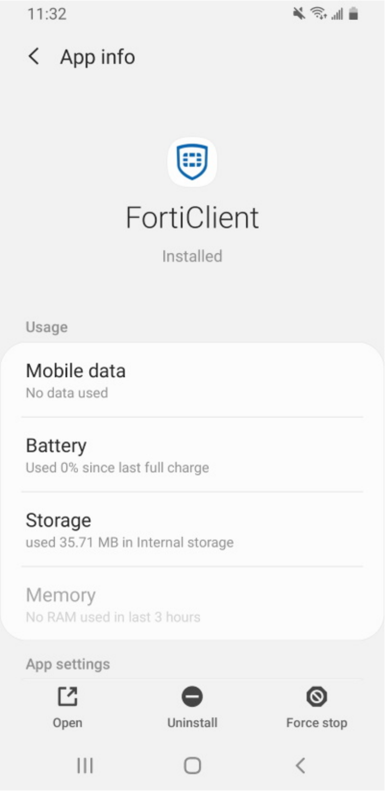
Quitting FortiClient (Android) from the app menu

You can quit FortiClient (Android) from the in-app menu.



Force stopping FortiClient (Android) from the Apps page

When the web security feature is enabled, FortiClient (Android) runs in the background to provide the web security service. To quit the application, go to the Android OS Settings page, then select *Apps* > *FortiClient* > *Force stop*. On this page you can also clear data and uninstall FortiClient (Android).



11:32

App info

FortiClient

Installed

Usage

Mobile data
No data used

Battery
Used 0% since last full charge

Storage
used 35.71 MB in Internal storage

Memory
No RAM used in last 3 hours

App settings

Web security

FortiClient (Android) 6.4 includes a web security feature to allow you to control web browsing on your Android device. You can allow or deny sites based on the FortiGuard site rating. The following table lists the web security groups and categories.

You can get up-to-date groups and categories from FortiGuard (http://www.fortiguard.com/static/webfiltering.html).

Groups	Categories
Security Risk	Malicious Websites, Phishing, Spam URLs
Potentially Liable	Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist Groups, Proxy Avoidance, Plagiarism, Child Abuse
Adult/Mature Content	Alternative Beliefs, Abortion, Other Adult Materials, Advocacy Organizations, Gambling, Nudity and Risque, Pornography, Dating, Weapons (Sales), Marijuana, Sex Education, Alcohol, Tobacco, Lingerie and Swimsuit, Sports Hunting and War Games
Bandwidth Consuming	Freeware and Software Downloads, File Sharing and Storage, Streaming Media and Download, Peer-to-peer File Sharing, Internet Radio and TV, Internet Telephony
General Interest - Business	Finance and Banking, Search Engines and Portals, General Organizations, Business, Information and Computer Security, Government and Legal Organizations, Information Technology, Armed Forces, Web Hosting, Secure Websites, Web-based Applications
General Interest - Personal	Advertising, Brokerage and Trading, Games, Web-based Email, Entertainment, Arts and Culture, Education, Health and Wellness, Job Search, Medicine, News and Media, Social Networking, Political Organizations, Reference, Global Religion, Shopping and Auction, Society and Lifestyles, Sports, Travel, Personal Vehicles, Dynamic Content, Meaningless Content, Folklore, Web Chat, Instant Messaging, Newsgroups and Message Boards, Digital Postcards, Child Education, Real Estate, Restaurant and Dining, Personal Websites and Blogs, Content Servers, Domain Parking, Personal Privacy
Unrated	Unrated

The web security module is only available in the full FortiClient (Android) app.

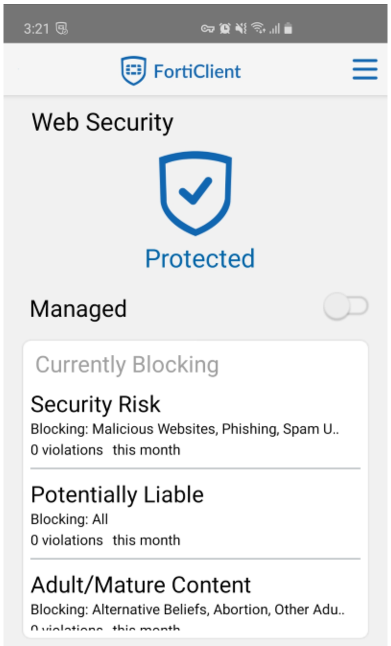
Provisioning of a web filter exclusion list is only available from FortiClient EMS. Exclusion lists can only be applied on the domain name, not the full URL.

For information on FortiGuard groups and categories, see http://www.fortiguard.com/static/webfiltering.html.

Web security status

The EMS administrator can enable or disable Web Filter. When the EMS administrator enables Web Filter, Web Filter options become available from the dropdown list. You can open the Web Filter page to check the categories that the administrator has enabled or blocked.

There are seven top-level categories with subcategories. The EMS administrator can enable, disable, or partially enable subcategories. The EMS administrator can also configure an exception list.



3:21

FortiClient

Web Security

Protected

Managed

Currently Blocking

Security Risk
Blocking: Malicious Websites, Phishing, Spam U..
0 violations this month

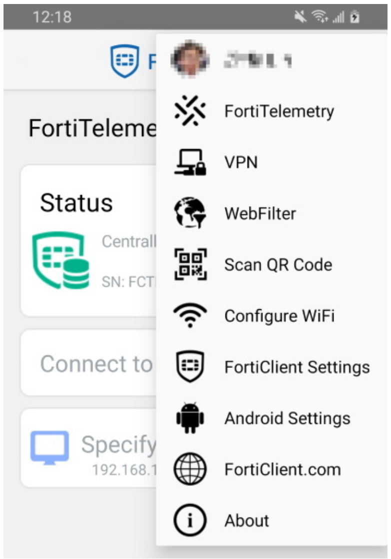
Potentially Liable
Blocking: All
0 violations this month

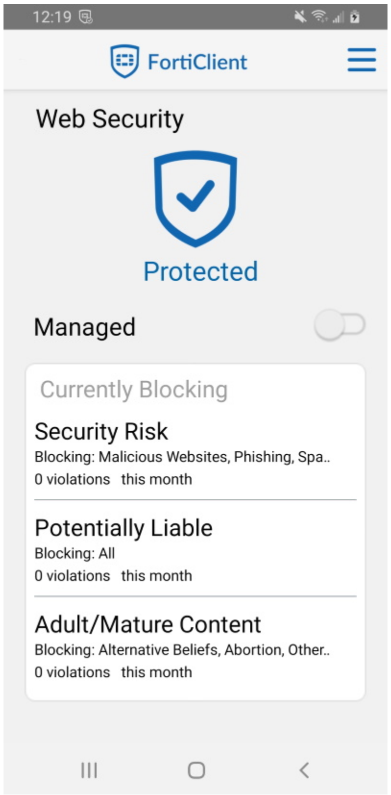
Adult/Mature Content
Blocking: Alternative Beliefs, Abortion, Other Adu..
0 violations this month

Web security settings

To change web security settings, select Web Security Settings. There are seven top level groups with various categories. When you select a top level group, a dropdown list appears. You can select to *Allow All*, *Deny All*, or allow or deny each category independently.

When FortiGate endpoint control is managing FortiClient, the web security setting is deployed from FortiGate and the user cannot change it.





Web Security

Protected

Managed

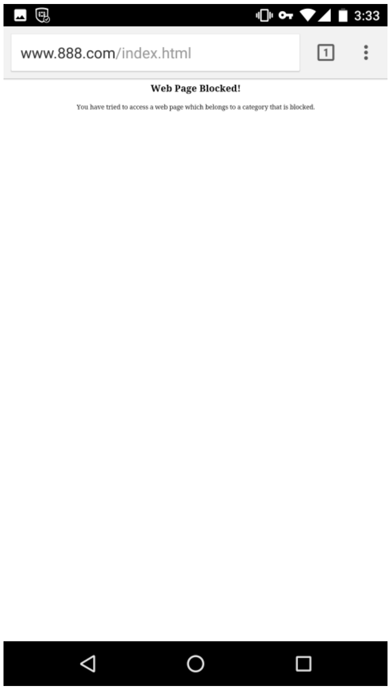
Currently Blocking

Security Risk
Blocking: Malicious Websites, Phishing, Spa..
0 violations this month

Potentially Liable
Blocking: All
0 violations this month

Adult/Mature Content
Blocking: Alternative Beliefs, Abortion, Other..
0 violations this month

When browsing to a website which falls into a denied category, you receive a web page blocked page.



www.888.com/index.html

Web Page Blocked!

You have tried to access a web page which belongs to a category that is blocked.

SSL VPN

FortiClient (Android) 6.4 supports tunnel mode SSL VPN connections. You can configure the SSL VPN in the FortiClient user interface or provision SSL VPN connections in an endpoint profile from FortiClient EMS. FortiClient EMS pushes provisioned SSL VPN configurations to your Android device after the FortiClient (Android) successfully connects with FortiGate for Endpoint Control and with FortiClient EMS for provisioning and monitoring.

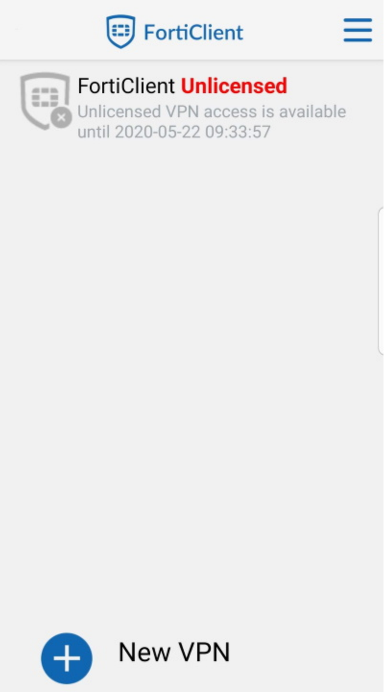
You can configure X.509 certificates, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

For three days after initial FortiClient (Android) installation, you can configure and establish a VPN connection to a FortiGate, allowing the endpoint to reach an EMS behind a FortiGate. This is especially useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient (Android) license.

Creating an SSL VPN connection

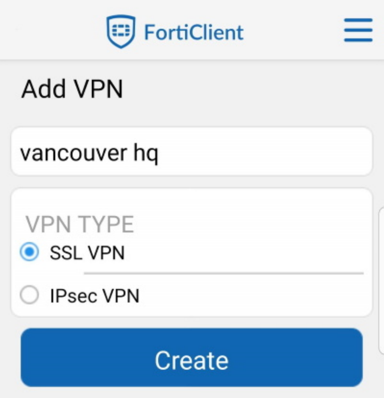
To create a new SSL VPN connection:

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



FortiClient
FortiClient Unlicensed
Unlicensed VPN access is available until 2020-05-22 09:33:57
New VPN

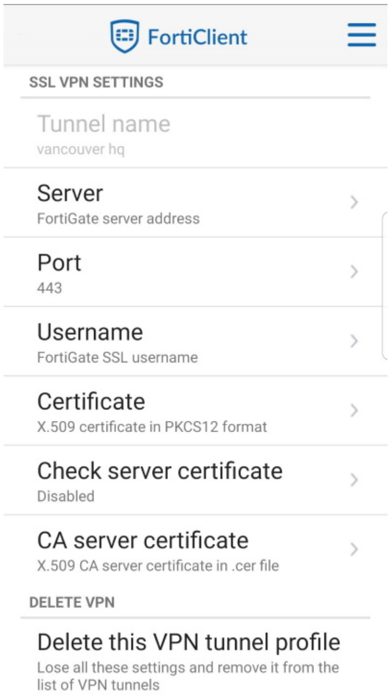
2. Enter a name for the new VPN connection, select *SSL VPN* under *VPN Type*, and select *Create*.



vancouver hq

VPN TYPE
● SSL VPN
○ IPsec VPN

The SSL VPN settings page displays.



SSL VPN SETTINGS

Tunnel name
vancouver hq

Server
FortiGate server address

Port
443

Username
FortiGate SSL username

Certificate
X.509 certificate in PKCS12 format

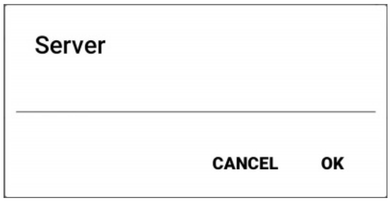
Check server certificate
Disabled

CA server certificate
X.509 CA server certificate in .cer file

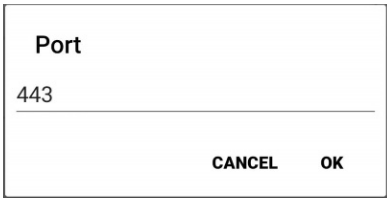
DELETE VPN

Delete this VPN tunnel profile
Lose all these settings and remove it from the list of VPN tunnels

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

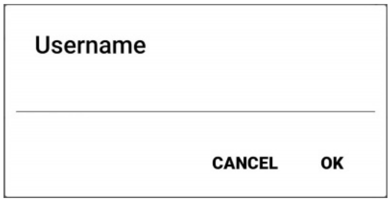


4. Select *Port*, enter the port number, and select *OK*. The default port is 443.



Port
443

5. Select *Username*, enter a username, and select *OK*.



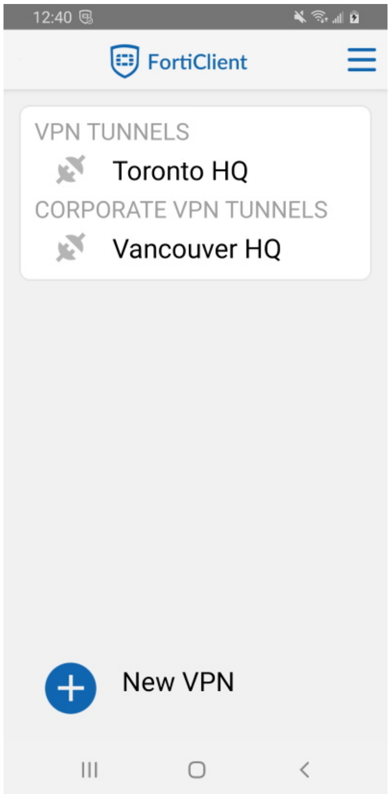
Username

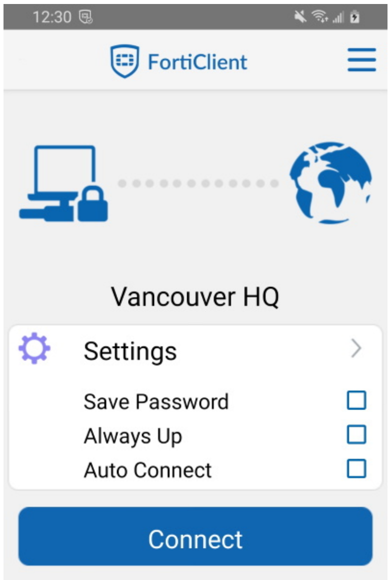
Connecting to the VPN

SSL VPN tunnel mode uses X.509 certificates (PKCS12 format) for authentication. You must configure certificate settings if authentication requires the client certificate. Otherwise, leave the certificate settings at their default values.

To connect to the SSL VPN:

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





12:30

FortiClient

Vancouver HQ

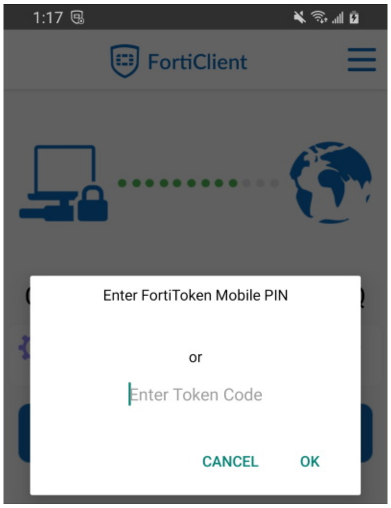
Settings

Save Password □

Always Up □

Auto Connect □

2. Enter your username and password then select *Login*.
   If the SSL VPN you are connecting to requires you to enter a FortiToken Mobile token, you are prompted to enter your FortiToken Mobile PIN or six-digit token.



1:17

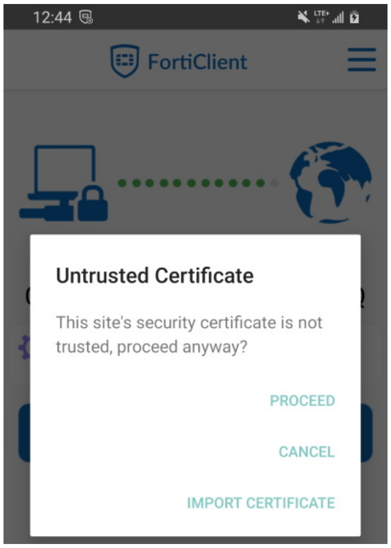
FortiClient

Enter FortiToken Mobile PIN

or

Enter Token Code

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



Untrusted Certificate

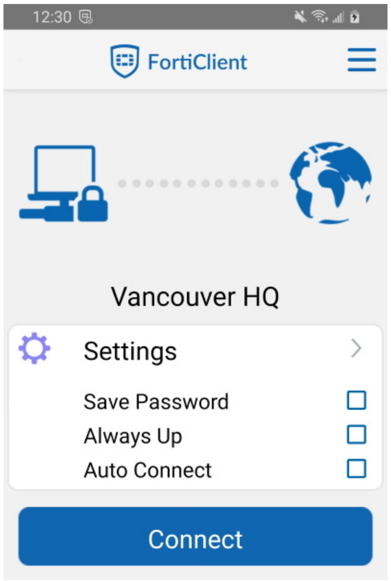
This site's security certificate is not trusted, proceed anyway?

4. Select *Import certificate*, browse for the certificate file, and 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's back button to return to the connection screen.
6. Select an available VPN to connect to.

For some devices, it may be necessary to change the TCP-MSS configuration to allow Telemetry connection after establishing an SSL VPN connection.

Editing SSL VPN settings or deleting a SSL VPN configuration

Select the SSL VPN, then *Settings*.



12:30

FortiClient

Vancouver HQ

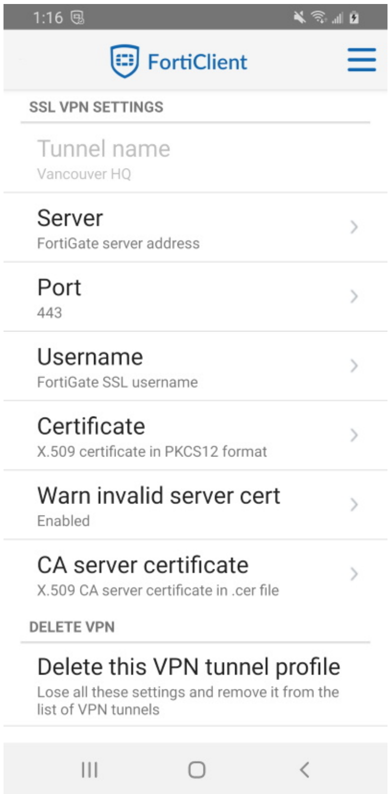
Settings

Save Password □

Always Up □

Auto Connect □

Connect



1:16

FortiClient

SSL VPN SETTINGS

Tunnel name
Vancouver HQ

Server
FortiGate server address

Port
443

Username
FortiGate SSL username

Certificate
X.509 certificate in PKCS12 format

Warn invalid server cert
Enabled

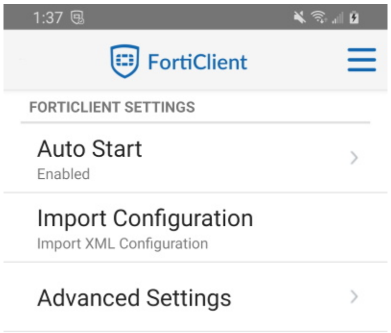
CA server certificate
X.509 CA server certificate in .cer file

DELETE VPN

Delete this VPN tunnel profile
Lose all these settings and remove it from the list of VPN tunnels

Enabling/disabling auto start

You can enable or disable auto start. To enable or disable auto start, select the menu icon, then *Settings* in the dropdown list. In the *FortiClient settings* page, select *Auto Start*, then *Enabled* or *Disabled*. By default, auto start is enabled.



1:37

FortiClient

FORTICLIENT SETTINGS

Auto Start
Enabled

Import Configuration
Import XML Configuration

Advanced Settings

IPsec VPN

FortiClient (Android) 6.4 supports IPsec VPN connections. You can configure the IPsec VPN in the FortiClient user interface or provision IPsec VPN connections in an endpoint profile from FortiClient EMS. FortiClient EMS pushes provisioned IPsec VPN configurations to your Android device after the FortiClient (Android) successfully connects with FortiGate for endpoint control and with FortiClient EMS for provisioning and monitoring.

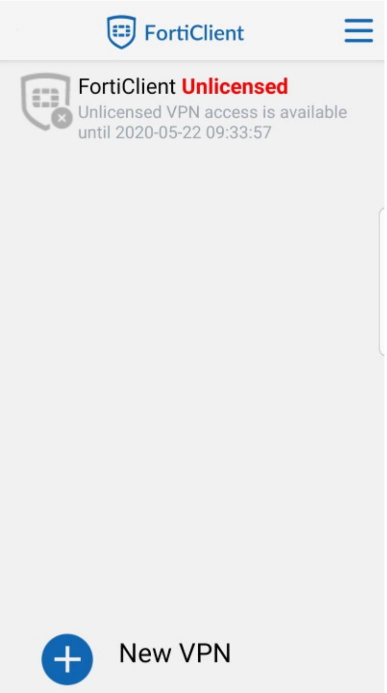
You can configure server, phase 1, phase 2, and XAuth settings.

For three days after initial FortiClient (Android) installation, you can configure and establish a VPN connection to a FortiGate, allowing the endpoint to reach an EMS behind a FortiGate. This is especially useful for remote users, as it allows them to connect to the corporate network to activate their FortiClient (Android) license.

Creating an IPsec VPN connection

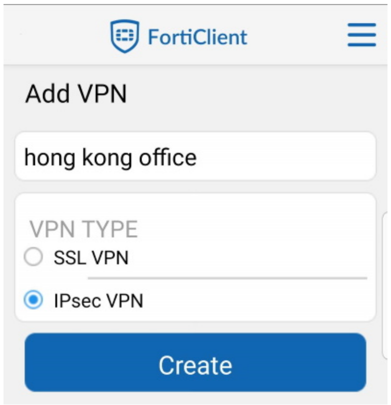
To create a new IPsec VPN connection:

1. Create the new IPsec VPN connection:
   a. Select *New VPN* from the toolbar at the bottom of the page.



FortiClient Unlicensed
Unlicensed VPN access is available until 2020-05-22 09:33:57

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



FortiClient

Add VPN

hong kong office

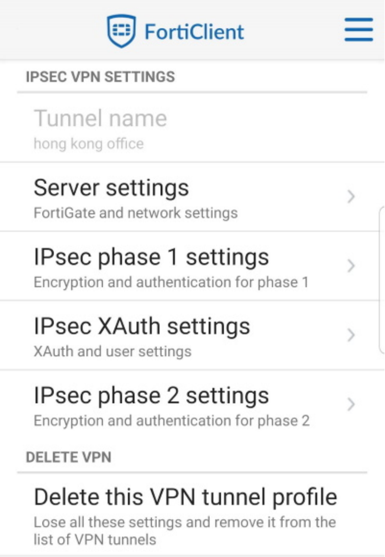
VPN TYPE

○ SSL VPN

● IPsec VPN

Create

The *IPsec VPN settings* page displays.



FortiClient

IPSEC VPN SETTINGS

Tunnel name
hong kong office

Server settings
FortiGate and network settings

IPsec phase 1 settings
Encryption and authentication for phase 1

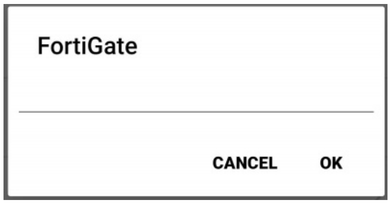
IPsec XAuth settings
XAuth and user settings

IPsec phase 2 settings
Encryption and authentication for phase 2

DELETE VPN

Delete this VPN tunnel profile
Lose all these settings and remove it from the list of VPN tunnels

2. Select *Server settings* > *Network settings* > *FortiGate*. Enter the server IP address or domain name, then select *OK*.

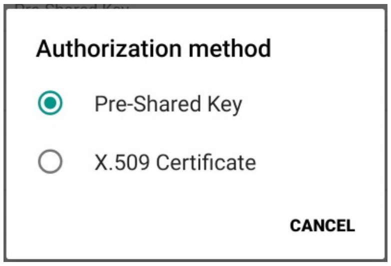


FortiGate

CANCEL OK

3. Configure authentication settings:

a. Under *Authentication settings*, select *Authorization method*, and select *Pre-Shared Key* or *X.509 Certificate*.

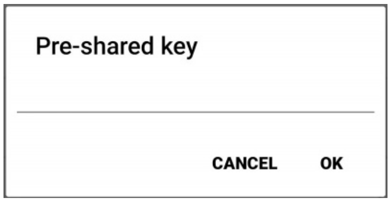


Authorization method

● Pre-Shared Key

○ X.509 Certificate

b. If desired, select *Pre-shared Key* to enter the pre-shared key value.



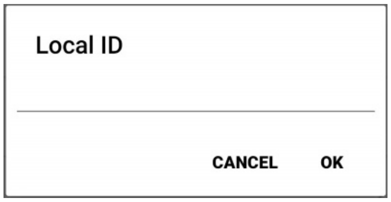
Pre-shared key

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 six 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 key configured on the FortiGate. Contact your network administrator for the key.

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



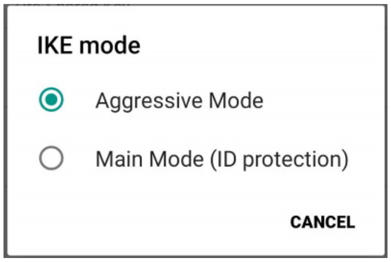
Local ID

d. For X.509 certificate select *Certificate*, 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.

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



IKE mode

● Aggressive Mode

○ Main Mode (ID protection)

In *Aggressive Mode*, the phase 1 parameters are exchanged in a single message with unencrypted authentication information.

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.

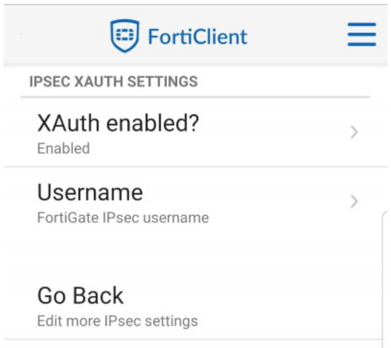
4. Select *Go Back* to return to the *IPsec VPN settings* page.
5. Select *IPsec phase 1 settings* to view or edit the phase 1 proposal encryption and authentication settings. You can choose to use the default settings.
   Select the encryption and authentication algorithms that will be used to generate 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.

6. Select *Go Back* to return to the *IPsec VPN settings* page.
7. 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.

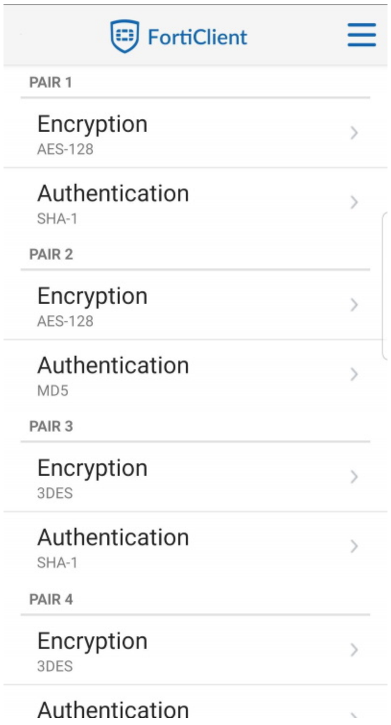


8. Select *Go Back* to return to the *IPsec VPN settings* page.

9. 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 groups 1, 2, 5, and 14. When using aggressive mode, DH groups cannot be negotiated.



PAIR 1

Encryption AES-128

Authentication SHA-1

PAIR 2

Encryption AES-128

Authentication MD5

PAIR 3

Encryption 3DES

Authentication SHA-1

PAIR 4

Encryption 3DES

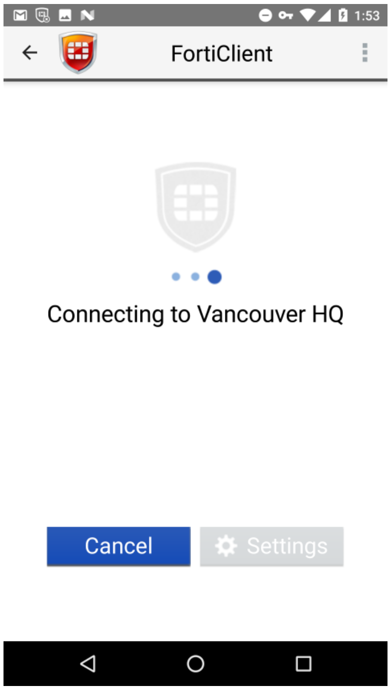
Authentication

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

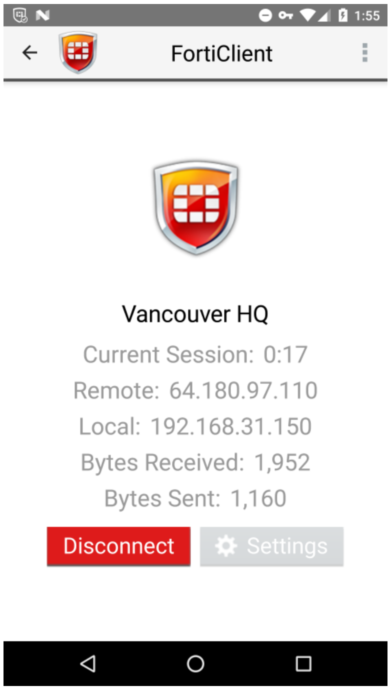
Connecting to an IPsec VPN

To connect to an IPsec VPN:

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



Connecting to Vancouver HQ



Vancouver HQ

Current Session: 0:17

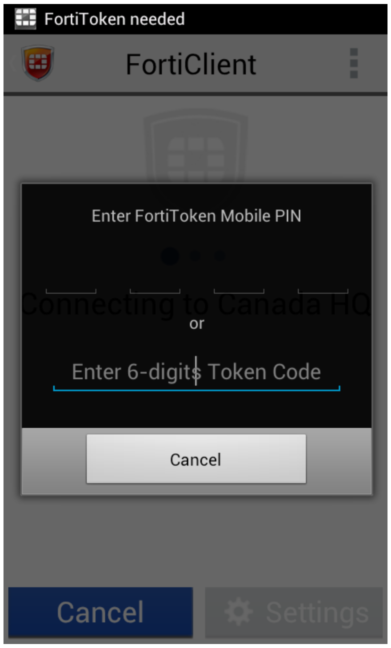
Remote: 64.180.97.110

Local: 192.168.31.150

Bytes Received: 1,952

Bytes Sent: 1,160

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



Enter FortiToken Mobile PIN

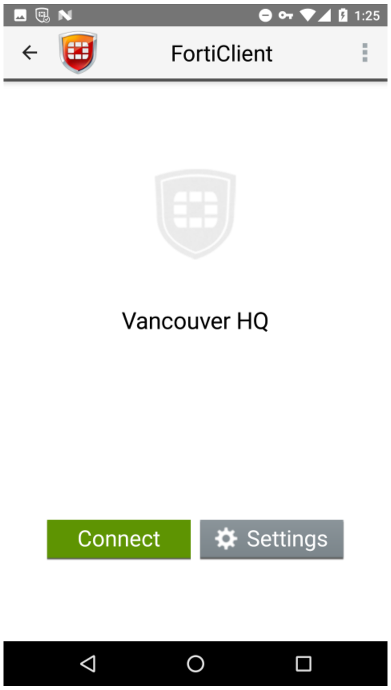
Connecting to Canada HQ

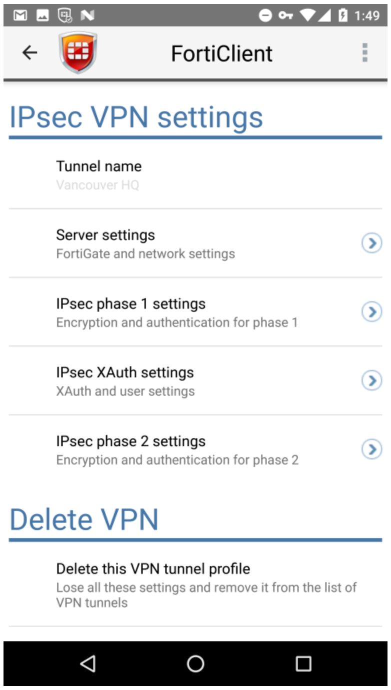
or

Enter 6-digits Token Code

Editing VPN settings or deleting a VPN configuration

Select the IPsec VPN, then the *Settings* button.





IPsec VPN settings

Tunnel name
Vancouver HQ

Server settings
FortiGate and network settings

IPsec phase 1 settings
Encryption and authentication for phase 1

IPsec XAuth settings
XAuth and user settings

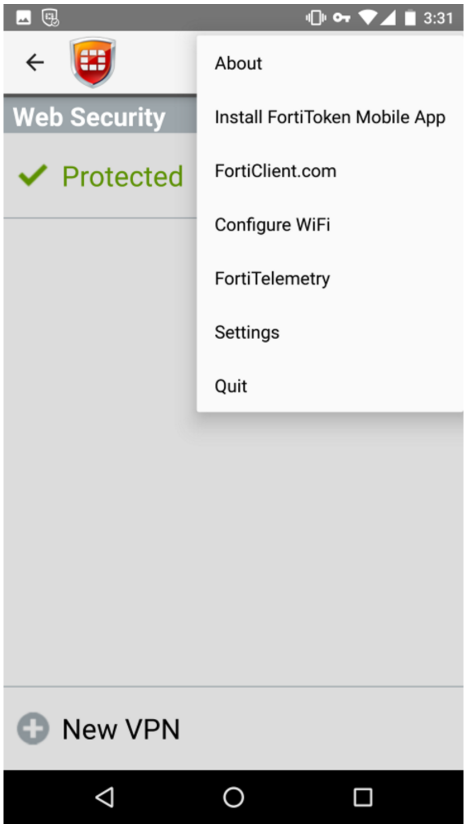
IPsec phase 2 settings
Encryption and authentication for phase 2

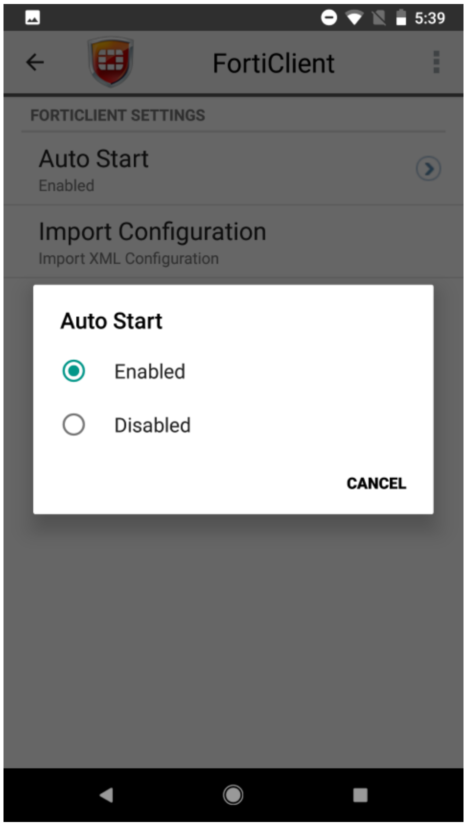
Delete VPN

Delete this VPN tunnel profile
Lose all these settings and remove it from the list of VPN tunnels

Enabling/disabling auto start

You can enable or disable auto start. To enable or disable auto start, select the menu icon, then *Settings* in the dropdown list. In the *FortiClient settings* page, select *Auto Start*, then *Enabled* or *Disabled*. By default, auto start is enabled.





Auto Start
Enabled

Import Configuration
Import XML Configuration

Auto Start

● Enabled

○ Disabled

CANCEL

Endpoint control

FortiClient (Android) 6.4 must register to EMS for all features to function. By default, FortiClient (Android) allows three days of free VPN access to allow you to register to EMS over VPN. The EMS administrator can push VPN configurations and enable or disable Web Filter.

FortiClient EMS

You use can use FortiClient EMS to create an endpoint profile and a gateway IP list.

Configuring FortiClient EMS endpoint profiles

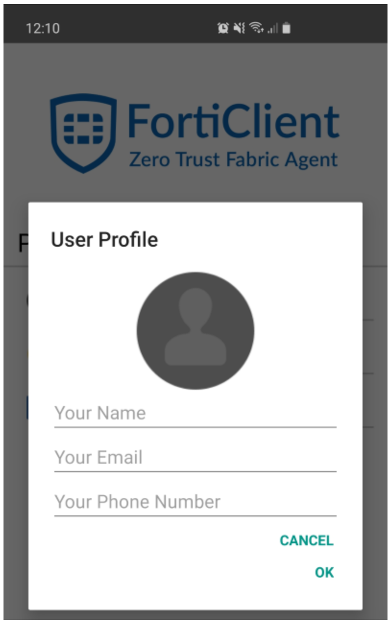
You can create a new endpoint profile or modify the default endpoint profile. The endpoint profile contains configuration information for FortiClient (Android), including VPN settings.

To configure FortiClient EMS endpoint profiles:

1. In FortiClient EMS, go to *Endpoint Profiles* > *Manage Profiles* > *Add*.
2. Configure the settings on the *Web Filter* tab.
3. Configure the settings on the *VPN* tab.
4. On the *System Settings* tab, select *Install CA Certificate on Client*.
5. Click *Save*.

Configuring the user profile

You can manually add a profile picture, name, email, and phone number to your user profile. You can enter this information when first downloading FortiClient (Android) or by going to *User Profile* in the toolbar.



User Profile

Your Name

Your Email

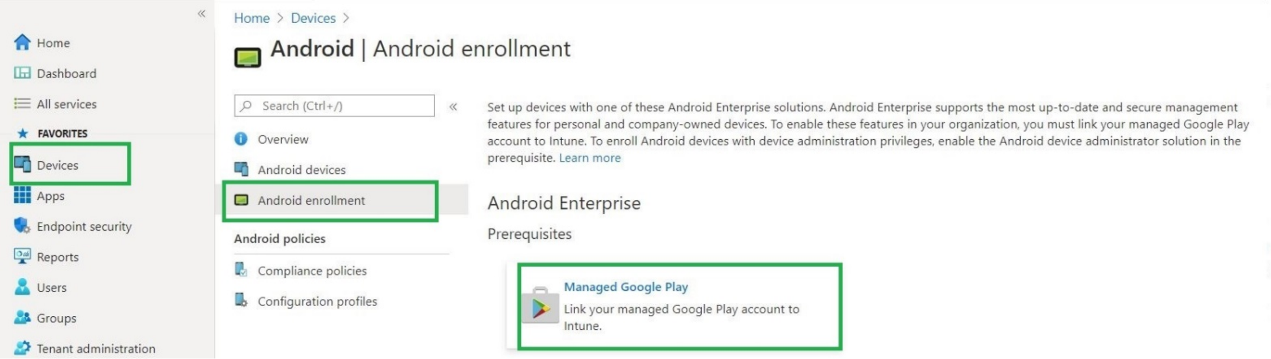
Your Phone Number

Configuring Microsoft IntuneFortiClient (Android) integration

Intune integration allows endpoints to connect to EMS.

To configure Microsoft Intune integration as the administrator:

1. Sign in to the Microsoft Endpoint Manager admin center. Go to *Devices* > *Android* > *Android enrollment* > *Managed Google Play*. Link your Managed Google Play account to your Intune tenant account.

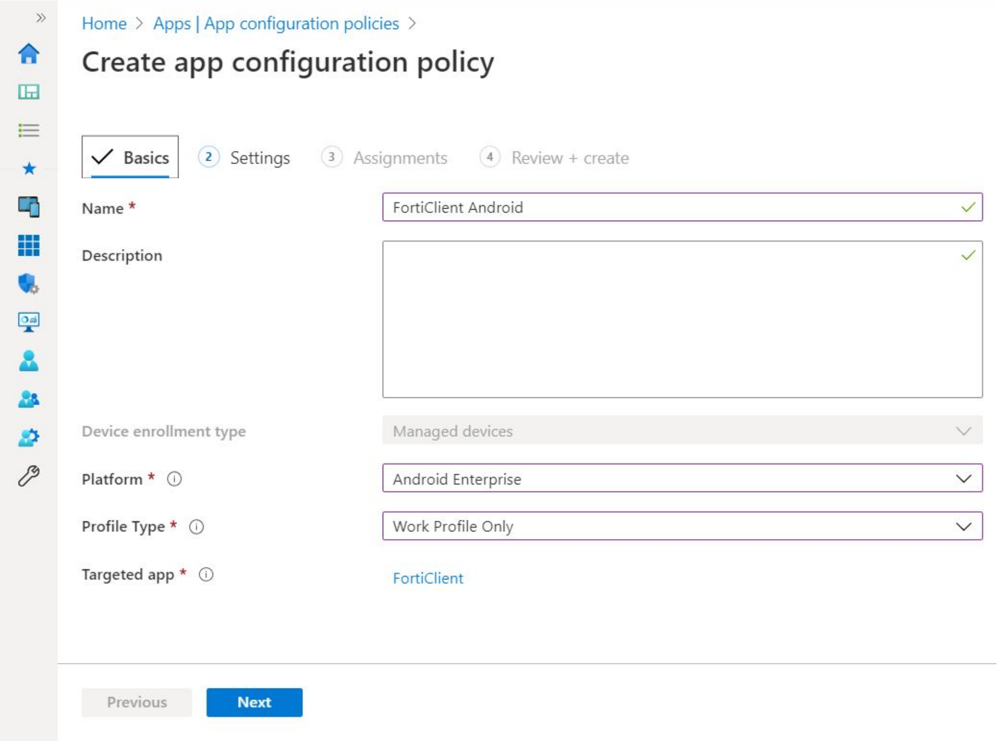


Set up devices with one of these Android Enterprise solutions. Android Enterprise supports the most up-to-date and secure management features for personal and company-owned devices. To enable these features in your organization, you must link your managed Google Play account to Intune. To enroll Android devices with device administration privileges, enable the Android device administrator solution in the prerequisite. Learn more

Managed Google Play

Link your managed Google Play account to Intune.

2. Go to *Apps* > *All apps* > *Add* > *Android enrollment* > *Managed Google Play*. Add and approve FortiClient (Android) from the app store to make it available to the end user.
3. Go to *App configuration policies* > *Managed devices*. Create a custom profile for the managed device:
   a. On the *Basics* page, configure the fields:
      i. From the *Platform* dropdown list, select *Android Enterprise*.
      ii. From the *Profile Type* dropdown list, select *Work Profile Only*.
      iii. For *Targeted app*, select *FortiClient*.



Home > Apps | App configuration policies >

Create app configuration policy

Name * FortiClient Android

Description

Device enrollment type: Managed devices

Platform *: Android Enterprise

Profile Type *: Work Profile Only

Targeted app *: FortiClient

b. Click *Next*.
c. From the *Configuration settings format* dropdown list, select *Use configuration designer*.
d. Under *Use the JSON editor to configure the detailed configuration keys*, click *Add*.
e. Select the desired configuration keys:
   i. If FortiClient (Android) will connect to an on-premise EMS, select *Enter EMS Server IP* and Enter *EMS Server Port*. In the configuration value fields, enter the EMS server port and IP address, respectively.
   ii. If FortiClient (Android) will connect to FortiClient Cloud, select *Enter Cloud Invite Code*. In the *Configuration value* field, enter the FortiClient Cloud invite code.
f. Click *Next*.
g. From the *Assign to* dropdown list, select the desired devices/users to assign the policy to. Click *Next*. You can view the policy under *Apps* > *App configuration policies*.

To configure Microsoft Intune integration as the end user:

1. Install Intune Company Portal from the Google Play store.
2. Log in to the Intune Company Portal app using credentials that your company or administrator provided.
3. After logging in, the app prompts you to set up a work profile. Click *Agree* and allow the necessary permissions to set up the profile.
4. Install FortiClient (Android) and other applications that the administrator has provisioned under the work profile. After FortiClient (Android) installs, it automatically registers to EMS according to the administrator spefications.

⚠ FortiClient (Android) does not currently support having the app installed simultaneously for both work and personal profiles.

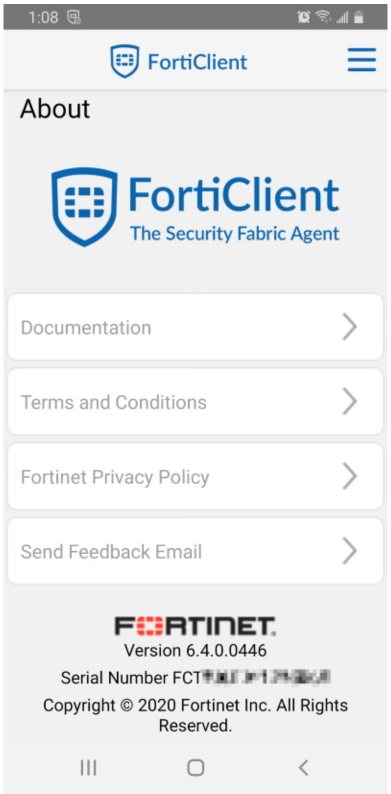
When provisioned through Intune, FortiClient (Android) does not support user login through Google accounts.

About

You can go to the *About* page using the right-side dropdown menu in the FortiClient (Android). The *About* page in FortiClient (Android) provides the following information:

- FortiClient (Android) version
- Copyright
- Privacy statement
- Documentation

You can use the *Send Feedback Email* option to provide feedback to Fortinet regarding FortiClient (Android).



Version 6.4.0.0446

Serial Number FCT[redacted]

Copyright © 2020 Fortinet Inc. All Rights Reserved.

Change log

Date	Change Description
2020-06-15	Initial release.
2020-10-07	Updated To launch FortiClient (Android) for the first time: on page 7.
2021-01-12	Updated To launch FortiClient (Android) for the first time: on page 7.