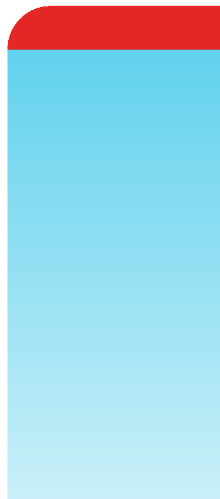


# Administration Guide

## FortiClient (Android) 7.0



**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 TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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



August 11, 2023

FortiClient (Android) 7.0 Administration Guide

04-700-757982-20230811

# TABLE OF CONTENTS

<b>Introduction</b>	<b>4</b>
Features	4
Downloading FortiClient (Android) 7.0	5
<b>Product integration and support</b>	<b>6</b>
<b>Getting started</b>	<b>7</b>
Launching FortiClient (Android) for the first time	7
Launching FortiClient (Android) from the notification bar	9
Quitting FortiClient (Android) from the app menu	9
Force stopping FortiClient (Android) from the Apps page	9
<b>Web security</b>	<b>11</b>
Web security status	12
Web security settings	12
<b>SSL VPN</b>	<b>15</b>
Creating an SSL VPN connection	15
Connecting to the VPN	20
Editing SSL VPN settings or deleting a SSL VPN configuration	22
Enabling/disabling auto start	23
<b>IPsec VPN</b>	<b>24</b>
Creating an IPsec VPN connection	24
Connecting to an IPsec VPN	28
Editing VPN settings or deleting a VPN configuration	29
Enabling/disabling auto start	30
<b>Standalone VPN client</b>	<b>32</b>
<b>Endpoint control</b>	<b>33</b>
FortiClient EMS	33
Configuring FortiClient EMS endpoint profiles	33
EMS connection mechanism under limited network access by device lock	33
Configuring the user profile	35
<b>Enterprise mobility management</b>	<b>36</b>
Configuring AirWatch integration	36
Configuring Microsoft Intune integration	40
<b>About</b>	<b>43</b>
<b>Change log</b>	<b>44</b>

# Introduction

FortiClient (Android) 7.0 includes support for IPsec and 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 Intune integration on page 40](#).

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) 7.0.

Feature	Description
<a href="#">IPsec VPN</a>	<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>
<a href="#">SSL VPN</a>	<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>
<a href="#">Web security</a>	<ul style="list-style-type: none"><li>• Allow or deny web browsing based on FortiGuard groups and categories.</li><li>• Monitor web browsing violations</li><li>• Client Web Filtering when On-Net.</li></ul>
<a href="#">Endpoint control</a>	<ul style="list-style-type: none"><li>• Connection to FortiClient EMS</li><li>• Connection to FortiClient Cloud</li><li>• Provision of web filtering profile</li><li>• Provision of VPN connections</li><li>• Deployment of CA certificate</li><li>• Disable disconnection from FortiClient EMS</li><li>• User profile picture (avatar)</li></ul>

## Downloading FortiClient (Android) 7.0

You can download the FortiClient (Android) 7.0 application from the [Google Play store](#).

# Product integration and support

The following table lists FortiClient (Android) 7.0 product integration and support information.

Android operating systems	<ul style="list-style-type: none"><li>• 12 (API 31)</li><li>• 11 (API 30)</li><li>• 10 (API 29)</li><li>• 9 Pie (API 28)</li><li>• 8.1.0 Oreo (API 27)</li><li>• 8.0.0 Oreo (API 26)</li><li>• 7.1 Nougat (API 25)</li><li>• 7.0.0 Nougat (API 24)</li><li>• 6.0.0 Marshmallow (API 23)</li><li>• 5.1.1 Lollipop (API 22)</li><li>• 5.0.1 Lollipop (API 21)</li></ul>
FortiOS	<ul style="list-style-type: none"><li>• 6.2.0 and later</li><li>• 6.0.0 and later</li><li>• 5.6.0 and later</li><li>• 5.4.0 and later</li><li>• 5.2.0 and later</li></ul>
FortiToken Mobile	<ul style="list-style-type: none"><li>• 4.0.0 and later</li></ul> <p>See the <a href="#">FortiToken Mobile User Guide</a>.</p>
FortiClient EMS	<ul style="list-style-type: none"><li>• 6.2.0 and later</li></ul>

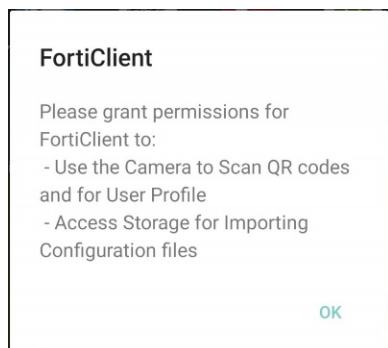
# Getting started

## 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.

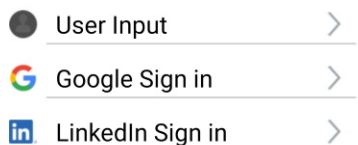
Depending on the EMS configuration, there may be additional permission requests.



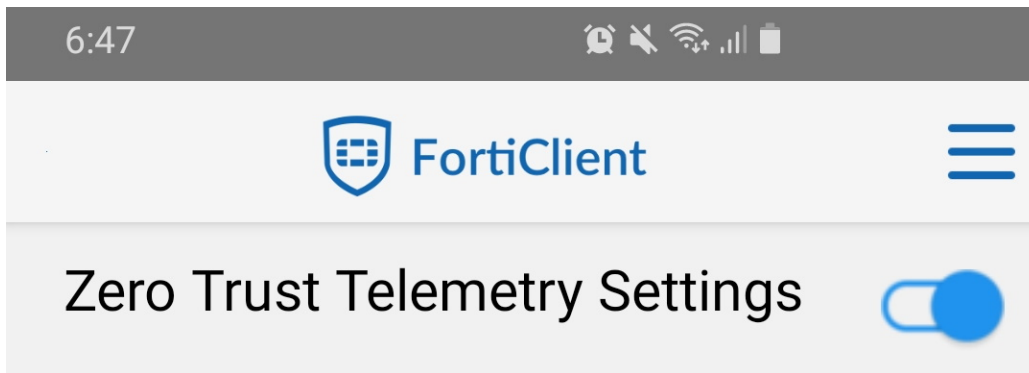
2. Log in to FortiClient (Android). You can log in by manually entering your user profile (name, email address, phone number, and avatar) or by logging in to your Google or LinkedIn account.



#### Please Login



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.



- 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.

## Enter Host and Port

Host: |

Port:

Site: (Optional)

CANCEL OK

- 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

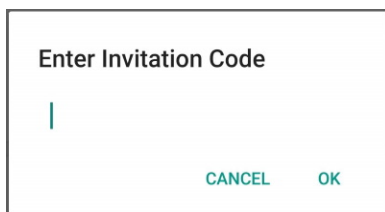
☐ EMS

☒ FortiClient Cloud

CANCEL OK

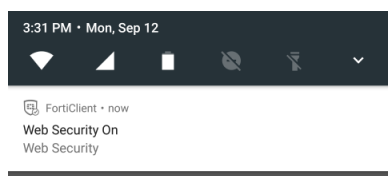
Select *Enter Invitation Code*. Enter the FortiClient Cloud invitation code, then select *OK*.





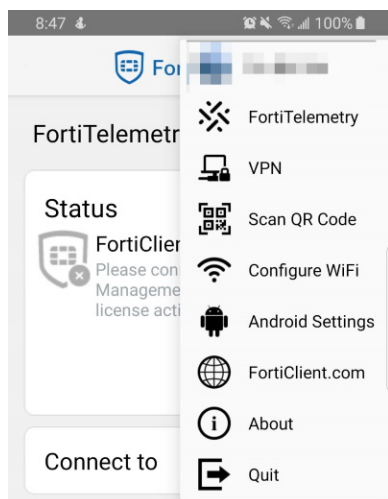
## Launching FortiClient (Android) from the notification bar

FortiClient (Android) 7.0 allows you to launch the application from the notification bar.



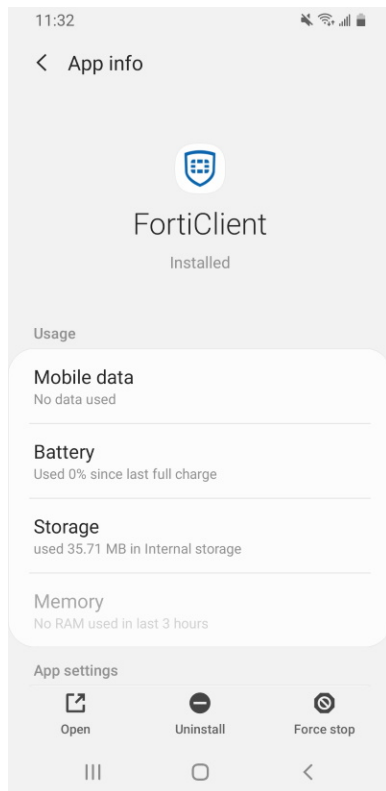
## Quitting FortiClient (Android) from the app menu

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).



# Web security

FortiClient (Android) 7.0 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](#).

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.

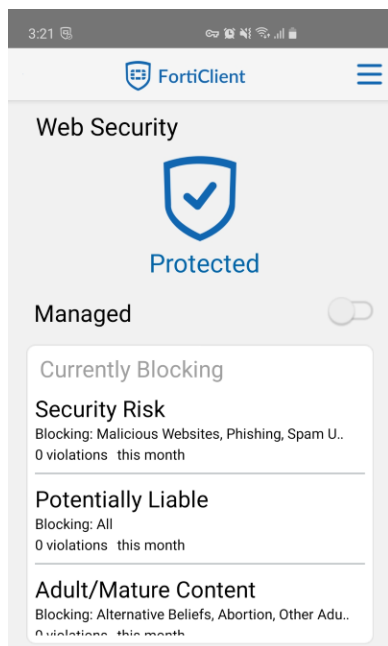


Provisioning of a web filter exclusion list is only available from FortiClient EMS. Exclusion lists can only be applied on the domain name, not the full URL.

## 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.

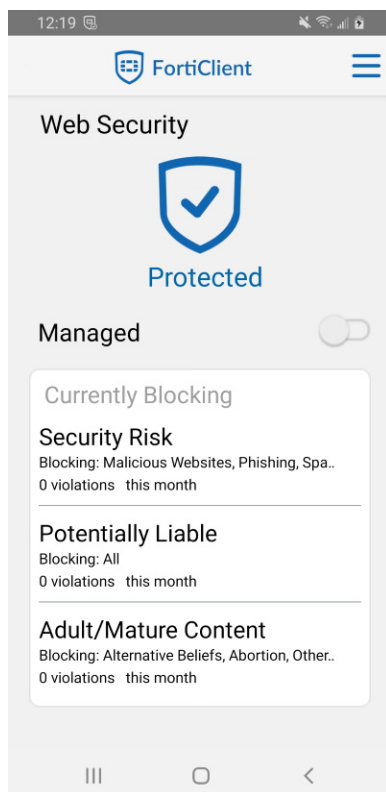
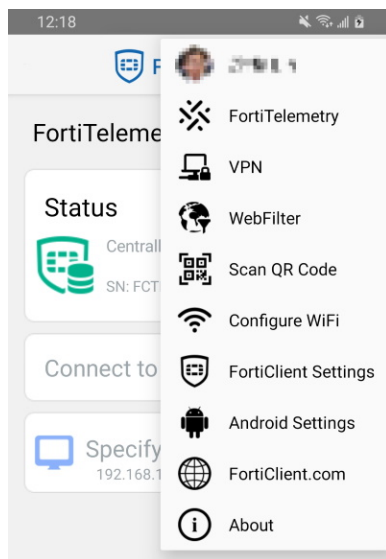


## Web security settings

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.



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



# SSL VPN

FortiClient (Android) 7.0 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, certificate authority server certificates, and check server certificates. You can also configure always up and autoconnect 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.

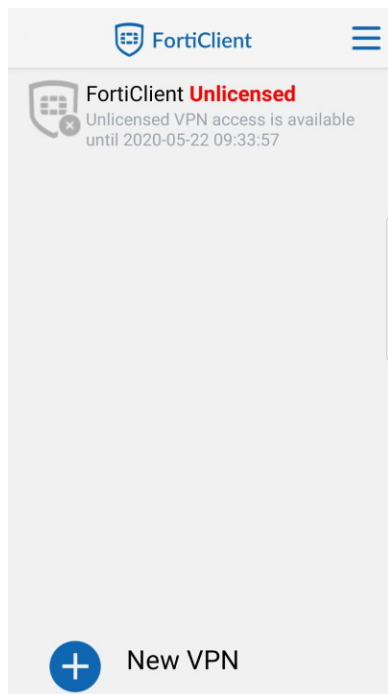
## Creating an SSL VPN connection

There are three ways to create a VPN connection on FortiClient (Android):

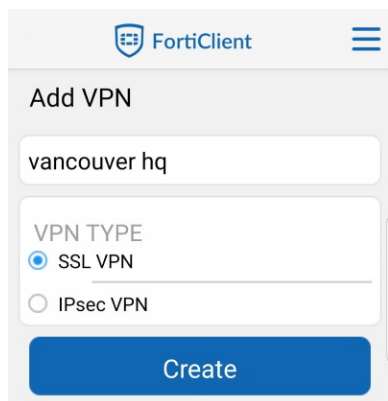
- Manually configure the VPN settings in the FortiClient (Android) app. See [To manually configure the VPN settings in the FortiClient \(Android\) app: on page 16](#).
- Receive VPN configuration from EMS. See [To receive VPN configuration from EMS: on page 17](#).
- Receive VPN configuration from FortiOS as a QR code. See [To receive VPN configuration from FortiOS as a QR code: on page 18](#).

**To manually configure the VPN settings in the FortiClient (Android) app:**

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 displays.



**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

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*.

Server

CANCEL OK

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

Port

443

CANCEL OK

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

Username

CANCEL OK

### To receive VPN configuration from EMS:

In the following instructions, the FortiClient (Android) end user takes some steps, while the FortiClient EMS administrator takes others.

1. (FortiClient (Android) end user) Connect FortiClient (Android) to EMS. See [Launching FortiClient \(Android\) for the first time on page 7](#).

2. (EMS administrator) Configure an endpoint profile in EMS to apply to the Android device.
3. (EMS administrator) Configure the desired SSL VPN settings in the profile that they created in step 2. See [SSL VPN](#).

### To receive VPN configuration from FortiOS as a QR code:

The following instructions assume that an SSL VPN exists on the FortiGate. For information on creating a new tunnel in FortiOS, see [SSL VPN](#). The FortiOS VPN settings that this example uses demonstrates the FortiClient QR code functionality. The example also assumes that FortiClient (Android) is already installed on the device.

In the following instructions, some step are taken by the FortiClient (Android) end user, while other steps are taken by the FortiOS administrator.

In the following example, the following settings have already been configured:

- A user group named `SSL_VPN_Employee`, which contains one user
- Authentication/portal mapping for the `SSL_VPN_Employee` user group

Authentication/Portal Mapping ⓘ	
<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Send SSL-VPN Configuration</a>	
Users/Groups ⇅	Portal ⇅
SSL_VPN_Employee	Employee-Access
SSL_VPN_Contractor	Contractor-Access
All Other Users/Groups	No-Access

- A policy that permits traffic from the SSL VPN tunnel
1. (FortiOS administrator) Do one of the following:
    - a. Go to *VPN > SSL-VPN Settings*. Under *Authentication/Portal Mapping*, click *Send SSL-VPN Configuration*.
    - b. Go to *User & Authentication > User Definition*. Edit the desired user, then click *Send SSL-VPN Configuration* on the right pane.
  2. (FortiOS administrator) In the *VPN Name* field, enter the desired name to appear in the FortiClient (Android) VPN menu.
  3. (FortiOS administrator) In the *Host* field, enter the IP address that FortiClient (Android) will attempt to connect to. By default, this field displays the IP address of the interface that SSL VPN is configured on.
  4. (FortiOS administrator) If desired, click *Edit SSL-VPN Provision User Email* to customize the message. The default email looks as follows:

How to set up the SSL-VPN connection on FortiClient-VPN

#### 1. Download and install FortiClient VPN

FortiClient securely connects your computer or mobile device to your network

[Download](#)

#### 2. Configure the connection

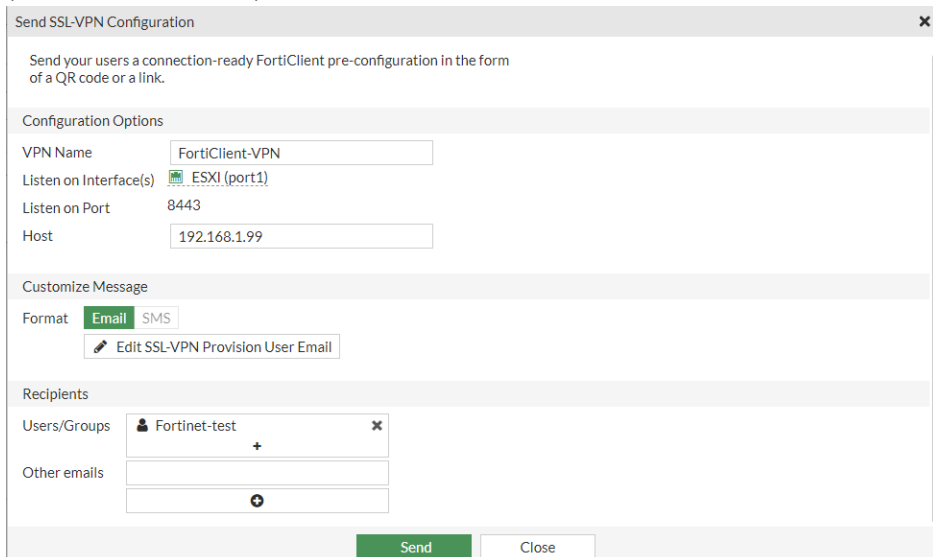
FortiClient VPN can configure your connection automatically.

Click on [this link](#), or scan the QR code below from the FortiClient VPN app.



Contact your network administrator if you require assistance.

5. (FortiOS administrator) Under *Recipients*, enter email address(es) as desired. You must manually enter an email address if no user or user in a user group has an email address associated with the user account.
6. (FortiOS administrator) Click *Send*.



Send SSL-VPN Configuration

Send your users a connection-ready FortiClient pre-configuration in the form of a QR code or a link.

Configuration Options

VPN Name: FortiClient-VPN

Listen on Interface(s): ESXi (port1)

Listen on Port: 8443

Host: 192.168.1.99

Customize Message

Format: Email SMS

Edit SSL-VPN Provision User Email

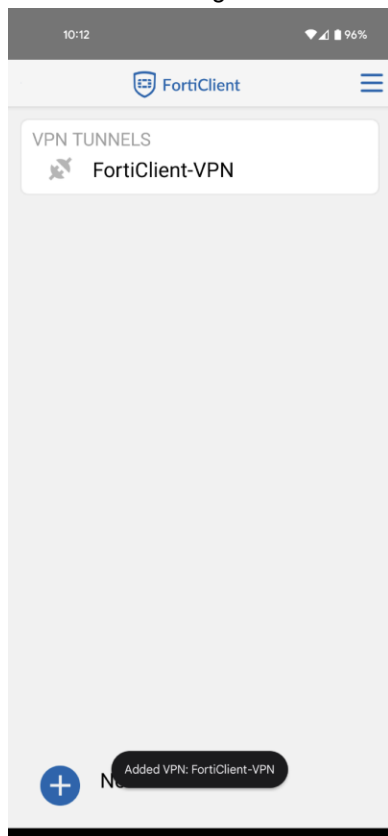
Recipients

Users/Groups: Fortinet-test

Other emails:

Send Close

7. (FortiClient (Android) end user) Open FortiClient (Android) on the mobile device.
8. (FortiClient (Android) end user) Select the menu icon in the upper right corner, then select *Scan QR Code*.
9. (FortiClient (Android) end user) Scan the QR code in the email that you received. The VPN tunnel list now includes the new VPN configuration from FortiOS.

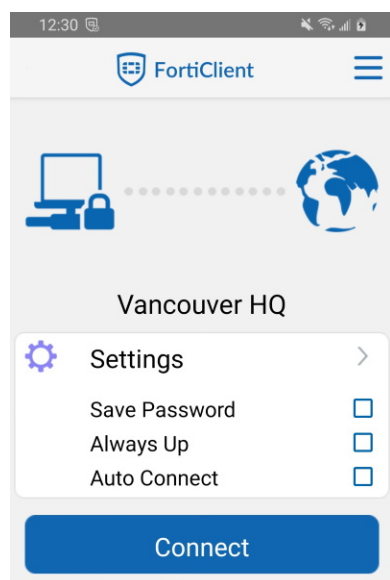
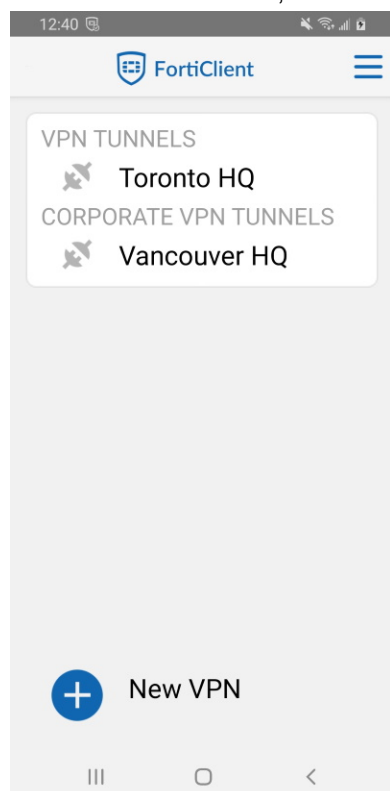


## Connecting to the VPN

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.

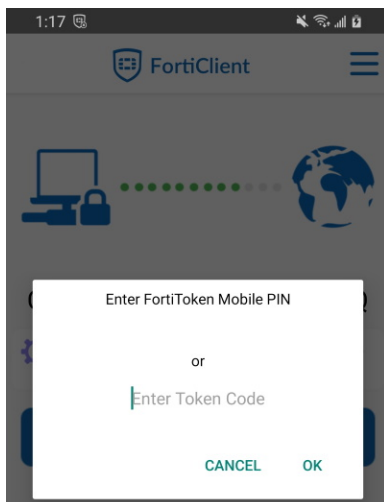
### To connect to the SSL VPN:

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

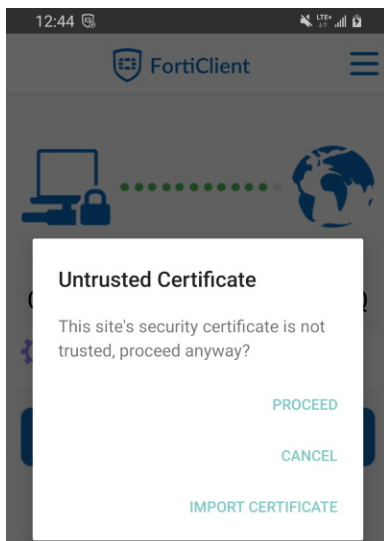


2. Enter your username and password then select *Login*.

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.



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



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.



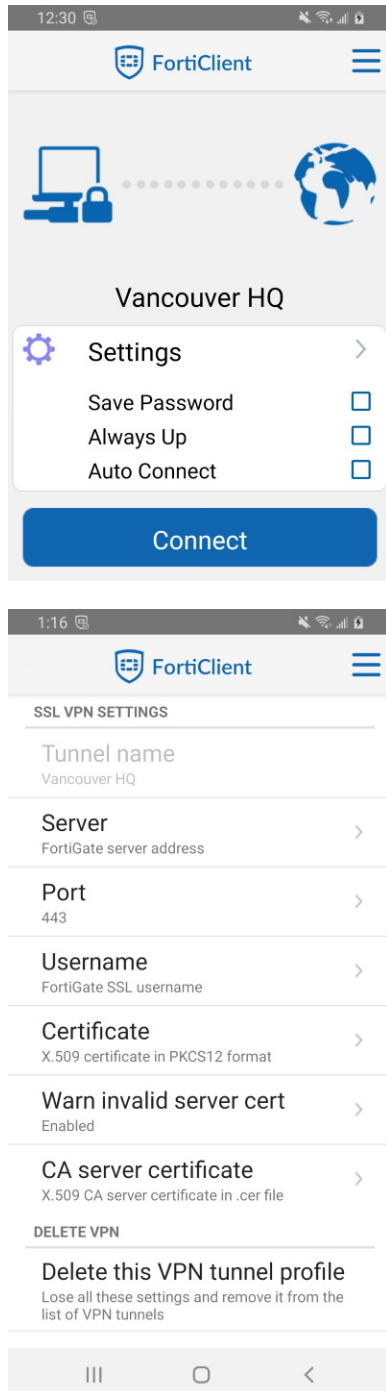
For some devices, it may be necessary to change the TCP-MSS configuration to allow Telemetry connection after establishing an SSL VPN connection.



Traffic to Google Play Store cannot be fully tunneled in SSL VPN full tunnel.

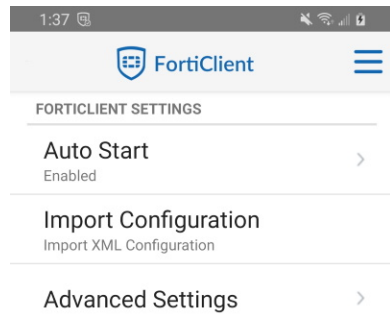
## Editing SSL VPN settings or deleting a SSL VPN configuration

Select the SSL VPN tunnel, then *Settings*.



## 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.



# IPsec VPN

FortiClient (Android) 7.0 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.

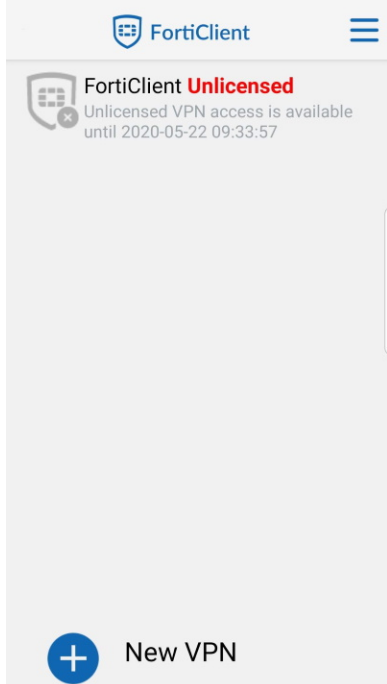
IKEv2 is not currently supported.

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

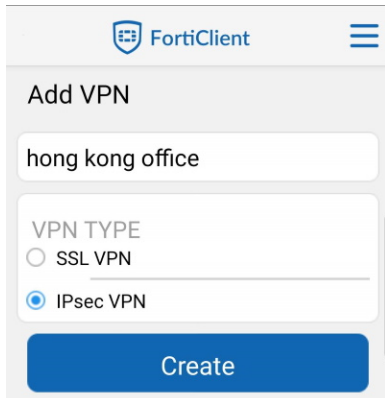
**To create a new IPsec VPN connection:**

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

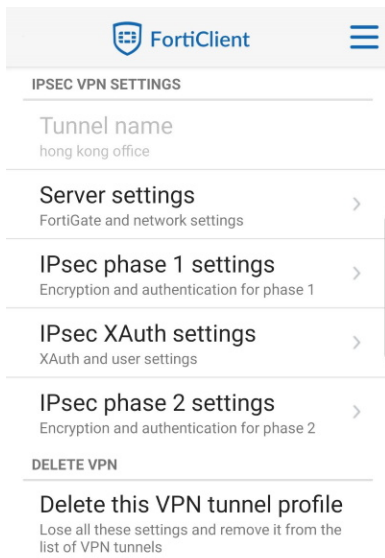




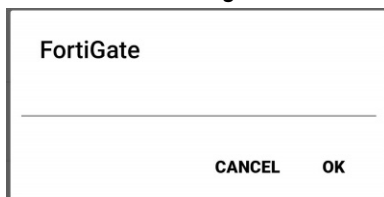
- b. Enter a name for the new VPN connection, select *IPsec VPN* under *VPN Type*, then select *Create*.



The *IPsec VPN settings* page displays.

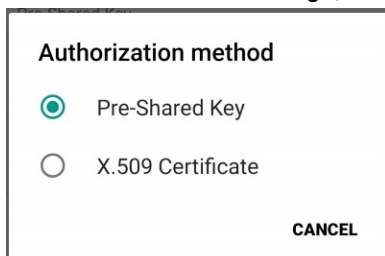


2. Select *Server settings* > *Network settings* > *FortiGate*. Enter the server IP address or domain name, then select *OK*.

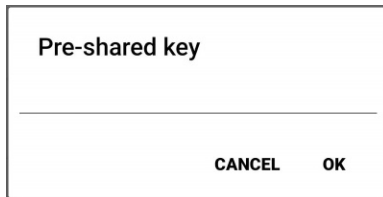


3. Configure authentication settings:

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



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

A dialog box titled "Pre-shared key" with a text input field and two buttons at the bottom: "CANCEL" and "OK".

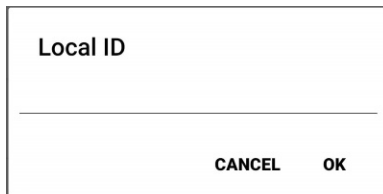
The simplest way to authenticate with the FortiGate unit is by means of a pre-shared key. This is less secure than using certificates, especially if it is used alone, without requiring peer IDs or extended authentication (XAuth).

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*.

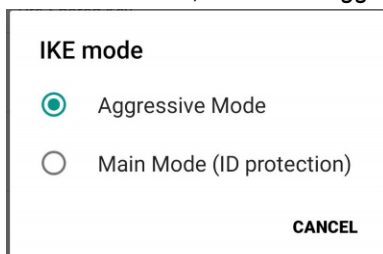
A dialog box titled "Local ID" with a text input field and two buttons at the bottom: "CANCEL" and "OK".

- 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)*.

A dialog box titled "IKE mode" with two radio button options: "Aggressive Mode" (selected) and "Main Mode (ID protection)". There is a "CANCEL" button at the bottom right.

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.

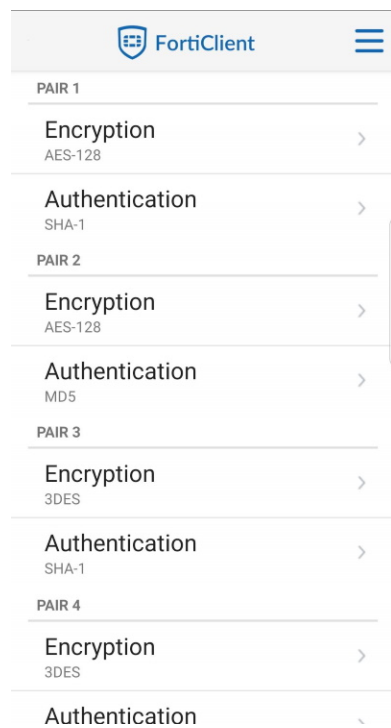
You can select any of the following symmetric-key algorithms:

- 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.

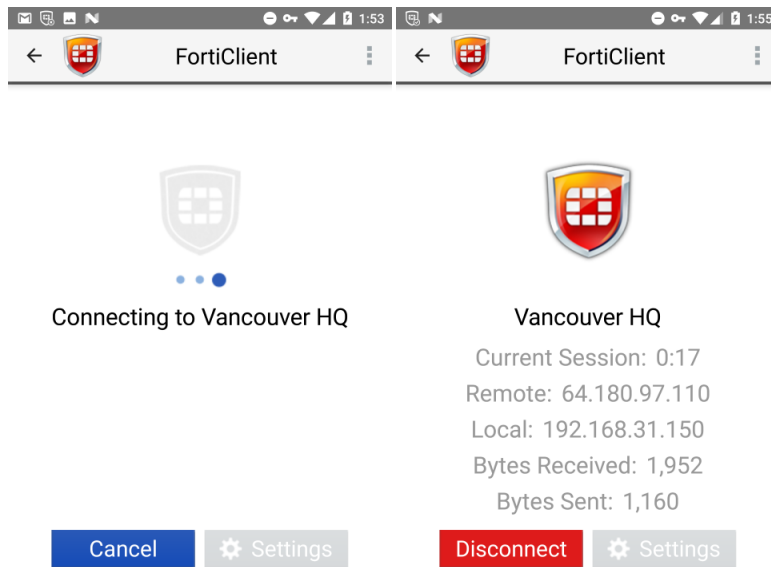


Contact your network administrator for the correct phase 2 encryption and authentication algorithms and DH group.

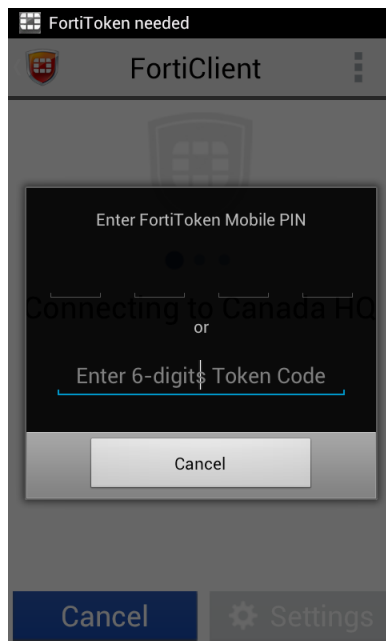
## Connecting to an IPsec VPN

### 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*.

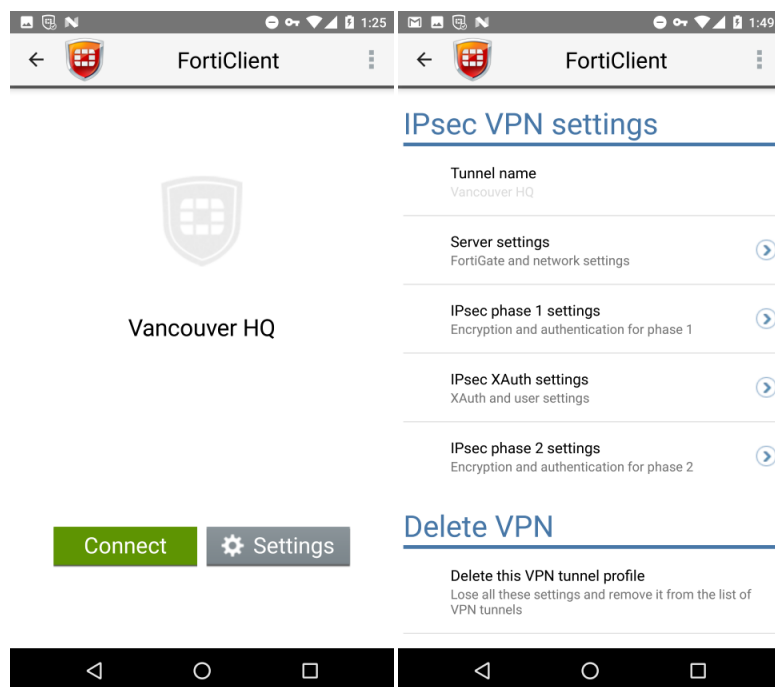


If the IPsec VPN you are connecting to requires you to enter a FortiToken Mobile token, you are prompted to enter your FortiToken Mobile PIN or six-digit token code.



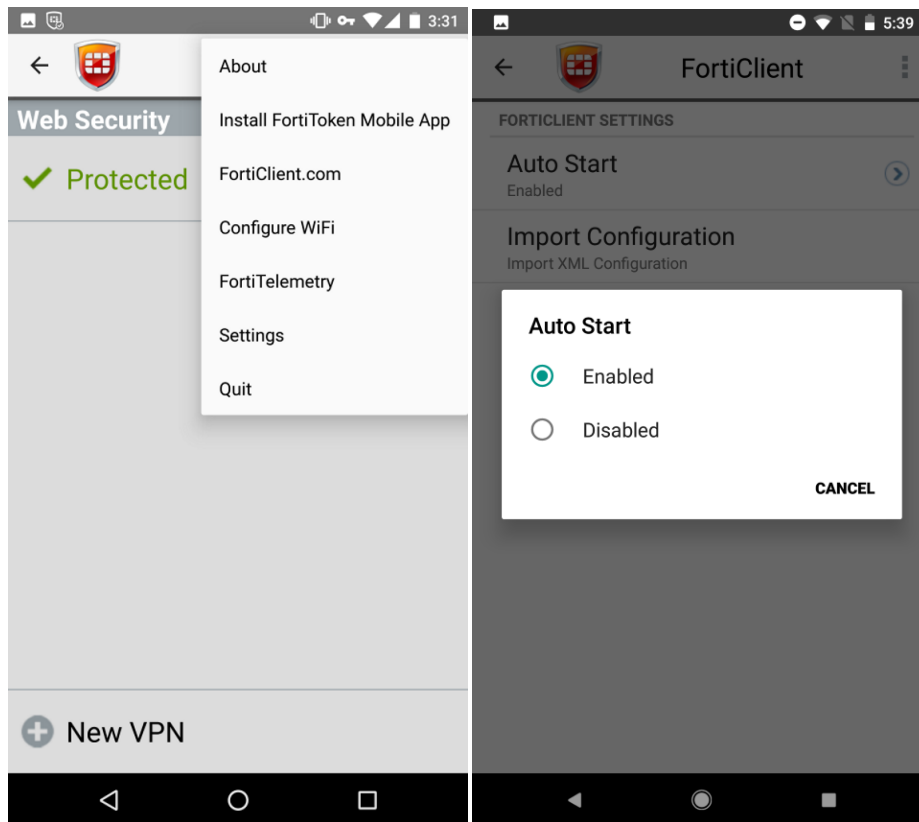
## Editing VPN settings or deleting a VPN configuration

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



## 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.

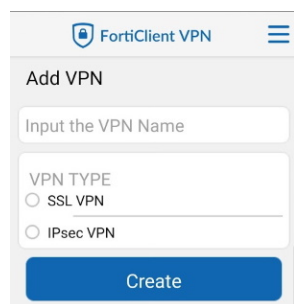


# Standalone VPN client

You can download a [VPN-only FortiClient \(Android\) app](#). This app is free, supports basic IPsec and SSL VPN, and does not require registration with EMS. This version does not include central management, technical support, or some advanced features such as always up, autoconnect, and so on.

Full-featured FortiClient (Android) requires registration to EMS. Each endpoint registered with EMS requires a license seat on EMS.

When you launch the free VPN-only FortiClient (Android) for the first time, it requests permissions to use the camera and access storage. Grant permissions as required. Only the VPN feature is available. Configuring settings for a new VPN connection on the free VPN-only FortiClient (Android) resembles doing the same on the full-featured FortiClient (Android). See [Creating an SSL VPN connection on page 15](#) or [Creating an IPsec VPN connection on page 24](#) for details on these procedures.



The screenshot shows the 'FortiClient VPN' app interface. At the top, there is a header bar with the app name and a menu icon. Below the header, the title 'Add VPN' is displayed. Underneath, there is a text input field labeled 'Input the VPN Name'. Below the input field, there is a section titled 'VPN TYPE' with two radio button options: 'SSL VPN' and 'IPsec VPN'. At the bottom of the form, there is a blue 'Create' button.



# Endpoint control

FortiClient (Android) 7.0 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 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:

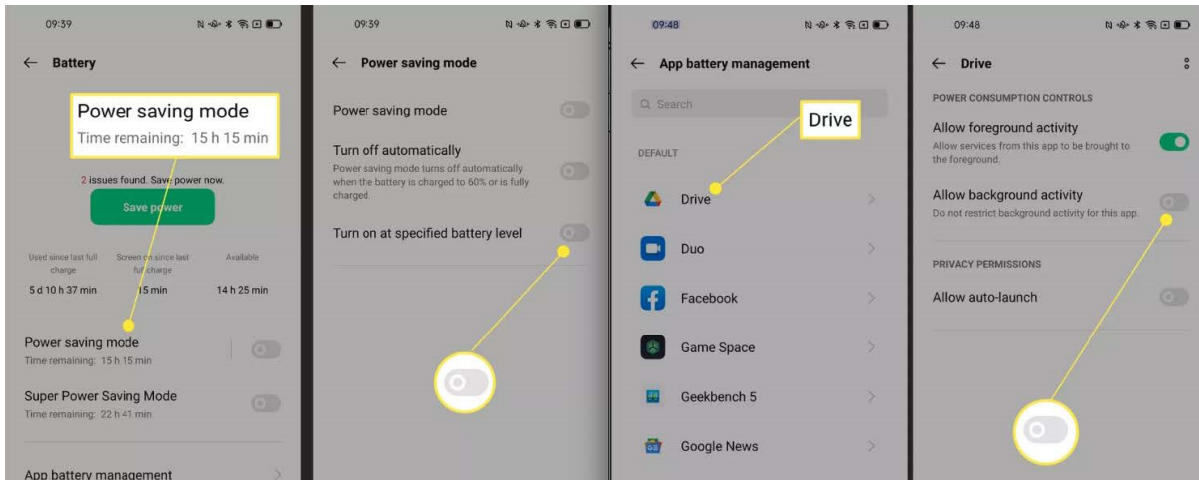
1. In FortiClient EMS, go to *Endpoint Profiles > Manage Profiles > Add*.
2. Configure the settings on the *Web Filter* tab.
3. Configure the settings on the *VPN* tab.
4. On the *System Settings* tab, select *Install CA Certificate on Client*.
5. Click *Save*.

### EMS connection mechanism under limited network access by device lock

For energy efficiency, an Android device allows limited network access for third party applications when the device is locked. Therefore, when an Android device is locked, FortiClient (Android) is offline.

FortiClient (Android) becomes online when a device is active (unlocked) for a longer time than the next keepalive (KA) interval. The default KA interval is 60 seconds. If a device becomes inactive during the KA interval, FortiClient (Android) is offline.

To allow FortiClient (Android) to run in the background, you should disable the device's battery save mode or allow background activity in the application's settings if applicable. The following shows example screenshots of configuring battery save mode and enabling background activity. Your settings pages may differ depending on your device type and Android version:

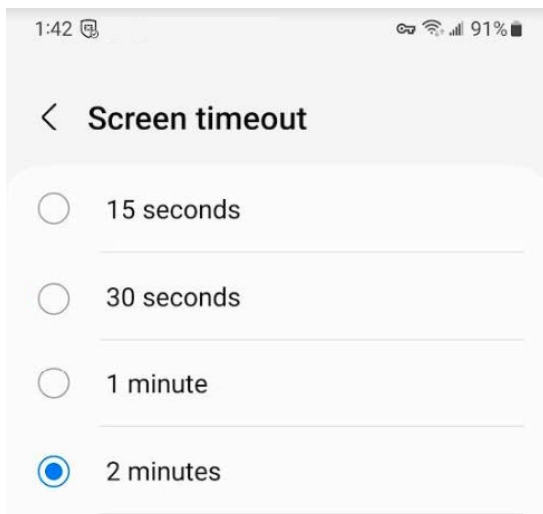


### To configure the device screen lock time to be longer than the KA interval:

1. In EMS, go to *System Settings > EMS Settings*.
2. Under *Endpoint Settings*, configure the *Keep alive interval* field as desired.

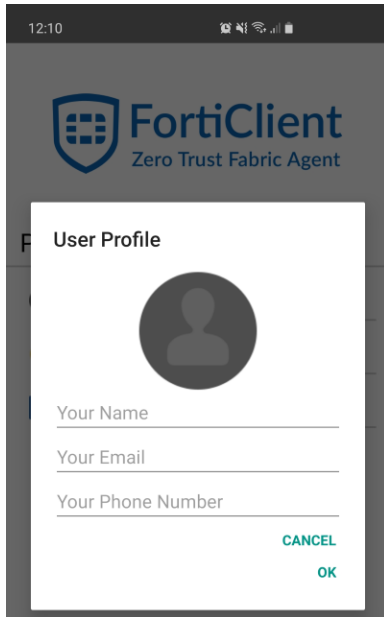
Endpoints Settings	
FortiClient telemetry connection key	Optional
Keep alive interval	60 seconds

3. On the Android device, configure the screen timeout to be longer than the value configured in EMS. The following shows an example screen timeout configuration page. Your page may differ depending on your device type and Android version:



## 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.



# Enterprise mobility management

FortiClient (Android) supports integration with enterprise mobility management software. Integration with enterprise mobility management software allows FortiClient (Android) endpoints to connect to EMS.

## Configuring AirWatch integration

AirWatch integration allows FortiClient (Android) endpoints to connect to EMS. This documentation is based on Workspace ONE UEM 219.0.0 (2109).

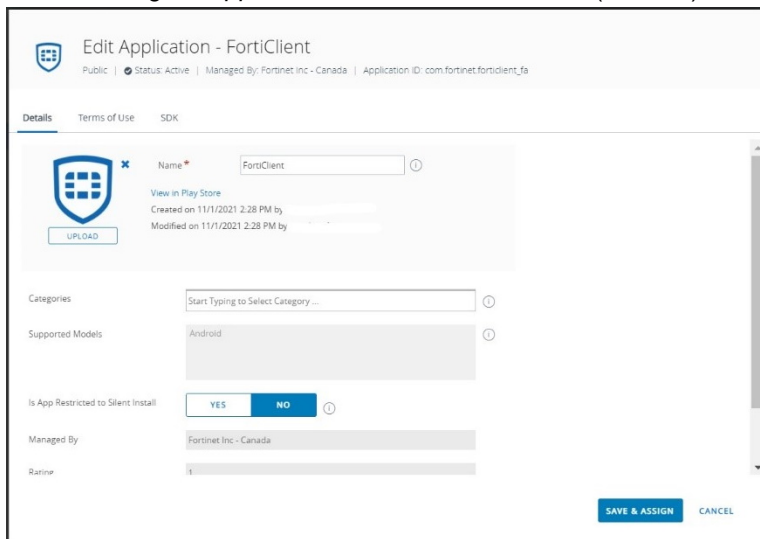
**To configure integration between AirWatch and FortiClient (Android):**

1. In AirWatch, go to *Assignment Groups*. Create a new assignment group.
2. Go to *Accounts*, and add a new user.

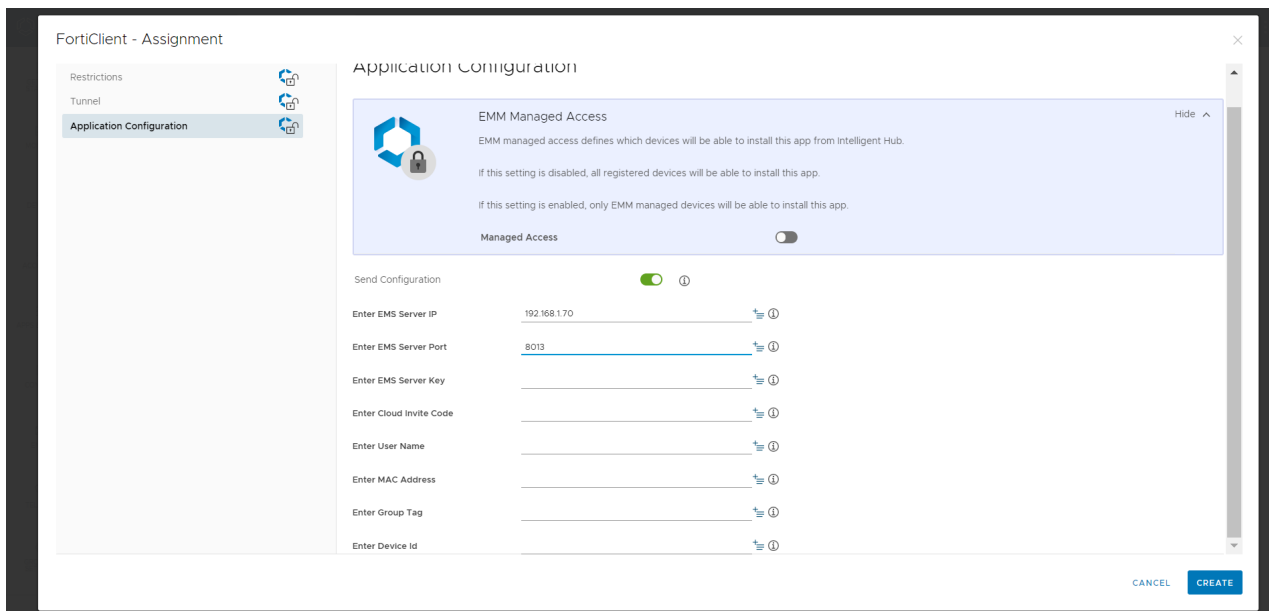
The screenshot shows the 'Add/Edit User' dialog box in AirWatch. The 'General' tab is active. The 'Security Type' is set to 'BASIC'. The 'Username' field contains 'jamesbaker'. The 'Password' and 'Confirm Password' fields are masked with dots. The 'Full Name' field is split into 'First Name' (James) and 'Last Name' (Baker). The 'Display Name' field is empty. The 'Email Address' field contains 'jamesbaker@example.com'. The 'Email Username' field also contains 'jamesbaker@example.com'. The 'Domain' field is empty. At the bottom, there are three buttons: 'SAVE', 'SAVE AND ADD DEVICE', and 'CANCEL'.

3. Add a new device for the user:
  - a. From the *Device Ownership Type* dropdown list, select *Corporate - Dedicated*.
  - b. From the *Platform* dropdown list, select *Any* or *Android*.
  - c. For *Message Type*, select *EMAIL*.
  - d. Save. This sends an AirWatch device activation email to the user.
4. The user installs Intelligent Hub on the device and scans the QR code in the activation email to enroll the device.

5. In AirWatch, go to *Apps & Books*, and add FortiClient (Android) from the public app store.



6. When adding an assignment, enter the desired name and select the desired assignment groups. Configure the deployment as desired.
- In *Application Configuration*, you can optionally add key-value pairs. FortiClient sends this information to EMS. The following shows the configuration for a FortiClient (Android) device that will connect Telemetry to on-premise EMS:



FortiClient - Assignment ✕

Details

Platform: Android Status: ● Active

Assignments Exclusions

Devices will receive application based on the configurations below. Devices with multiple assignments will receive policies in priority order. Adjusting the priority for a single assignment will automatically reprioritize other assignments. Select the assignment to edit. Adding a new assignment will create a new rule at the bottom of the list.

ADD ASSIGNMENT

Priority	Assignment Name	Description	Smart Groups	App Delivery Method	EMM Managed Access
0	Corporate-Android-Policy		3	On Demand	<span>●</span> Enabled

Page Size 5 Items 1 - 1 of 1


CANCEL SAVE

Supported keys include the following:


Key	Description
Mac address	Android device MAC address.
Device ID	Android device UDID.
Ems server IP	EMS server IP address.
Ems server port	EMS port number.
Ems server key	EMS Telemetry key.
Group tag	This value is used as a group tag for configuration in EMS. See <a href="#">FortiClient EMS Administration Guide</a> .
Cloud invite code	This value is used for connecting FortiClient (Android) to FortiClient Cloud. Enter the invite code received from FortiClient Cloud.

- You can add more assignments and use different Group tag values.
- When FortiClient starts on the device, it automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration.


The following shows the on-premise EMS GUI after FortiClient (Android) connects Telemetry.




0  
Not Installed




0  
Not Registered




0  
Out-Of-Sync



0  
Security Risk



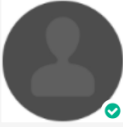
0  
Quarantined

Endpoints 

Search All Fields


Filters

Summary Webfilter Events System Events



James


James  
jamesbaker@example.com

 Other Endpoints

Device

Pixel 5

OS

 Android Phone 12

IP

192.168.1.78

MAC

56-87-61-80-5d-66

Public IP

108.172.38.156

Status

Online

Location

On-Fabric

Owner

Organization

Connection

Managed by EMS

Configuration

Policy

Default

Profile

Default

Off-Fabric Profile

Not assigned

Installer

Not assigned

FortiClient Version

7.0.0.0015

FortiClient Serial Number

FCTE

FortiClient ID

41B395302CEA3B01...

ZTNA Status

Pending CSR

Status

Managed

Features

Antivirus not installed

Anti-Ransomware not installed

Cloud Based Malware Outbreak Detection not installed

Sandbox not installed

Sandbox Cloud not installed

Web Filter enabled

Application Firewall not installed

Remote Access configured

Vulnerability Scan not installed

SSOMA not installed

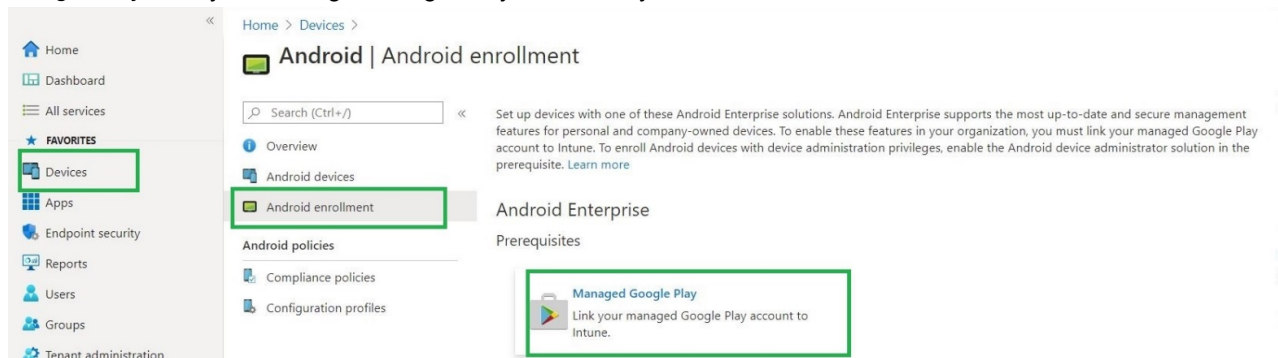
Showing: 3 Total: 3

# Configuring Microsoft Intune 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.



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

✓ Basics 2 Settings 3 Assignments 4 Review + create

Name \* FortiClient Android ✓

Description ✓

Device enrollment type Managed devices ✓

Platform \* ① Android Enterprise ✓

Profile Type \* ① Work Profile Only ✓

Targeted app \* ① FortiClient

Previous Next

- 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 specifications.



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.

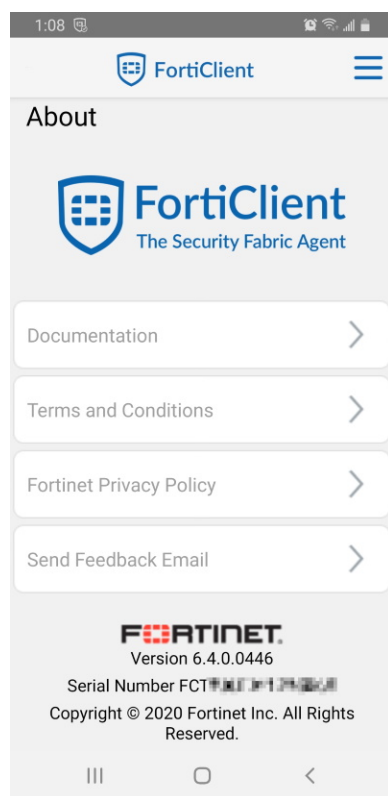
---

# 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).



## Change log

Date	Change Description
2021-11-02	Initial release.
2022-01-28	Updated <a href="#">Creating an SSL VPN connection on page 15</a> .
2022-09-26	Updated <a href="#">IPsec VPN on page 24</a> .
2023-08-11	Added <a href="#">EMS connection mechanism under limited network access by device lock on page 33</a> .



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.