Change log
Introduction

FortiClient (Android) 6.0 includes support for IPsec VPN, SSL VPN, Web Security, Endpoint Control, and FortiClient Enterprise Management Server (EMS).

FortiClient (Android) 6.0 features

The following table lists and describes features supported in FortiClient (Android) 6.0.

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

Downloading FortiClient (Android) 6.0

You can download the FortiClient (Android) 6.0 application from the Google Play store or at https://play.google.com/store.
The following table lists FortiClient (Android) 6.0 product integration and support information.

<table>
<thead>
<tr>
<th>Android operating systems</th>
<th>4.1 Jelly Bean (API level 16)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4.2 Jelly Bean (API level 17)</td>
</tr>
<tr>
<td></td>
<td>4.3 Jelly Bean (API level 18)</td>
</tr>
<tr>
<td></td>
<td>4.4.3 KitKat (API level 19)</td>
</tr>
<tr>
<td></td>
<td>4.4.4 KitKat (API level 20)</td>
</tr>
<tr>
<td></td>
<td>5.0.1 Lollipop (API level 21)</td>
</tr>
<tr>
<td></td>
<td>5.1.1 Lollipop (API level 22)</td>
</tr>
<tr>
<td></td>
<td>6.0.0 Marshmallow (API 23)</td>
</tr>
<tr>
<td></td>
<td>7.0.0 Nougat (API 24)</td>
</tr>
<tr>
<td></td>
<td>7.1 Nougat (API 25)</td>
</tr>
<tr>
<td></td>
<td>8.0.0 Oreo (API 26)</td>
</tr>
<tr>
<td></td>
<td>8.1.0 Oreo (API 27)</td>
</tr>
<tr>
<td>FortiOS</td>
<td>5.2.0 and later</td>
</tr>
<tr>
<td></td>
<td>5.4.0 and later</td>
</tr>
<tr>
<td></td>
<td>5.6.0 and later</td>
</tr>
<tr>
<td>FortiToken Mobile</td>
<td>4.0.0 and later</td>
</tr>
<tr>
<td></td>
<td>See the FortiToken Mobile User Guide for Android.</td>
</tr>
<tr>
<td>FortiClient EMS</td>
<td>1.2.0 and later</td>
</tr>
</tbody>
</table>
Getting started

Launching FortiClient (Android) for the first time

FortiClient (Android) includes a Web Security feature to help protect your device from malicious sites. When opening FortiClient, you are prompted to enable the Web Security feature and respond to several questions. After that, FortiClient (Android) automatically starts when Android OS starts.

To launch FortiClient (Android) for the first time:

1. When you open FortiClient (Android), the Welcome to FortiClient! dialog displays. Click OK.
2. Information about requiring a VPN connection for web security displays. Click OK.

3. Information about enabling web security displays. Click OK.
4. Depending on the Android operating system, you may see the following pop-ups about permissions. Select *Allow*.

5. The *Connection request* page displays. Click *OK*.

### Launching FortiClient (Android) from the notification bar

FortiClient (Android) 6.0 allows you to launch the application from the notification bar.
Getting started

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) 6.0 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 (http://www.fortiguard.com/static/webfiltering.html).

<table>
<thead>
<tr>
<th>Groups</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk</td>
<td>Malicious Websites, Phishing, Spam URLs</td>
</tr>
<tr>
<td>Potentially Liable</td>
<td>Drug Abuse, Hacking, Illegal or Unethical, Discrimination, Explicit Violence, Extremist Groups, Proxy Avoidance, Plagiarism, Child Abuse</td>
</tr>
<tr>
<td>Adult/Mature Content</td>
<td>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</td>
</tr>
<tr>
<td>Bandwidth Consuming</td>
<td>Freeware and Software Downloads, File Sharing and Storage, Streaming Media and Download, Peer-to-peer File Sharing, Internet Radio and TV, Internet Telephony</td>
</tr>
<tr>
<td>Unrated</td>
<td>Unrated</td>
</tr>
</tbody>
</table>

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 or FortiGate. 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 web security status displays Protected or Unprotected. When this feature is enabled, select Protected to view the blocked categories and the number of violations this month.

Enabling and disabling web security

To enable web security, select Unprotected, then toggle the Disabled switch to On. To disable web security, toggle the Enabled switch to Off.

When FortiGate endpoint control is managing FortiClient, the user cannot enable or disable web security.

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.

<table>
<thead>
<tr>
<th>Web Security settings</th>
<th>Web Security settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Risk</strong></td>
<td><strong>Allow All</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Deny All</strong></td>
</tr>
<tr>
<td>Malicious Websites</td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Spam URLs</td>
<td></td>
</tr>
<tr>
<td>Dynamic DNS</td>
<td></td>
</tr>
<tr>
<td><strong>Potentially Liable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Adult/Mature Content</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Bandwidth Consuming</strong></td>
<td></td>
</tr>
</tbody>
</table>

When browsing a website which falls into a denied category, you receive a webpage blocked page.
SSL VPN

FortiClient (Android) 6.0 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, CA server certificates, and check server certificates. You can also configure always up and auto connect for the VPN connection.

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

The SSL VPN settings page displays.
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 username, and select *OK*.

**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.

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

Select the SSL VPN, 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) 6.0 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.

Creating an IPsec VPN connection

To create a new IPsec VPN connection:

1. Select *New VPN* from the toolbar at the bottom of the page.
2. Enter a name for the new VPN connection, select IPsec VPN under VPN Type, then select Create.

![Add VPN](image)

The **IPsec VPN settings** page displays.

![IPsec VPN settings](image)

3. Select **Server settings > Network settings > FortiGate**. Enter the server IP address or domain name, then select **OK**.
4. Under Authentication, select Authorization method, and select either Pre-Shared Key or X.509 Certificate.

5. If desired, 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 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.
Select Local ID, enter the local ID, and select OK.

6. 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.
7. Select IKE mode, and select Aggressive Mode or 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.

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.

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

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

**Connecting to an IPsec VPN**

**To connect to an IPsec VPN:**

1. Select an available IPsec VPN connection, then select **Connect**.
2. 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.
Endpoint control

FortiClient (Android) 6.0 allows you to connect to a FortiGate for endpoint control and to FortiClient EMS for provisioning and monitoring.

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 FortiClient Telemetry gateway IP list

The FortiClient Telemetry gateway IP list contains the IP address for one or more FortiGates and for FortiClient EMS. FortiClient (Android) can use the FortiClient Telemetry gateway IP list to connect to a FortiGate for Endpoint Control and to FortiClient EMS for endpoint provisioning and monitoring.

To configure FortiClient Telemetry gateway IP lists:

1. In FortiClient EMS, go to Gateway IP Lists > Manage Gateway Lists > Add.
2. Configure the settings, then select Save.

Assigning endpoint profiles and FortiClient Telemetry gateway IP lists

To push custom endpoint profiles and FortiClient Telemetry gateway IP lists to endpoints, you must assign them to domains or workgroups.
To assign endpoint profiles and FortiClient Telemetry gateway IP lists:

1. In FortiClient EMS, go to *Endpoints*.
2. Right-click a domain or group, select *Assign profile*, then the profile. A confirmation dialog box displays.
3. Click Yes. The profile is assigned.
4. Right-click a domain or workgroup, select *Assign gateway list*, then the desired list. The gateway list is assigned to the domain or workgroup.

**Connecting to the FortiGate**

To connect to the FortiGate:

1. On the Android device, open FortiClient.
2. Do one of the following:
   a. If you have a QR code distributed by your FortiClient EMS administrator, select the menu icon in the toolbar, then select *Scan QR Code*. Using your device’s camera, scan the QR code. This automatically enables FortiTelemetry and uses the provided information to try connect to FortiClient EMS and the FortiGate. You can manually change the host IP address and port number from the *FortiTelemetry* page if desired.
   b. If you do not have a QR code, select the menu icon in the toolbar, then select *FortiTelemetry*.

3. FortiClient searches for available FortiGates listed in the gateway IP list. When FortiClient (Android) uses the FortiTelemetry settings to connect to a FortiGate, FortiClient (Android) also connects to and receives a profile from FortiClient EMS.
4. If FortiClient cannot locate a FortiGate, you can select Preferred Host and enter the FortiGate host IP and port number.

5. When a FortiGate is discovered, a dialog appears to confirm connection with the FortiGate serial number and IP address. Depending on the FortiGate configuration, you need to enter a FortiClient registration key.
6. A confirmation dialog appears when connection to the FortiGate is complete.

7. Upon successful connection with the FortiGate, FortiClient (Android) receives the profile. The following image provides an example of FortiClient (Android) connected to a FortiGate with web category filtering and provisioned VPN connections.
If FortiClient (Android) is connected to the FortiGate, it auto-starts when the phone is turned on and brings up the GUI.

Disconnecting from the FortiGate

To disconnect from the FortiGate, in the Endpoint Control settings page, select the close icon in the Status section. A confirmation dialog appears.
Configuring the FortiTelemetry profile

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

- Your Name
- Your Email
- Your Phone Number

- CAPTURE PHOTO
- SELECT PHOTO
  - SKIP
  - OK
Appendix A: FortiClient (Android) permission use

Static permissions

Static permissions are shown only on devices running Android 4.x and 5.x. All permissions are dynamic on devices running Android 6.x and 7.x. Android 6.x and 7.x automatically grant many permissions.

<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.RESTART_PACKAGES"/>
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
<uses-permission android:name="com.android.email.permission.ACCESS_PROVIDER"/>
<uses-permission android:name="com.android.email.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.gm.email.permission.ACCESS_PROVIDER"/>
<uses-permission android:name="com.google.android.gm.email.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.READ_GMAIL"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.WRITE_GMAIL"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.READ_ATTACHMENT_PREVIEW"/>
<uses-permission android:name="com.google.android.permission.READ_PROFILE"/>
<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.CAMERA"/>

Network usage

<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.INTERNET"/>

VPN management daemons

<uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
Autoconnect permissions

<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.RESTART_PACKAGES"/>

Import certificate permissions

<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>

Load user profile for FortiTelemetry permissions

<uses-permission android:name="android.permission.READ_PROFILE"/>

Send feedback by email permissions

<uses-permission android:name="com.android.email.permission.ACCESS_PROVIDER"/>
<uses-permission android:name="com.android.email.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.gm.email.permission.ACCESS_PROVIDER"/>
<uses-permission android:name="com.google.android.gm.email.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.gm.email.permission.READ_ATTACHMENT_PREVIEW"/>
<uses-permission android:name="com.google.android.gm.permission.READ_CONTENT_PROVIDER"/>
<uses-permission android:name="com.google.android.gm.permission.READ_GMAIL"/>
<uses-permission android:name="com.google.android.gm.permission.WRITE_GMAIL"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.READ_ATTACHMENT"/>
<uses-permission android:name="com.google.android.providers.gmail.permission.READ_GMAIL"/>

Debugging permissions

<uses-permission android:name="android.permission.VIBRATE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
<uses-permission android:name="android.permission.CAMERA"/>
# Change log

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-03-19</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>