# TABLE OF CONTENTS

**Introduction** ........................................................................................................ 4
  Features ............................................................................................................... 4
    SSL DNS server for split tunnel ........................................................................ 4
  Supported platforms ............................................................................................ 5

**Initial configuration** .......................................................................................... 6
  Running FortiClient iOS ...................................................................................... 6
  Creating a Mobileconfig profile ......................................................................... 9
  Web Filtering ..................................................................................................... 10
  FortiTelemetry ................................................................................................ 13
  User profile ....................................................................................................... 14

**Enterprise mobility management** ...................................................................... 17
  Configuring AirWatch integration .................................................................... 17
  Configuring Jamf integration ......................................................................... 23

**Logs** .................................................................................................................. 29

**Change log** ...................................................................................................... 31
Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet’s Advanced Threat Protection (ATP) to end user devices. As the endpoint is the ultimate destination for malware that is seeking credentials, network access, and sensitive information, ensuring that your endpoint security combines strong prevention with detection and mitigation is critical.

This guide describes how to install and set up FortiClient iOS for the first time.

Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| SSL VPN (tunnel mode) | SSL VPN in tunnel mode supports the following:  
  - IPv4  
    Example: https://24.1.20.17  
  - IPv6  
    Example: https://[1002:470:71f1:63::2]  
  - Full tunnel and split tunnel (IP address and subnet-based)  
  - SSL realm, custom DNS server, DNS suffix  
  - Username and password authentication  
  - PKI user with a personal certificate, FortiToken & Client Certificate  
  FortiClient iOS does not support SSL VPN resiliency. |

Web Filter | FortiClient iOS supports all browser traffic. |

FortiTelemetry | Connect to FortiGate and EMS for central management.  
  mobileconfig | Use the mobileconfig file to preconfigure a FortiClient Telemetry preferred host. Once FortiClient starts, it uses this preferred host to connect. |

FortiAnalyzer support | Send logs to FortiAnalyzer when configured from FortiClient EMS. See the FortiClient EMS Administration Guide. |

SSL DNS server for split tunnel

To use the SSL DNS server for split tunnel, you must configure the DNS suffix on the FortiGate side. Following is an example of configuring SSL DNS server for split tunnel using FortiOS:

```
config vpn ssl settings
  set dns-suffix
  "domain1.com;domain2.com;domain3.com;domain4.com;domain5.com;domain6.com;domain7.com;domain8.com"
  set dns-server1 10.10.10.10
  set dns-server2 10.10.10.11
end
```
config vpn ssl web portal
   edit "full-access"
      set dns-server1 10.10.10.10
      set dns-server2 10.10.10.11
      set split-tunneling enable
   next
end

If you configure the split tunnel, only DNS requests that match DNS suffixes use the DNS servers configured in the VPN. Due to iOS limitations, the DNS suffixes are not used for search as in Windows. Using short (not fully qualified domain name (FQDN)) names may not be possible.

Supported platforms

FortiClient iOS is supported by iOS versions 9, 10, 11, and 12.
Initial configuration

Running FortiClient iOS

After downloading the FortiClient installer and running the application for the first time, you must acknowledge some popups before continuing to add a VPN configuration. Acknowledge the notifications shown below.

To add a VPN connection:

1. In the Add VPN Configurations popup, tap Allow.
2. Tap the VPN icon at the bottom of the screen to switch to the VPN page.
3. Tap Connections > Edit > Add Configuration, then configure the following. Enter your passcode to confirm adding the VPN.
4. Tap *Done* twice.

The *Name*, *Host* and *Port* fields are required. The *User*, *Hide invalid certificate warning*, and *User Certificate* fields are optional.

To enable a VPN connection:

1. Tap a *VPN connection*. A checkmark appears beside the VPN connection to indicate it is selected.
2. Tap the < button.

3. Swipe right to enable the VPN connection.

4. If the username and password are not configured, enter the *username and passcode* in the popup.

5. Tap OK. When connected, the tunnel interface IP, duration, and the bytes sent and received information display.
To disable a VPN connection:

1. Select the VPN connection.
2. Swipe left to disable the VPN connection.

To edit or delete a VPN connection:

1. Select a VPN connection.
2. Tap Edit or Delete.
3. Tap Done twice.

Creating a Mobileconfig profile

To enable web filtering, the iOS device must be supervised and you must install a Mobileconfig profile with a content filter on the device. The following is required to install a mobileconfig profile:

- Apple Configurator 2 (or equivalent mobile device management (MDM) application) installed.
- iOS devices are supervised.

You can find instructions on how to supervise your iOS devices on the Apple Configurator 2 Help (or your MDM application) website.

To create a mobileconfig profile for FortiClient web filtering:

1. Launch Apple Configurator 2.
2. Go to File > New Profile.
3. Enter a Name for the profile.
4. Select Content Filter from the left panel.
5. Click Configure.
6. Select Plugin (Third Party App) from the Filter Type dropdown list.
7. Configure the following:

<table>
<thead>
<tr>
<th>Filter Name</th>
<th>FortiClient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>com.fortinet.forticlient</td>
</tr>
<tr>
<td>Service Address</td>
<td>fgd1.fortigate.com</td>
</tr>
<tr>
<td>Organization</td>
<td>Fortinet, Inc.</td>
</tr>
<tr>
<td>User Name</td>
<td>You can use this field to specify the EMS (IP address or FQDN), port, and connection key (optional). For example, the following string allows FortiClient iOS to connect to the EMS at ems.example.com at port 8013, with key “ConnectionKey”: ems.example.com:8013 ConnectionKey</td>
</tr>
<tr>
<td>Filter WebKit Traffic</td>
<td>Select the <em>Filter WebKit Traffic</em> checkbox.</td>
</tr>
<tr>
<td>Filter Socket Traffic</td>
<td>Select the <em>Filter Socket Traffic</em> checkbox.</td>
</tr>
</tbody>
</table>

8. Click Save.

Due to restrictions that Apple set, you must launch FortiClient iOS once before the configuration takes effect. You can use FortiGate compliance enforcement to ensure users launch FortiClient iOS before browsing the Internet. For details, see *FortiClient Compliance Profiles* in the *FortiOS Handbook*.

---

**Web Filtering**

Web Filtering is disabled by default. To enable Web Filtering, the iOS device must be supervised and a Mobileconfig profile with a content filter must be installed on the device. See *Creating a Mobileconfig profile*.
To configure the Web Filtering settings:

1. Tap Settings.
2. Tap Web Security Settings.
3. Enter the passcode in the FortiClient Authentication popup.
4. Enable the Web Filter by swiping right.
5. Configure the Website Blocking by Categories to suit requirements.
When a website is blocked, a restricted website error page appears.

Enter iPhone passcode for “FortiClient”
FortiClient needs authentication

1 2 3
A B C D E F

4 5 6
G H I J K L M N O

7 8 9
P Q R S T U V W X Y Z

0

Cancel
FortiTelemetry

To configure the FortiClient Telemetry settings:

1. Tap Settings at the bottom of the screen.
2. Tap FortiClient Telemetry.

3. Enable FortiClient Telemetry by swiping right. When FortiClient detects a FortiTelemetry server, a confirmation popup appears.

4. Tap Send FortiClient Telemetry Data to connect to the FortiTelemetry server.
To specify a FortiTelemetry server:

1. Tap Specify Preferred Host.

<table>
<thead>
<tr>
<th>2:41</th>
<th>WiFi</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>FortiClient Telemetry</td>
<td></td>
</tr>
</tbody>
</table>

   **STATUS**
   - Connected to ssidemo.fortinet.com
     - SN: FCTEM2619167971

   - Specify Preferred Host
     - ssidemo.fortinet.com

   - FortiClient Telemetry Connection
     - On

   - Default Gateway...
     - 172.17.250.1

2. Enter Host and Port.

<table>
<thead>
<tr>
<th>1:59</th>
<th>WiFi</th>
<th>Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiClient Telemetry</td>
<td>Preferred Host</td>
<td>Done</td>
</tr>
</tbody>
</table>

   **PREFERRED CONNECTION**
   - Host
     - Host name or IP
   - Port
     - Port number, like 8013

3. Tap Done.

You can use the mobileconfig file to preconfigure a FortiClient Telemetry preferred host. Once FortiClient starts, it uses this preferred host to register. See Creating a Mobileconfig profile on page 9.

User profile

You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Facebook
You can also manually add or edit a name, phone number, and email address in FortiClient. FortiClient iOS sends this user data to FortiClient EMS, where it displays on the Endpoints content pane.

To retrieve user details from a cloud application:

1. Tap Settings at the bottom of the screen.
2. Tap User Profile.

3. Tap the desired cloud application.

4. If you are not logged into the cloud application already on this device, you must log in. Grant FortiClient iOS permission to use your information.
To add user details manually:

1. Tap Settings at the bottom of the screen.
2. Tap User Profile.

3. Tap User Input.

4. Tap to edit the photo, name, email, and phone number as desired.

5. Tap Save.
Enterprise mobility management

FortiClient iOS supports integration with enterprise mobility management software including AirWatch and Jamf. Integration with AirWatch or Jamf allows FortiClient iOS endpoints to connect to EMS. Only FortiClient iOS 6.0.1 and later versions support MDM through Jamf and AirWatch.

Configuring AirWatch integration

AirWatch integration allows FortiClient iOS endpoints to connect to EMS.

To configure integration between AirWatch and FortiClient iOS:

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

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 *Apple iOS*.
   c. For *Message Type*, select *EMAIL*.
d. Save. This sends an AirWatch device activation email to the user.

4. The user installs AirWatch agent 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 iOS from the public app store.

6. When adding an assignment, scroll to the bottom and enable **Application Configuration**. Optionally, you can add key-value pairs as shown.
This enables FortiClient iOS to read the MAC address and UDID from the iOS device. FortiClient sends this information to EMS. Supported keys include the following:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>The iOS device's MAC address.</td>
</tr>
<tr>
<td>udid</td>
<td>The iOS device's UDID.</td>
</tr>
<tr>
<td>group_tag</td>
<td>This value is used as a group tag for configuration in EMS. In the example below, the string &quot;field_engineer&quot; is used as a group tag, which is used when FortiClient iOS initially connects to EMS. See Group assignment rules in the FortiClient EMS Administration Guide.</td>
</tr>
</tbody>
</table>

7. You can add more assignments and use different group_tag values.
8. Go to Devices, and add a profile:
   a. Go to the Content Filter section. In the User name field, enter the EMS URL.
   b. Go to Single App Mode, and configure as shown below to enable single app mode. This makes FortiClient iOS run.
   c. Assign the profile to the device.

9. When FortiClient starts on the device, it automatically connects to EMS. Once FortiClient connects to EMS, disable single app mode for the device. Keep the EMS URL in the Content Filter section.
The below shows the EMS GUI after FortiClient iOS connects Telemetry.
Configuring Jamf integration

To configure integration between Jamf and FortiClient iOS:

1. In Jamf, go to All Settings. Configure the settings in SMTP Server and Push Certificates.

2. Go to Global Management, and enable User-Initiated Enrollment.

3. Go to Mobile Device Apps and add FortiClient from the App Store or by uploading it.
4. Configure how the app is installed.

5. Add App Configuration for FortiClient iOS. This enables FortiClient iOS to read the MAC address and UDID from the iOS device. FortiClient sends this information to EMS. Supported keys include the following:

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>The iOS device's MAC address.</td>
</tr>
<tr>
<td>udid</td>
<td>The iOS device's UDID.</td>
</tr>
<tr>
<td>group_tag</td>
<td>This value is used as a group tag for configuration in EMS. In the example below, the string &quot;field_engineer&quot; is used as a group tag, which is used when FortiClient iOS initially connects to EMS. See Group assignment rules in the FortiClient EMS Administration Guide.</td>
</tr>
</tbody>
</table>

![FortiClient iOS User Guide](image-url)
6. Configure a configuration profile:

a. Go to Configuration Profiles and add a configuration profile.

b. Under Options, select Content Filter. Add a content filter to point to the desired EMS.

c. Enable Single App Mode for FortiClient. Single app mode launches the FortiClient app and connects it to
EMS. If FortiClient is not launched in single app mode, it does not connect to EMS.

7. Enroll the device:
   a. Go to Devices > Enrollment Invitations, then send an enrollment invitation to the device.
b. Enroll the device.

8. When the device is enrolled, FortiClient iOS automatically connects to EMS. Once FortiClient iOS is connected to EMS, disable single app mode for the device. Keep the EMS URL in the Content Filter section.
The below shows the EMS GUI after FortiClient iOS connects Telemetry.
Logs

You can email FortiClient iOS logs to Fortinet.

**To email logs to Fortinet:**

1. Tap *About*.
2. Tap *Diagnostic*.
3. Swipe right to enable *Logging*.
4. Tap *Email Logs*. 
## Change log

<table>
<thead>
<tr>
<th>Date</th>
<th>Change Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-09-25</td>
<td>Initial release.</td>
</tr>
<tr>
<td>2018-10-16</td>
<td>Added <strong>Configuring AirWatch integration on page 17</strong>.</td>
</tr>
<tr>
<td>2018-11-28</td>
<td>Release of FortiClient iOS 6.0.1. Added <strong>Configuring Jamf integration on page 23</strong> and added MAC address and UDID detail for <strong>Configuring AirWatch integration on page 17</strong>.</td>
</tr>
<tr>
<td>2019-01-29</td>
<td>Updated <strong>Features on page 4</strong>.</td>
</tr>
<tr>
<td>2019-02-04</td>
<td>Updated <strong>Configuring AirWatch integration on page 17</strong> and <strong>Configuring Jamf integration on page 23</strong>.</td>
</tr>
</tbody>
</table>