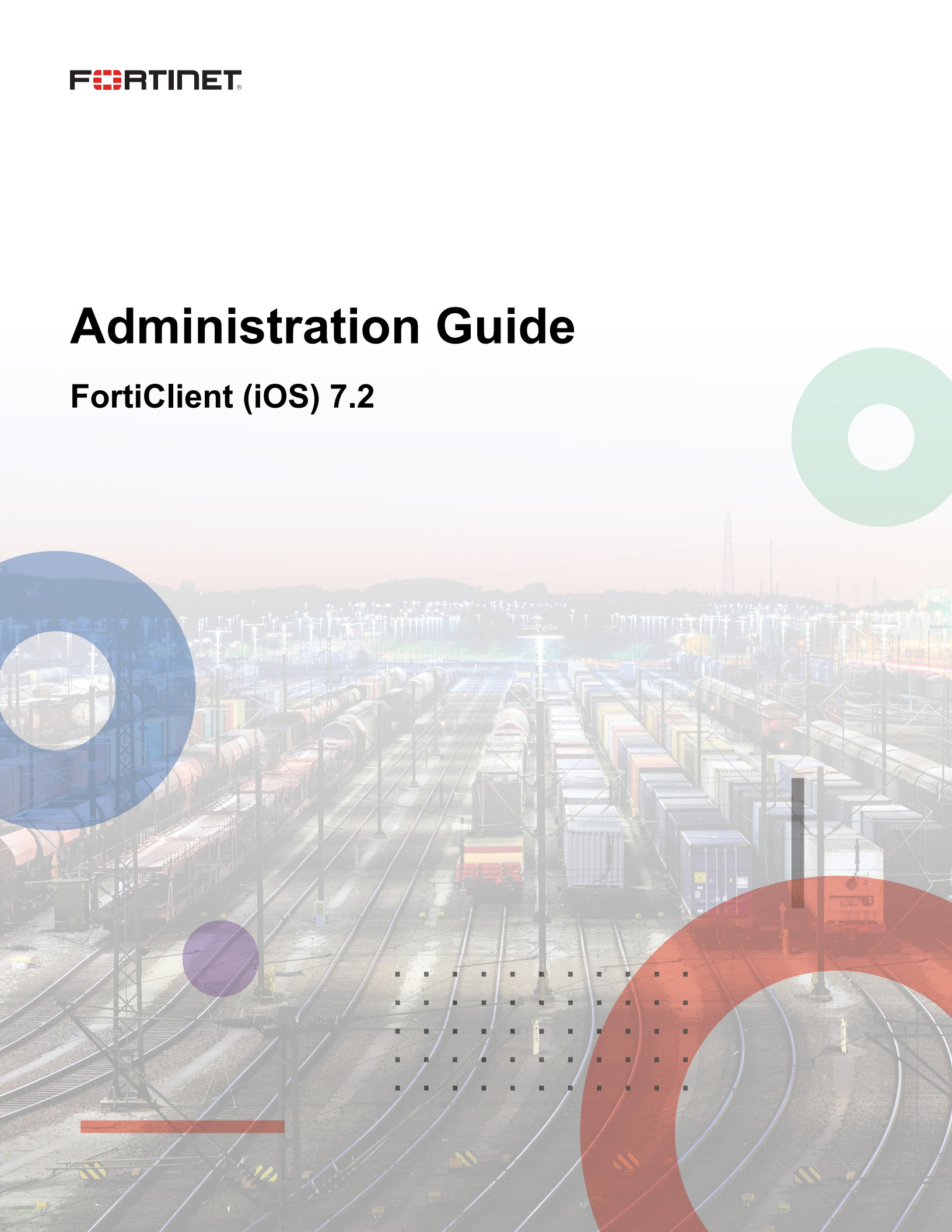


Administration Guide

FortiClient (iOS) 7.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<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 LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



January 30, 2024

FortiClient (iOS) 7.2 Administration Guide

04-720-943123-20240130

TABLE OF CONTENTS

Introduction	4
Features	4
SSL DNS server for split tunnel	5
Supported platforms	5
Initial configuration	6
Running FortiClient (iOS)	6
Creating a Mobileconfig profile	7
Configuring a Mobileconfig profile to enable Web Filter	7
Configuring a Mobileconfig VPN profile to install certificates	8
Web Filter	10
Zero Trust Telemetry	12
User profile	14
SSL VPN	16
Enterprise mobility management	19
Logs	20
Standalone VPN client	22
Change log	23

Introduction

FortiClient is an all-in-one comprehensive endpoint security solution that extends the power of Fortinet's Advanced Threat Protection 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.

You must license FortiClient (iOS) for use. See [Windows, macOS, and Linux licenses](#) for available license bundle descriptions. You can license FortiClient (iOS) by applying the license to EMS, then connecting Zero Trust Telemetry from FortiClient (iOS) to EMS. See [Zero Trust Telemetry on page 12](#).

FortiClient (iOS) does not communicate EMS when it runs in the background.

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

Features

Feature	Description
SSL VPN (tunnel mode)	<p>SSL VPN in tunnel mode supports the following:</p> <ul style="list-style-type: none">• IPv4 Example: <code>https://24.1.20.17</code>• IPv6 Example: <code>https://[1002:470:71f1:63::2]</code>• Full tunnel and split tunnel (IP address and subnet-based), including negative split tunnel• SSL realm, custom DNS server, DNS suffix• Username and password authentication• PKI user with a personal certificate, FortiToken, and client certificate• Always up <p>FortiClient (iOS) does not support SSL VPN resiliency.</p>
Web Filter	FortiClient (iOS) supports all browser traffic.
Zero Trust Telemetry	Connect to FortiGate and EMS for central management.
mobileconfig	Use the mobileconfig file to preconfigure a Zero Trust 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

iOS versions 9, 10, 11, 12, 13, 14, 15, 16, and 17 support FortiClient (iOS). FortiClient (iOS) also includes support for iPad OS.



iOS versions 15 and later require FortiClient (iOS) 7.0.6 or later.


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.

Privacy Policy Highlights

Forticlient DOES NOT collect any user specific personal information like username, photos or email address.

 **Analytics**
FortiClient Application may collect some anonymous usage information and send to Fortinet for App enhancements & usability improvements.

 **VPN**
FortiClient Application does not monitor user's VPN traffic.

 **WebFilter**
FortiClient webfilter feature, if enabled, submits website urls to Fortinet servers for category rating.

By selecting "I accept" below, you agree to FortiClient Apps [Terms of Service](#) and [Privacy Policy](#).

[I accept](#)

FortiClient

The FortiClient App has been upgraded to support the following new features:

- * Tunnel mode SSLVPN
- * WebFilter (now supports all browsers)

[OK, got it](#)

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.

To connect to a VPN tunnel using SAML authentication:

If your EMS administrator has enabled it, you can establish an SSL VPN tunnel connection using SAML authentication. See [SAML support for SSL VPN](#).

1. In FortiClient (iOS), go to the *VPN* tab.
2. Select the desired VPN tunnel.
3. Tap *SAML Login*.
4. FortiClient displays an identity provider authorization page. Enter your login credentials. Tap *Login*. Once authenticated, FortiClient establishes the SSL VPN tunnel.

Creating a Mobileconfig profile

You can create a Mobileconfig profile to enable FortiClient (iOS) features, such as Web Filter and VPN:

Configuring a Mobileconfig profile to enable Web Filter

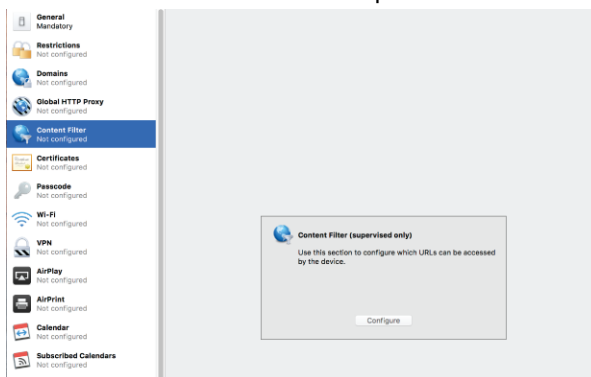
To enable Web Filter, the iOS device must be supervised and you must install a Mobileconfig profile with a content filter on the device. Installing a mobileconfig profile requires the following:

- 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 Filter:

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:

Filter Name	FortiClient
Identifier	com.fortinet.forticlient.fabricagent
Service Address	fgd1.fortigate.com
Organization	Fortinet, Inc.
User Name	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
Filter WebKit Traffic	Select the <i>Filter WebKit Traffic</i> checkbox.

8. Click Save.

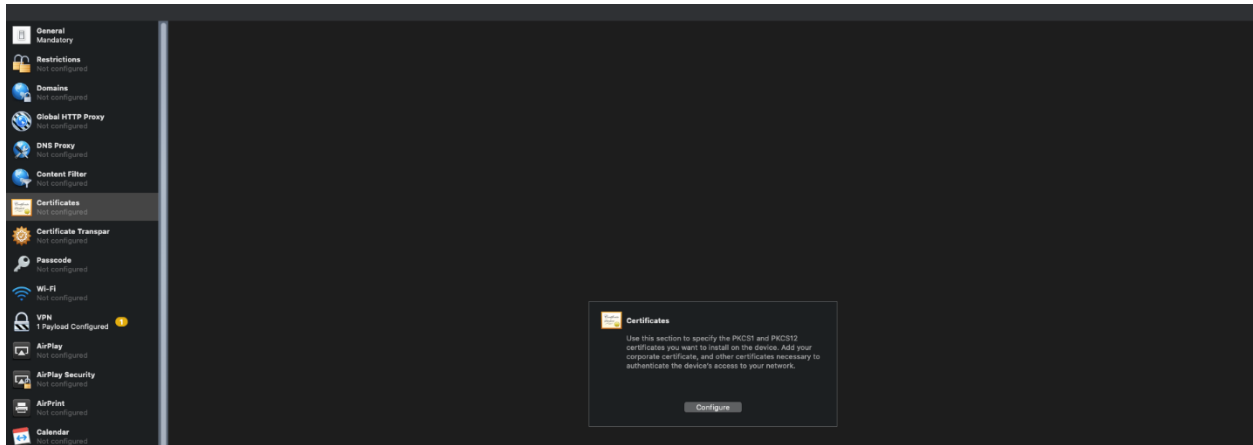


Due to restrictions that Apple set, you must launch FortiClient (iOS) once before the configuration takes effect. You can use EMS Zero Trust tagging rules to ensure users launch FortiClient (iOS) before browsing the Internet. See [Adding a Zero Trust tagging rule set](#).

Configuring a Mobileconfig VPN profile to install certificates

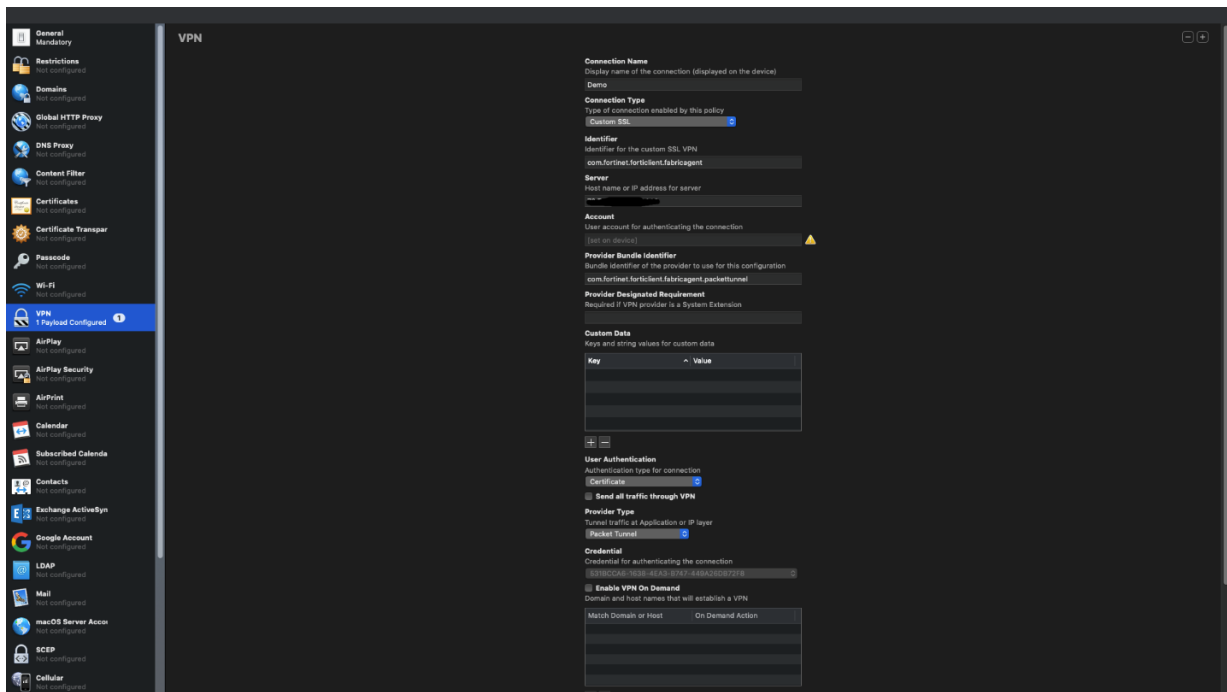
To configure a Mobileconfig VPN profile to install certificates:

1. In Apple Configurator 2, go to *File > New Profile*.
2. Go to *Certificates* and configure a certificate for VPN client authentication.

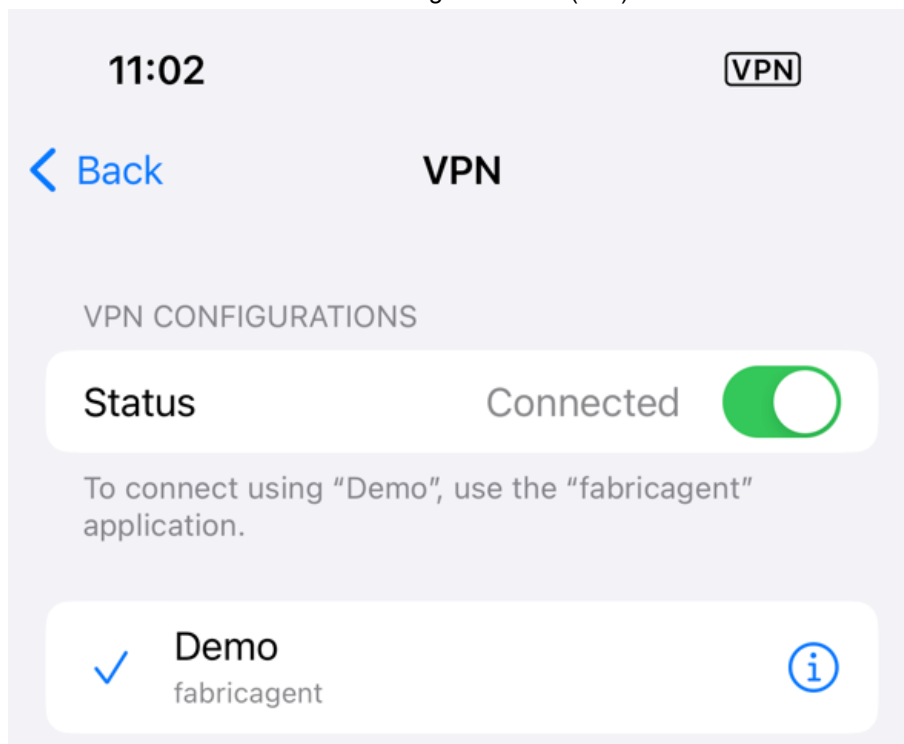


3. Go to *VPN*, and configure the following fields:
 - a. For *Connection Type*, select *Custom SSL*.
 - b. In the *Identifier* field, enter com.fortinet.forticlient.fabricagent.
 - c. In the *Server* field, enter the VPN server address as an IP address or fully qualified domain name.
 - d. In the *Provider Bundle Identifier* field, enter com.fortinet.forticlient.fabricagent.packettunnel.

- e. For *User Authentication*, select *Certificate*.



4. Install the Mobileconfig file on the device. This adds a VPN account to the device settings, which the end user cannot view in their FortiClient (iOS) application.
5. The end user can access the VPN profile from the iOS settings menu. Go to *General Settings > VPN & Device management > VPN*. Select the VPN profile, and connect. When the end user enables the VPN tunnel in settings, iOS launches an SSL VPN tunnel using FortiClient (iOS).



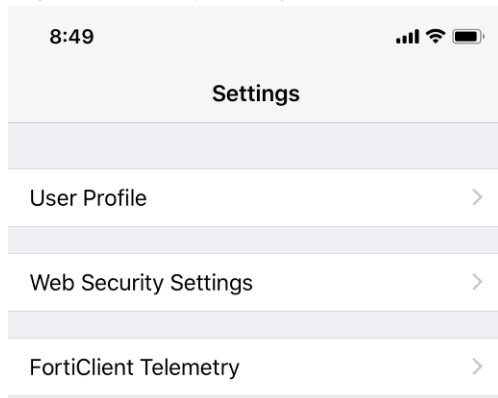
Web Filter



By default, FortiClient (iOS) disables Web Filter. To enable Web Filter, the iOS device must be supervised and you must install a Mobileconfig profile with a content filter on the device. See [Creating a Mobileconfig profile](#).

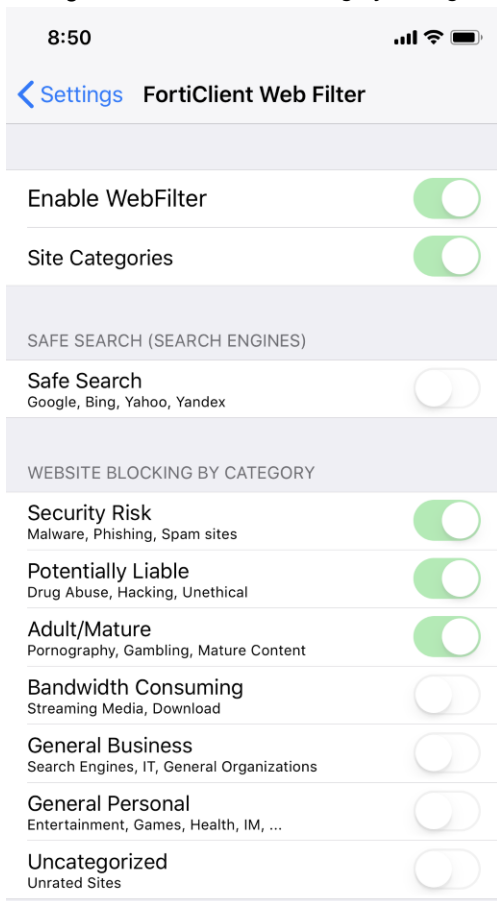
To configure Web Filter settings:

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.



Enter iPhone passcode for
"FortiClient"

FortiClient needs authentication

○ ○ ○ ○ ○ ○

1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
0		

Cancel



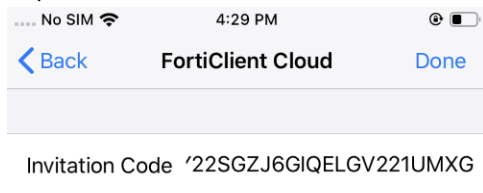
When FortiClient (iOS) blocks a website, a restricted website error page appears.

Zero Trust Telemetry

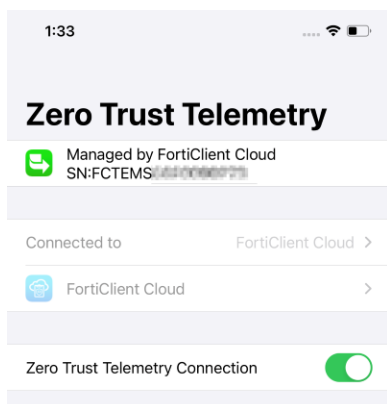
To connect Telemetry to on-premise EMS or FortiClient Cloud:

1. Go to *Zero Trust Telemetry*.
2. Do one of the following:
 - a. To automatically detect and connect to an on-premise EMS:
 - i. Enable *Zero Trust Telemetry Connection* by swiping right. When FortiClient detects a Telemetry server, a confirmation popup appears.

- ii. Tap *Send Zero Trust Telemetry Data* to connect to the server.
- b. To connect to an on-premise EMS by entering the server IP address:
 - i. Tap *Connect to*.
 - ii. In the *Select Connection* dialog, tap *EMS*.
 - iii. Enter the EMS server IP address. FortiClient (iOS) connects to the specified EMS server.
- c. To connect to an on-premise EMS or FortiClient Cloud using an invitation code:
 - i. Tap *Connect to*.
 - ii. In the *Select Connection* dialog, tap *EMS* or *FortiClient Cloud*.
 - iii. In the *Invitation Code* field, enter the invitation code.
 - iv. Tap *Done*.



When FortiClient (iOS) connects to EMS or FortiClient Cloud, it becomes managed and receives a license.



- iii. Scan the QR code with the device camera. You must allow FortiClient (iOS) permissions to access the device camera. FortiClient (iOS) automatically connects to the EMS server based on the scanned QR code.
- d. To connect to an on-premise EMS or FortiClient Cloud using a QR code:
 - i. Tap *Connect to*.
 - ii. In the *Select Connection* dialog, tap *Scan QR Code*.
 - iii. Scan the QR code with the device camera. You must allow FortiClient (iOS) permissions to access the device camera. FortiClient (iOS) automatically connects to the EMS server based on the scanned QR code.

To specify a Zero Trust Telemetry server:

1. Tap *Specify Preferred Host*.
2. Enter *Host* and *Port*.
3. If the EMS administrator has enabled multitenancy, in the *Site* field, enter the site name.
4. Tap *Done*.



You can use the mobileconfig file to preconfigure a Telemetry preferred host. Once FortiClient starts, it uses this preferred host to register. See [Creating a Mobileconfig profile on page 7](#).

User profile

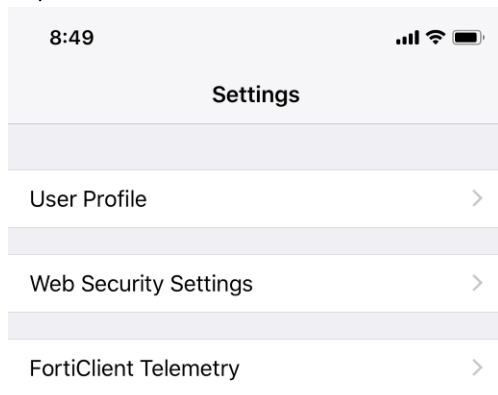
You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Facebook

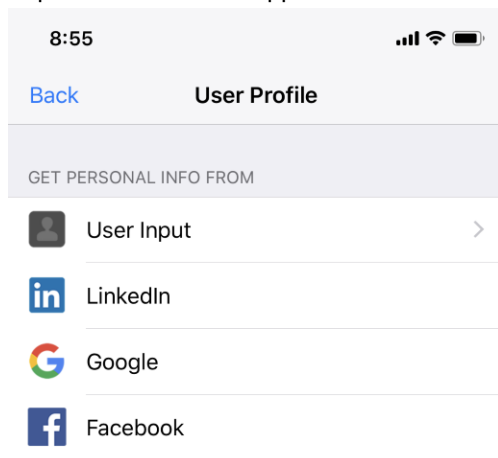
You can also manually add or edit a name, phone number, and email address in FortiClient. FortiClient (iOS) sends this user data to FortiClient EMS, where it displays on the *Endpoints* content pane.

To retrieve user details from a cloud application:

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



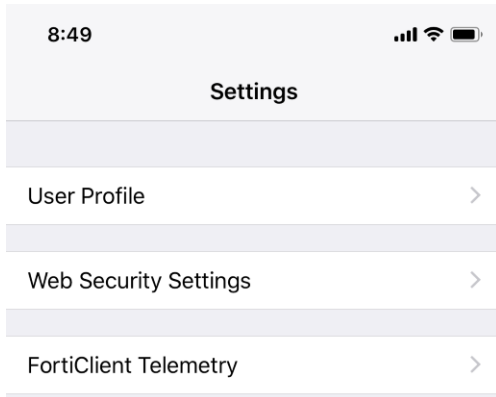
3. Tap the desired cloud application.



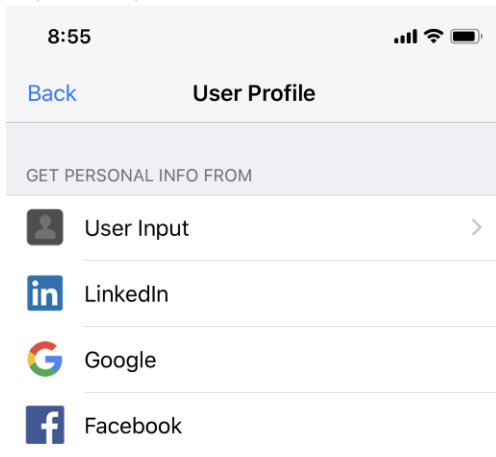
4. If you are not logged into the cloud application already on this device, you must log in. Grant FortiClient (iOS) permission to use your information.

To add user details manually:

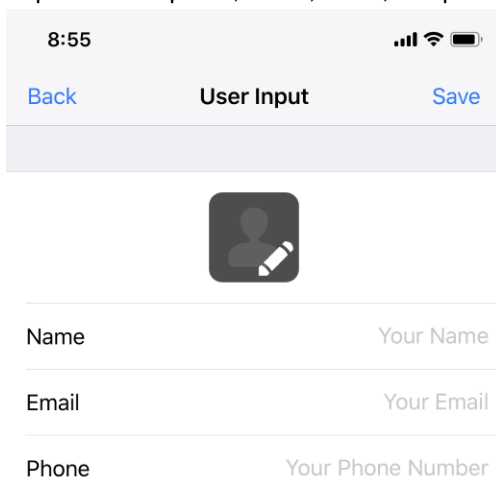
1. Tap *Settings* at the bottom of the screen.
2. Tap *User Profile*.



3. Tap *User Input*.



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



5. Tap *Save*.

SSL VPN

FortiClient (iOS) supports the following ways to add a VPN connection:

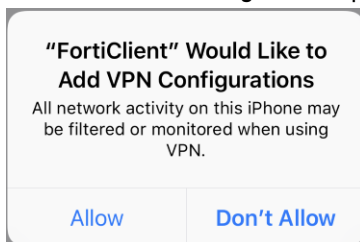
- Manually configure the VPN tunnel settings in the FortiClient (iOS) app. See [To manually configure a VPN connection: on page 16](#).
- Provision a VPN tunnel in EMS and assign the profile to the mobile device. See [To provision a VPN tunnel in EMS and assign the profile to the mobile device: on page 17](#).
- Scan a QR code to load VPN tunnel settings. See [To scan a QR code to load VPN tunnel settings: on page 17](#).
- Receive a VPN configuration via a Mobileconfig profile. See [Configuring a Mobileconfig VPN profile to install certificates on page 8](#).

FortiClient (iOS) also supports the following configurations for VPN:

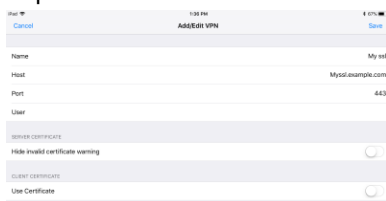
- To configure per-application VPN, see the following:
 - [Workspace ONE Per-application VPN](#)
 - [Intune Per-application VPN](#)
- To push certificates for VPN authentication to FortiClient (iOS), see [Pushing certificates for VPN authentication to FortiClient \(iOS\)](#).

To manually configure a VPN connection:

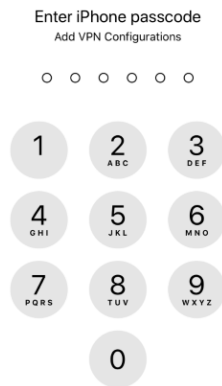
1. In the *Add VPN Configurations* popup, tap *Allow*.



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 fields as desired.



4. Enter your passcode to confirm adding the VPN.



5. Tap *Done* twice.



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

To provision a VPN tunnel in EMS and assign the profile to the mobile device:

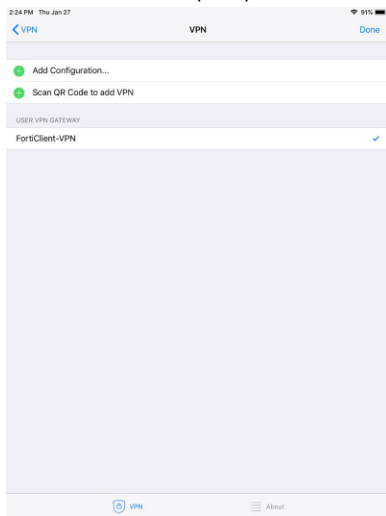
In the following instructions, the FortiClient end user takes some steps, while the FortiClient EMS administrator takes others.

1. (FortiClient (iOS) end user) Connect FortiClient to EMS. See [Zero Trust Telemetry on page 12](#).
2. (EMS administrator) Configure an endpoint profile in EMS to apply to the iOS device.
3. (EMS administrator) Configure the desired SSL VPN settings in the profile that they created in step 2. See [SSL VPN](#).

To scan a QR code to load VPN tunnel settings:

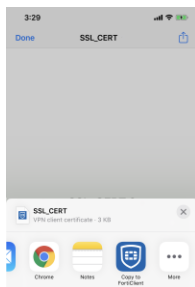
1. In the *Add VPN Configurations* popup, tap *Allow*.
2. Tap *VPN* at the bottom of the screen to switch to the VPN page.
3. Select *Scan QR Code to add VPN*.

- Once FortiClient (iOS) has scanned the code, the VPN menu lists the new tunnel.



To install a certificate received via email:

- Open the email, then download the received certificate. The certificate must have the .fctp12 extension for FortiClient (iOS) to import it. If the certificate does not have the .fctp12 extension, rename it so that it does.
- After downloading the certificate, select *Copy to FortiClient*. FortiClient (iOS) imports the certificate.



- In FortiClient (iOS), go to the *VPN* tab.
- Edit a VPN tunnel and enable *Use Certificate*.
- Tap *File Name*.
- Select the certificate imported earlier.
- On the *Add/Edit VPN* page, enter a passphrase to initiate the VPN connection.

Enterprise mobility management

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

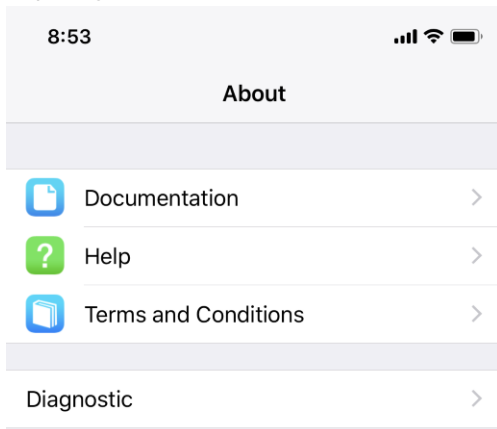
- [Configuring Workspace ONE integration to allow FortiClient \(iOS\) to connect to EMS](#)
- [Configuring Microsoft Intune integration to allow FortiClient \(iOS\) to connect to EMS](#)
- [Configuring Jamf integration to allow FortiClient \(iOS\) to connect to EMS](#)

Logs

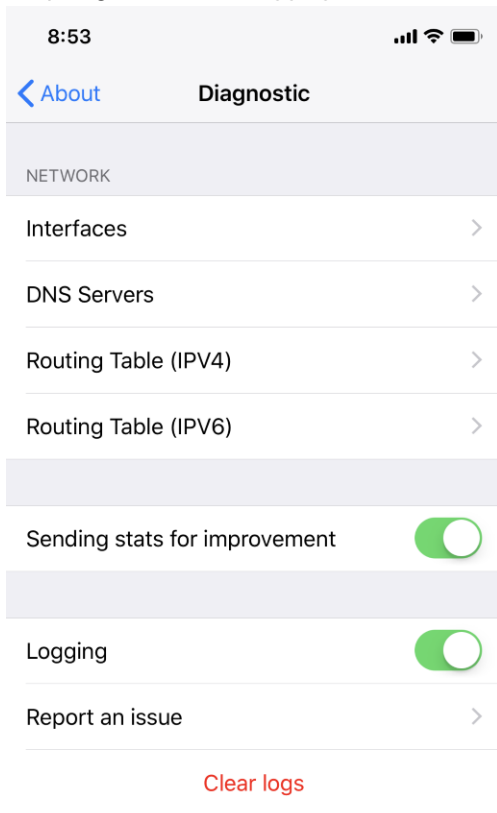
You can email FortiClient (iOS) logs to Fortinet.

To email logs to Fortinet:

1. Tap *About*.
2. Tap *Diagnostic*.



3. Swipe right to enable *Logging*.



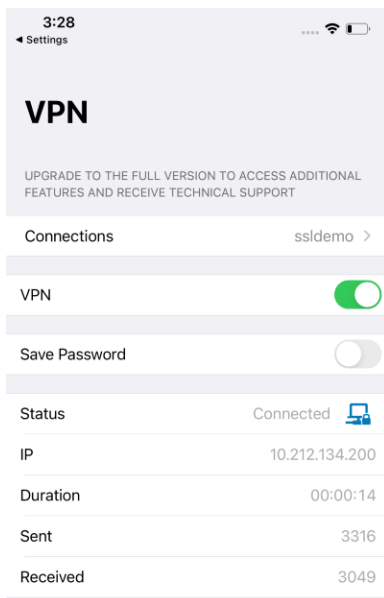
4. Tap *Email Logs*.

Standalone VPN client

You can download a [VPN-only FortiClient \(iOS\) app](#). This app is free, supports basic 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 (iOS) requires registration to EMS. Each endpoint registered with EMS requires a license seat on EMS.

When you launch the free VPN-only FortiClient (iOS) 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 (iOS) resembles doing the same on the full-featured FortiClient (iOS). See [SSL VPN on page 16](#) for details.



Change log

Date	Change Description
2023-08-15	Initial release.
2023-08-25	Updated Configuring Workspace ONE integration.
2023-12-12	Updated: <ul style="list-style-type: none">• Configuring Workspace ONE integration• Configuring Jamf integration• Configuring Microsoft Intune integration
2024-01-11	Updated Enterprise mobility management on page 19 .
2024-01-30	Updated SSL VPN on page 16 .



www.fortinet.com

Copyright© 2024 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.