



FortiClient iOS - Administration Guide

Version 6.2

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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



March 03, 2020

FortiClient iOS 6.2 Administration Guide

04-620-576352-20200303

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
Fabric Telemetry	13
User profile	16
Enterprise mobility management	19
Configuring AirWatch integration	19
Configuring Jamf integration	25
Configuring Microsoft Intune integration	30
Logs	33
Change log	35

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.

You must license FortiClient iOS for use. You can license FortiClient iOS by applying the license to EMS, then connecting Telemetry from FortiClient iOS to EMS. See [Fabric Telemetry on page 13](#).

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

Features

Feature	Description
SSL VPN (tunnel mode)	SSL VPN in tunnel mode supports the following: <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)• 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.

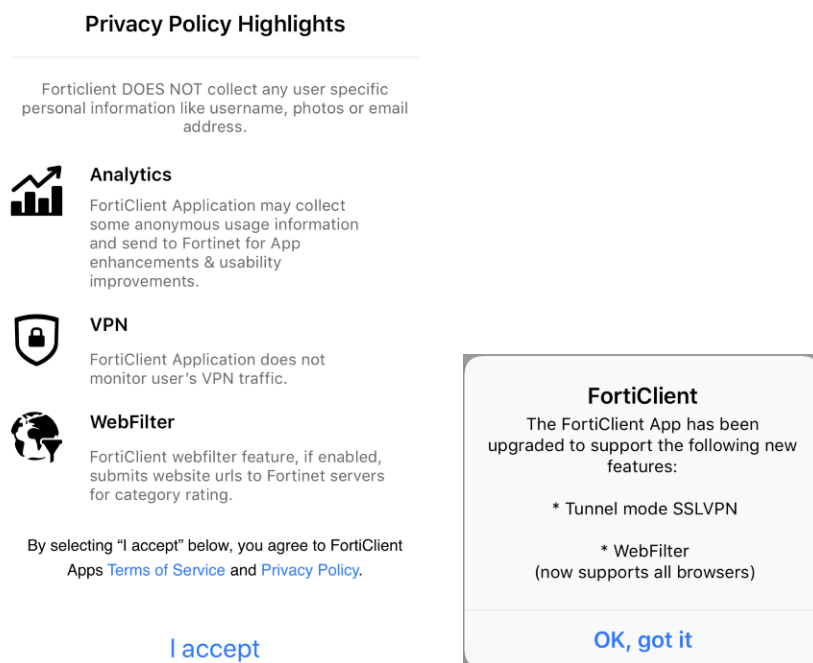
Supported platforms

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

Initial configuration

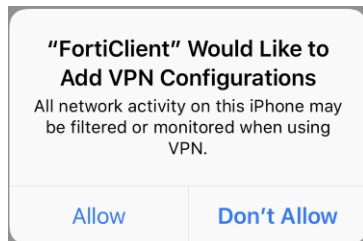
Running FortiClient iOS

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.

iPad 1:36 PM 67%

Cancel Add/Edit VPN Save

Name My ssl

Host Myssl.example.com

Port 443

User

SERVER CERTIFICATE

Hide invalid certificate warning ☐

CLIENT CERTIFICATE

Use Certificate ☐

Enter iPhone passcode
Add VPN Configurations

○ ○ ○ ○ ○ ○

1 2 3
4 5 6
7 8 9
0

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.

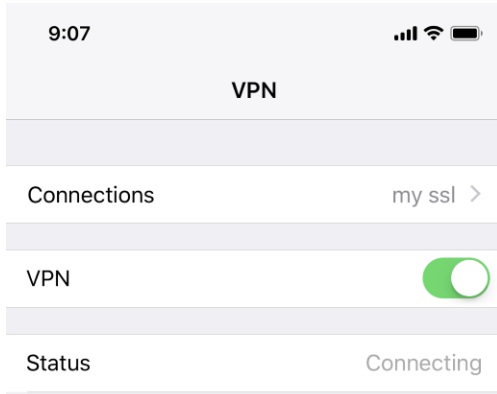
9:06

< VPN VPN Edit

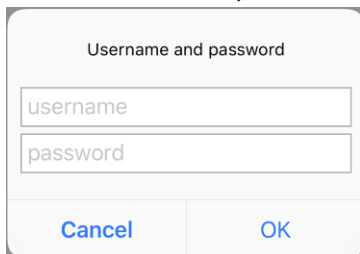
USER VPN GATEWAY

my ssl ✓

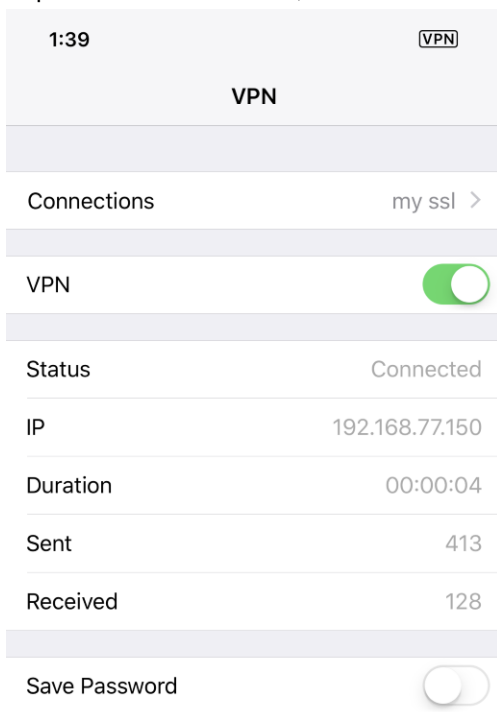
2. Tap the < button.
3. Swipe right to enable the VPN connection.



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



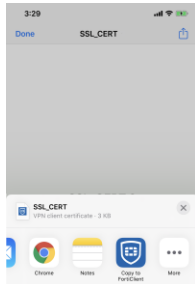
5. Tap OK. When connected, the tunnel interface IP, duration, and the bytes sent and received information display.



To install a certificate received via email:

This feature is only available for FortiClient iOS 6.2.3 and later versions.

1. 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.
2. After downloading the certificate, select *Copy to FortiClient*. FortiClient iOS imports the certificate.



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

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. Installing a mobileconfig profile requires the following:

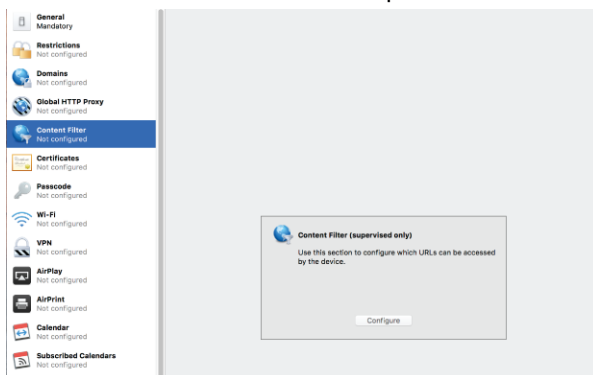
- Apple Configurator 2 (or equivalent mobile device management (MDM) application) installed.
- iOS devices are supervised.

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 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:

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 <code>ems.example.com</code> at port 8013, with key "ConnectionKey": <code>ems.example.com:8013 ConnectionKey</code>
Filter WebKit Traffic	Select the <i>Filter WebKit Traffic</i> checkbox.
Filter Socket Traffic	Deselect the <i>Filter Socket 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 compliance verification rules to ensure users launch FortiClient iOS before browsing the Internet. See the [FortiClient EMS Administration Guide](#).

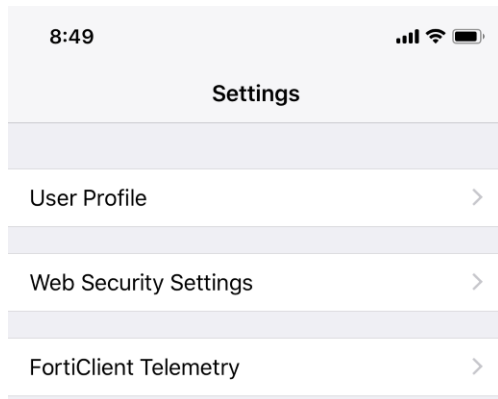
Web Filtering



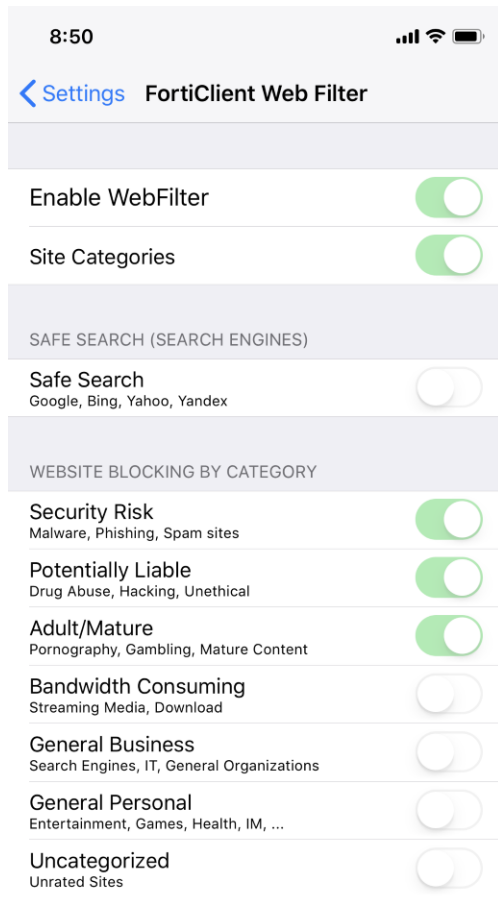
By default, FortiClient iOS disables Web Filtering. To enable Web Filtering, the iOS device must be supervised and you must install a Mobileconfig profile with a content filter on the device. See [Creating a Mobileconfig profile](#).

To configure the Web Filtering settings:

1. Tap *Settings*.
2. Tap *Web Security Settings*.



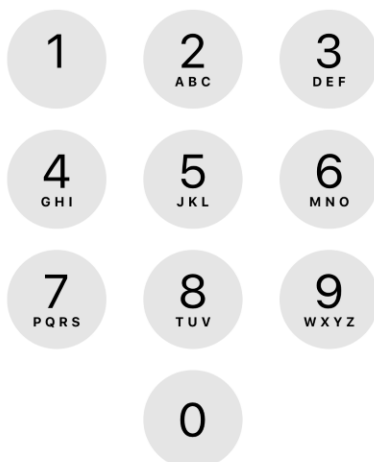
3. Enter the passcode in the *FortiClient Authentication* popup.
4. Enable the *Web Filter* by swiping right.
5. Configure the *Website Blocking by Categories* to suit requirements.



Enter iPhone passcode for
"FortiClient"

FortiClient needs authentication

○ ○ ○ ○ ○ ○



Cancel

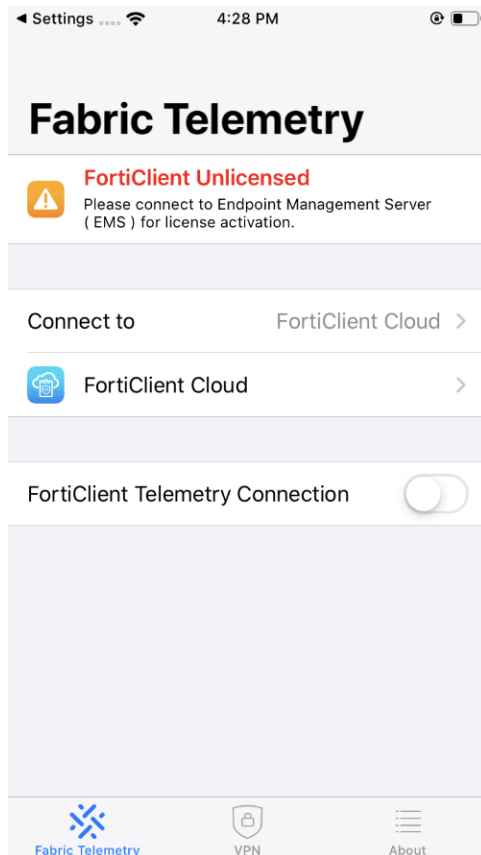


When FortiClient iOS blocks a website, a restricted website error page appears.

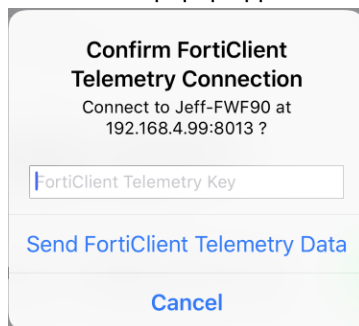
Fabric Telemetry

To connect Telemetry to an on-premise EMS:

1. Tap *Settings* at the bottom of the screen.
2. Tap *Fabric Telemetry*.



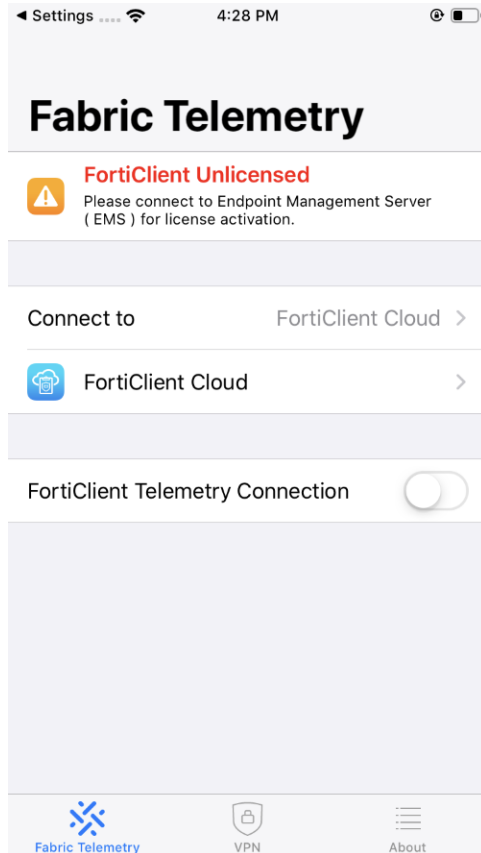
3. Enable *FortiClient Telemetry Connection* by swiping right. When FortiClient detects a Telemetry server, a confirmation popup appears.



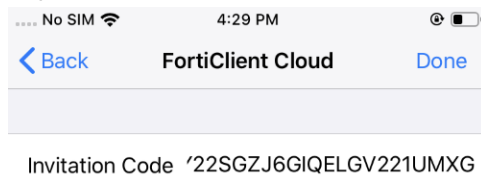
4. Tap *Send FortiClient Telemetry Data* to connect to the FortiTelemetry server.

To connect Telemetry to FortiClient Cloud:

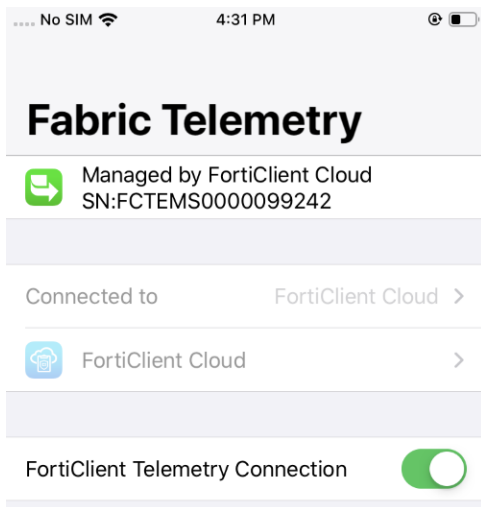
1. Tap *Settings* at the bottom of the screen.
2. Tap *Fabric Telemetry*.
3. Tap *Connect to*, then select *FortiClient Cloud*.



4. Tap *FortiClient Cloud*. In the Invitation Code field, enter the FortiClient Cloud invitation code. Tap *Done*.

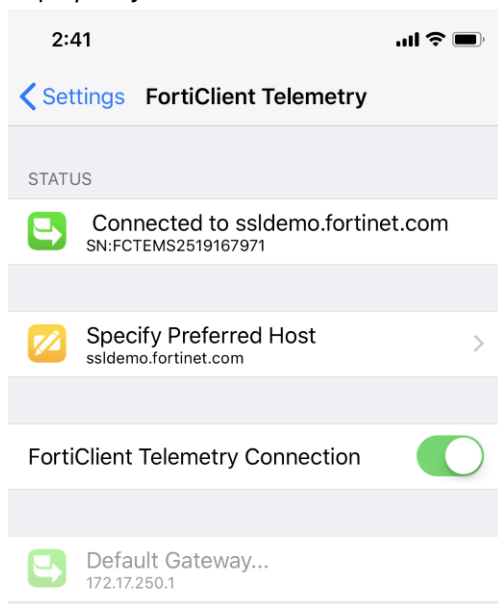


When FortiClient iOS achieves connection to FortiClient Cloud, it becomes managed by FortiClient Cloud and receives a license.

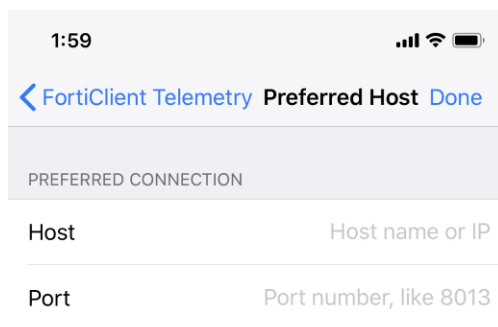


To specify a FortiTelemetry server:

1. Tap *Specify Preferred Host*.



2. Enter *Host* and *Port*.



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

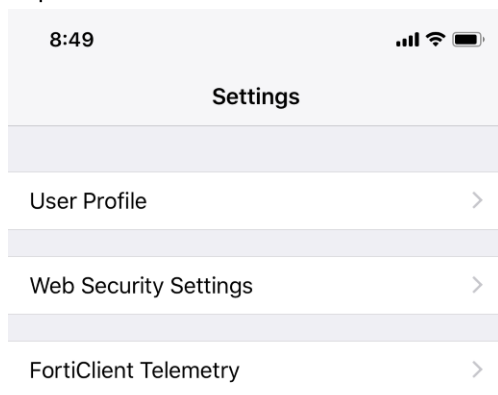
You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Facebook

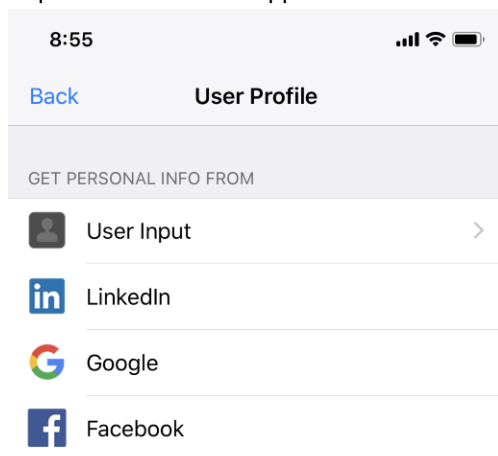
You can also manually add or edit a name, phone number, and email address in FortiClient. FortiClient iOS sends this user data to FortiClient EMS, where it displays on the *Endpoints* content pane.

To retrieve user details from a cloud application:

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



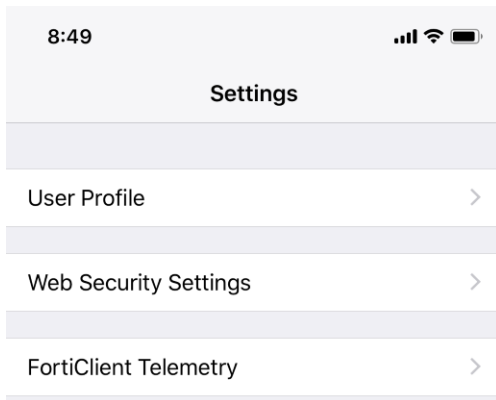
3. Tap the desired cloud application.



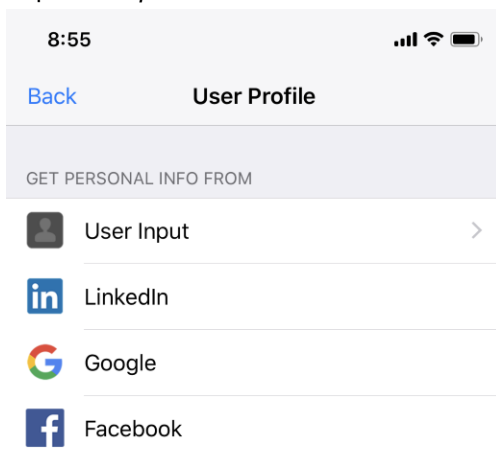
4. If you are not logged into the cloud application already on this device, you must log in. Grant FortiClient iOS permission to use your information.

To add user details manually:

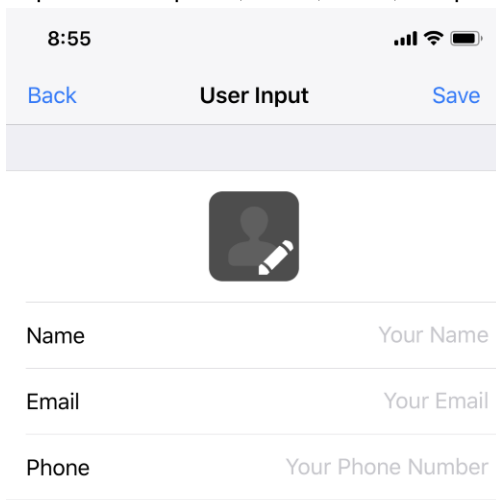
1. Tap *Settings* at the bottom of the screen.
2. Tap *User Profile*.



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. Integration with enterprise mobility management software allows FortiClient iOS endpoints to connect to EMS.

Configuring AirWatch integration

AirWatch integration allows FortiClient iOS endpoints to connect to EMS.

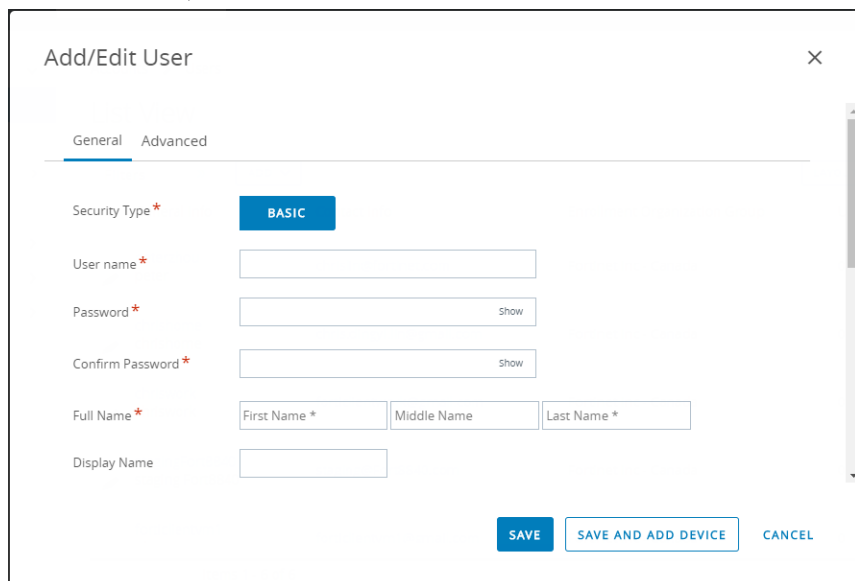
To configure integration between AirWatch and FortiClient iOS:

1. In AirWatch, go to *Groups & Settings > Assignment Groups*. Create a new assignment group.

The screenshot displays the Workspace ONE UEM console interface. The left sidebar contains navigation options: GETTING STARTED, HUB, DEVICES, ACCOUNTS, APPS & BOOKS, CONTENT, EMAIL, TELECOM, and GROUPS & SETTINGS (highlighted). The main content area is titled 'Assignment Groups' and shows a table of existing groups. The table has columns for Groups, Managed By, Group Type, Assignments, Exclusions, and Devices. The data rows are as follows:

Groups	Managed By	Group Type	Assignments	Exclusions	Devices
All Corporate Dedicated Devices	Fortinet Inc - Canada	Smart Group	1	0	1
All Corporate Shared Devices	Fortinet Inc - Canada	Smart Group	1	0	0
All Devices	Fortinet Inc - Canada	Smart Group	12	0	1
All Employee Owned Devices	Fortinet Inc - Canada	Smart Group	0	0	0
Fortinet Inc - Canada (Fortinet Inc - ...)	Fortinet Inc - Canada	Organization Group	1	0	1

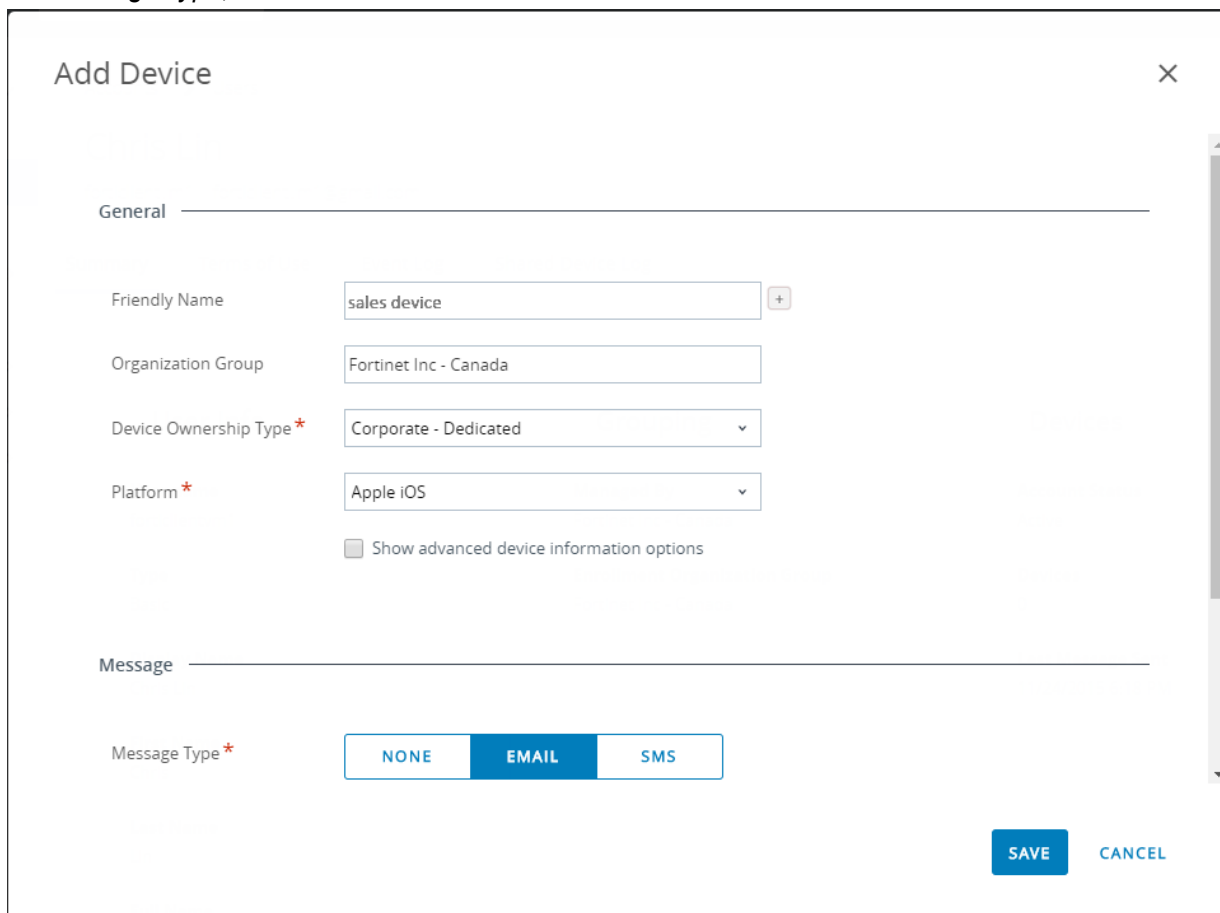
At the bottom of the page, there is a pagination bar showing 'Items 1 - 5 of 5' and a 'Page Size: 50' dropdown menu.

2. Go to *Accounts*, and add a new user.

The 'Add/Edit User' dialog box features a close button (X) in the top right corner. It has two tabs: 'General' (selected) and 'Advanced'. Under the 'General' tab, there is a 'Security Type' section with a blue 'BASIC' button. Below this are input fields for 'User name *', 'Password *' (with a 'Show' link), and 'Confirm Password *' (with a 'Show' link). The 'Full Name *' field is split into 'First Name *', 'Middle Name', and 'Last Name *'. There is also a 'Display Name' field. At the bottom right, there are three buttons: 'SAVE' (blue), 'SAVE AND ADD DEVICE' (blue), and 'CANCEL' (light blue).

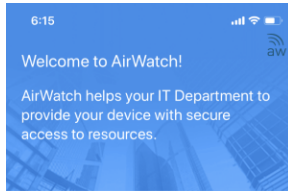
3. Add a new device for the user:

- 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*.



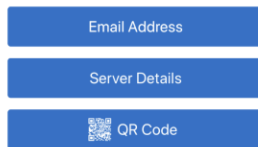
The 'Add Device' dialog box has a close button (X) in the top right corner. It features a 'General' tab. Under this tab, there are input fields for 'Friendly Name' (containing 'sales device' and a '+' icon), 'Organization Group' (containing 'Fortinet Inc - Canada'), 'Device Ownership Type *' (a dropdown menu set to 'Corporate - Dedicated'), and 'Platform *' (a dropdown menu set to 'Apple iOS'). Below these is a checkbox labeled 'Show advanced device information options'. A 'Message' section follows, containing a 'Message Type *' field with three buttons: 'NONE', 'EMAIL' (selected), and 'SMS'. At the bottom right, there are 'SAVE' (blue) and 'CANCEL' (light blue) buttons.

- 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.



The multi-step enrollment process begins with authentication.

Choose authentication method:



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

A screenshot of the AirWatch web console 'Edit Application - FortiClient' page. The page has a header with the FortiClient logo, status 'Public', 'Status: Active', 'Managed By: Fortinet Inc - Canada', and 'Application ID: com.fortinet.forticlient'. Below the header are tabs for 'Details', 'Terms of Use', and 'SDK'. The 'Details' tab is active. It shows a large input field for 'Name' with 'FortiClient' entered. Below the name field is a 'View in App Store' link and creation/modification dates. There is an 'UPLOAD' button next to the app icon. At the bottom, there is a 'Categories' section with a dropdown menu showing 'Utilities (System)'. At the very bottom are 'SAVE & ASSIGN' and 'CANCEL' buttons.

6. When adding an assignment, scroll to the bottom and enable *Application Configuration*. Optionally, you can add key-value pairs as shown.

FortiClient - Add Assignment

☒ Managed if User Installed
 ☐ Disabled

App Tunneling: ☒ Enabled ☐ Disabled

Application Configuration: ☒ Enabled ☐ Disabled

Enter Key-Value pairs to configure applications for users:

Configuration Key	Value Type	Configuration Value
mac_address	String	{DeviceWLANMac}
udid	String	{DeviceUid}
group_tag	String	field_engineer

This enables FortiClient iOS to read the MAC address and UDID from the iOS device. FortiClient sends this information to EMS.

The following shows the configuration for a FortiClient iOS device that will connect Telemetry to FortiClient Cloud:

FortiClient Fabric Agent - Add Assignment

Adaptive Management Level: **Managed Access**

Apply policies that give users access to apps based on administrative management of devices.

Would you like to enable Data Loss Prevention (DLP)?

DLP policies provide controlled exchange of data between managed and unmanaged applications on the device. To prevent data loss on this application, make it "Managed Access" and create "Restriction" profile policies for desired device types

Managed Access: ☒ Enabled ☐ Disabled

App Tunneling: ☒ Enabled ☐ Disabled

Application Configuration: ☒ Enabled ☐ Disabled

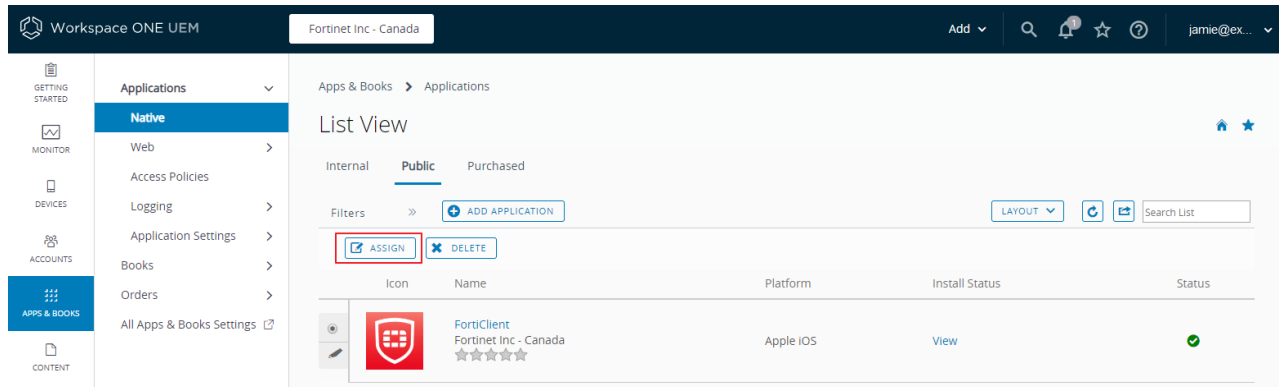
Enter Key-Value pairs to configure applications for users:

Configuration Key	Value Type	Configuration Value
cloud_invite_code	String	V1A8FKMFMH37QEMFW8ROD0 QZP8R3DYW6

Supported keys include the following:

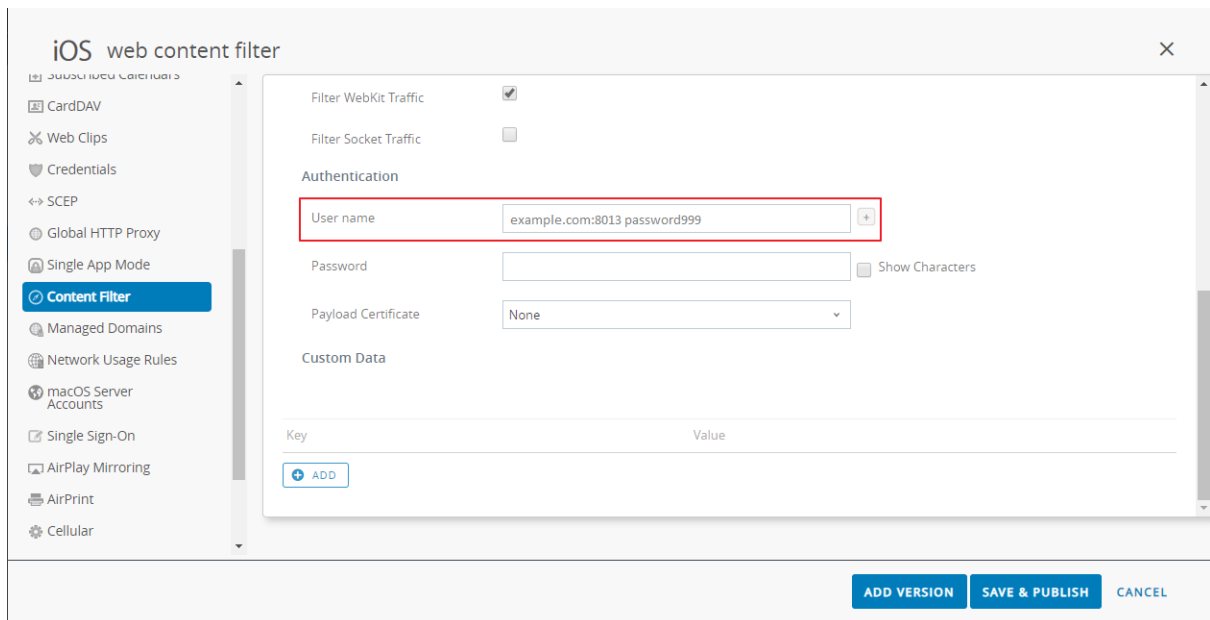
Key	Description
mac_address	The iOS device's MAC address.
udid	The iOS device's UDID.
group_tag	This value is used as a group tag for configuration in EMS. In the example below, the string "field_engineer" is used as a group tag, which is used when FortiClient iOS initially connects to EMS. See <i>Group assignment rules</i> in the FortiClient EMS Administration Guide .
cloud_invite_code	This value is used for connecting FortiClient iOS to FortiClient Cloud. Enter the invite code received from FortiClient Cloud.

7. You can add more assignments and use different group_tag values.

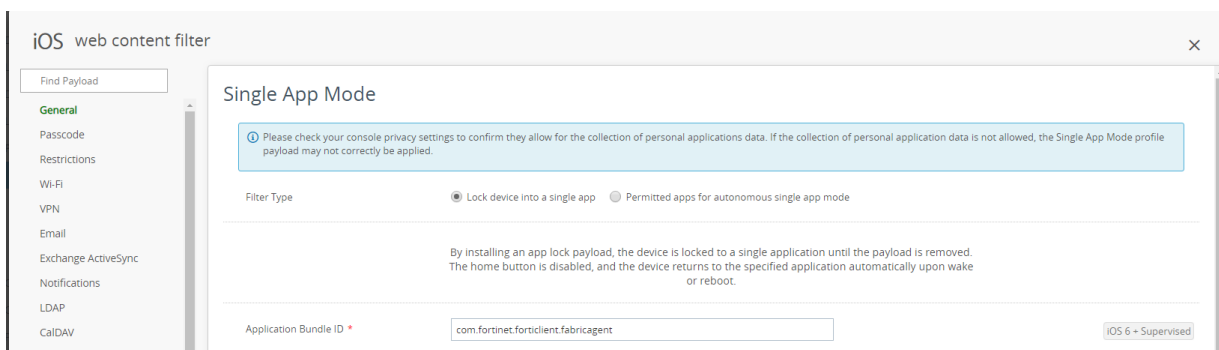


8. Go to *Devices*, and add a profile:

- a. Go to the *Content Filter* section. In the *User name* field, enter the EMS URL.

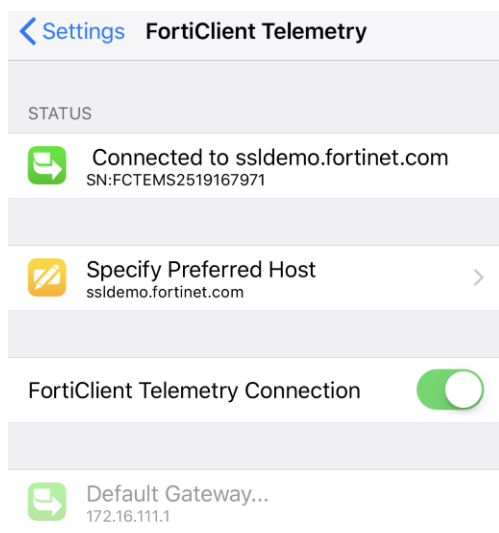


- b. Go to *Single App Mode*, and configure as shown below to enable single app mode. This makes FortiClient iOS run.

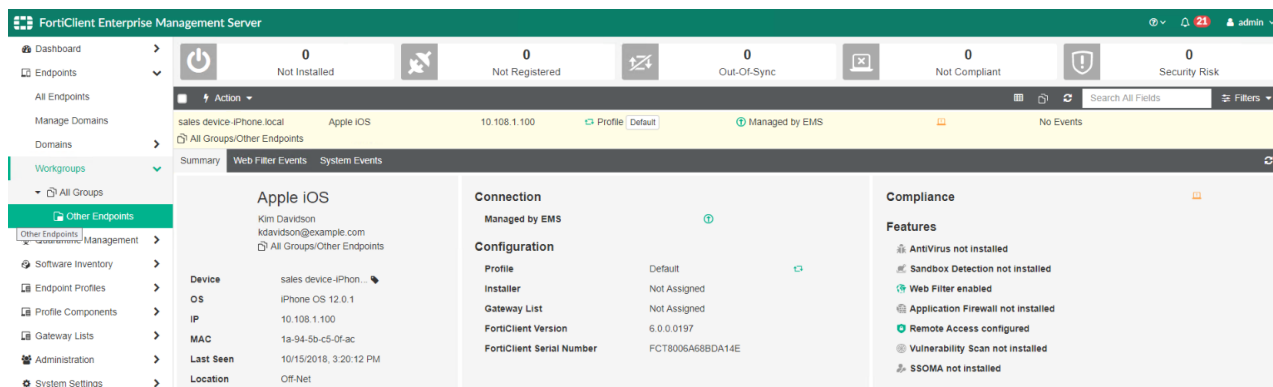


c. Assign the profile to the device.

9. When FortiClient starts on the device, it automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration. Once FortiClient connects to EMS, disable single app mode for the device. Keep the EMS URL in the *Content Filter* section.



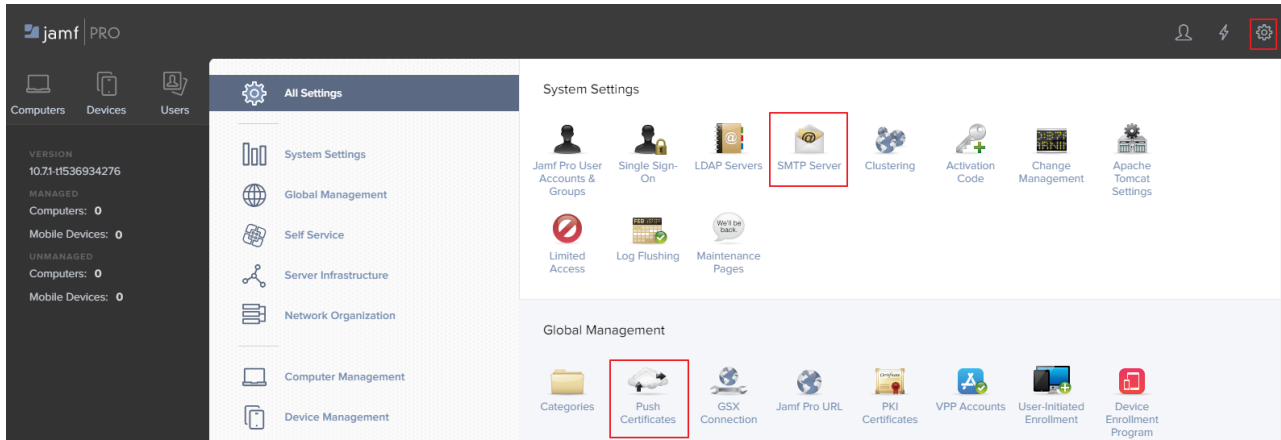
The below shows the on-premise EMS GUI after FortiClient iOS connects Telemetry.



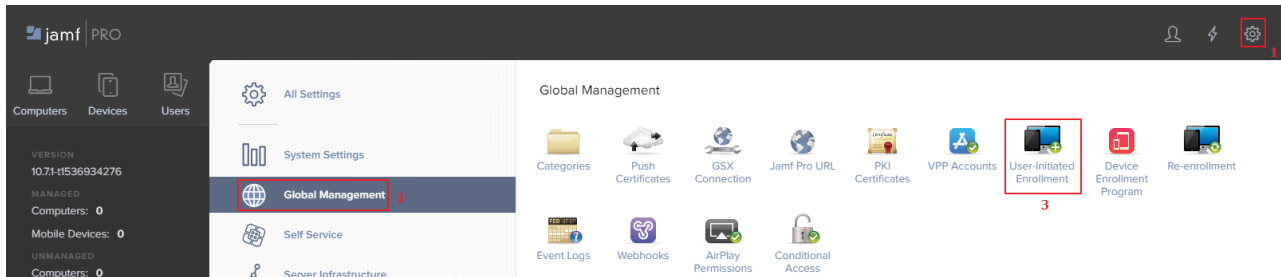
Configuring Jamf integration

To configure integration between Jamf and FortiClient iOS:

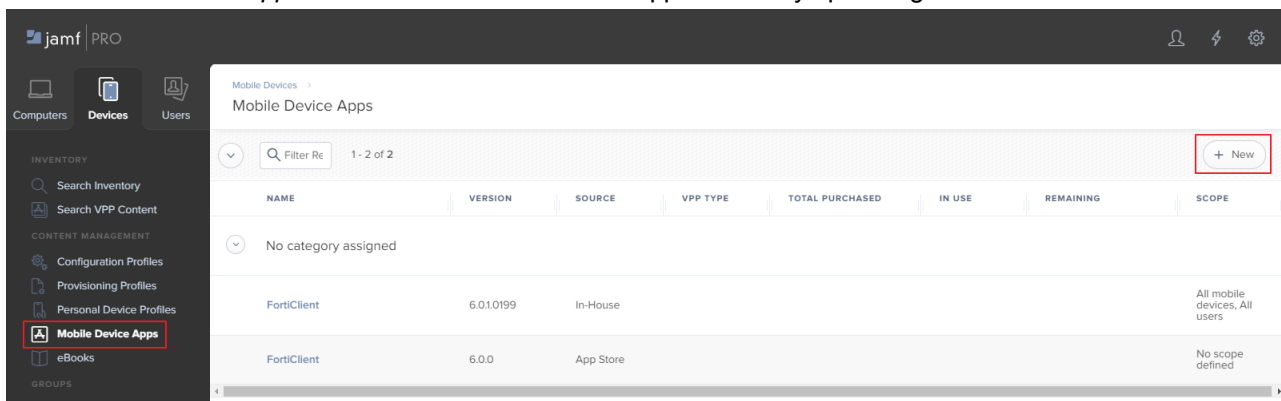
1. In Jamf, go to *All Settings*. Configure the settings in *SMTP Server* and *Push Certificates*.



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.

Mobile Devices > Mobile Device Apps > FortiClient for field engineer

General Scope VPP App Configuration

DISPLAY NAME Display name for the app
FortiClient for field engineer

☒ Enabled

CATEGORY Category to add the app to
None

VERSION Version of the app
6.0.0

BUNDLE IDENTIFIER Bundle identifier for the app
com.fortinet.forticlient

☒ Free
App is free

DISTRIBUTION METHOD Method to use for distributing the app
Install Automatically/Prompt Users to Install

☐ Display app in Self Service after it is installed

Cancel Save

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:

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

Mobile Devices > Mobile Device Apps > FortiClient for field engineer

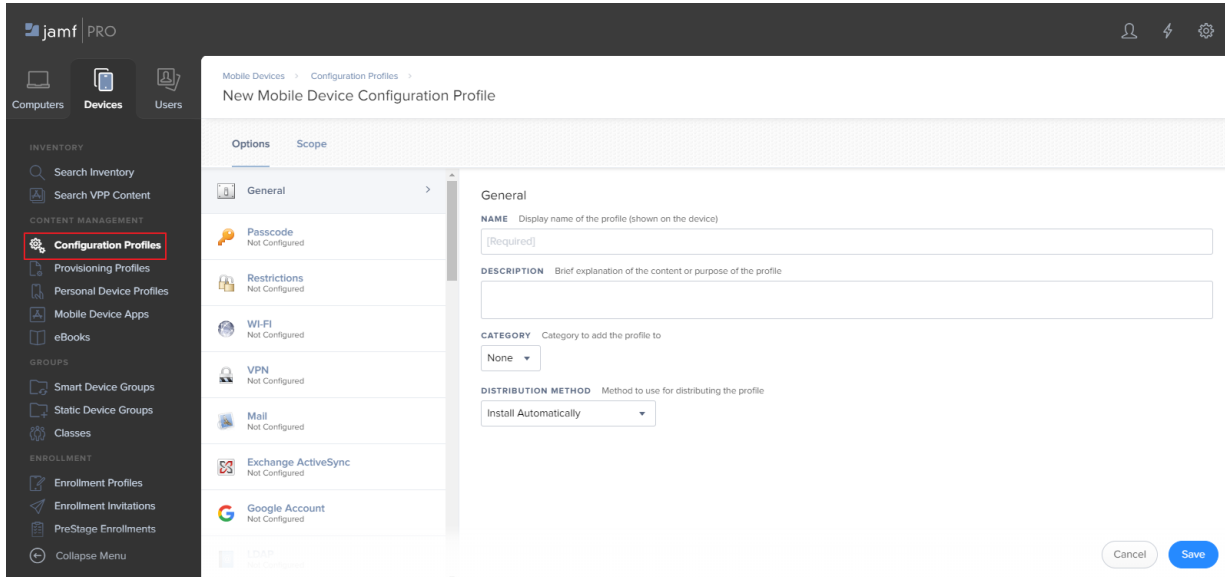
General Scope VPP App Configuration

PREFERENCES Configuration dictionary to be applied to the app on mobile devices with iOS 7 or later

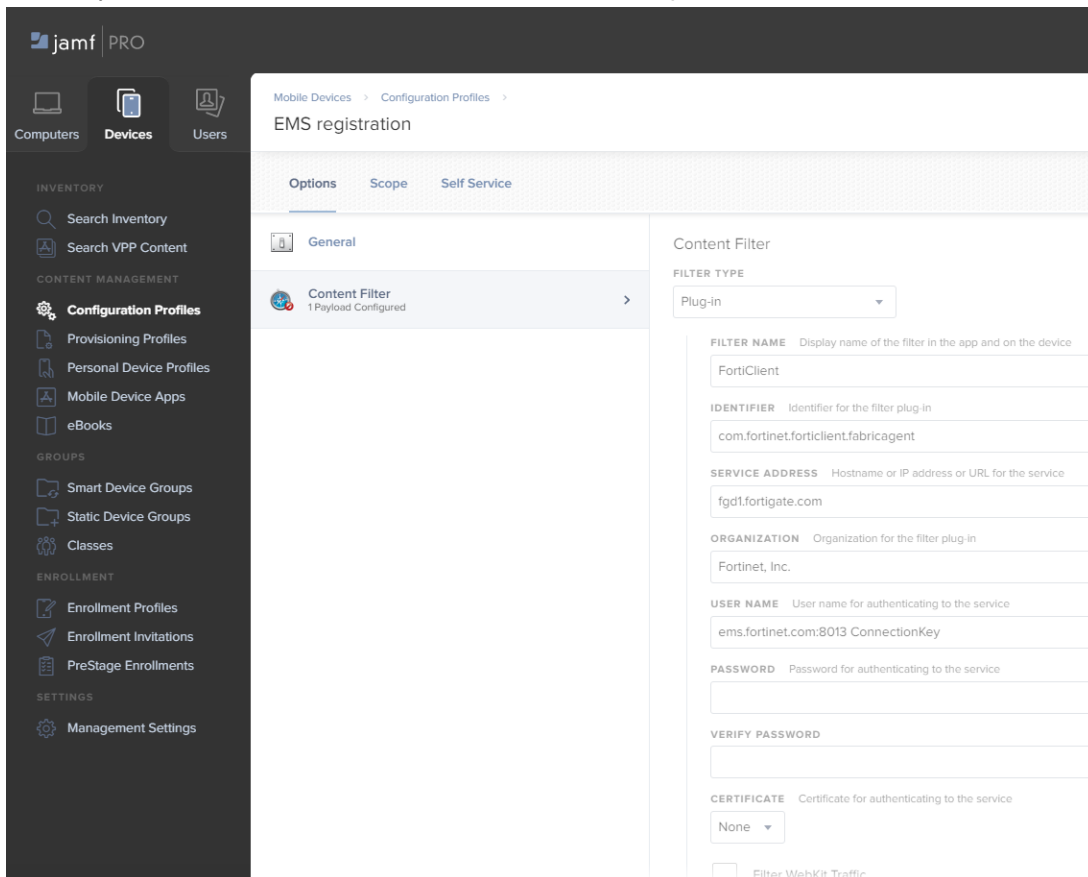
```
<dict>
  <key>mac_address</key>
  <string>$MACADDRESS</string>
  <key>udid</key>
  <string>$UUID</string>
  <key>group_tag</key>
  <string>field_engineer</string>
</dict>
```

6. Configure a configuration profile:

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

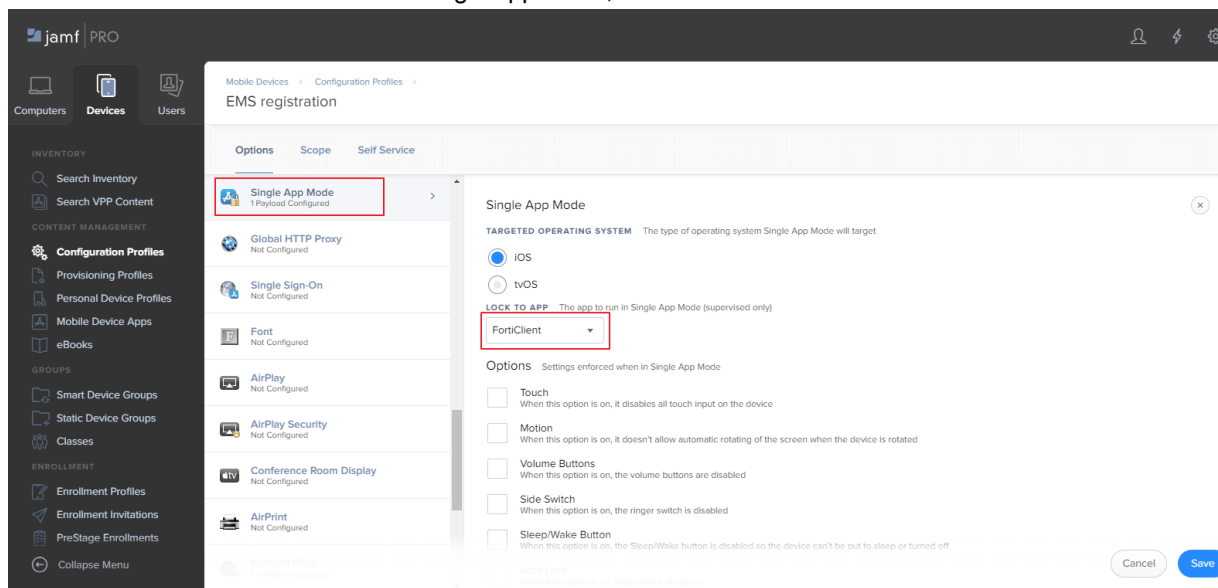


- b. Under *Options*, select *Content Filter*. Add a content filter to point to the desired EMS.



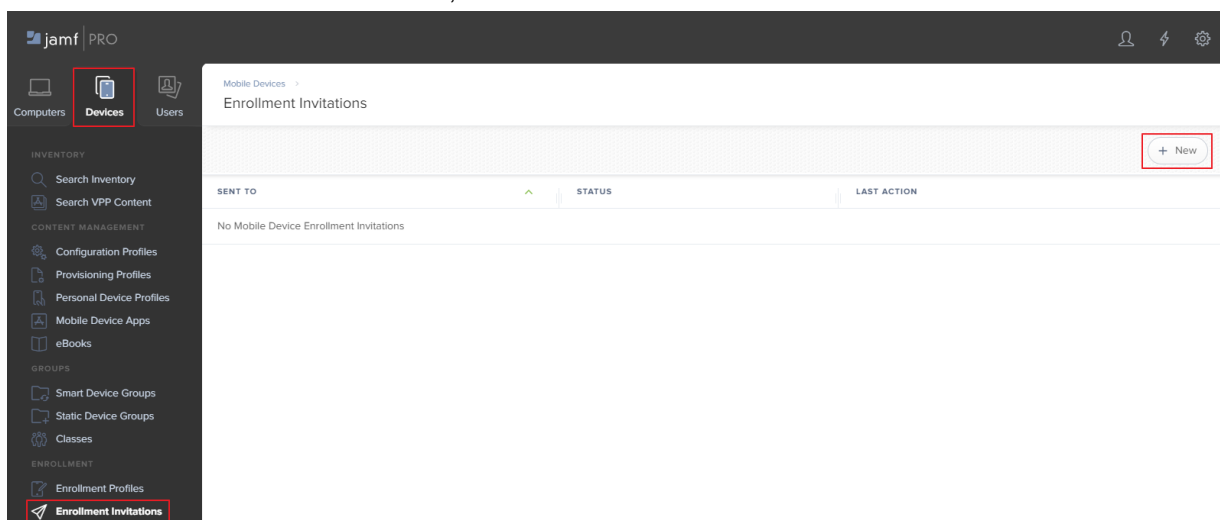
- c. Enable *Single App Mode* for FortiClient. Single app mode launches the FortiClient app and connects it to

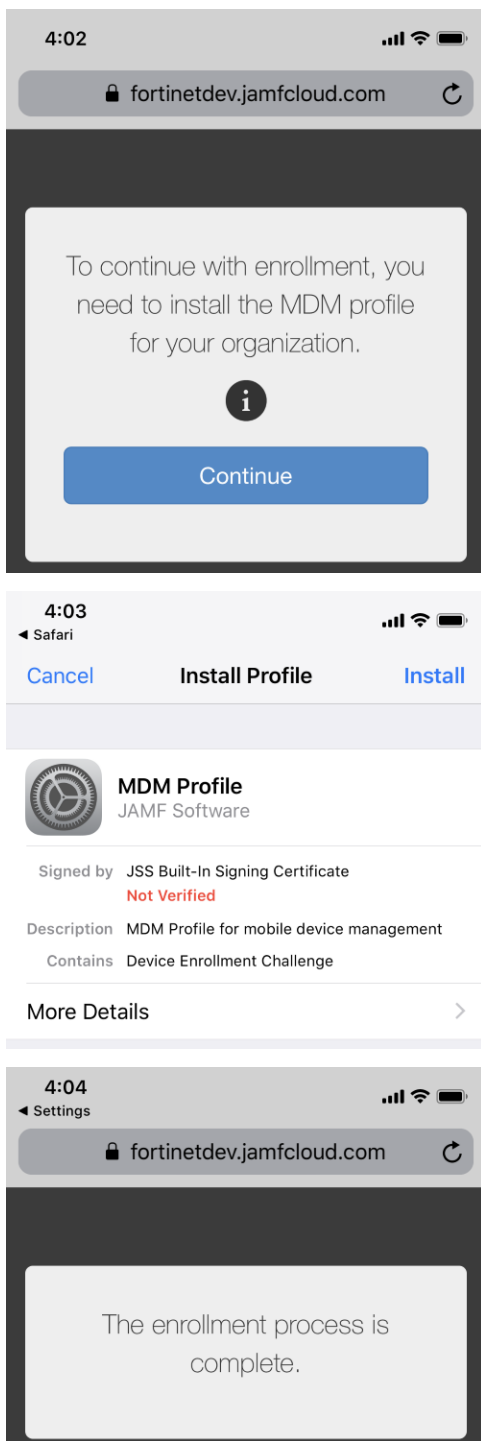
EMS. If FortiClient is not launched in single app mode, it does not connect to EMS.



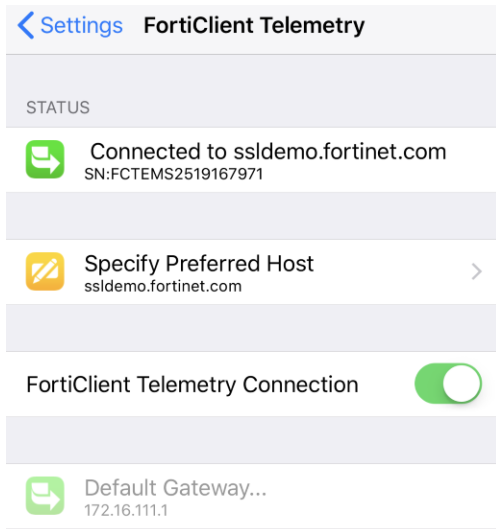
7. Enroll the device:

- a. Go to **Devices > Enrollment Invitations**, then send an enrollment invitation to the device.

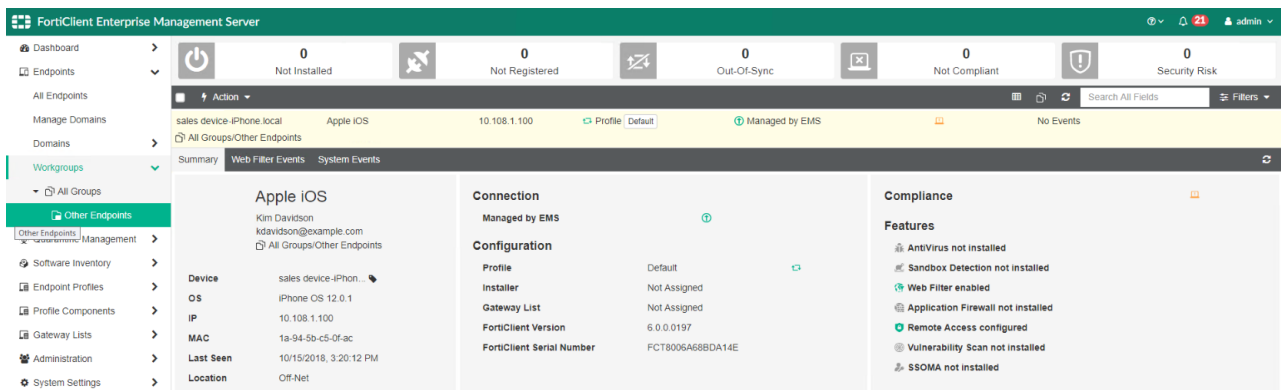


b. Enroll the device.

8. When the device is enrolled, FortiClient iOS automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration. 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 on-premise EMS GUI after FortiClient iOS connects Telemetry.



Configuring Microsoft Intune integration

Intune integration allows FortiClient iOS endpoints to connect to EMS. FortiClient iOS 6.2.2 and later versions support integration with Intune.

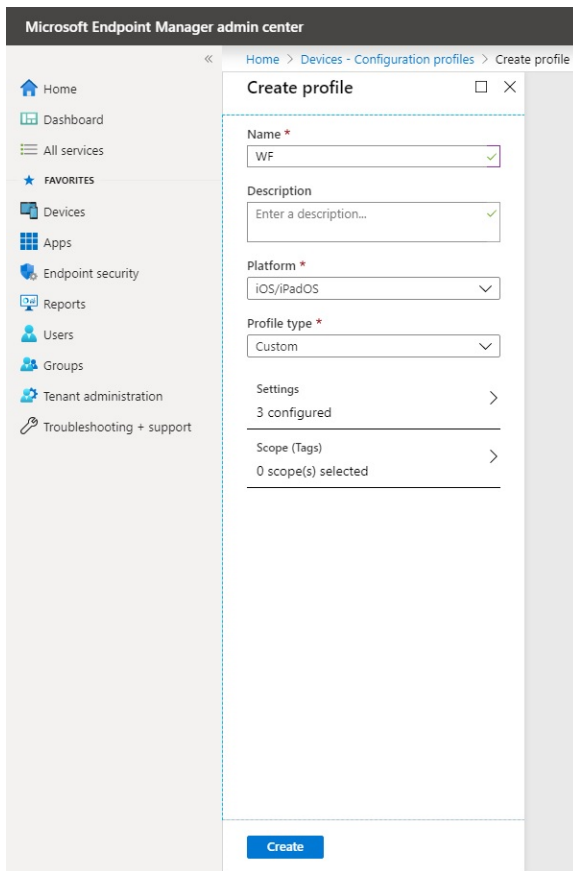
To configure Microsoft Intune integration:

1. Add FortiClient iOS to Microsoft Intune.
2. [Add the default instance for iOS using App Config](#). Supported App Config keys include the following:

Key	Description
mac_address	iOS device's MAC address.
udid	iOS device's UDID.

Key	Description
group_tag	This value is used as a group tag for configuration in EMS. For example, you can use the string "field_engineer" as a group tag, which is used when FortiClient iOS initially connects to EMS. See Group assignment rules .
cloud_invite_code	This value is used for connecting FortiClient iOS to FortiClient Cloud. Enter the invite code received from FortiClient Cloud.
user_name	FortiClient iOS username.
ems_server	EMS IP address or hostname.
ems_port	Port number for FortiClient iOS to connect Telemetry to EMS. By default, this is 8013.
ems_key	FortiClient Telemetry connection key. The EMS administrator may require FortiClient iOS to provide this key during connection.

3. To enable Web Filter:
 - a. Log in to [Microsoft Endpoint Manager admin center](#).
 - b. Go to *Devices - Configuration profiles*.
 - c. Click *Create profile*.
 - d. Configure the profile:
 - i. From the *Platform* dropdown list, select *iOS/iPadOS*.
 - ii. From the *Profile type* dropdown list, select *Custom*.
 - iii. From the *Custom configuration profile name* dropdown list, select the desired profile.
 - iv. In the *Configuration profile file* field, select the Web Filter Mobileconfig profile that you created in [Creating a Mobileconfig profile on page 9](#). Click *OK*.

e. Click *Create*.

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar contains navigation links: Home, Dashboard, All services, FAVORITES, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Create profile' and includes the following fields and sections:

- Name ***: A text input field containing 'WF' with a green checkmark.
- Description**: A text input field with the placeholder 'Enter a description...' and a green checkmark.
- Platform ***: A dropdown menu showing 'iOS/iPadOS'.
- Profile type ***: A dropdown menu showing 'Custom'.
- Settings**: A section with '3 configured' and a right-pointing chevron.
- Scope (Tags)**: A section with '0 scope(s) selected' and a right-pointing chevron.
- Create**: A blue button at the bottom of the form.

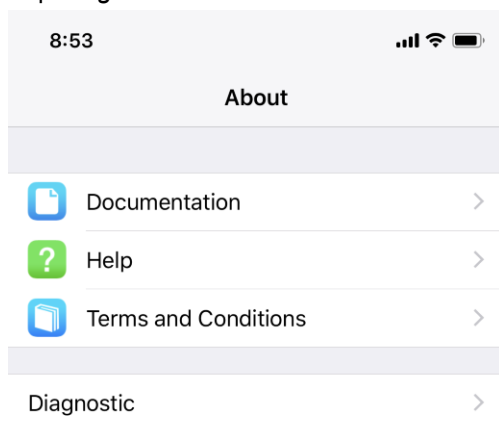
- f. Go to *Assignments*, then select the desired groups/users/devices to enable Web Filter for.
- g. After enrolling the iOS device to the Intune portal, ensure that the device receives the Web Filter Mobileconfig profile:
 - i. On the device, go to *Settings > General > Device Management*.
 - ii. In the management profile, go to *Restrictions*.
 - iii. Verify that the *Plug-In Bundle ID* field contains the following URI: `com.fortinet.forticlient.fabricagent`.

Logs

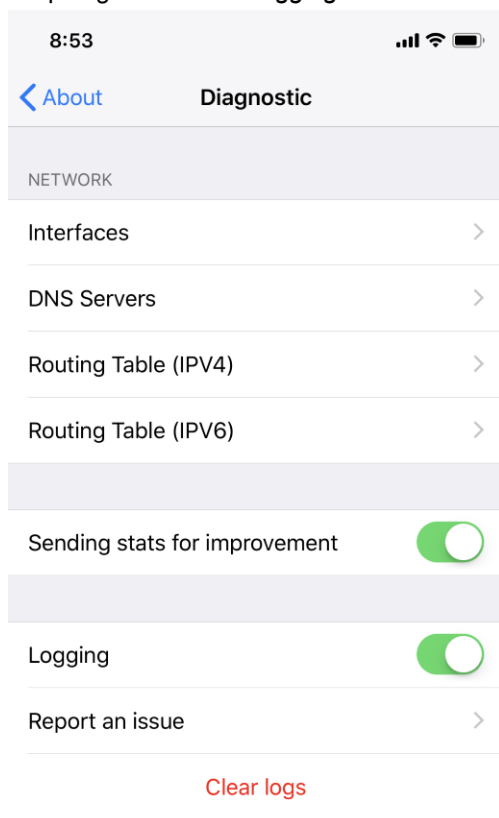
You can email FortiClient iOS logs to Fortinet.

To email logs to Fortinet:

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



3. Swipe right to enable *Logging*.



4. Tap *Email Logs*.

Change log

Date	Change Description
2019-09-23	Initial release.
2019-11-06	Added Configuring Microsoft Intune integration on page 30 .
2019-12-05	Updated Creating a Mobileconfig profile on page 9 .
2019-12-24	Updated for 6.2.3. Added To install a certificate received via email: on page 8 .
2020-03-03	Updated To configure Microsoft Intune integration: on page 30 .



FORTINET®



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.