FortiClient iOS - Administration Guide

Version 6.4

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://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 29, 2021
FortiClient iOS 6.4 Administration Guide
04-640-656798-20210129

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
Zero Trust Telemetry 12
User profile 14
Enterprise mobility management **17**
Configuring AirWatch integration 17
Configuring Jamf integration 25
Configuring Microsoft Intune integration 30
Logs **34**
Standalone VPN client **36**
Change log **37**

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 Zero Trust Telemetry from FortiClient iOS to EMS. See Zero Trust Telemetry on page 12.

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: • 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.
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.

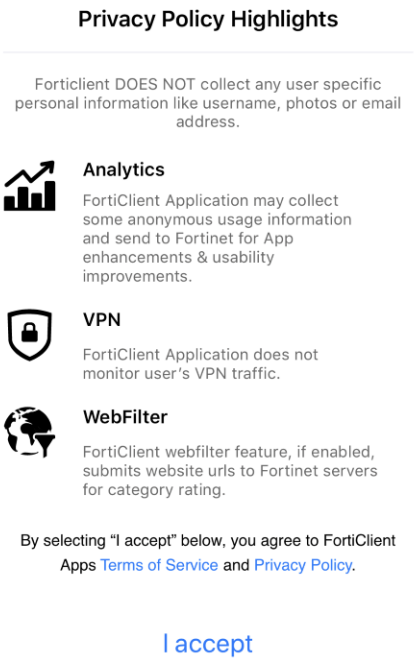
Supported platforms

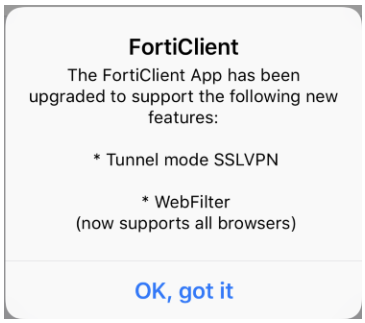
iOS versions 9, 10, 11, 12, 13, and 14 support FortiClient iOS.

Initial configuration

Running FortiClient iOS

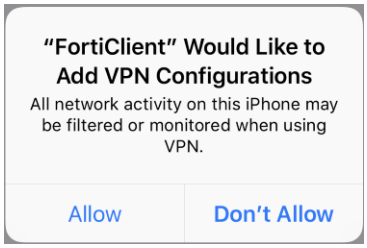
After downloading the FortiClient installer and running the application for the first time, you must acknowledge some popups before continuing to add a VPN configuration. Acknowledge the notifications shown.



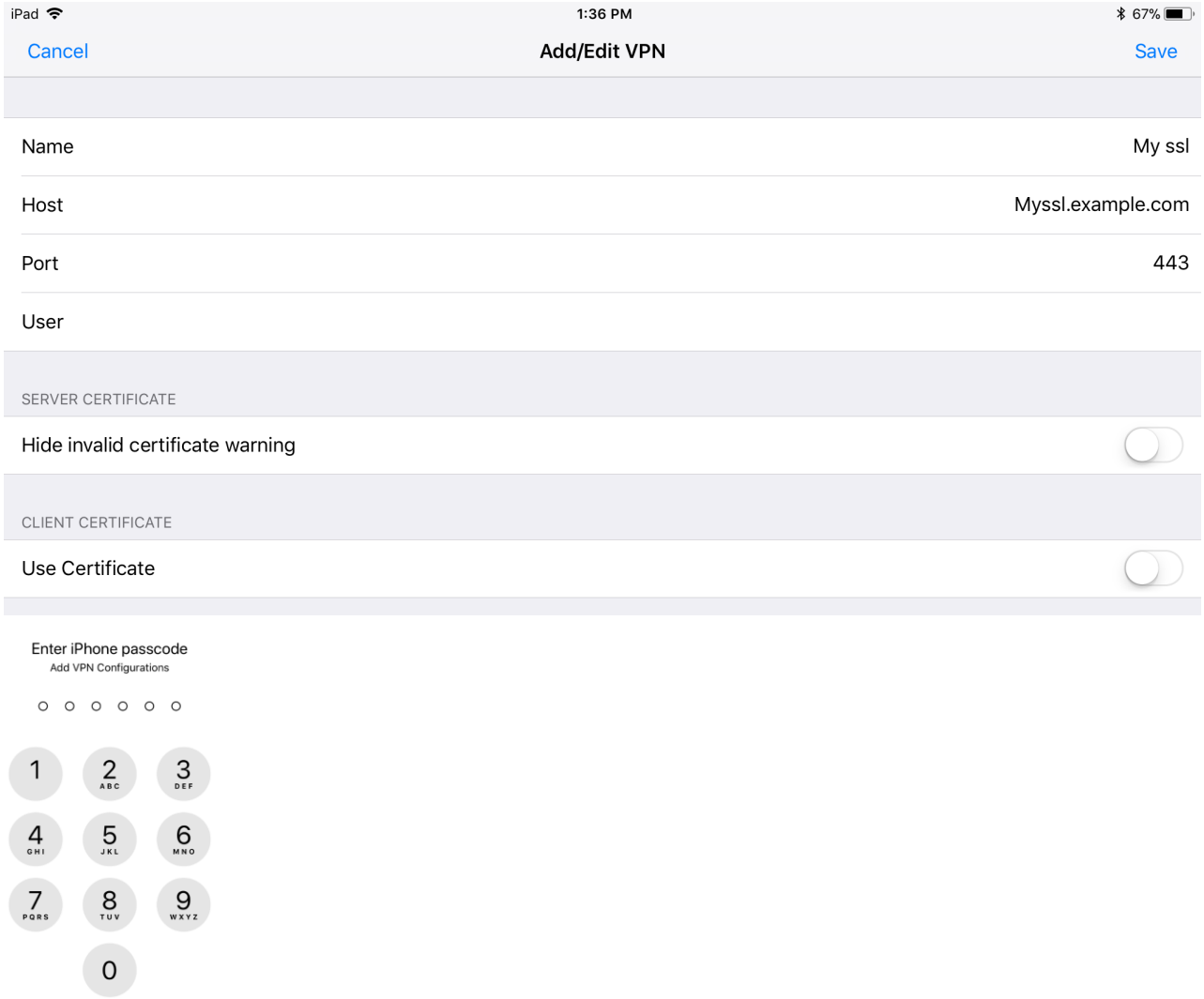


To add a VPN connection:

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.

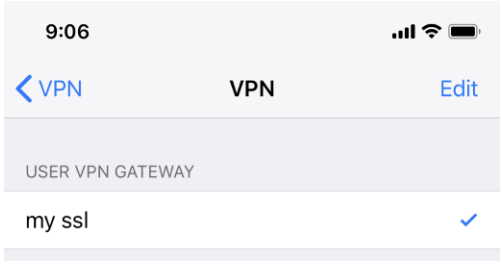


4. Tap *Done* twice.

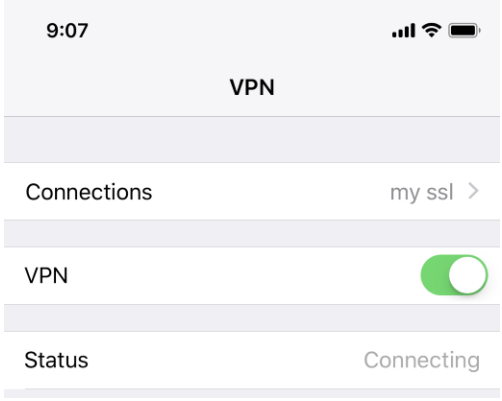
The *Name*, *Host*, and *Port* fields are required. The *User*, *Hide invalid certificate warning*, and *User Certificate* fields are optional.

To enable a VPN connection:

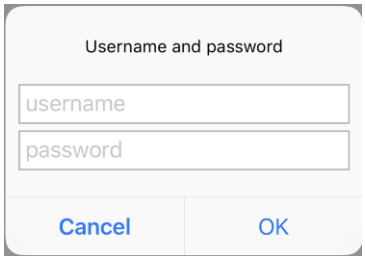
1. Tap a VPN connection. A checkmark appears beside the VPN connection to indicate it is selected.



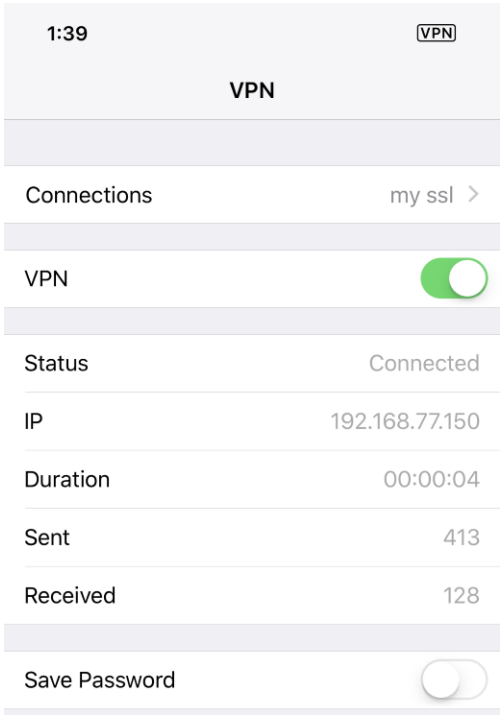
2. Tap the < button.
3. Swipe right to enable the VPN connection.



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

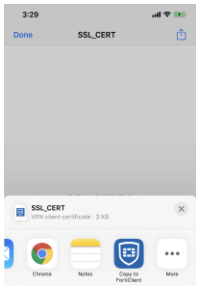


5. Tap *OK*. When connected, the tunnel interface IP address, duration, and the bytes sent and received information display.



To install a certificate received via email:

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:

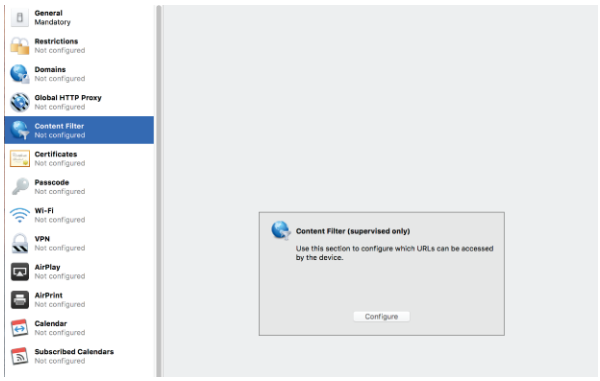
- Apple Configurator 2 (or equivalent mobile device management (MDM) application) installed.
- iOS devices are supervised.

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 ems.example.com at port 8013, with key “ConnectionKey”: ems.example.com:8013 ConnectionKey
Filter WebKit Traffic	Select the *Filter WebKit Traffic* checkbox.

8. Click *Save*.

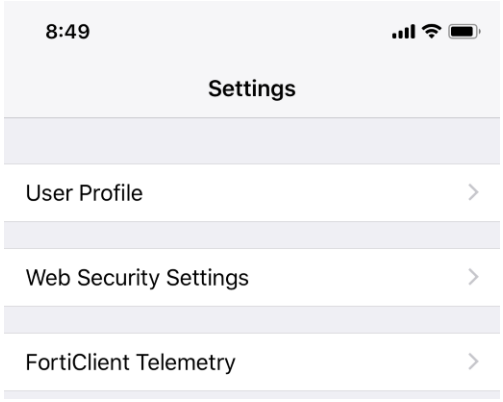
Due to restrictions that Apple set, you must launch FortiClient iOS once before the configuration takes effect. You can use EMS compliance verification rules to ensure users launch FortiClient iOS before browsing the Internet. See the *FortiClient EMS Administration Guide*.

Web Filtering

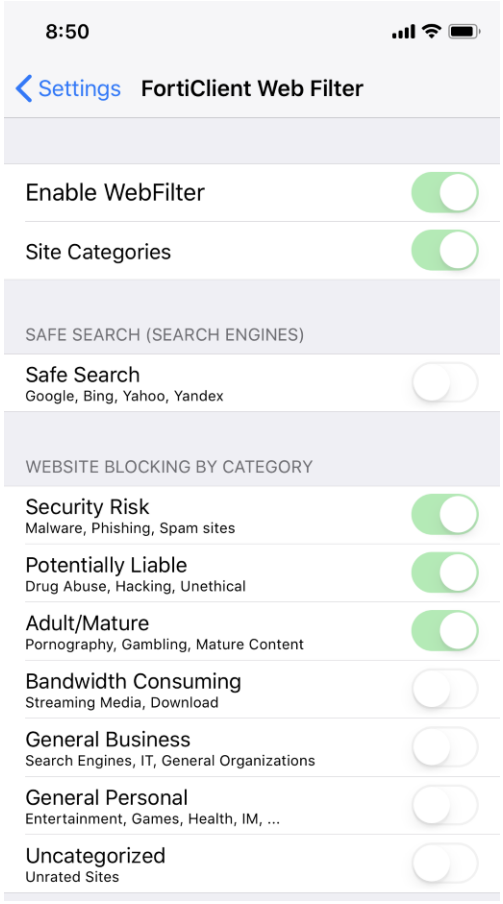
By default, FortiClient iOS disables Web Filtering.To enable Web Filtering, the iOS device must be supervised and you must install a Mobileconfig profile with a content filter on the device. See Creating a Mobileconfig profile.

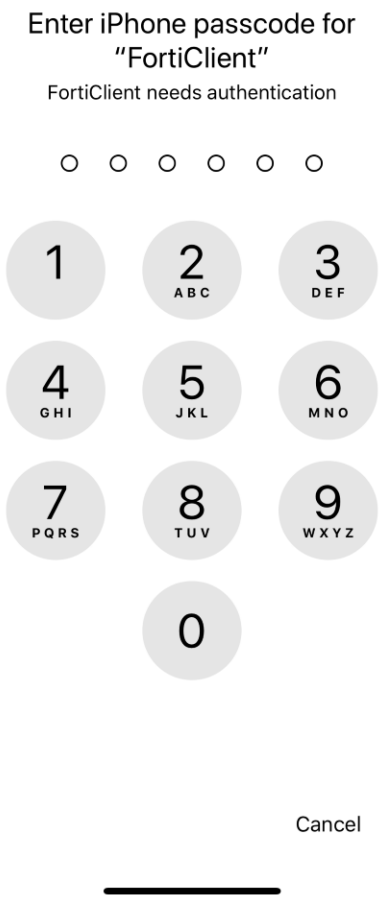
To configure the Web Filtering settings:

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.





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

Zero Trust Telemetry

To connect Telemetry to an on-premise EMS:

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

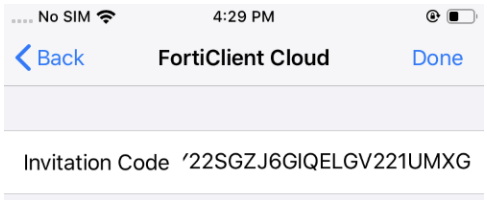
ii. Tap *Send Zero Trust Telemetry Data* to connect to the server.

b. To connect to 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.

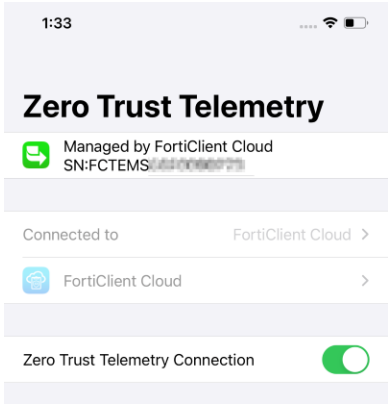
c. To connect to EMS using a QR code:
   i. Tap *Connect to*.
   ii. In the *Select Connection* dialog, tap *Scan QR Code*.
   iii. Scan the QR code with the device camera. You must allow FortiClient iOS permissions to access the device camera. FortiClient iOS automatically connects to the EMS server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

To connect Telemetry to FortiClient Cloud:

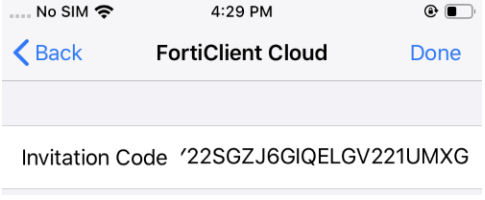
1. Tap *Settings* at the bottom of the screen.
2. Tap *Zero Trust Telemetry*.
3. Connect to FortiClient Cloud using an invitation code:
   a. Tap *Connect to*, then select *FortiClient Cloud*.
   b. Tap *FortiClient Cloud*. In the *Invitation Code* field, enter the FortiClient Cloud invitation code. Tap *Done*.



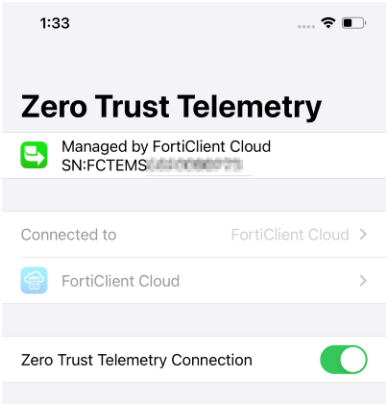
When FortiClient iOS achieves connection to FortiClient Cloud, it becomes managed by FortiClient Cloud and receives a license.



4. Do one of the following:
   a. To connect to FortiClient Cloud using an invitation code:
      i. Tap *Connect to*, then select *FortiClient Cloud*.
      ii. 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.



b. To connect to 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 FortiClient Cloud 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 9.

User profile

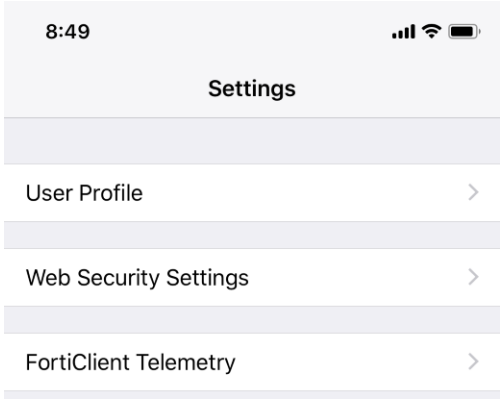
You can direct FortiClient to retrieve information about you from one of the following cloud applications, if you have an account:

- LinkedIn
- Google
- Facebook

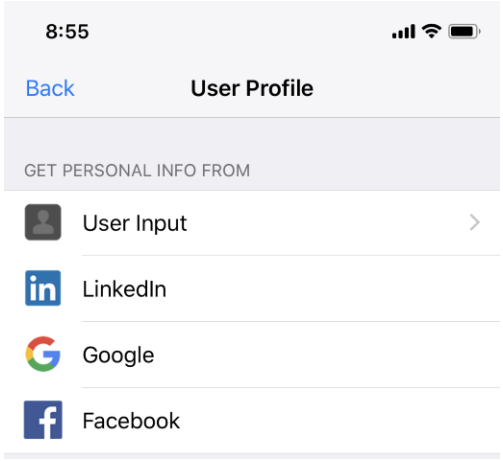
You can also manually add or edit a name, phone number, and email address in FortiClient. FortiClient iOS sends this user data to FortiClient EMS, where it displays on the *Endpoints* content pane.

To retrieve user details from a cloud application:

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



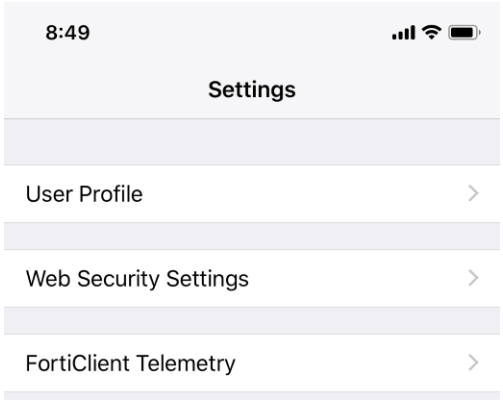
3. Tap the desired cloud application.



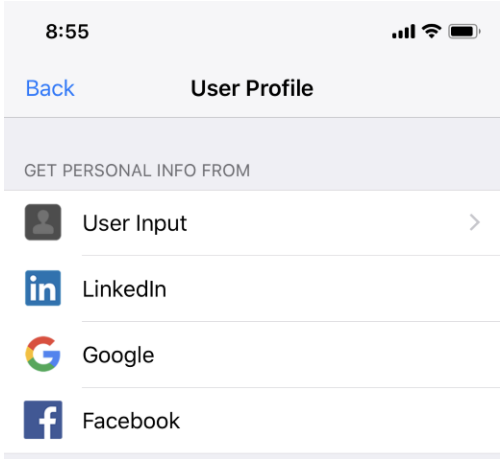
4. If you are not logged into the cloud application already on this device, you must log in. Grant FortiClient iOS permission to use your information.

To add user details manually:

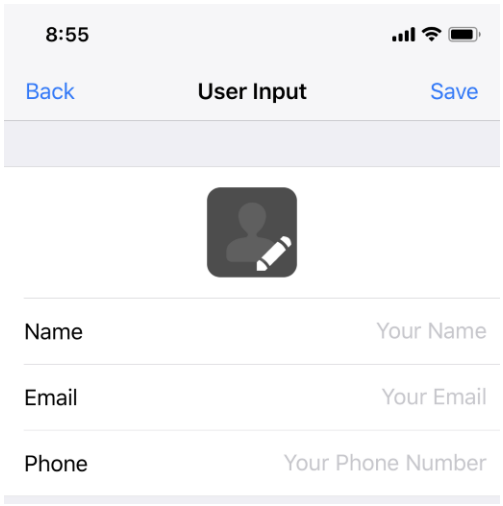
1. Tap *Settings* at the bottom of the screen.
2. Tap *User Profile*.



3. Tap *User Input*.



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



5. Tap *Save*.

Enterprise mobility management

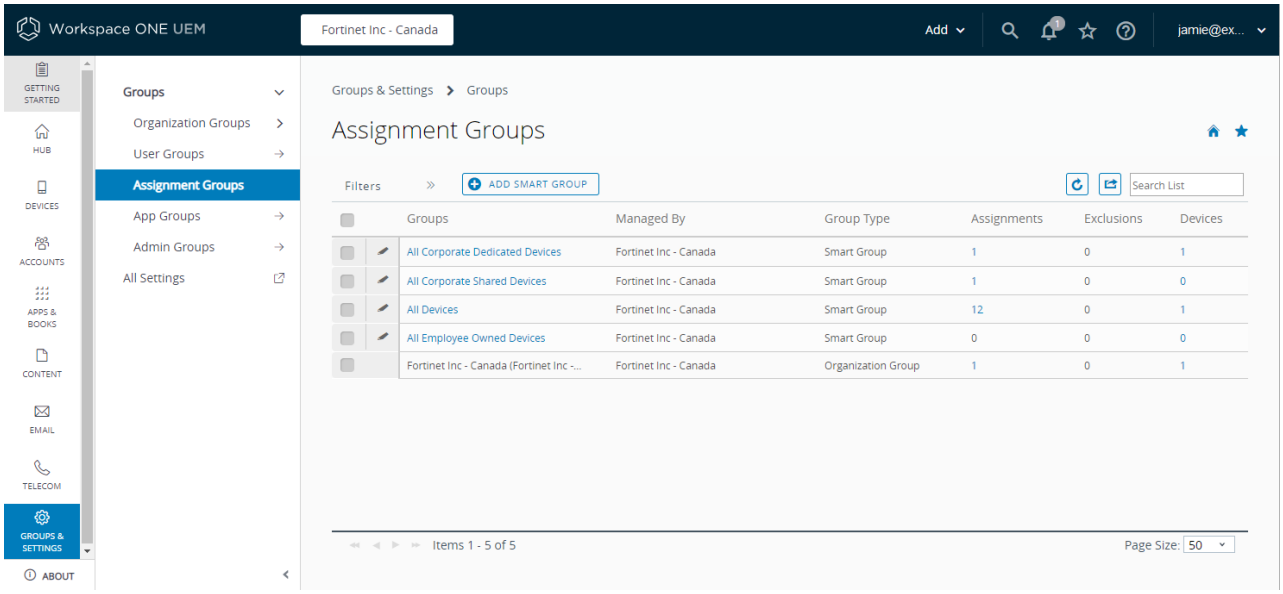
FortiClient iOS supports integration with enterprise mobility management software. Integration with enterprise mobility management software allows FortiClient iOS endpoints to connect to EMS.

Configuring AirWatch integration

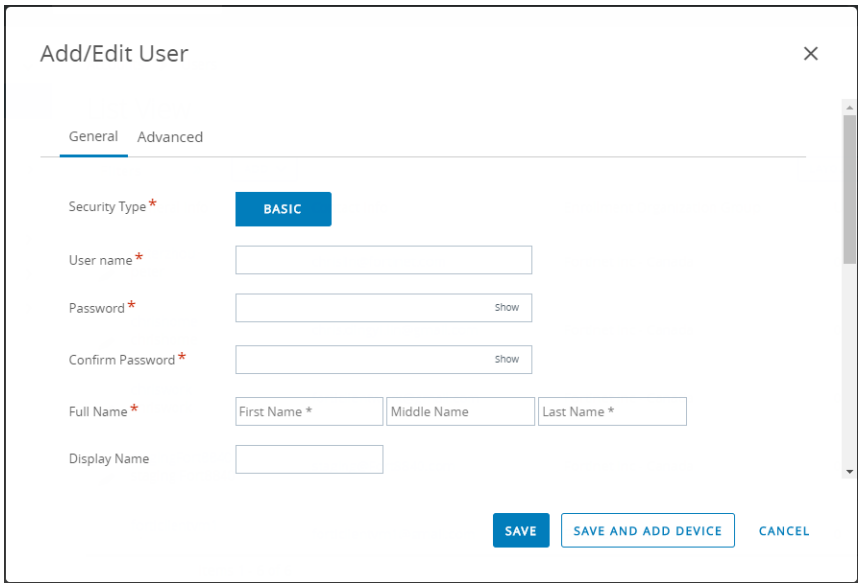
AirWatch integration allows FortiClient iOS endpoints to connect to EMS. This documentation is based on Workspace ONE UEM 20.8.0.6.

To configure integration between AirWatch and FortiClient iOS:

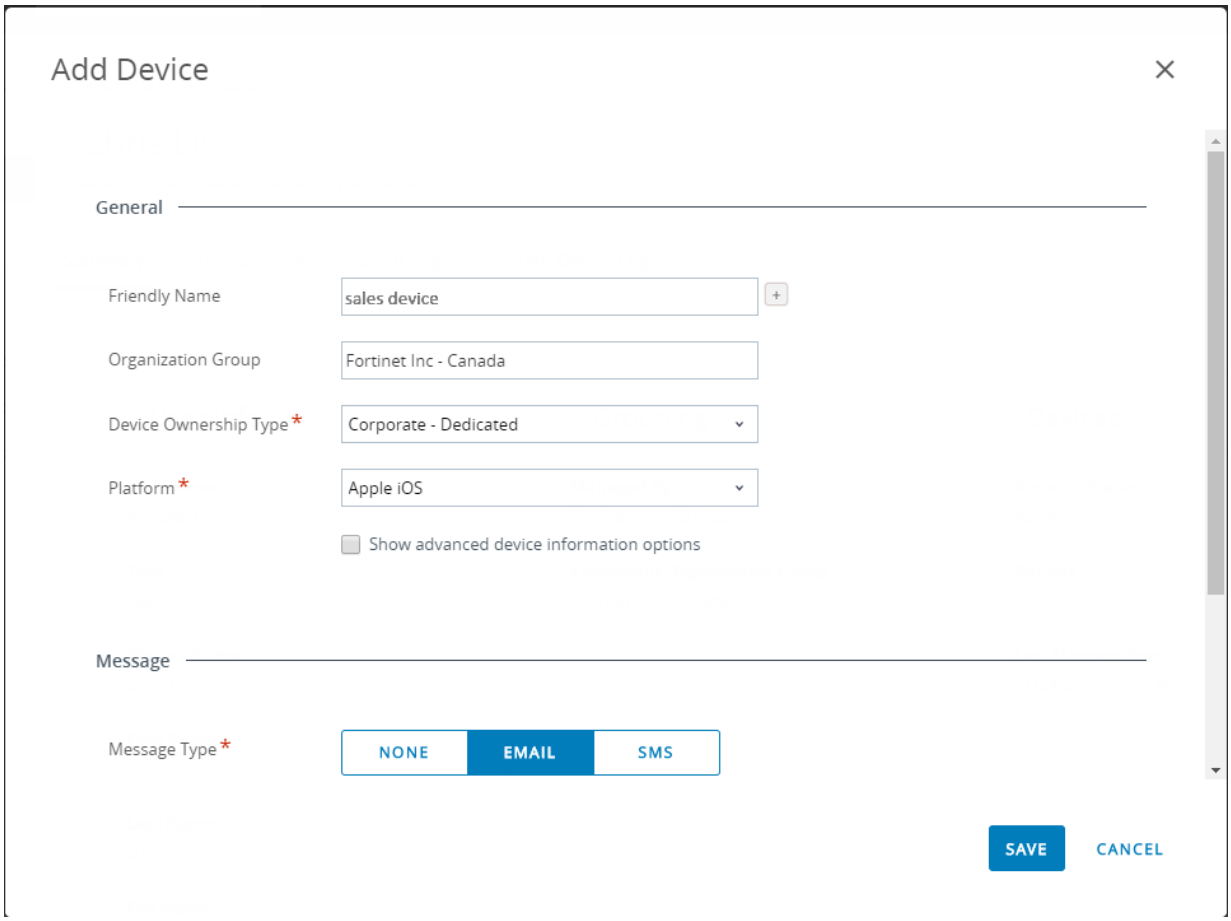
1. In AirWatch, go to *Assignment Groups*. Create a new assignment group.



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

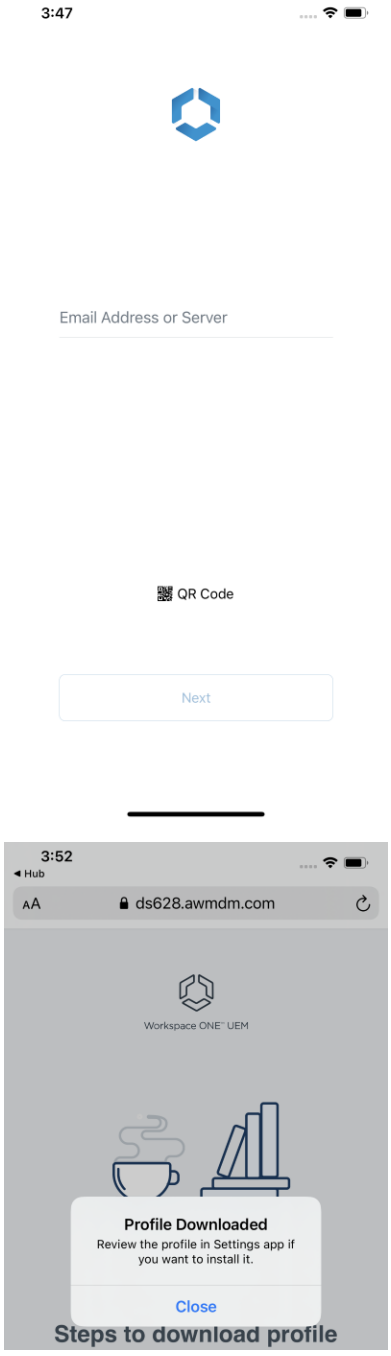


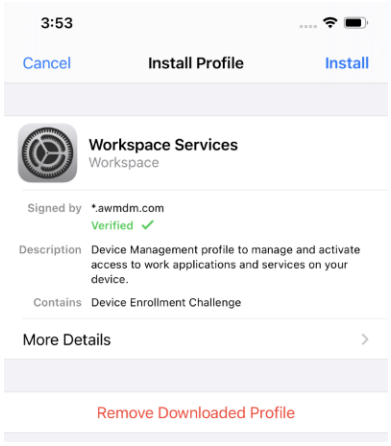
3. Add a new device for the user:
   a. From the *Device Ownership Type* dropdown list, select *Corporate - Dedicated*.
   b. From the *Platform* dropdown list, select *Apple iOS*.
   c. For *Message Type*, select *EMAIL*.



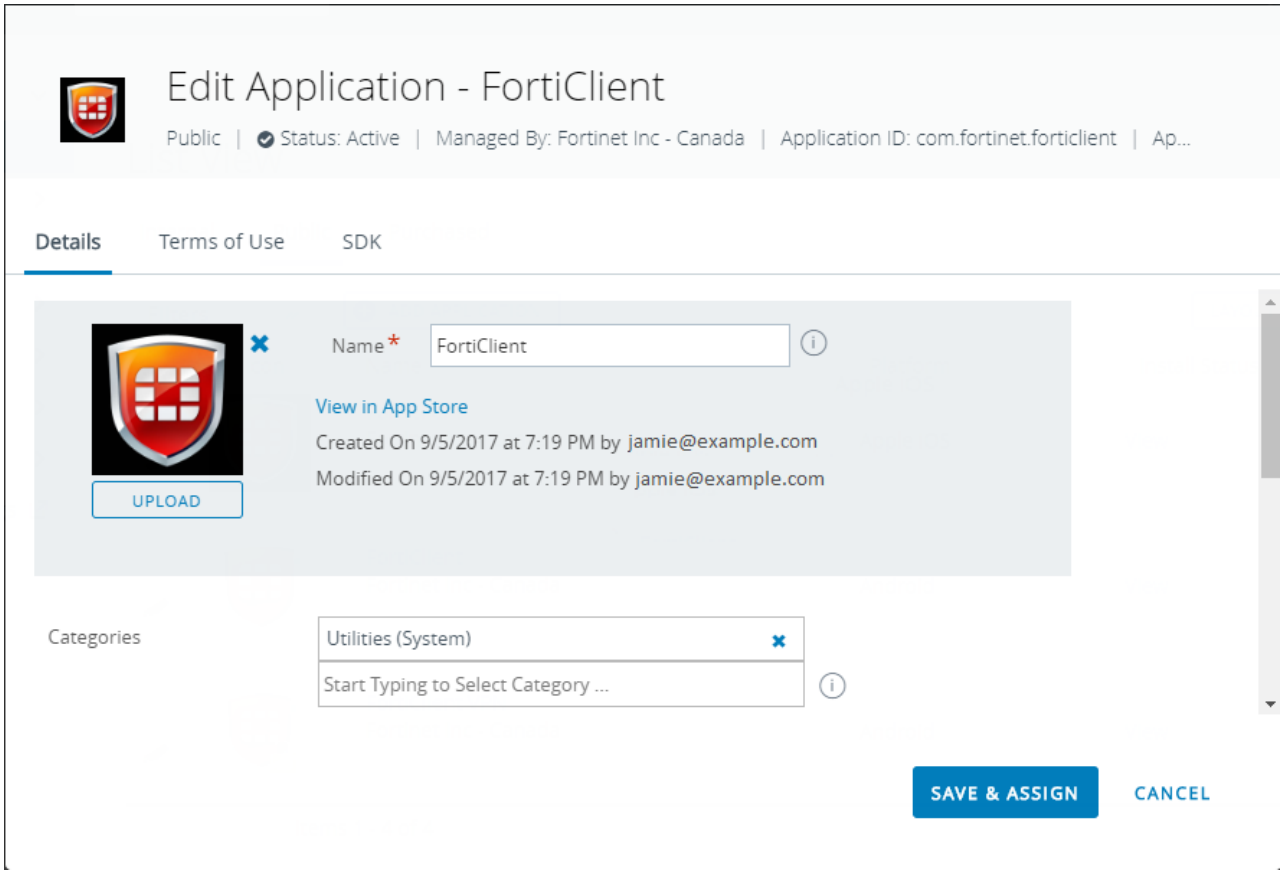
d. Save. This sends an AirWatch device activation email to the user.

4. The user installs Intelligent Hub on the device and scans the QR code in the activation email to enroll the device.

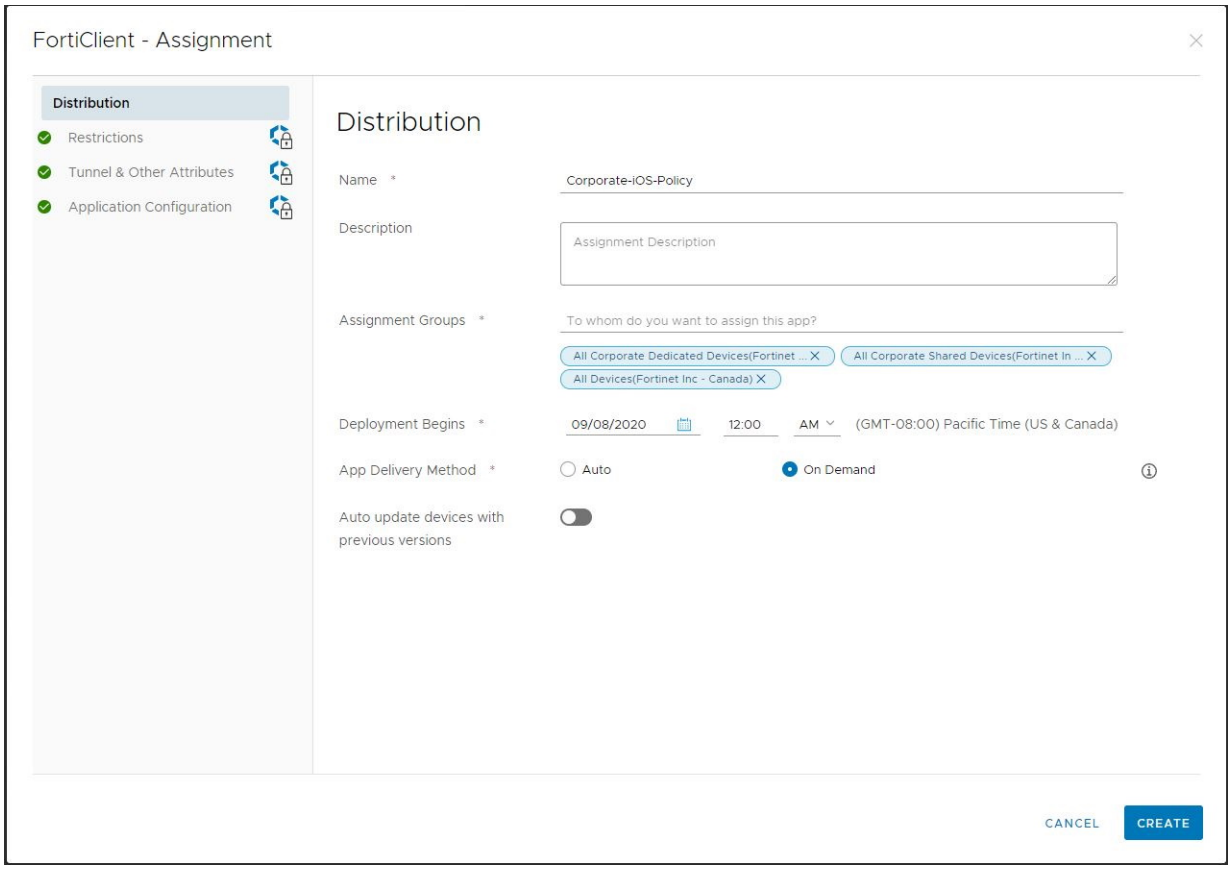




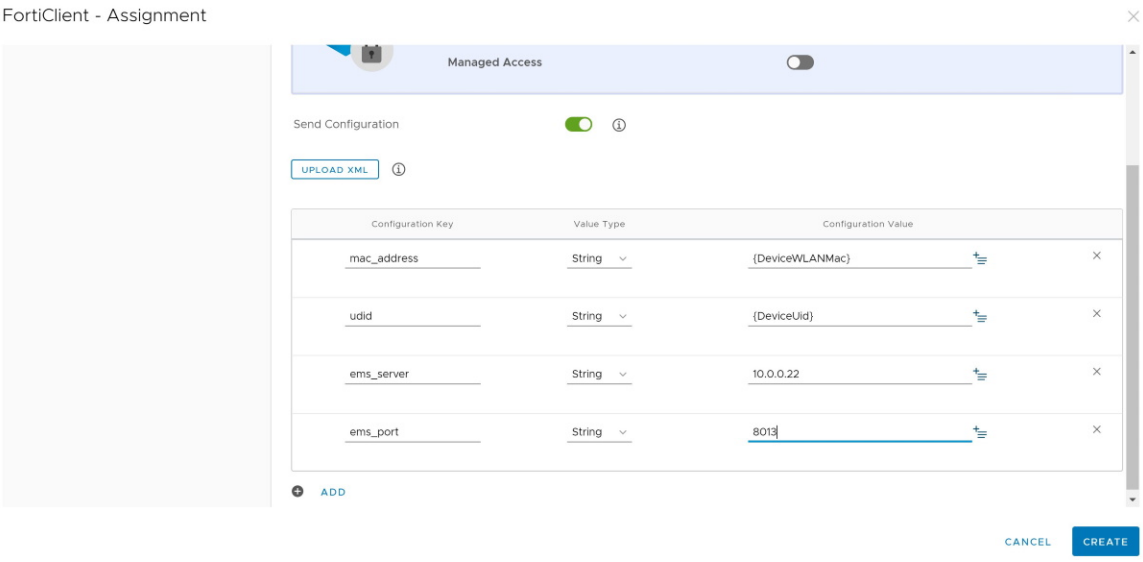
5. In AirWatch, go to *Apps & Books*, and add FortiClient iOS from the public app store.



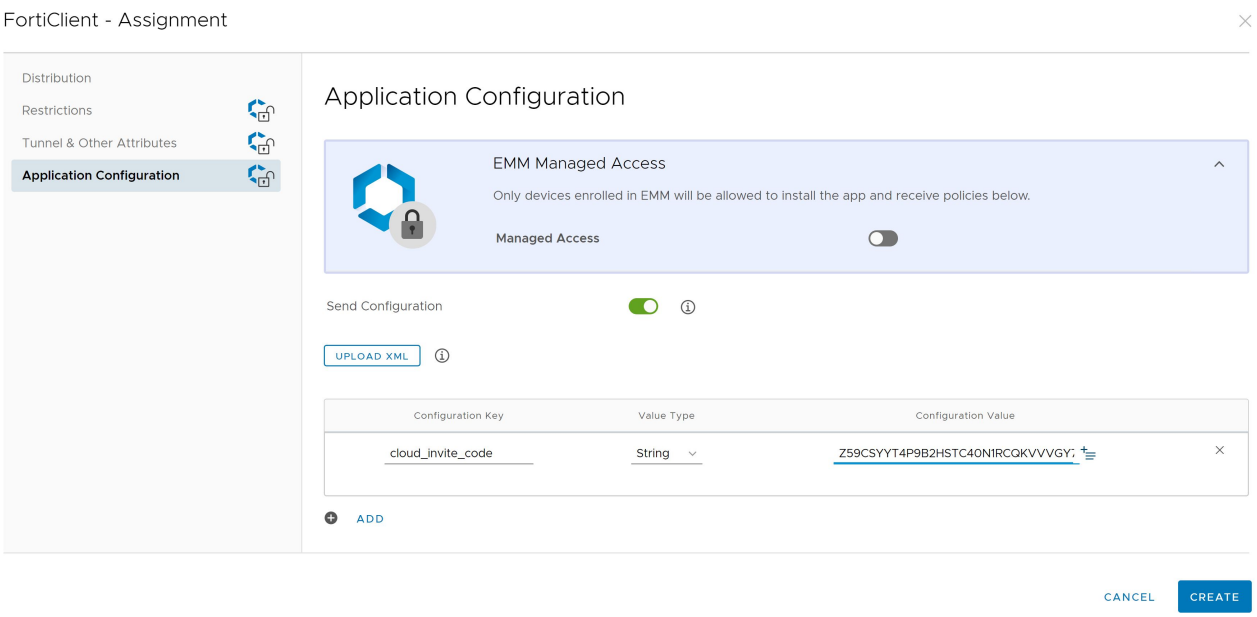
6. When adding an assignment, enter the desired name and select the desired assignment groups. Configure the deployment as desired.



In *Application Configuration*, you can optionally add key-value pairs as shown. This enables FortiClient iOS to read the MAC address and UDID from the iOS device. FortiClient sends this information to EMS.

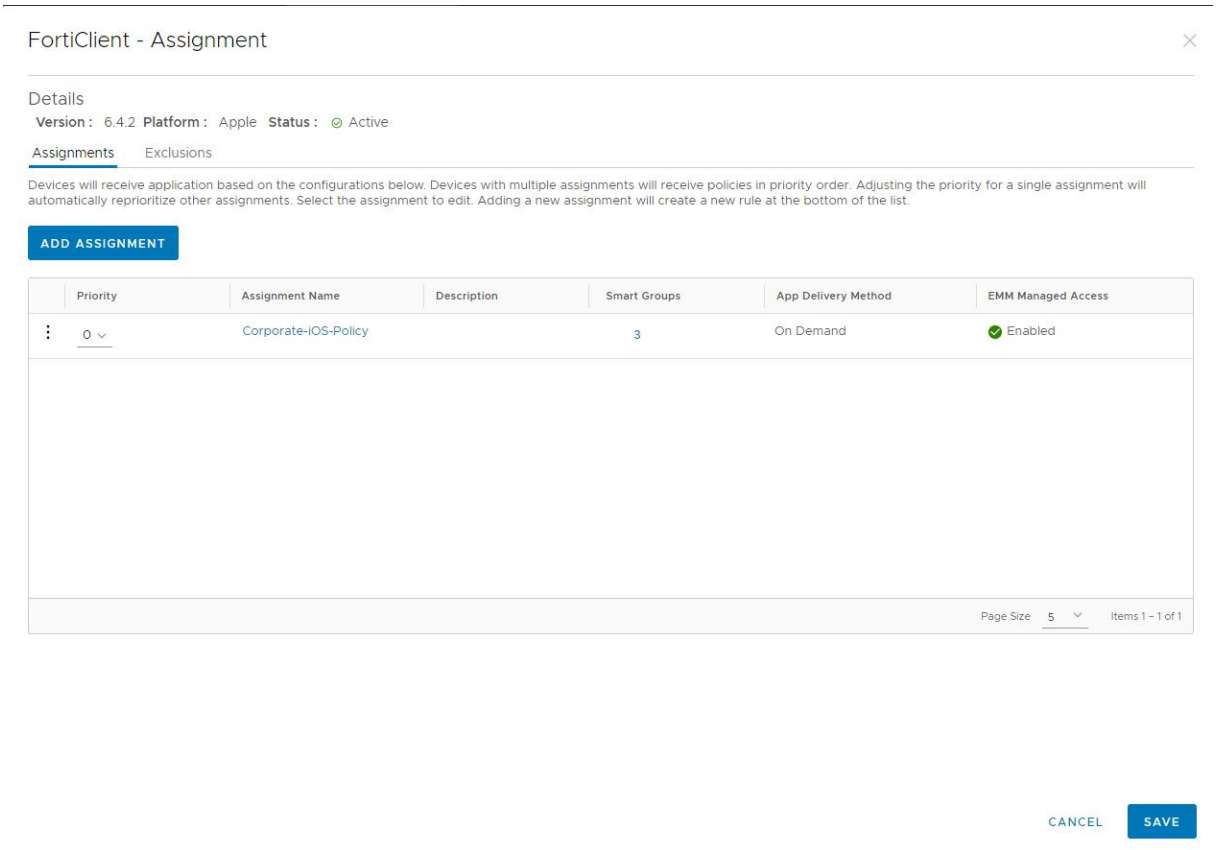


The following shows the configuration for a FortiClient iOS device that will connect Telemetry to FortiClient Cloud:

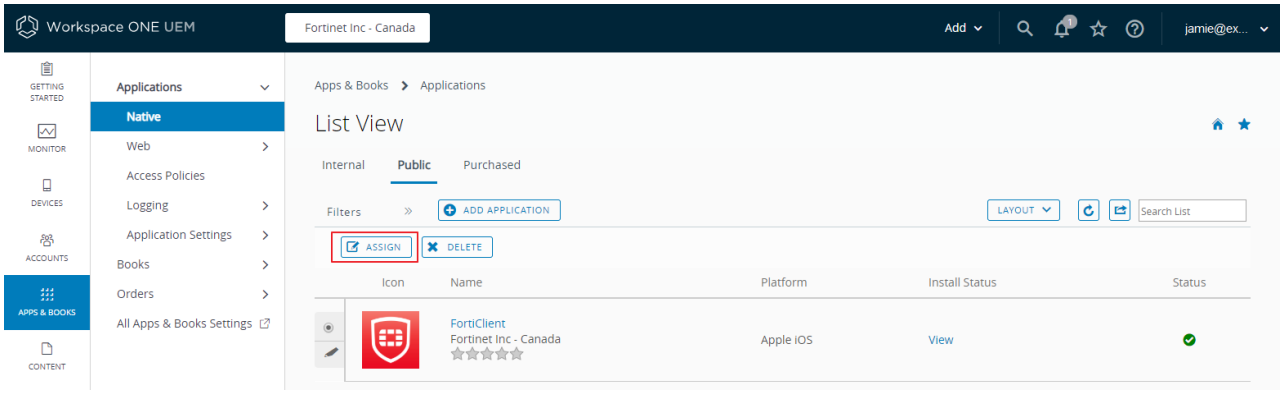


Supported keys include the following:

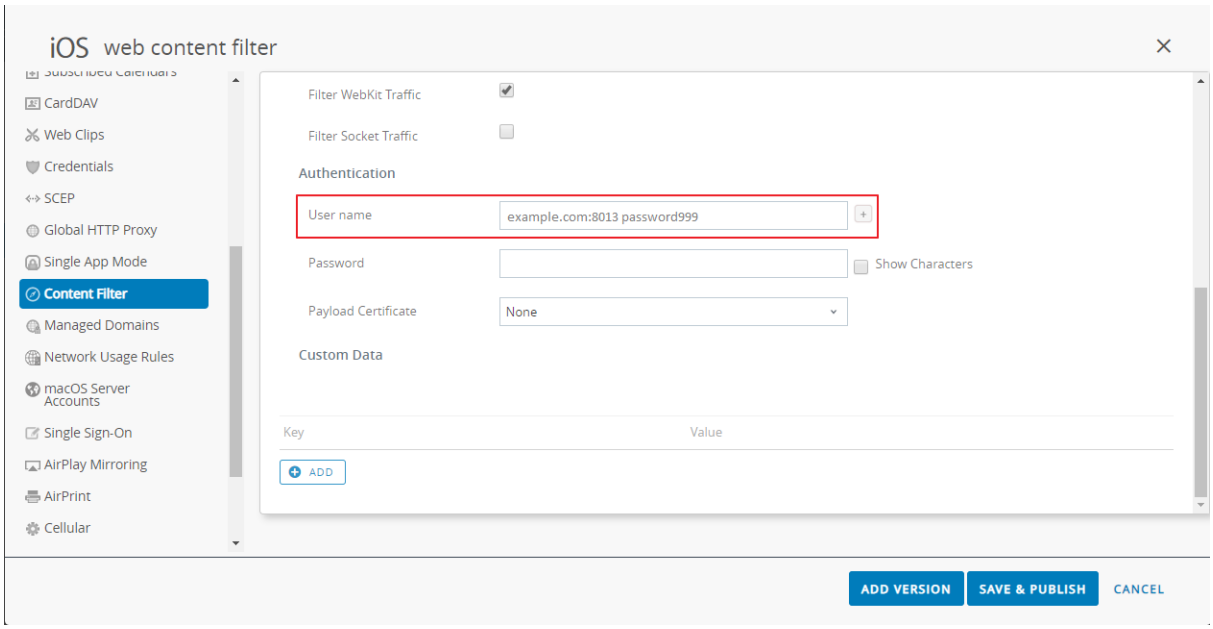
Key	Description
mac_address	iOS device MAC address.
udid	iOS device UDID.
ems_server	EMS server IP address.
ems_port	EMS port number.
group_tag	This value is used as a group tag for configuration in EMS. See *FortiClient EMS Administration Guide*.
cloud_invite_code	This value is used for connecting FortiClient iOS to FortiClient Cloud. Enter the invite code received from FortiClient Cloud.



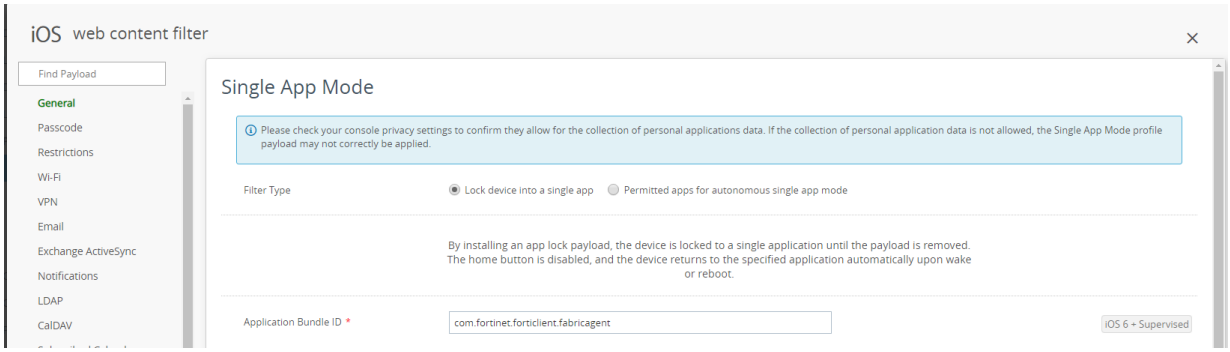
7. You can add more assignments and use different group_tag values.



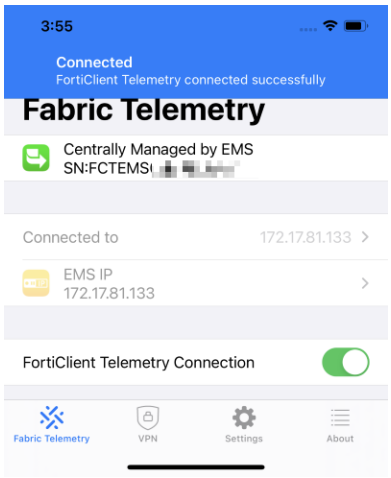
8. Go to *Devices*, and add a profile:
   a. Go to the *Content Filter* section. In the *User name* field, enter the EMS URL.



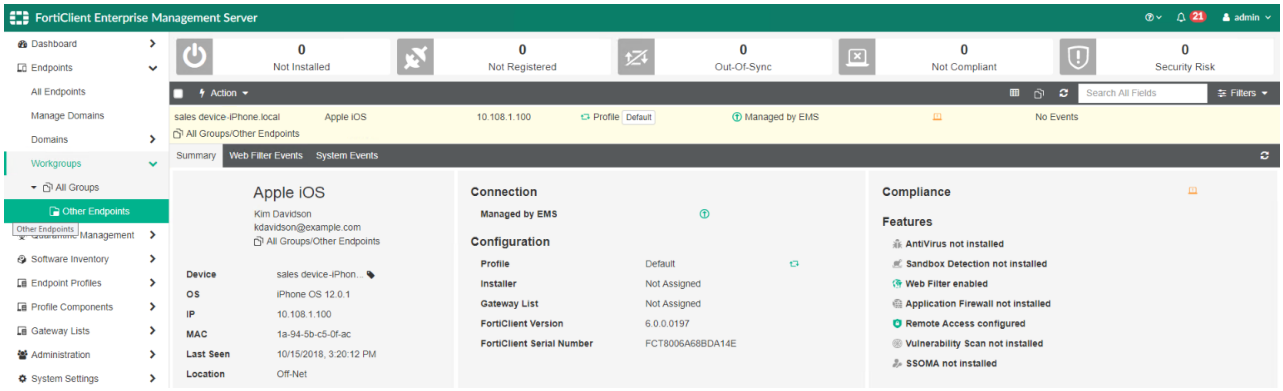
   b. Go to *Single App Mode*, and configure as shown to enable single app mode. This makes FortiClient iOS run.



   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.



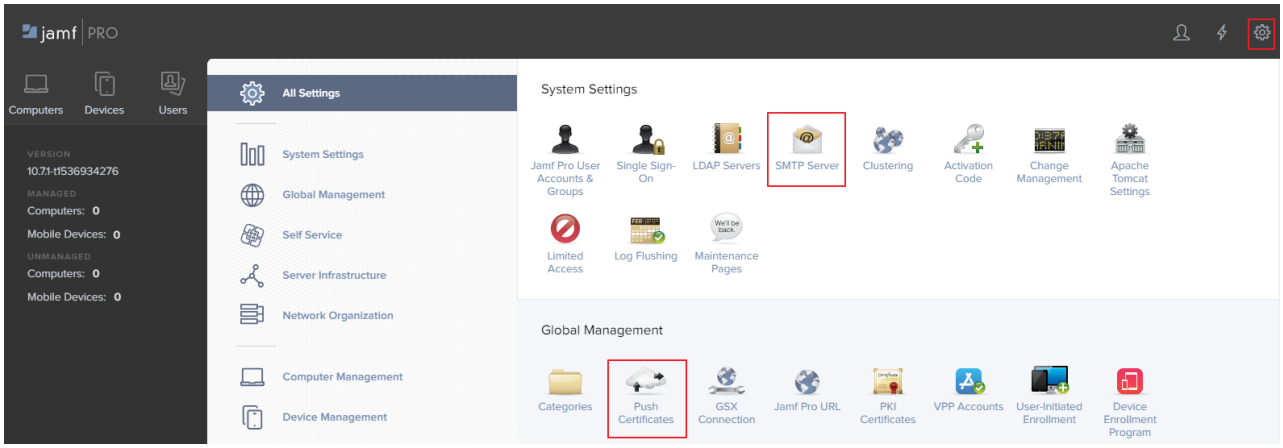
The following shows the on-premise EMS GUI after FortiClient iOS connects Telemetry.



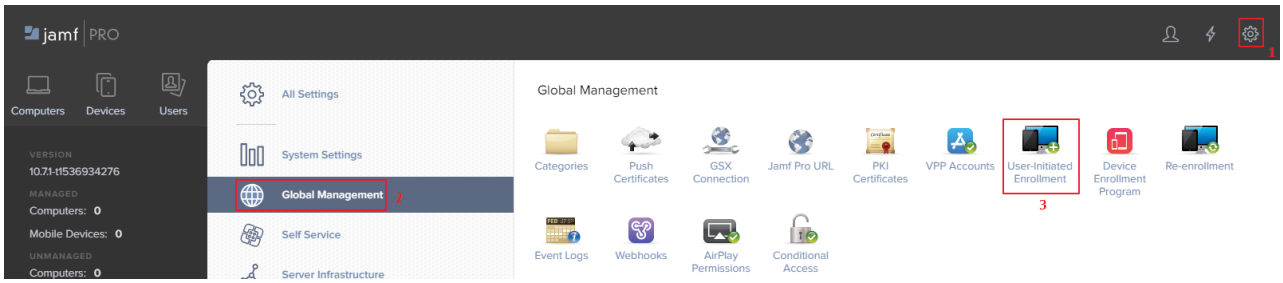
Configuring Jamf integration

To configure integration between Jamf and FortiClient iOS:

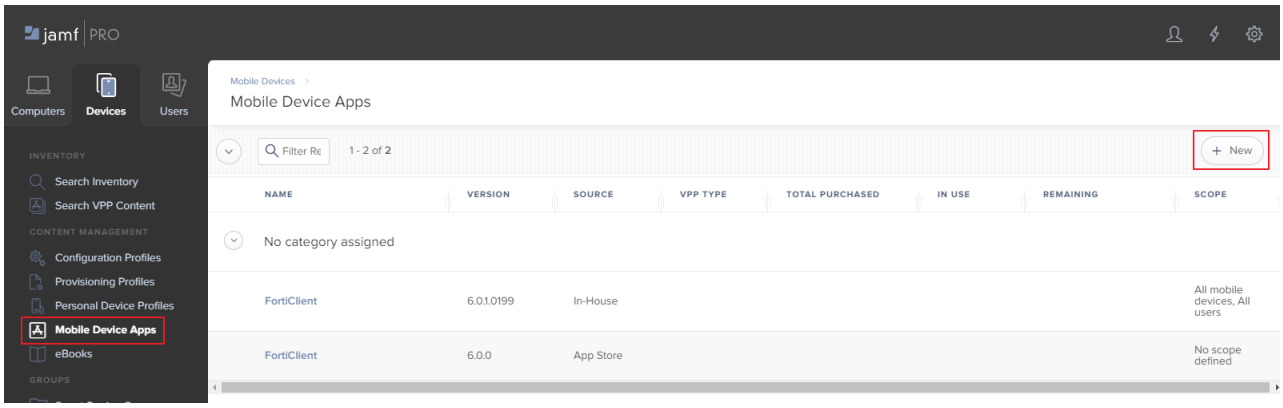
1. In Jamf, go to *All Settings*. Configure the settings in *SMTP Server* and *Push Certificates*.



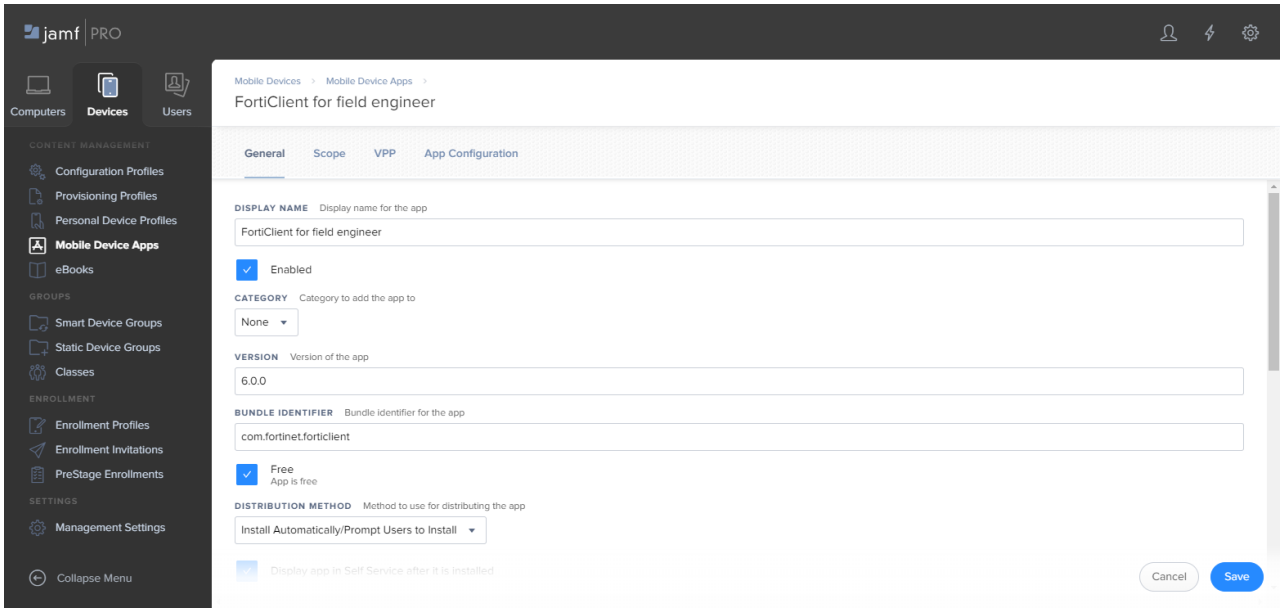
2. Go to *Global Management*, and enable *User-Initiated Enrollment*.



3. Go to *Mobile Device Apps* and add FortiClient from the App Store or by uploading it.



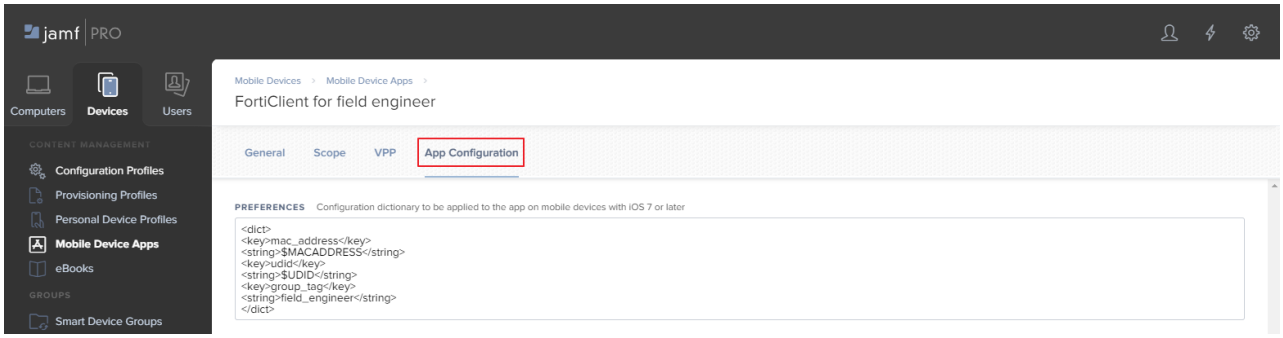
4. Configure how the app is installed.



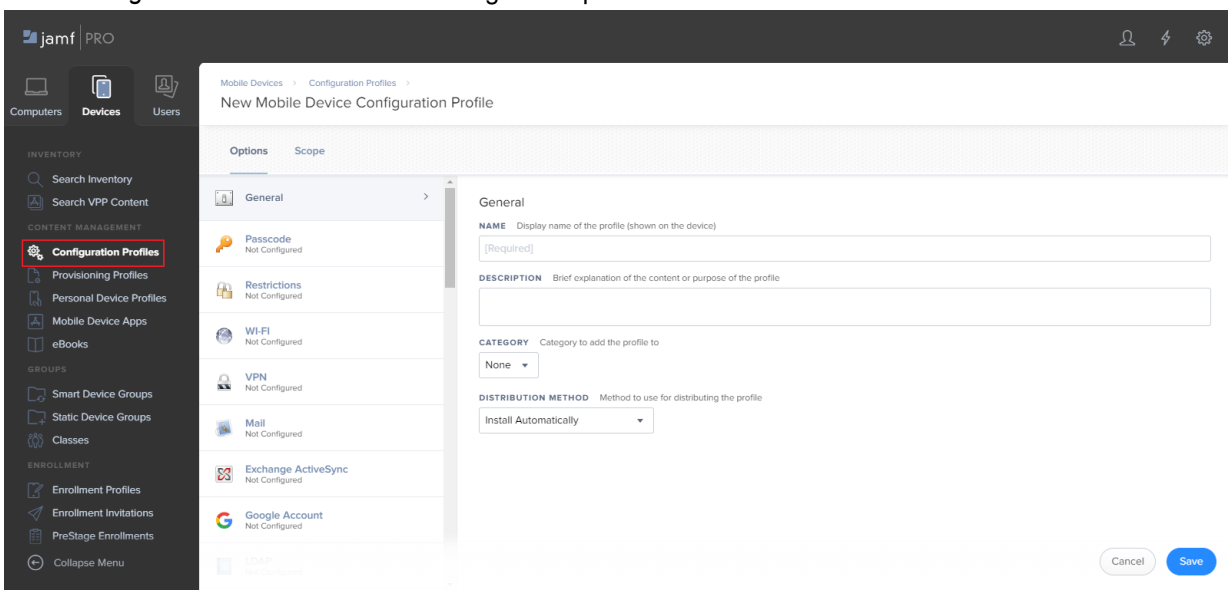
5. Add *App Configuration* for FortiClient iOS. This enables FortiClient iOS to read the MAC address and UDID from the iOS device. FortiClient sends this information to EMS. Supported keys include the following:

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

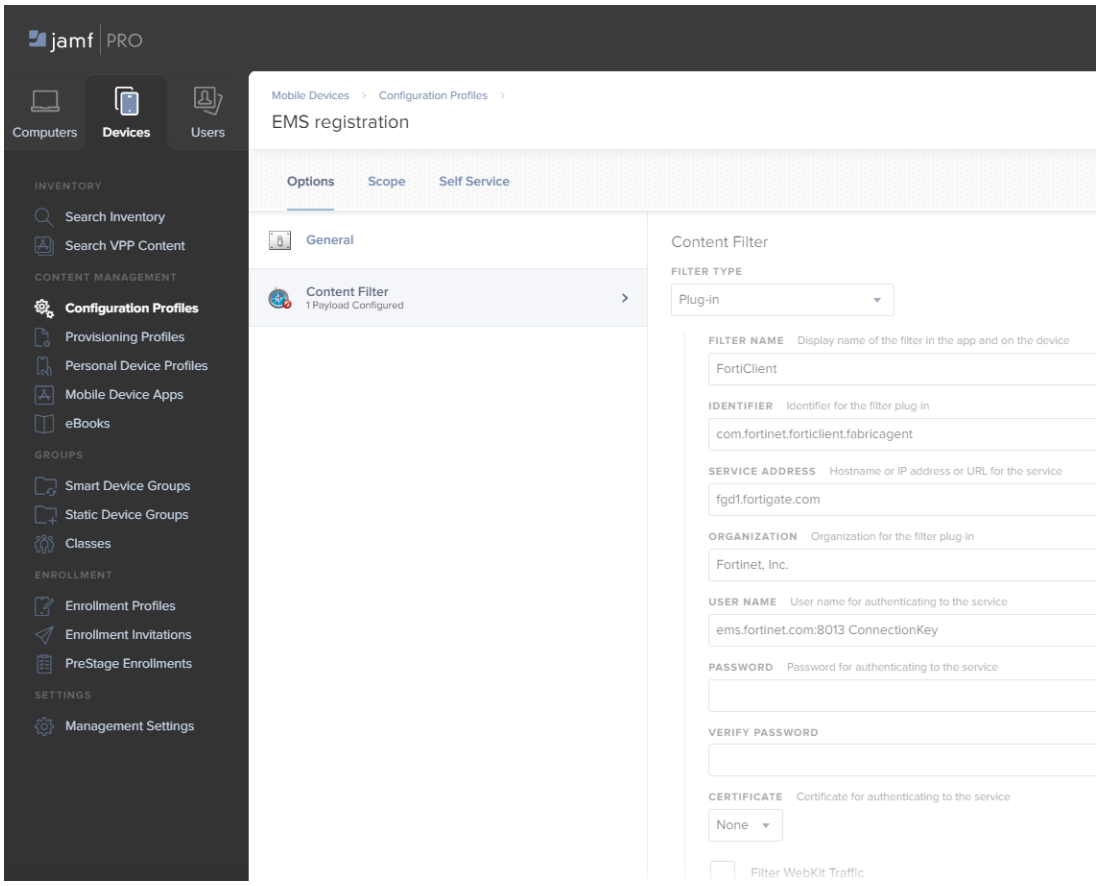
Key	Description
group_tag	This value is used as a group tag for configuration in EMS. The example uses the string "field_engineer" as a group tag, which is used when FortiClient iOS initially connects to EMS. See *Group assignment rules* in the *FortiClient EMS Administration Guide*.
cloud_invite_code	This value is used for connecting FortiClient iOS to FortiClient Cloud. Enter the invite code received from FortiClient Cloud.



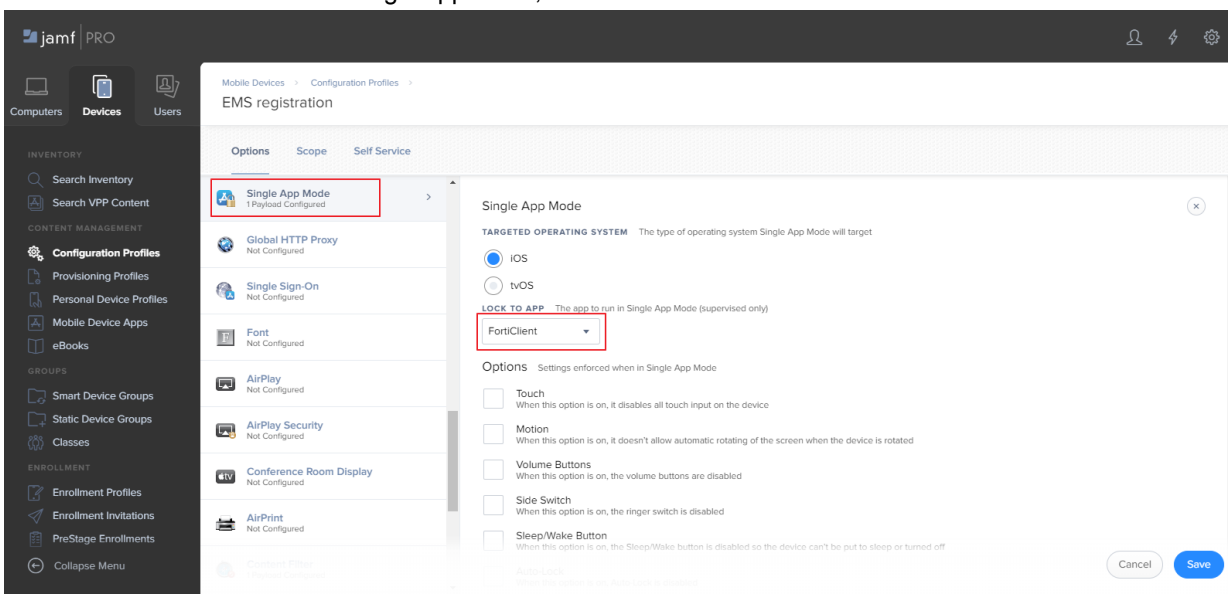
6. Configure a configuration profile:
   a. Go to *Configuration Profiles* and add a configuration profile.



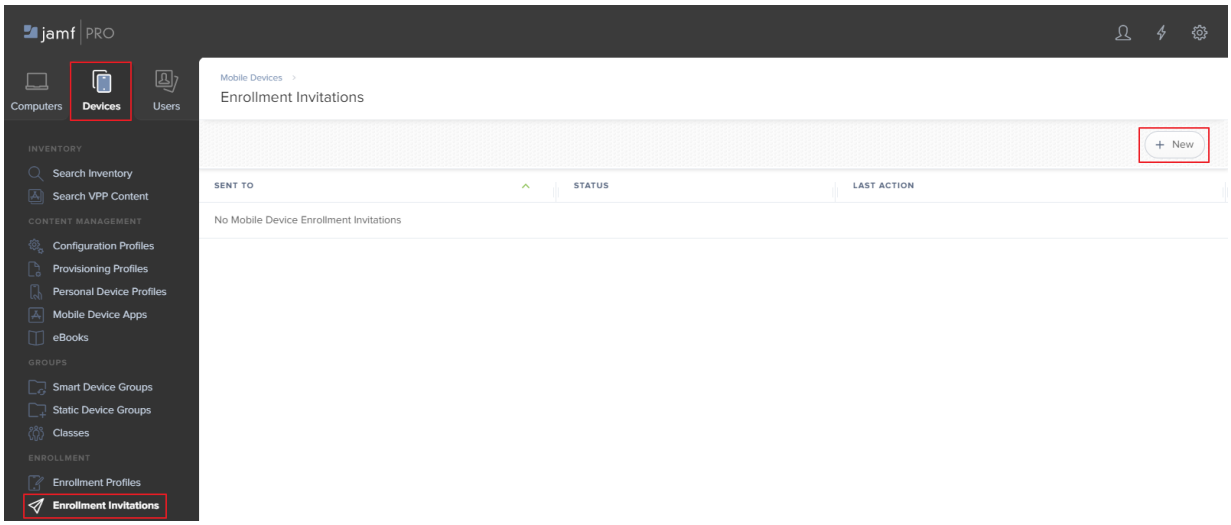
b. Under *Options*, select *Content Filter*. Add a content filter to point to the desired EMS.



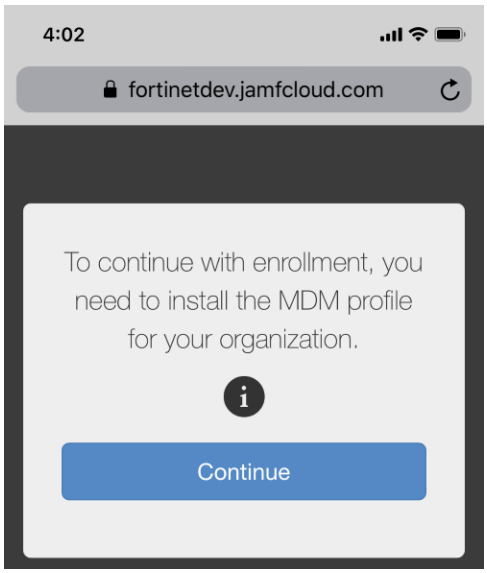
c. Enable *Single App Mode* for FortiClient. Single app mode launches the FortiClient app and connects it to EMS. If FortiClient does not launch in single app mode, it does not connect to EMS.

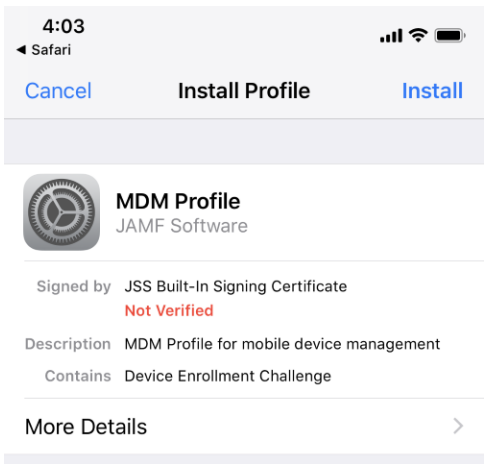


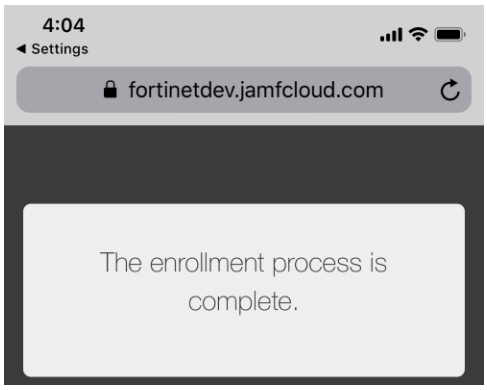
7. Enroll the device:
   a. Go to *Devices* > *Enrollment Invitations*, then send an enrollment invitation to the device.



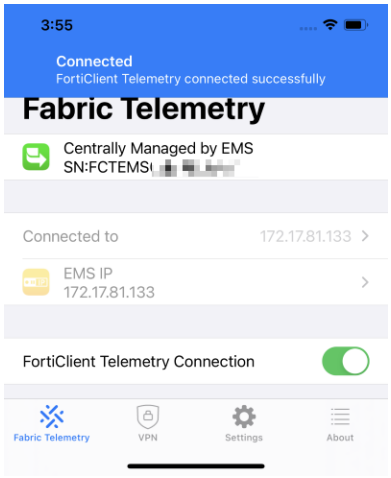
   b. Enroll the device.



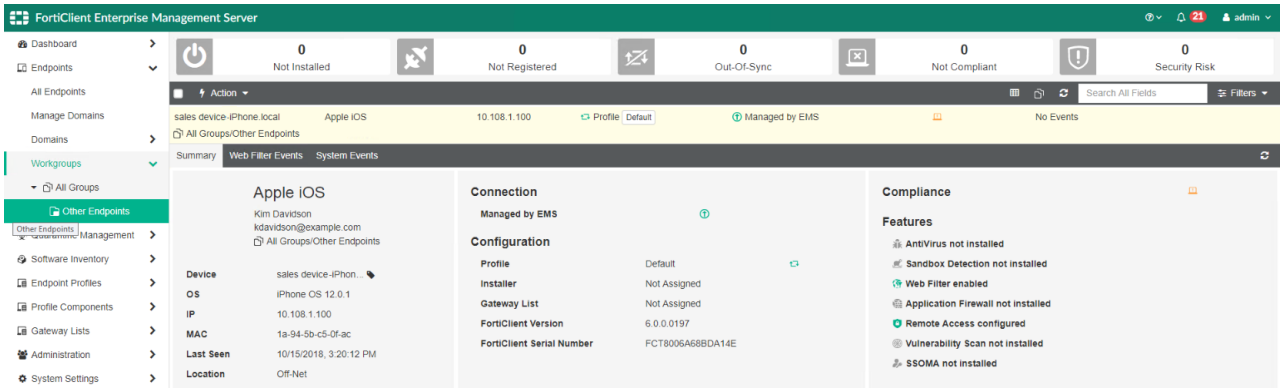




8. When the device is enrolled, FortiClient iOS automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration. Once FortiClient iOS is connected to EMS, disable single app mode for the device. Keep the EMS URL in the *Content Filter* section.



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

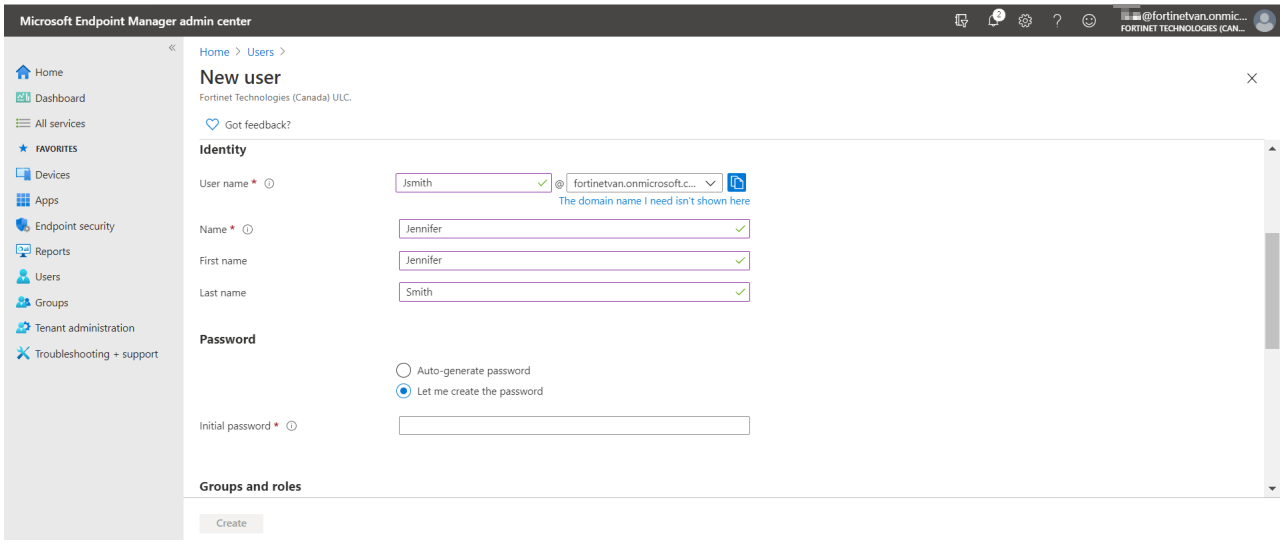


Configuring Microsoft Intune integration

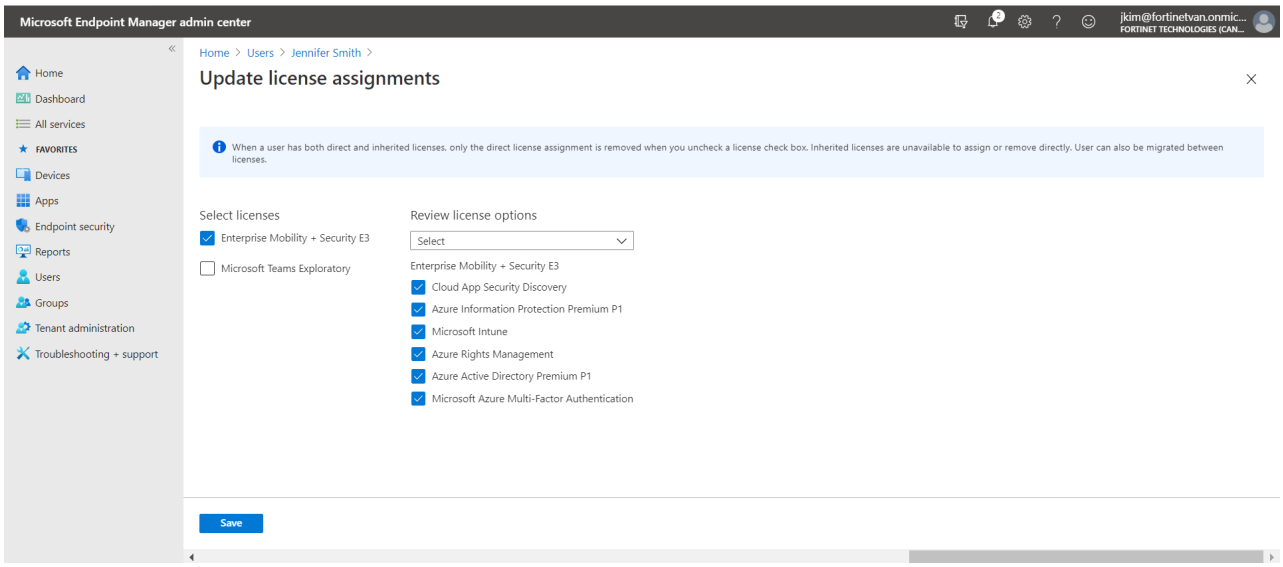
Intune integration allows FortiClient iOS endpoints to connect to EMS. FortiClient iOS 6.2.2 and later versions support integration with Intune.

To configure integration between Microsoft Intune and FortiClient iOS:

1. In Microsoft Intune, go to *Users* > *All users* and select *New user*. Configure the user as desired. Click *Create*.

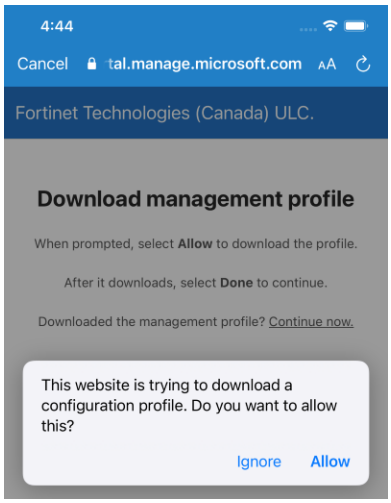


2. Select the user that you created, then go to *license*.
3. Under *Select licenses*, select *Enterprise Mobility + Security E3*. Under *Enterprise Mobility + Security E3*, enable *Microsoft Intune*. Enrolling devices requires the license. Click *Save*.

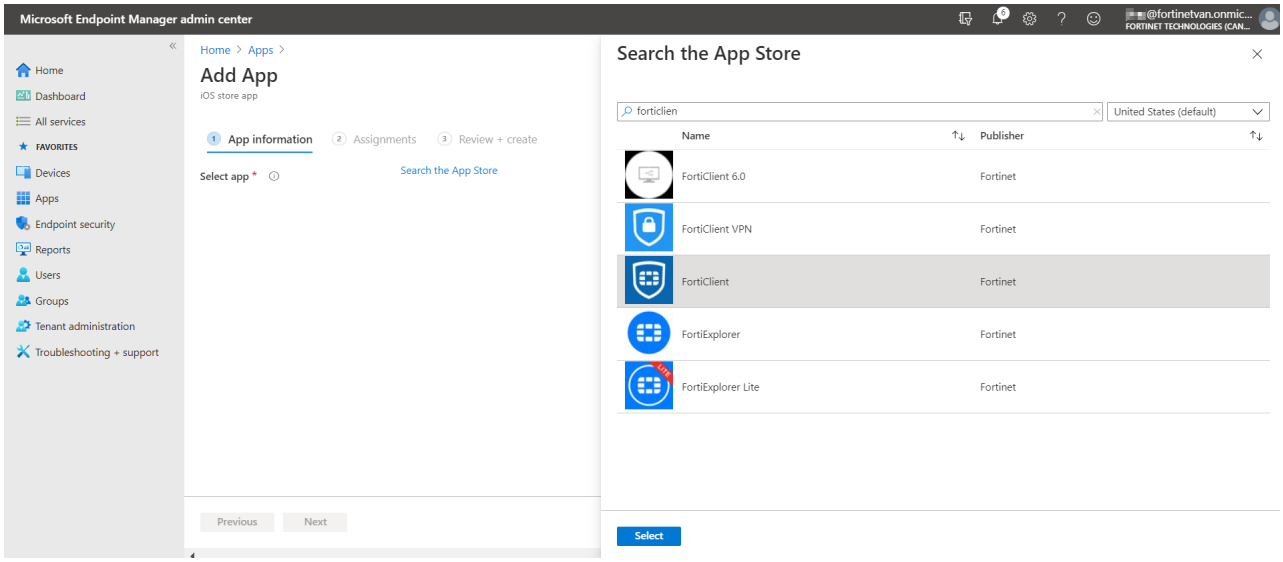


4. Go to *Groups*. Select *New Group*, then configure the group as desired. Click *Create*.
5. Go to the group that you created, then go to *Members*. Click *Add members* to add desired members to the group, including the user that you created in step 1.

6. Enroll the device to the user:
   a. Download the Intune Company Portal app from the App Store.
   b. Enter the user credentials that you configured in step 1 to download and install the profile.



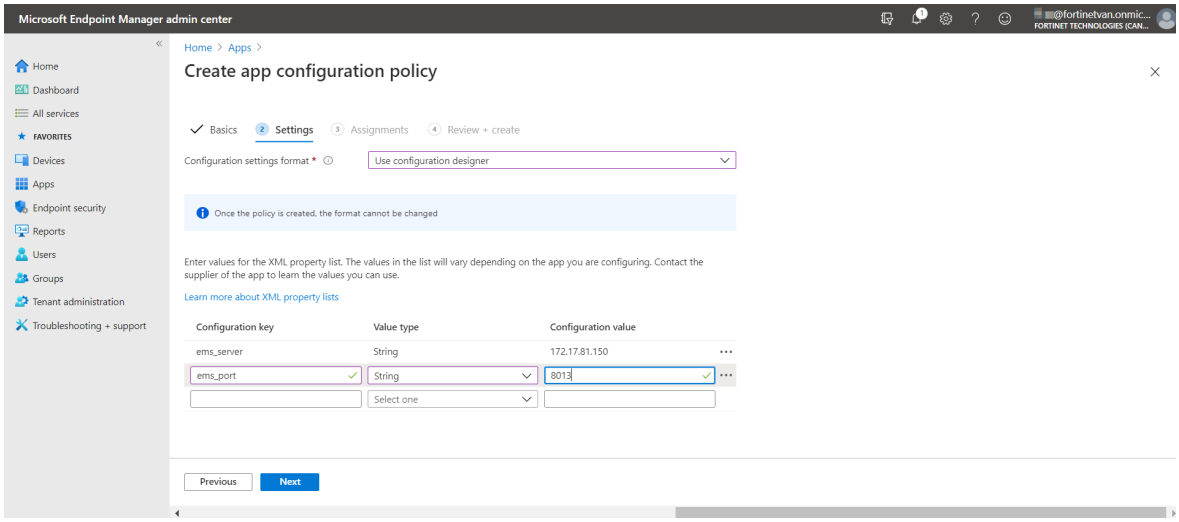
7. In Intune, go to *Apps* > *All apps*. Click *Add*, then search for and select FortiClient iOS from the public App Store. On the *Assignments* tab, click *Add group*, then select the group that you created in step 4.



8. Create an app configuration policy:
   a. Go to *Apps* > *App configuration policies*, then click *Create app configuration policy*.
   b. On the *Basics* tab, from the *Platform* dropdown list, select *iOS/iPadOS*. Click *Next*.
   c. On the *Settings* tab, configure the following:
      i. From the *Configuration settings format* dropdown list, select *Use configuration designer*.
      ii. Under *Configuration key*, enter keys to allow FortiClient iOS to register to and send information to EMS. Intune supports the following keys:

Key	Description
mac_address	iOS device MAC address.

Key	Description
udid	iOS device UDID.
group_tag	This value is used as a group tag for configuration in EMS. See *FortiClient EMS Administration Guide*.
cloud_invite_code	FortiClient iOS uses this value to connect to FortiClient Cloud. Enter the invite code that you 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	Telemetry connection key. The EMS administrator may require FortiClient iOS to provide this key during connection.



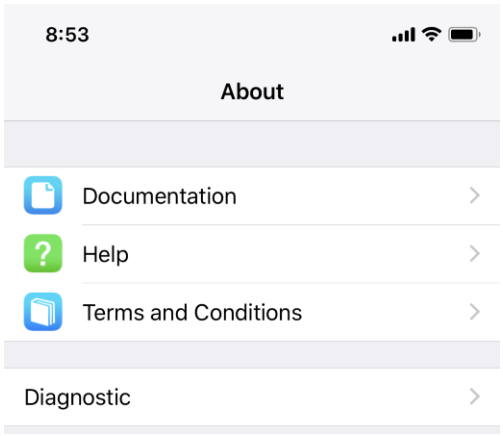
9. When FortiClient iOS starts on the device, it automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration.

Logs

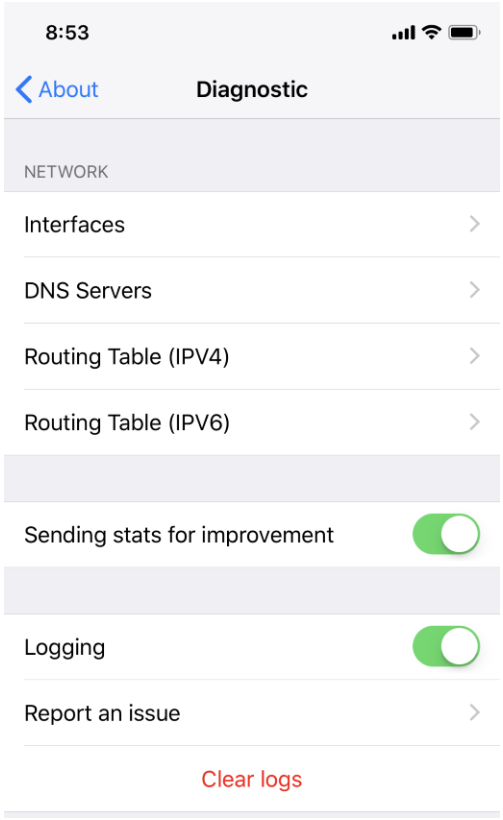
You can email FortiClient iOS logs to Fortinet.

To email logs to Fortinet:

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



3. Swipe right to enable *Logging*.



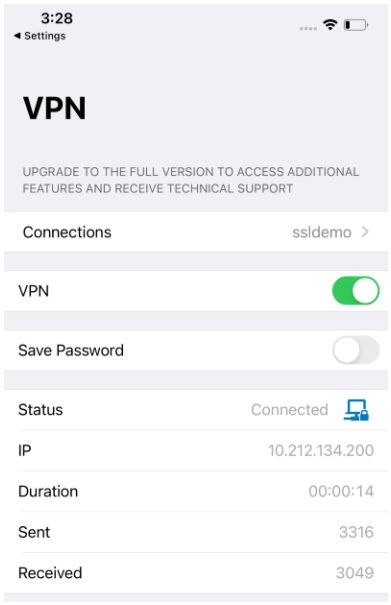
4. Tap *Email Logs*.

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 To add a VPN connection: on page 6 for details.



Change log

Date	Change Description
2020-08-07	Initial release.
2020-09-16	Updated Configuring AirWatch integration on page 17.
2020-10-02	Updated Configuring AirWatch integration on page 17.
2020-10-05	Updated Supported platforms on page 5.
2020-10-07	Updated To connect Telemetry to an on-premise EMS: on page 12.
2020-11-27	Updated Configuring Microsoft Intune integration on page 30.
2020-12-17	Added Standalone VPN client on page 36. Updated Zero Trust Telemetry on page 12.
2021-01-05	Updated Configuring Jamf integration on page 25.
2021-01-29	Updated Standalone VPN client on page 36.

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.