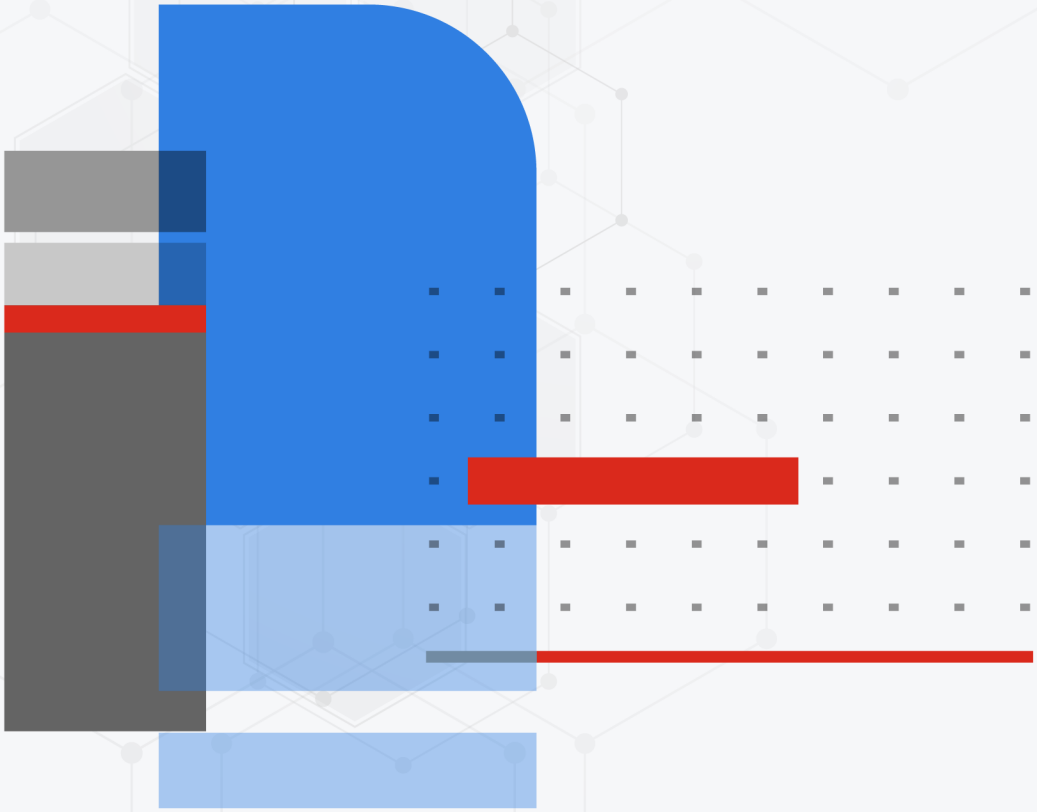
ManageEngine Deployment Guide

FortiClient 7.4



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 23, 2025
FortiClient 7.4 ManageEngine Deployment Guide
04-74-1091319-20250123

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Configuring ManageEngine integration on EMS **6**
Configuring ManageEngine integration to allow FortiClient (iOS) to connect to EMS **8**
Configuring ManageEngine integration to allow FortiClient (Android) to connect to EMS **10**

Change log

Date	Change description
2024-11-01	Initial release.
2024-11-12	Updated: • Configuring ManageEngine integration to allow FortiClient (iOS) to connect to EMS on page 8 • Configuring ManageEngine integration to allow FortiClient (Android) to connect to EMS on page 10
2025-01-23	Updated Configuring ManageEngine integration to allow FortiClient (Android) to connect to EMS on page 10.

Introduction

This document provides information about deploying FortiClient using ManageEngine mobile device management.

This integration supports FortiClient (iOS) and (Android). You can only configure this integration with EMS 7.4.1 and later versions.

This document does not cover enrolling devices to ManageEngine. For instructions on enrolling endpoints, see MDM Enrollment Methods.

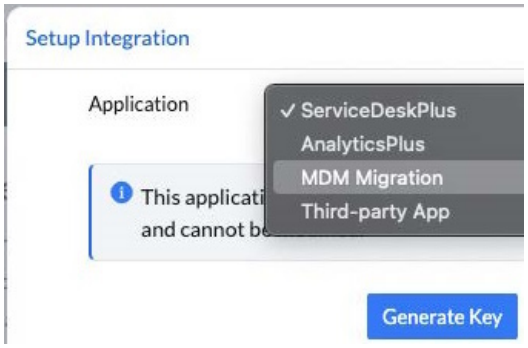
Configuring ManageEngine integration on EMS

ManageEngine integration allows FortiClient endpoints to connect to EMS. You can use on-premise or cloud ManageEngine.

To configure integration between on-premise ManageEngine and EMS:

EMS must have an API key with adequate privileges. If EMS does not meet the privileges requirement, the integration test fails with a detailed message indicating the missing privileges.

1. In on-premise ManageEngine, go to *Admin* > *Integrations* > *API Key Generation*.
2. From the *Application* dropdown list, select *MDM Migration*.
3. Click *Generate Key*.

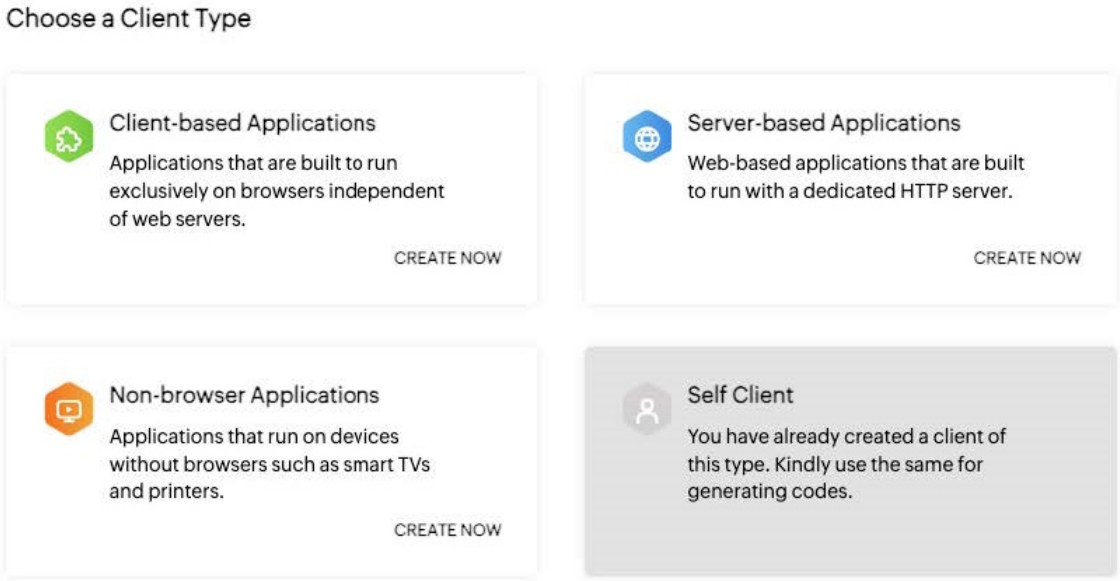


4. In EMS, go to *System Settings* > *MDM Integration*.
5. Click *Enable MDM Integration*.
6. From the *Vendor* dropdown list, select *ManageEngine MDM Plus*.
7. For *Deployment*, select *On-Premise*.
8. In the *Site URL* field, enter your ManageEngine server URL.
9. In the *API Key* field, enter the key that you generated in step 3.

To configure integration between cloud ManageEngine and EMS:

EMS must have a set of Zoho OAuth credentials: client ID and secret.

1. In the Zoho developer console, under *Choose a Client Type*, click *Self Client*.



   The console displays a client ID and secret set.
2. In EMS, go to *System Settings* > *MDM Integration*.
3. Click *Enable MDM Integration*.
4. From the *Vendor* dropdown list, select *ManageEngine MDM Plus*.
5. For *Deployment*, select *Cloud*.
6. From the *Region* dropdown list, select your assigned geographic region.
7. In the *Client ID* field, enter your ManageEngine client ID that you generated in step 1.
8. In the *Client Secret* field, enter your ManageEngine client secret that you generated in step 1.

Configuring ManageEngine integration to allow FortiClient (iOS) to connect to EMS

ManageEngine integration allows FortiClient endpoints to connect to EMS.

To configure integration between ManageEngine and FortiClient (iOS):

1. In ManageEngine Endpoint Central, go to *Mobile Device Mgmt* > *Management* > *App Repository*.
2. Under *Apps*, click *Add App*.
3. Search for and select FortiClient (iOS).
4. Open a text editor and configure an XML file to upload to ManageEngine. The following provides an example that only configures the `manageengine_device_id` key:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>manageengine_device_id</key>
    <string>%devicename%|%udid%</string>
  </dict>
</plist>
```

Key	Description
`cloud_invite_code`	This value is used for connecting FortiClient to FortiClient Cloud. Enter the invite code received from FortiClient Cloud. This key is mainly meant to support 7.2.2 and earlier versions, as the new `invitation_code` key is available for FortiClient (iOS) 7.2.3 and later versions. However, you can continue to use `cloud_invite_code` for FortiClient (iOS) 7.2.3 and later versions if you do not configure `invitation_code`. This key does not support configuring invitation codes from on-premise EMS.
`ems_key`	Telemetry connection key. The EMS administrator may require FortiClient to provide this key during connection.
`ems_port`	EMS port number.
`ems_server`	EMS server IP address.
`group_tag`	This value is used as a group tag for configuration in EMS. EMS uses this value as an installer ID to assign the endpoint to a group. See Group assignment rule types.
`invitation_code`	Enter the FortiClient Cloud or on-premise EMS invitation code. FortiClient 7.2.3 and later versions support this key.

Key	Description
`mac_address`	iOS device MAC address.
`udid`	iOS device UDID.
`should_show_login_page`	Set to true or false to configure whether FortiClient displays a login page and privacy policy highlights to the user upon launch.

You can use one of `cloud_invite_code`, `ems_server` and `ems_port`, or `invitation_code` to define the FortiClient to EMS connection. For example, you cannot configure both `cloud_invite_code` and `ems_server` and `ems_port`. Invitation codes include the EMS IP address and port.

5. Save the file as an XML file
6. In ManageEngine, in the *App Configurations* field, browse to and upload the XML file.
7. Click *Save*.
8. When FortiClient starts on the device, it automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration.

Configuring ManageEngine integration to allow FortiClient (Android) to connect to EMS

ManageEngine integration allows FortiClient endpoints to connect to EMS.

To configure integration between ManageEngine and FortiClient (Android):

1. In ManageEngine Endpoint Central, go to *Mobile Device Mgmt* > *Management* > *App Repository*.
2. Under *Apps*, click *Add App*.
3. Search for and select FortiClient (Android).
4. Configure the following fields:

Field	Description
Enter EMS Server IP	EMS IP address or hostname.
Enter EMS Server Port	Port number for FortiClient to connect Telemetry to EMS. By default, this is 8013.
Enter EMS Server Key	Telemetry connection key. The EMS administrator may require FortiClient to provide this key during connection.
Enter Cloud Invite Code	FortiClient uses this value to connect to FortiClient Cloud. Enter the invite code that you received from FortiClient Cloud.
Enter Invitation Code	Enter the FortiClient Cloud or on-premise EMS invitation code. FortiClient 7.2.3 and later versions support this key.
Enter User Name	FortiClient username. You may want to avoid showing users the option to configure their own username. You must also configure *Should Show Login Page* to *false* so that users do not see the login page where they can provide their username.
Enter MAC Address	Device MAC address.
Enter Group Tag	This value is used as a group tag for configuration in EMS. EMS uses this value as an installer ID to assign the endpoint to a group. See Group assignment rule types.
Should Show Login Page	Configure whether FortiClient presents a login page to the user. Enter `true` to present the login page and `false` to skip the login page.
ManageEngine Device Id	Enter %devicename%|%udid%

   You can use one of *Enter Cloud Invite Code*, *Enter EMS Server IP* and *Enter EMS Server Port*, or *Enter Invitation Code* to define the FortiClient to EMS connection. For example, you cannot configure both *Enter Cloud Invite Code* and *Enter EMS Server IP* and *Enter EMS Server Port*. Invitation codes include the EMS IP address and port.
5. Click *Save*.
6. When FortiClient starts on the device, it automatically connects to on-premise EMS or FortiClient Cloud, depending on the configuration.

www.fortinet.com

Copyright© 2025 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 Chief Legal Officer, 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.