



FortiAP Cloud - Administration Guide

Version 3.3.2

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 COOKBOOK

<https://cookbook.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: techdocs@fortinet.com



January 28, 2019

FortiAP Cloud 3.3.2 Administration Guide

32-332-535363-20190128

TABLE OF CONTENTS

FortiAP Cloud	4
Frequently asked questions	5
What is FortiAP Cloud?	5
How can I register a FortiAP to my FortiAP Cloud account?	6
What is the recommended FortiAP version to use with FortiAP Cloud 3.3?	6
What port numbers are used by FortiAP devices connecting to FortiAP Cloud?	6
What happens if my FortiAP loses connection with FortiAP Cloud?	6
I have an older FortiAP that doesn't include a FortiAP Cloud key. Is there some way I can add my device to FortiAP Cloud?	6
What FortiAP models are supported by FortiAP Cloud?	7
Does FortiAP Cloud support FortiWiFi?	7
Is there a minimum FortiAP firmware version that I need for FortiAP Cloud to work?	7
Does my internal wireless/networking traffic get sent to FortiAP Cloud?	7
Do I need to use a FortiGate in conjunction with FortiAP Cloud?	7
What is the price of FortiAP Cloud?	7
Can FortiAP devices be managed by FortiAP Cloud and work with FortiPresence?	8
Is there a maximum number of FortiAP devices that can be managed via FortiAP Cloud?	8
How does roaming work for a FortiAP Cloud-managed FortiAP?	8
What is the admin password for my FortiAP?	8
What is the Social Media Captive Web Portal?	8
What is the Self-Registered Guest Captive Portal?	8
What is the NAT IP subnet of my FortiAP SSID configuration?	9
What is Floorplan in Maps?	9
What are Folders?	9
How do dynamic VLANs work?	9
What is Bonjour Relay?	9
What is blocking of intra-SSID traffic?	10
Why do I need to change my radio rates in the Enterprise Management section?	10
FortiAP Cloud Cookbook	11
Adding a standalone FortiAP to FortiAP Cloud	11
Configuring a basic secure SSID	11
Configuring a guest SSID	11

FortiAP Cloud

This guide provides information about FortiAP Cloud. It's divided into the following sections:

- [Frequently asked questions](#): answers to commonly asked questions about FortiAP Cloud.
- [FortiAP Cloud Cookbook](#): a series of short-form tutorials that teach how to perform tasks in FortiAP Cloud, ranging from basic to complex.



As of FortiCloud 3.2.2, the FortiCloud service has been separated into two distinct parts: FortiCloud, which you use to manage FortiGate devices, and FortiAP Cloud, which you use to manage FortiAP devices (FortiAP Cloud contains functions formerly called FortiAP Network).

This guide contains information about FortiAP Cloud. For information about FortiCloud, please see the FortiCloud Administration Guide.

Frequently asked questions

This section includes the following general questions:

- [What is FortiAP Cloud?](#)
- [How can I register a FortiAP to my FortiAP Cloud account?](#)
- [What is the recommended FortiAP version to use with FortiAP Cloud 3.3?](#)
- [What port numbers are used by FortiAP devices connecting to FortiAP Cloud?](#)
- [What happens if my FortiAP loses connection with FortiAP Cloud?](#)
- [I have an older FortiAP that doesn't include a FortiAP Cloud key. Is there some way I can add my device to FortiAP Cloud?](#)
- [What FortiAP models are supported by FortiAP Cloud?](#)
- [Does FortiAP Cloud support FortiWiFi?](#)
- [Is there a minimum FortiAP firmware version that I need for FortiAP Cloud to work?](#)
- [Does my internal wireless/networking traffic get sent to FortiAP Cloud?](#)
- [Do I need to use a FortiGate in conjunction with FortiAP Cloud?](#)
- [What is the price of FortiAP Cloud?](#)
- [Can FortiAP devices be managed by FortiAP Cloud and work with FortiPresence?](#)
- [Is there a maximum number of FortiAP devices that can be managed via FortiAP Cloud?](#)
- [How does roaming work for a FortiAP Cloud-managed FortiAP?](#)
- [What is the admin password for my FortiAP?](#)
- [What is the Social Media Captive Web Portal?](#)
- [What is the Self-Registered Guest Captive Portal?](#)
- [What is the NAT IP subnet of my FortiAP SSID configuration?](#)
- [What is Floorplan in Maps?](#)
- [What are Folders?](#)
- [How do dynamic VLANs work?](#)
- [What is Bonjour Relay?](#)
- [What is blocking of intra-SSID traffic?](#)
- [Why do I need to change my radio rates in the Enterprise Management section?](#)

What is FortiAP Cloud?

This feature allows administrators to remotely configure FortiAP devices, modify wireless management settings and visualize wireless-related events. Examples of configuration changes include FortiAP name and SSID configuration, power settings and rogue AP detection. Wireless management settings include RADIUS details, standard users/groups/guests and SSIDs/security. There are a robust set of visualizations including real-time and historical charting of traffic usage, FortiAP client counts and client usage. Think of it as a comprehensive way to manage your wireless infrastructure via the cloud.

How can I register a FortiAP to my FortiAP Cloud account?

Supported FortiAP models include a sticker with a unique FortiAP Cloud key affixed. This key must be entered into the FortiCloud interface to register the FortiAP to your FortiAP Cloud account.

What is the recommended FortiAP version to use with FortiAP Cloud 3.3?

We recommend FortiAP version 5.6 or later for use with FortiAP Cloud 3.3. It is always our recommendation that you run the latest GA firmware on your FortiAP devices.

What port numbers are used by FortiAP devices connecting to FortiAP Cloud?

Please note that these should be required by OUTBOUND traffic only. On request, we can supply the destination IP addresses to add to an outbound policy, if required.

Device	Purpose	Protocol/Port
FortiAP, FortiAP-S, FortiAP-C, FortiAP-U	Initial Discovery	TCP/443
FortiAP, FortiAP-S, FortiAP-C, FortiAP-U	CAPWAP Tunnel, Event Logs	UDP/5246, UDP/5247
FortiAP, FortiAP-S, FortiAP-C, FortiAP-U	Syslog, OFTP, Registration, Quarantine, Log & Report	TCP/514
FortiAP-S	FortiGuard	UDP/53, UDP/8888

What happens if my FortiAP loses connection with FortiAP Cloud?

If your FortiAP loses connection to FortiAP Cloud, or in the unlikely event that the FortiAP Cloud service is unavailable, then all functions which are not hosted in FortiAP Cloud will continue to work without interruption. The configuration is held locally on the FortiAP, and will continue to function.

Only SSIDs with authentication in FortiAP Cloud will be disrupted: FortiAP Cloud-hosted Captive Web Portals, and FortiAP Cloud User Groups. Open, WPA2 PSK, and WPA2 802.1X RADIUS SSIDs that are not using FortiAP Cloud-hosted authentication (such as ones using local RADIUS server or Local Captive Portal) will continue to work uninterrupted.

I have an older FortiAP that doesn't include a FortiAP Cloud key. Is there some way I can add my device to FortiAP Cloud?

Older FortiAP devices that have shipped without a FortiAP Cloud key can be added to FortiAP Cloud. Open the FortiAP management interface, and in **WTP-Configuration** select **FortiCloud**. Enter your FortiAP Cloud credentials, and select **Apply**. Log in to FortiAP Cloud and select **Inventory > Unused APs** to see the list of FortiAP devices. Select **Deploy to AP Network > Existing AP Network**.

What FortiAP models are supported by FortiAP Cloud?

FortiAP Cloud supports all FortiAP models.

Does FortiAP Cloud support FortiWiFi?

FortiAP Cloud doesn't current support FortiWiFi devices.

Is there a minimum FortiAP firmware version that I need for FortiAP Cloud to work?

The FortiAP must be running FortiAP OS 5.2 at a minimum. It is recommended to run the latest software build on the FortiAP to guarantee FortiAP Cloud functionality.

Does my internal wireless/networking traffic get sent to FortiAP Cloud?

No. Fortinet uses an out of band management architecture, meaning that only management data flows through the FortiAP Cloud infrastructure. No user traffic passes through Fortinet's datacenters, and your data stays on your network.

Do I need to use a FortiGate in conjunction with FortiAP Cloud?

No. We recommend you register your FortiAP to be directly managed by FortiAP Cloud. You do not need to use a FortiGate unit as a proxy to manage FortiAP devices from FortiAP Cloud.

What is the price of FortiAP Cloud?

A no-charge service option is available with unlimited storage is available for one week.

There is also an annual-subscription-based service, with one, two, or three-year service terms. The new service provides 1 year of history, regardless of size. To activate FortiAP Cloud, you need to acquire a subscription license based on the following SKUs, available with 1, 2, and 3-year service terms:

Description	SKU
FortiAP Cloud Enterprise AP Licenses	
FAP/FAP-U/FAP-C	FC-10-90AP1-170-02-DD
FAP-S	FC-10-90APS-170-02-12

For pricing information, please contact your Fortinet partner or reseller.

Can FortiAP devices be managed by FortiAP Cloud and work with FortiPresence?

Yes, FortiPresence is supported by FortiAP devices and managed by FortiAP Cloud. For location analytics, the FortiAP uses a Push API to communicate with FortiPresence. You can configure this under **Configure > FortiPresence**.

Is there a maximum number of FortiAP devices that can be managed via FortiAP Cloud?

There is no licensing limit for the number of FortiAP devices that can be managed with FortiAP Cloud.

How does roaming work for a FortiAP Cloud-managed FortiAP?

FortiAP devices that are in the same management subnet communicate using encrypted communications and share station and authentication information. This means that when a client connected via Captive Web Portal, 802.1X or PSK moves from one access point to another, there is no re-authentication required and a session transition should happen once the client decides to roam.

What is the admin password for my FortiAP?

When you add FortiAP Cloud, you are asked to define a password for it. This password is used as the admin password for all FortiAP devices inside FortiAP Cloud. You can change the password by going to **Configuration > Miscellaneous**.

What is the Social Media Captive Web Portal?

Social Media Captive Web Portal is the functionality that creates a Captive Web portal where a user's social media login is used as authentication. This is hosted in FortiAP Cloud, and currently supports Facebook, Google+, LinkedIn, and Twitter accounts. The Captive Web Portal can be customized with different colors and logos.

We recommend a Terms of Use be added to the Captive Web Portal, matching with the legal requirements of your jurisdiction. Please see the disclaimer on the configuration page for more details.

What is the Self-Registered Guest Captive Portal?

Self-Registered Guest Captive Portal is the functionality that creates a Captive Web portal that requires a user to create an account, by specifying some information you choose. You can choose what form the username takes, and the Captive Web Portal can be customized with different colors and logos.

We recommend a Terms of Use be added to the Captive Web Portal, matching with the legal requirements of your jurisdiction. Please see the disclaimer on the configuration page for more details.

What is the NAT IP subnet of my FortiAP SSID configuration?

If you want each FortiAP to provide its own NAT boundary rather than bridge users directly onto the local network, you can now assign the subnet for the FortiAP to use in the SSID configuration.



A known limitation is that the subnet will be assigned only on the 2.4Ghz radio. The 5Ghz radio will use a subnet 17 octets higher. For example, if the 2.4Ghz radio is set to use 10.10.10.1/24, the 5Ghz radio will use 10.10.17.1/24. This limitation will be addressed in a future software release.

What is Floorplan in Maps?

In FortiAP Cloud, you can now add a floorplan and zoom into it to place your FortiAP devices and see their statistics and RF information. Previously, you could use Google Maps integration to see a floorplan overlaid over a building, but now full zoom and positioning controls have been added.

What are Folders?

Folders are a simple way to group FortiAP devices together for management purposes, and can be used to organize FortiAP devices into groups, sites or any other organization you see fit. You can create subfolders and also assign new addresses and locations to FortiAP devices.

How do dynamic VLANs work?

RADIUS servers can be configured to pass class attributes back in response to a successful authentication. One of these attributes is the VLAN to which the client should be assigned. With an Enterprise license and this feature enabled, it is possible to place different types of users connected to the same SSID into different VLANs, based on their user credentials.

What is Bonjour Relay?

Bonjour is a protocol where (typically Apple) devices broadcast their services. For example, an Apple TV sends a Bonjour broadcast, so that an iPad knows it is there and can connect to it.

The issue is that these broadcasts are layer 2 – so if the iPad and the Apple TV are on different VLANs, then they will not be able to talk. Bonjour Relay is a simple mechanism to fix this. The FortiAP-S series can be set to operate with a service network (where the Apple TV is), and a client network (where the iPad is), allowing the FortiAP-S to re-transmit the Bonjour requests from the service network onto the client network, allowing the iPad to learn where the Apple TV is and create a session.

To set it up, enter one or more services as Service VLAN and Client VLAN, along with a definition of the service, e.g. you may choose to only send the information about the Apple TV to a meeting room, and not the printer in reception. Once these services have been defined, simply select the FortiAP that will perform the Bonjour Relay function.

What is blocking of intra-SSID traffic?

This feature blocks all traffic from one client to another on the same SSID. This helps to avoid a common issue of clients sending data between themselves on the same SSID, without traversing and being protected by the firewall.

Why do I need to change my radio rates in the Enterprise Management section?

Wireless operates at many different data rates based on the quality of the radio signal. For example, an 802.11n 2.4GHz client is capable of running at 450 Mbps on a 3x3 FortiAP, but it is equally capable of running at 1 Mbps.

Inconsistent radio rates can lead to clients remaining connected to an FortiAP long after they should have reconnected to a better FortiAP. A client running at 1 Mbps has great range, but its slow throughput will have a degrading effect on the network performance as a whole. The new data rate control feature in 3.1 allows you to restrict which data rates are allowed, to ensure clients that are too far away are not slowing down the overall system.

FortiAP Cloud Cookbook

This series of short tutorials will show you how to enable and set up various FortiAP Cloud services and features.

Adding a standalone FortiAP to FortiAP Cloud

1. Connect to FortiAP Cloud.
2. Select **Add Device** and enter the unique FortiCloud key located on your FortiAP device.
3. Deploy the FortiAP to an existing AP network or create a new AP network.
4. Associate your FortiAP with an SSID.
5. Connect your FortiAP to an internet connection, and wait for it to self-configure.
6. Log into the [FortiCloud Portal](#) to configure the FortiAP further.

Configuring a basic secure SSID

1. Go to **Configure > SSIDs** and select **Add SSID**.
2. Configure the **Access Control** settings as required.
3. Configure the required **Security** settings.
4. Configure **Availability**.
5. Preview the settings for the SSID. If they are correct, select **Apply**.

Configuring a guest SSID

1. Go to **Configure > SSIDs** and select **Add SSID**.
2. In **Access Control**, set **Captive Portal** to **FortiCloud Captive Portal** and set **Sign on Method** to **Self-Registered Guests**.
3. Configure additional **Access Control** settings as required.
4. Configure the required **Security** settings.
5. Configure **Availability**.
6. In **Captive Portal**, select **Self-Registered** and configure settings as required.
7. Configure additional **Captive Portal** settings as required.
8. Preview the settings for the SSID. If they are correct, select **Apply**.



FORTINET[®]



Copyright© 2019 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.