

FortiPresence

Release 4.3.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://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

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

[Email: techdocs@fortinet.com](mailto:techdocs@fortinet.com)

Contents

Product Overview	4
Supported Browsers and Platforms	6
Signing-on for FortiPresence.....	7
Registering on <i>Fortinet One</i>	9
Accessing FortiPresence	9
New Features	11
Site Business Time	11
Automatic Exclusion of Fixed Assets	11
SMS Integration for Portal Logins	12
Email Notification for Inactive APs	12
Sorting Discovered APs Per Site	12
Additional Notes	13
Fixed Issues	14
Known Issues.....	15
FortiPresence.....	15
FortiWLC.....	15
END USER LICENSE AGREEMENT	16
Contact.....	16

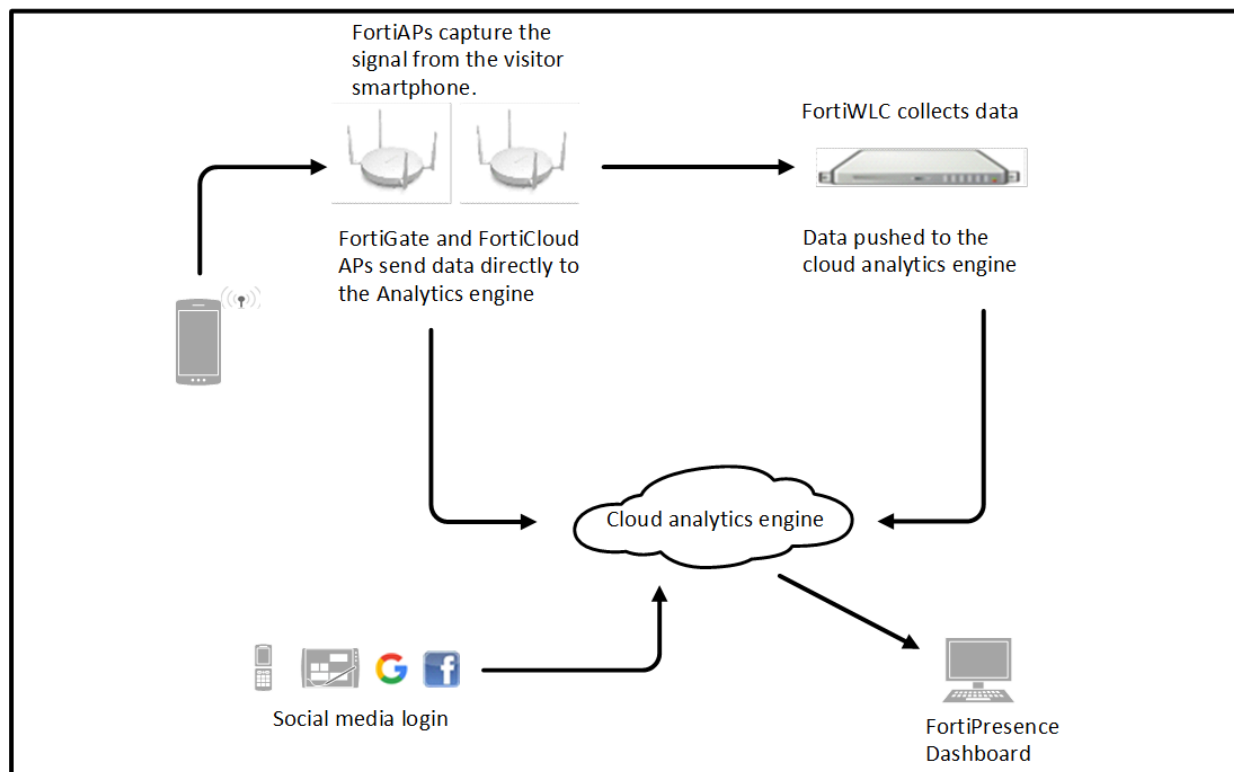
Product Overview

FortiPresence is a secure cloud-based comprehensive data analytics solution designed for analyzing user traffic and derives usage patterns. By capturing analytics of consumer traffic patterns, businesses can learn more about their customers. FortiPresence combines WiFi and analytics to deliver end-to-end solution by providing data needed to understand customer behaviour. It includes comprehensive dashboards for data analysis and reports.

The existing Fortinet access points deployed at business establishments are leveraged to detect Wifi signals from customer. In a typical business setup, visitor smartphones/devices probe for wireless access points, FortiPresence uses the signals emitted from these smartphones/devices to detect customer presence and record their location and movements. This information along with the social network authentication logins with Facebook, Google, or FortiPresence using your WiFi infrastructure is then processed in a cloud based analytics engine and presented on the customizable dashboards on the FortiPresence GUI.

FortiPresence provides an end-to-end presence analytics solution with the following key features:

- **Cloud-based Service** — No hardware to procure or maintain implies reduction of costs and quick and easy deployment.
- **Presence and Positioning Analytics** — The customizable dashboards and reports provide real-time location trends and presence analytics with animated maps and video play options to view and compare visitor data across sites.
- **Site and Portal Management** — The sites can be located using Google maps/created and floors planned for effective visitor data analysis. The visitor can login into your WiFi infrastructure using Facebook, Google social authentication, or a customized visitor portal.
- **Access Point Support** — The FortiPresence solution supports all Fortinet wireless access points. FortiGate, FortiCloud wireless access points (send visitor data in the form of station reports directly to FortiPresence), and FortiWLC wireless access points (send visitor data in the form of station reports to the FortiWLC controller which redirects data to FortiPresence).



This is an example of FortiPresence in a retail setup.

1. Smartphone emits a WiFi probe signal and the FortiAPs capture the MAC address information.
2. FortiAPs or FortiWLC summarizes and forwards the data records.
3. FortiPresence analytics engine receives data via a secure SSL connection and processes it.

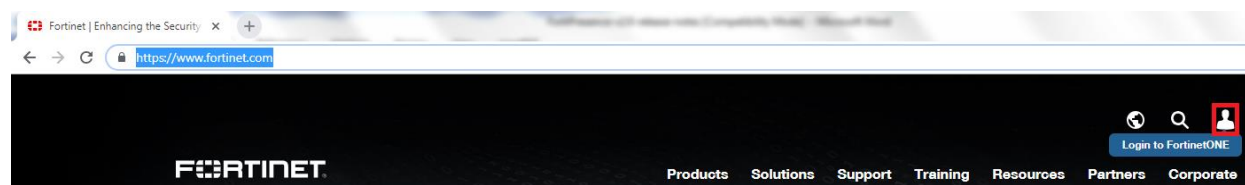
Supported Browsers and Platforms

These are the browsers and platforms supported for FortiPresence.

Supported Browsers	
Operating System/Device	Browser
Windows	• Google Chrome (76.0.3809.100) • Mozilla Firefox (68.0.1)
Apple MAC	• Google Chrome (76.0.3809.100) • Safari (12.1.2(14607.3.9)) • Mozilla Firefox (68.0.1)
Supported Platforms	
• FortiWLC • FortiGate • FortiCloud	

Signing-on for FortiPresence

This release provides single sign-on support for FortiPresence along with *Fortinet One* suite of products. FortiPresence is accessible via the *Fortinet One* GUI - <https://support.fortinet.com> and <https://presence.fortinet.com>. However, if you access <https://presence.fortinet.com>, you are redirected to the *Fortinet One* login page. The *Fortinet One* login page can also be accessed via <https://www.fortinet.com/>.



How do I login if...?	Steps
I am a new user of FortiPresence	1. Registering on Fortinet One 2. Accessing FortiPresence
I am an existing user of FortiPresence but not registered on https://support.fortinet.com	
I am an existing user of FortiPresence and registered on https://support.fortinet.com with the same email ID as that of the FortiPresence account.	1. Accessing FortiPresence
I am an existing user of FortiPresence and registered on https://support.fortinet.com with a different email ID as that of the FortiPresence account.	1. Login into https://support.fortinet.com to map your <i>Fortinet One</i> email ID to your existing FortiPresence account. 2. Once logged in, select FortiPresence from the product banner as described in Accessing FortiPresence, you are provided with options to setup a new FortiPresence account or migrate your existing account. 3. Select the option to migrate the existing FortiPresence account and then provide your FortiPresence account details - email ID, password, and other fields.

Register to FortiPresence

New Registration

Migrate

FortiPresence Email* :

Enter FortiPresence email

It is an optional field. Enter your FortiPresence email id. We will link your existing FortiPresence account with support account.

FortiPresence Password* :

Enter FortiPresence password

Enter FortiPresence password.

Support Email* :

abhissodhar6@gmail.com

This is your support email id.

Select Country* :

Select Country

Select country for your account.

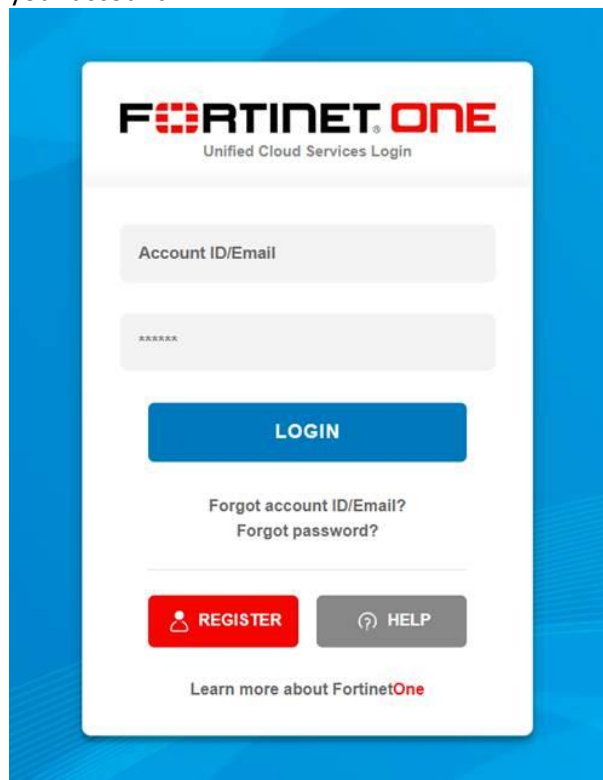
Submit

Your FortiPresence account is migrated to the <https://support.fortinet.com> registered email ID.

Registering on Fortinet One

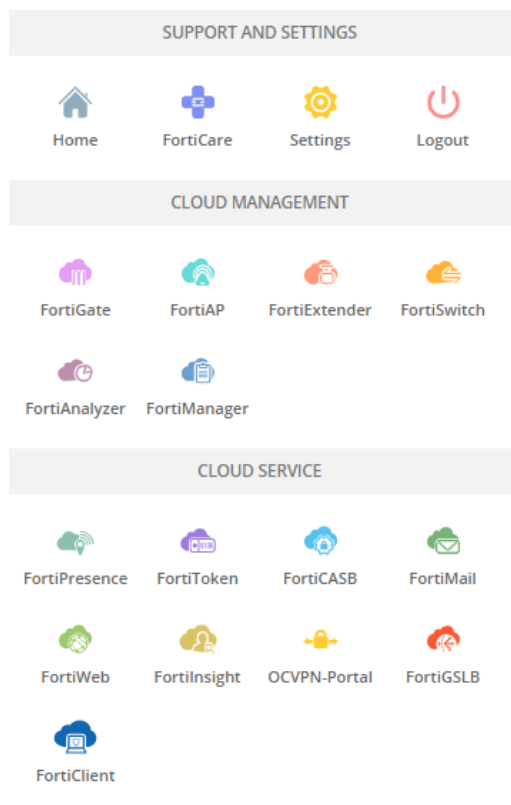
Prior to using FortiPresence, you are required to register on the *Fortinet One* portal.

Use the <https://support.fortinet.com> access link to register on the *Fortinet One* portal. A security code is emailed to the address specified during registration; use the code to complete registration and activate your account.



Accessing FortiPresence

Any user registered on <https://support.fortinet.com> can access FortiPresence. Once you login into *Fortinet One*, click on your email ID, a banner with Fortinet products is displayed. Select **FortiPresence**. You are redirected to the FortiPresence GUI - <https://presence.fortinet.com>.



Notes:

1. This product banner is available on the FortiPresence GUI as well for you to toggle to any other registered products.
2. RBAC users created under **User Management** are required to have the respective user email accounts registered in *Fortinet One* in order to use FortiPresence. Consider the following example, with these registered login credentials for different accounts:
 - FortiPresence Account owner – **alpha@gmail.com**
 - *Fortinet One* Account owner – **alpha@gmail.com**
 - FortiPresence RBAC user – **beta@gmail.com**

The RBAC user can register on the *Fortinet One* portal for an individual account (**beta@gmail.com**) which is the master account and he is the owner.

OR

The RBAC user can also be added as a sub-account under the master account of the *Fortinet One* (**alpha@gmail.com**).

In both these scenarios, the RBAC user is able to login into FortiPresence and view the account of **alpha@gmail.com**.

New Features

This release of FortiPresence includes the following new features.

- [Site Business Time](#)
- [Automatic Exclusion of Fixed Assets](#)
- [SMS Integration for Portal Logins](#)
- [Email Notification for Inactive APs](#)
- [Sorting Discovered APs Per Site](#)

Site Business Time

You can now configure data collection for the FortiPresence dashboards for a specific number of hours during a day. Configure the **Opening Time** and **Closing Time**; this threshold is configured per site.

Note: This feature is available only for paid tier users.

Navigate to *Admin > Settings > Threshold > Site Business Time*.

Site business time:

This setting helps in having the data collected only during Site's business hours. For ex. Only between 9.00 am to 5.00 pm instead of collecting data for whole day.

This setting is applicable only for **all the dashboards**

Opening Time	HH 10	▼	:	MM 30	▼
Closing Time	HH 17	▼	:	MM 30	▼

Automatic Exclusion of Fixed Assets

You can specify threshold parameters that determine fixed assets to be excluded from analytics.

If a device MAC address is detected for more than the configured number of hours per day for the configured number of (consecutive) days then that device is declared a fixed asset and is excluded from analytics.

Note: This feature is available only for paid tier users.

Navigate to *Admin > Settings > Threshold > Detected Fixed Assets*.

Detected Fixed Assets:

This setting helps in having the data collected for selected number of hours for last configured consecutive days.

☒ **Filter Fixed Assets**

HH 4	▼	DD 5	▼
---------	---	---------	---

SMS Integration for Portal Logins

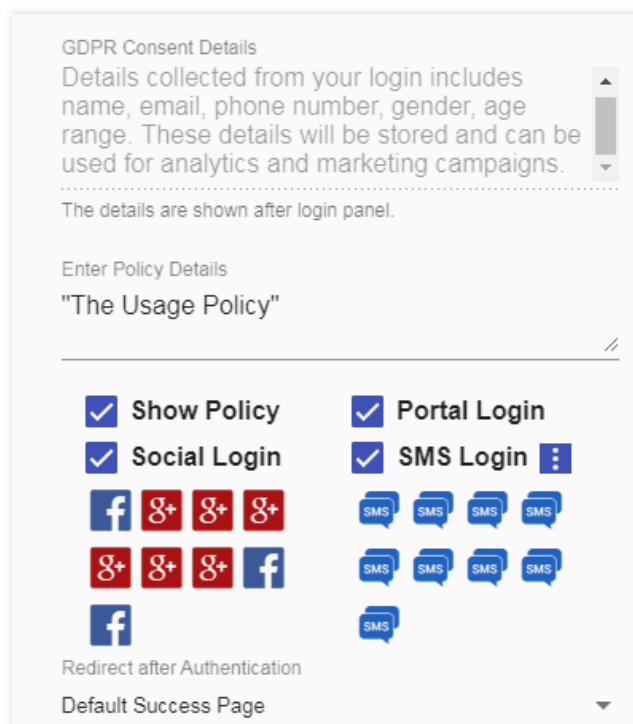
Visitors can now login to portals using a One Time Password (OTP) sent via SMS on the user provided mobile number. A specific SMS provider is configured and attached to each portal. All SMS OTP based logins are included in the *FortiPresence* authentication type in the dashboard and reports.

Note: This feature is available only for paid tier users.

To configure the SMS provider, navigate to *Admin > Settings > SMS Provider*.

To attach the SMS provider to new or existing portals, navigate to *Admin > Portal Management* (add new portal or edit an existing portal).

Add Portal



The screenshot shows the 'Add Portal' configuration interface. It includes a 'GDPR Consent Details' section with a text area for consent information and a 'Show Policy' checkbox. Below this is the 'Enter Policy Details' section with a text area for the policy name, currently set to 'The Usage Policy'. The 'Portal Login' section contains checkboxes for 'Show Policy', 'Social Login', 'Portal Login', and 'SMS Login'. The 'Social Login' section displays icons for Facebook, Google+, and Twitter. The 'SMS Login' section displays icons for various SMS providers. At the bottom, there is a 'Redirect after Authentication' section with a 'Default Success Page' dropdown menu.

Email Notification for Inactive APs

If FortiPresence does not receive the Identification (ID) packets for any of the planned APs in the discovered AP list (*Admin > Settings > Discovered APs*) for more than 24 hours, a notification is sent to the FortiPresence registered email address of the account containing the list of such AP/APs which are in inactive state. The email notification is sent once every day until all planned APs return to active state.

Note: This feature is available only for paid tier users.

Sorting Discovered APs Per Site

In the Discovered APs tab, you can sort data per site in order to visualize easily which APs are planned/unplanned.

Navigate to *Admin > Settings > Discovered APs*.

Additional Notes

This section describes some generic guidelines/information to using FortiPresence.

- Any create and delete operation can take up to a maximum of 3 minutes to be visible on the FortiPresence GUI.
- For setups involving multiple devices (FortiWLC/FortiGate) behind the NAT sharing the same public IP address, you are required to create a RADIUS client entry for each device type on the FortiPresence GUI.
- **FortiWLC:** The FortiWLC SSID must be configured in the tunnel mode; SSIDs in the bridge mode are NOT supported for Captive Portals.
- **FortiGate/FortiCloud:** While configuring settings on SSID, set the *Redirect URL* to *Specific URL* and configure <https://connect.presence.fortinet.com/portal/success> as the URL. This is required for FortiPresence to register the device and user details. FortiPresence Portal Management provides options to set redirect after authentication to *Original Request URL*, *Specific URL*, or *Default Success Page*.
- **FortiGate:** The supported authentication methods for FortiPresence are PAP, MS-CHAP, MS-CHAP-v2.
- FortiPresence is **General Data Protection Regulation (GDPR)** compliant.
 - MAC addresses are not stored in FortiPresence; each visitor is referred by a unique *User Key*.
 - Personal details are not stored without the visitor's consent - While logging on to FortiPresence, the visitor is presented with clear information about personal details being collected from the social network logins. Personal details, such as, name, gender, age, email etc. are stored only if the visitor gives an *explicit consent*, else such information is not stored.

Fixed Issues

These issues are fixed in this release of FortiPresence.

Bug ID	Description
536110	GUI sluggishness observed when a large number of APs and sites are added.
567847	Unable to download the Device reports with huge data.
533294	Sometimes, there is error in downloading the Device/Network/Site reports with huge data or with filters applied.
536860	The reports and dashboard keep refreshing when the GUI pages fail to load due to huge data size.
534133/532240	Large data for the Presence dashboard and reports does not load on the GUI with error 502.
568851	Unable to retrieve data in the reports based on data filters.
558936	Incorrect dwell time calculations observed.
568467	Unable to download Multisite report.
536596	The <i>Cutoff-RSSI</i> value on AP already placed on a plan could not be modified.
520487	Improved the visualization of connected user-unknown user, male and female clients for floor analytics.
506664	Optimized the performance of APIs for social network, visitor area chart and delete AP.
457872	Repeat users for the current day not considered in FortiPresence.
567838	Incorrect date (1 month delay) displayed in the hover over text for visitor details in floor analytics.
541235	On the Presence dashboard, values for New Visitors vs Repeated Visitors and Bounce Rate are incorrect for a floor or building.
541242	The Presence dashboard always displays an extra day (and displays averaged values including that extra day).
541241	On the FortiPresence dashboard, the dwell time for the week and the average dwell time do not match.
541247	Site report statistics for visitor per day inconsistent with the data on the Presence dashboard.
520255	Add timestamps to display device sample in floor analytics dashboard.
520265	Device report shows repeated entries with only one visit.
522305	The AP's TX power level (EIRP) cannot be modified once an AP has been configured and placed on the floor plan.

Known Issues

These are the known issues in this release of FortiPresence.

FortiPresence

Bug ID	Description	Workaround
527117	Video playback throws error 502 when the data populated is huge.	Select video playback for a lesser date range and for a data set less than 200K devices.
506661	Playback video performance degrades with huge data.	Ensure that the total number of devices seen during the selected date range for video playback does not exceed 200K.
486027	URL redirection from HTTP to HTTPs not happening for presence.fortinet.com.	
541212	Inaccurate location tracking for a stationary client on the map.	
462376	RADIUS authentication fails when two RADIUS clients are created with the same public IP address and different shared secrets.	Use same shared secrets for both RADIUS clients.
560678	The heat map information is accurate only when the current view time threshold is short.	
560397	No filters available in the heat maps.	
554639	Area analytics does not monitor transitions between multiple floors or multiple sites.	
462644	In the Current View dashboard, with ALL selected as the filter, inaccurate data is displayed. This issue is observed when sites are added/deleted.	
482396	While importing APs the required Tx power is per AP and not per radio.	
527116	Changes in the <i>Fortinet One</i> account details such as user name and company name do not get updated in the FortiPresence dashboard.	
577888	Users authenticating via Google have to authenticate twice to login successfully.	

FortiWLC

Bug ID	Description	Workaround
574550	Radio MAC address is not displayed on ID and STA packets for all APs after upgrade.	

END USER LICENSE AGREEMENT

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

Contact

For assistance, contact Fortinet Customer Service and Support 24 hours a day at +1 408-542-7780, or by using one of the [local contact numbers](#), or through the Support portal at <https://support.fortinet.com/>

Fortinet Customer Service and Support provide end users and channel partners with the following:

- Technical Support
- Software Updates
- Parts replacement service



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.