

Administration Guide

FortiPresence 22.4



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://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

December 06, 2022

FortiPresence 22.4 Administration Guide

69-224-865552-20221206

TABLE OF CONTENTS

Change log	5
Overview	6
How FortiPresence Works	8
FortiPresence User Interface overview	10
GUI Data Limits – Dashboards and Reports	12
Licensing	13
Viewing License Information	14
Signing-on for FortiPresence	15
Registering on FortiCloud	16
Accessing FortiPresence	19
External IDP Authentication	20
Dashboards and Reports	23
Presence Dashboard	23
Dashboards Filtering	24
Average Statistics	24
Visitor Analytics	24
Device Analytics	26
Site Analytics	27
Current View Dashboard	29
Reports	30
Connected Visitor Reports	30
Network Reports	31
Site Report	32
Multi Site Report	33
Device Report	34
Location Analytics	35
Floor Analytics	35
Heat maps	35
Footfall	36
Area Analytics	36
Administering FortiPresence	38
Site Management	38
Portal Management	43
Creating a Portal	43
Configuring Site Rules and Users	47
RADIUS Configuration	48
Portal Settings	48
Administrative Settings	49
User Management	51
Configuring Location Services	52
FortiLAN Cloud	52
FortiGate	53

FortiWLC	54
Configuring Captive Portal	56
FortiLAN Cloud	57
FortiGate	58
FortiWLC	62
Schedule Configuration	64

Change log

Date	Change description
2022-12-06	FortiPresence version 22.4 release document.

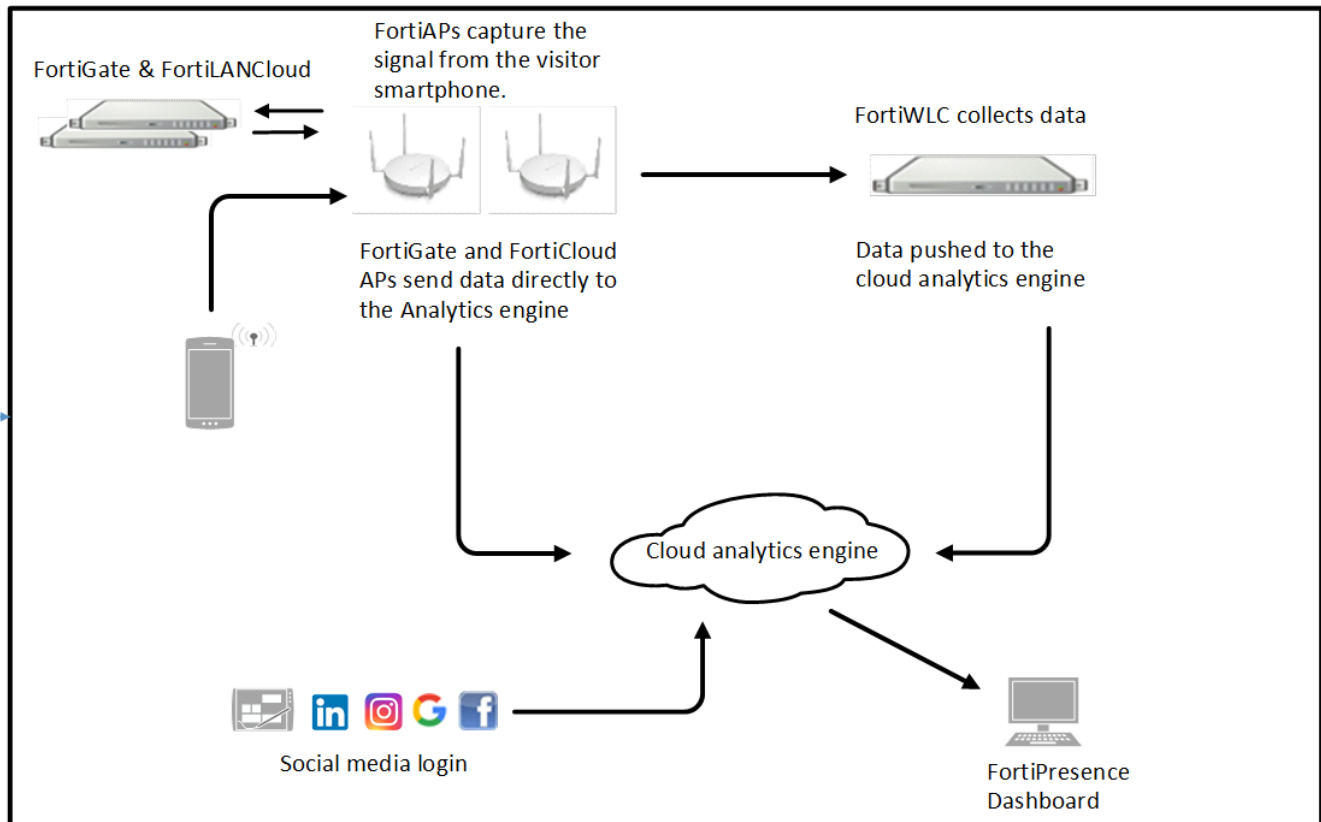
Overview

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, Instagram, LinkedIn, 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, Instagram, or LinkedIn social authentication, or a captive portal user.
- **Access Point Support** — The FortiPresence solution supports all Fortinet wireless access points. FortiGate, FortiLANCloud 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.

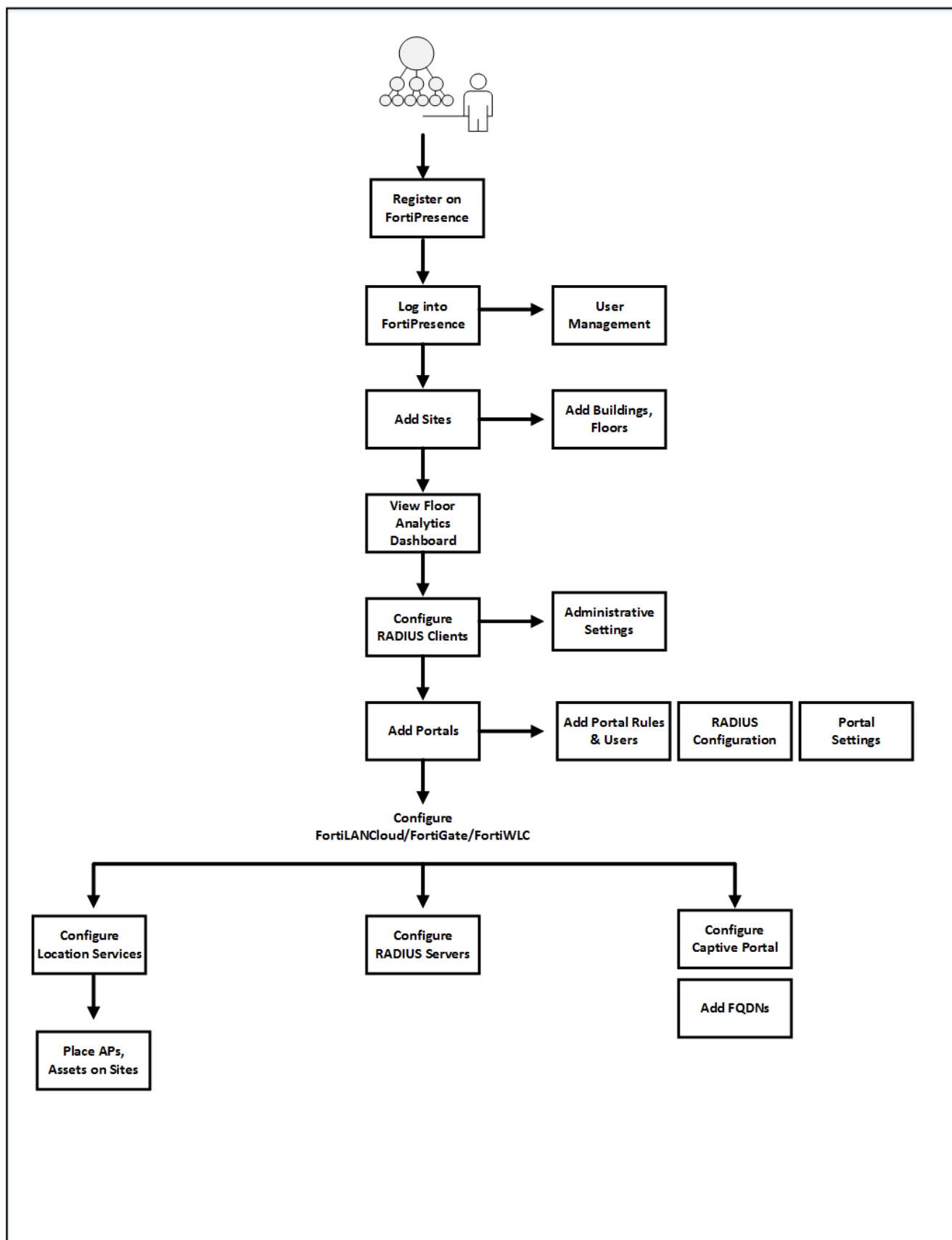
FortiPresence is **General Data Protection Regulation (GDPR)** compliant.

- 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.

How FortiPresence Works

This document describes the configurations and management operations on FortiPresence, FortiLANCloud, FortiGate, and FortiWLC to enable location services for location analytics and Captive Portal configurations for social media logins and internet access. You can add and manage sites using the integrated Google maps and manoeuvre your hardware infrastructure easily.

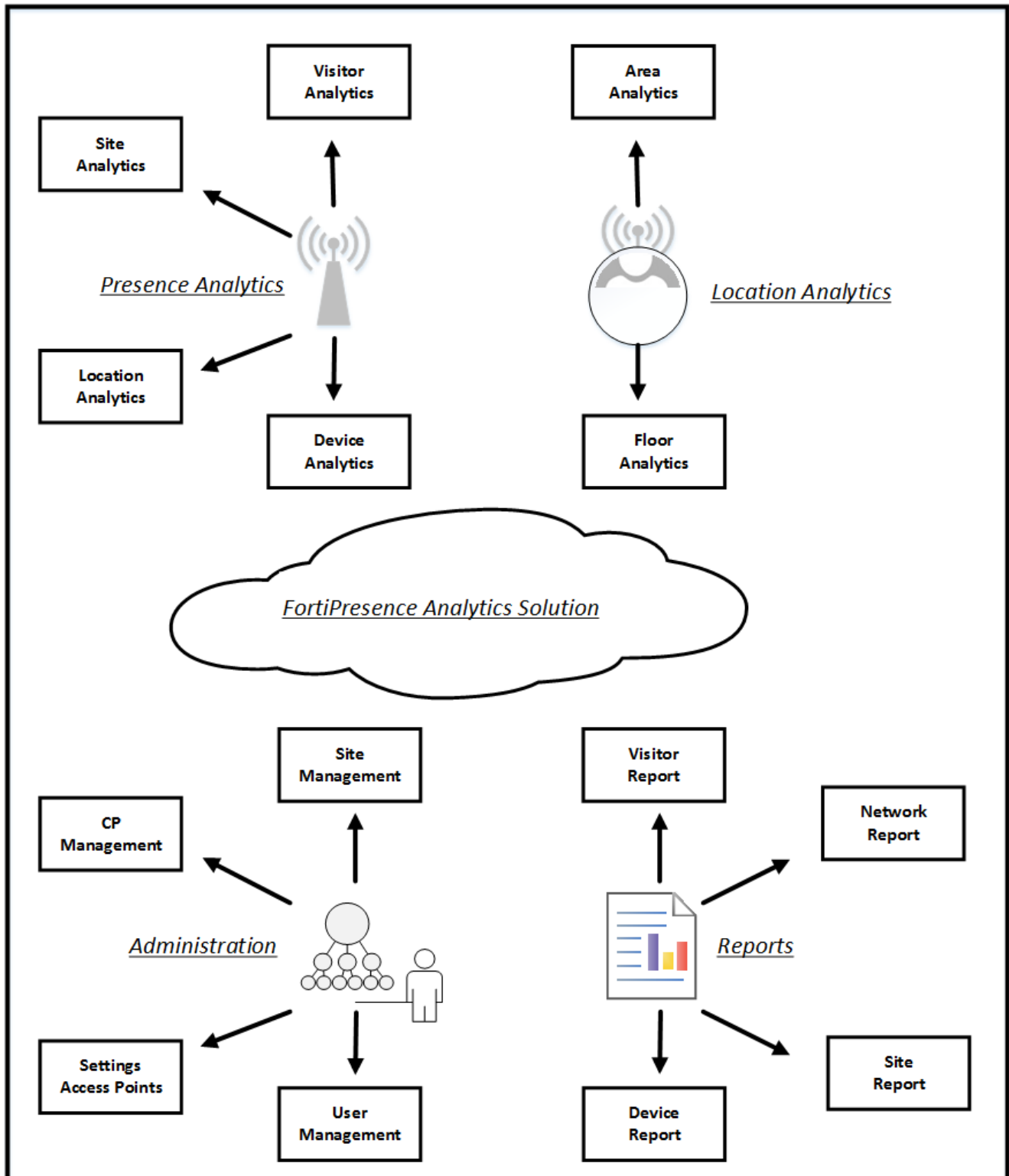
For configuration details on FortiWLC, FortiGate, and FortiLANCloud, see the respective *product documentation*.



FortiPresence User Interface overview

The FortiPresence analytics solution comes with an interactive and easy to use GUI which enables easy site administration and device management. The detailed dashboards and customized reports make presence analytics for your business comprehensive.

The components of the GUI are explained in the subsequent chapters of this document.



GUI Data Limits – Dashboards and Reports

The allowed views and downloads for different dashboards and reports are listed in this section.

Dashboards	View limit for a selected date range	Download limit for a selected date range
Current View Dashboard	Up to 17,00,000 devices	NA
Presence Dashboard	Up to 850,000 devices	Up to 850,000 devices
Device Report	Up to 1,000,000 devices	Up to 1,000,000 devices
Site Report	Up to 480,000 devices	Up to 480,000 devices
Visitor Report	Up to 15,000 devices (tested)	Up to 15,000 devices (tested)
Network Report	Up to 15,000 devices (tested)	Up to 15,000 devices (tested)
Multisite Report	Up to 80,000 devices	Up to 80,000 devices

Note: For the selected date range, if the number of devices exceeds the specified limit, the GUI becomes unresponsive with an exit error message. To work around this, select a reduced date range or individual sites/areas.

Licensing

Important: Register your access point on *FortiCloud* and then map the registered access point to the FortiPresence license in *FortiCloud*, with the main FortiPresence account holder.

The FortiPresence license is issued per access point for any supported platform (FortiWLC, FortiGate, and FortiLAN Cloud). The license for *FortiLAN Cloud* access points is valid for 1 year and the licenses for *FortiWLC* and *FortiGate* platform access points are valid for 1, 3 or 5 years.

When the license expires, a grace period of 30 days is available to renew the license; if the license is not renewed during the grace period, then your FortiPresence access is converted into an unlicensed version. Data retention for unlicensed (free) FortiPresence versions/access points is 7 days.

In such a scenario, where the license is not renewed, the following is the data retention pattern. This is an example for FortiLAN Cloud access points.

1 year (Licensed version) → 30 days (Grace period) → 7 days (Unlicensed version)

Notes:

- You can either have all licensed or all unlicensed access points per site. A combination of licensed and unlicensed is not allowed.
- The customer has access to paid features as long as even 1 access point is licensed.
- The site is considered free or paid based on whether the first access point placed is licensed or unlicensed.
- If the licenses for access points in one site expire (after grace period), only that site is converted into a free site with data retention of 7 days. All other paid sites continue as is.
- If licenses of one or some of the access points placed in a site expire and are not renewed, then those access points can be removed with full data retention still available till the other access points' licenses in the site expire.
- Unlicensed user accounts are paused for data processing after 37 days of login inactivity with requisite warning messages via email notifications. To resume the account access, log in into FortiPresence and you are directed to the resume option in the GUI; select it. After resumption of account access, restart the location services on all platforms, FortiWLC, FortiLAN Cloud, and FortiGate to start processing data immediately.

The features available to licensed and unlicensed users are described in this table.

Feature	Licensed	Unlicensed
The following features are paid for at the account level.		
Number of Sites	Unlimited	5
Data Retention	1 year	7 days
Number of concurrent Captive Portal sessions	Unlimited	200
User Management	Yes	No
Multi-Site Report	Yes	No

Feature	Licensed	Unlicensed
Specifying the RSSI of the AP while adding it in a site.	Yes	No
RSSI Threshold	Yes	No
Email notification for inactive APs	Yes	No
Schedule Configuration (Reports)	Yes	No
The following features are paid for at the site level.		
Collect email and phone number for portal users.	Yes	No
Site Business Time	Yes	No
Automatic exclusion of fixed assets	Yes	No
Email verification	Yes	No
Social authentication via Instagram and linkedIn	Yes	No
Captive Portal customization	Yes	No
Themes and images for captive portal	Yes	Yes
Language support for captive portal	Yes (site level)	No

Viewing License Information

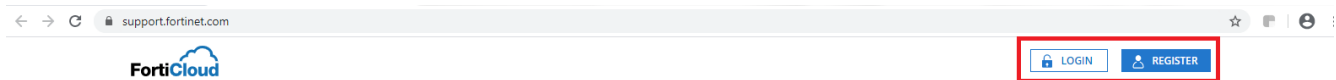
To view licensing information for access points navigate to **Admin > Settings > Discovered APs**.

Sync Licensed APs ⓘ						
Name	Mac	Serial No	Timestamp	Planning	Expiry Date	State ⓘ
5S5EC	██████████	FP421E3X17001633	3/7/2019 10:32:59	Planned	2/20/2018 0:0:0	Inactive
AP-1	██████████	00:0c:e6:39:19:b0	3/7/2019 10:42:53	Unplanned	-	Inactive

- Access points with expiry dates populated are the ones which are licensed; all others are unlicensed. If you have a licensed access point and it appears as unlicensed, click **Sync Licensed APs** to refresh the status.
- Each time a license is renewed, click **Sync Licensed APs** to refresh the status on the GUI.
- The expiry date listed excludes the grace period.
- You receive email reminders on license renewals and notifications on FortiPresence logins, as the expiry date draws near.

Signing-on for FortiPresence

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

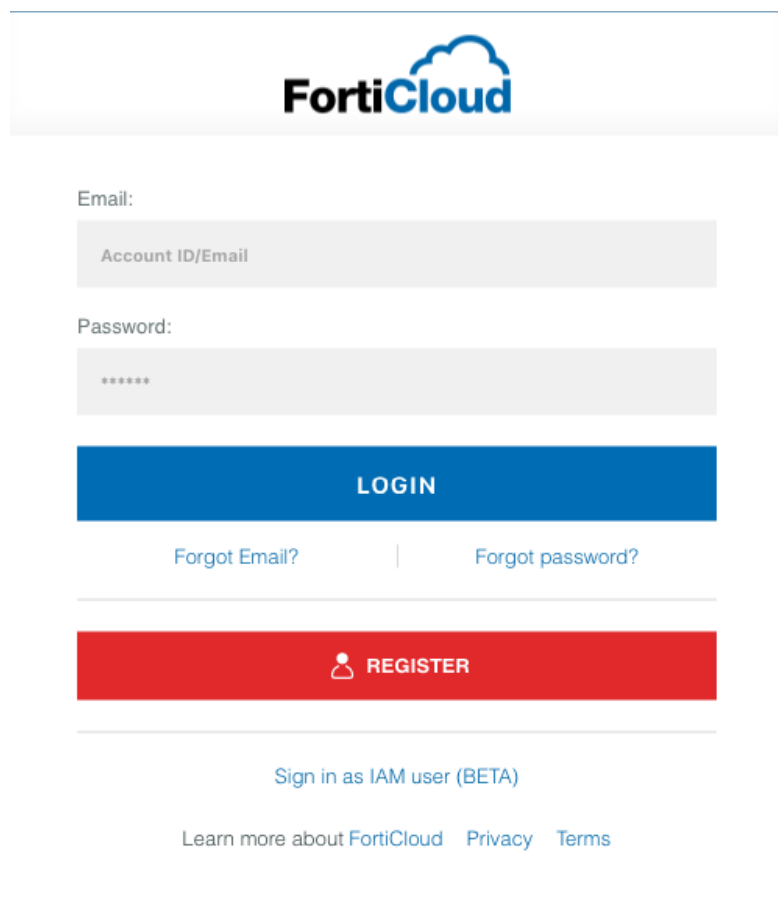


How do I login if...?	Steps
I am a new user of FortiPresence	1. Registering on FortiCloud on page 16
I am an existing user of FortiPresence but not registered on https://support.fortinet.com	2. Accessing FortiPresence on page 19
I am an existing user of FortiPresence and registered on https://support.fortinet.com with the same email ID as that of the FortiPresence account.	1. Accessing FortiPresence on page 19
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.	<ol style="list-style-type: none"> 1. Login into https://support.fortinet.com to map your FortiCloud email ID to your existing FortiPresence account. 2. Once logged in, select FortiPresence from the product banner as described in Accessing FortiPresence on page 19, 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.

How do I login if...?	Steps
	<div><div>Register to FortiPresence</div><div>New Registration Migrate</div><div>FortiPresence Email* : <input type="text" value="Enter FortiPresence email"/> <small>It is an optional field. Enter your FortiPresence email id. We will link your existing FortiPresence account with support account.</small></div><div>FortiPresence Password* : <input type="password" value="Enter FortiPresence password"/> <small>Enter FortiPresence password.</small></div><div>Support Email* : <input type="text" value="abhissodhar6@gmail.com"/> <small>This is your support email id.</small></div><div>Select Country* : <input type="text" value="Select Country"/> <small>Select country for your account.</small></div><div><input type="button" value="Submit"/></div></div> <div>Your FortiPresence account is migrated to the https://support.fortinet.com registered email ID.</div>

Registering on FortiCloud

Prior to using FortiPresence, you are required to register on the *FortiCloud* portal. Use the <https://support.fortinet.com> access link to register on the *FortiCloud* portal. A security code is emailed to the address specified during registration; use the code to complete registration and activate your account.



The image shows the FortiCloud login and registration interface. At the top is the FortiCloud logo. Below it are two input fields: 'Email:' with a placeholder 'Account ID/Email' and 'Password:' with a placeholder '*****'. A blue 'LOGIN' button is positioned below the password field. To the left of the login button are links for 'Forgot Email?' and 'Forgot password?'. Below the login button is a red 'REGISTER' button with a user icon. At the bottom, there is a link 'Sign in as IAM user (BETA)' and a footer with links 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

Adding IAM Users

The Identity and Access Management (IAM) is a service to help you control access to FortiCloud portals and assets. You can use the portal to manage users, authentication credentials, and asset permissions. For more information, see [FortiCloud](#) documentation. Access the IAM service from the FortiCloud portal using the master FortiPresence account.

1. Navigate to **IAM Users** and click **Add IAM User**.
2. (Optional) Click **Apply same permissions as existing User**, and then select a user from the dropdown. You can configure the permissions later.

3. To create a new user, enter a unique **Username**, **Full Name**, **Email** address, **Phone** number, and **Description** (optional).

1. User Details

IAM User Information

Username: *

Full Name: *

Email: *

Phone: *

Description

Adopt Permissions

☐ Apply same permissions as existing User :

Select an existing User ▼

*Note: Checking 'Apply same permission as an existing User' allows you to easily assign a pre-configured Permission setup. User Permission settings are still fully configurable in the next step.

< CANCEL
NEXT >

4. Click **Next** and configure **User Permissions**. (Optional) Add the user to an IAM user group, click **IAM User Group**, and select a group from the dropdown. The **Effect Asset Permissions** and the **Effective Portal Permissions** are displayed. Click **Next**.

OR

5. Select an asset group from the **Asset Permissions** list.
6. Configure the **Portal Permissions** for the required portals. Click on the edit icon against the portal, update the following and click **Confirm**.

Permission	Description
Allow Portal Access	Toggle Yes to allow access to a portal.
Access Type	Select the Access Type that is defined by the selected portal. The allowed access types can vary for different portals.
Additional Permission	Allow Additional Permission based on the selected access type. The additional permission also varies for different portals.

7. Configure the **Cloud Management & Services** permissions to enable access to FortiPresence. Click add (+) and select **FortiPresence** from the list.
8. Click the edit icon and configure the required permissions for FortiPresence.
- Toggle **Yes** to allow access to FortiPresence.
 - Select the required **Access Type**, *Admin* (all permissions similar to the master account) or *Read-Only* (only view permissions).

- Click **Confirm**.

2. User Permissions
IAM User Registration: FortiPresence

☐ **IAM User Group** (Permissions controlled by IAM User Group)

None

* NOTE : User will adopt the Permission of the assigned Group. You cannot edit Asset or Portal Permissions while user is assigned to a Group. Remove user from any group to enable Permissions to be editable.

Asset Permissions *

My Assets

Portal Permissions

Portals	Access	Access Type	Additional Permission
Asset Management	✓	Admin	-
FortiCare	✗	Denied	-
FortiOS SSO	✗	Denied	-

Cloud Management & Service	Access	Access Type	Additional Permission
FortiPresence	✓	Admin	-

< CANCEL
< BACK
NEXT >

- Click **Next** and review the displayed user information.

3. Confirmation
IAM User Registration: FortiPresence

IAM User Information

Full Name: FortiPresence User

Email: [redacted]@fortinet.com

IAM User Group

Effective Asset Permissions

None

My Assets

Effective Portal Permissions

Portals	Access	Access Type	Additional Permission
Asset Management	✓	Admin	-
FortiCare	✗	Denied	-
FortiOS SSO	✗	Denied	-

Cloud Management & Service	Access	Access Type	Additional Permission
FortiPresence	✓	Admin	-

< CANCEL
< BACK
CONFIRM >

- Click **Confirm**. Click **Download CSV** to download the new user's credentials.
After this procedure is successfully completed, you are sent the login credentials after the required validation.

Accessing FortiPresence

Any user registered on <https://support.fortinet.com> can access FortiPresence. Once you login into *FortiCloud*, 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 *FortiCloud* in order to use FortiPresence. Consider the following example, with these registered login credentials for different accounts:
 - FortiPresence Account owner – **alpha@gmail.com**
 - *FortiCloud* Account owner – **alpha@gmail.com**
 - FortiPresence RBAC user – **beta@gmail.com**

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

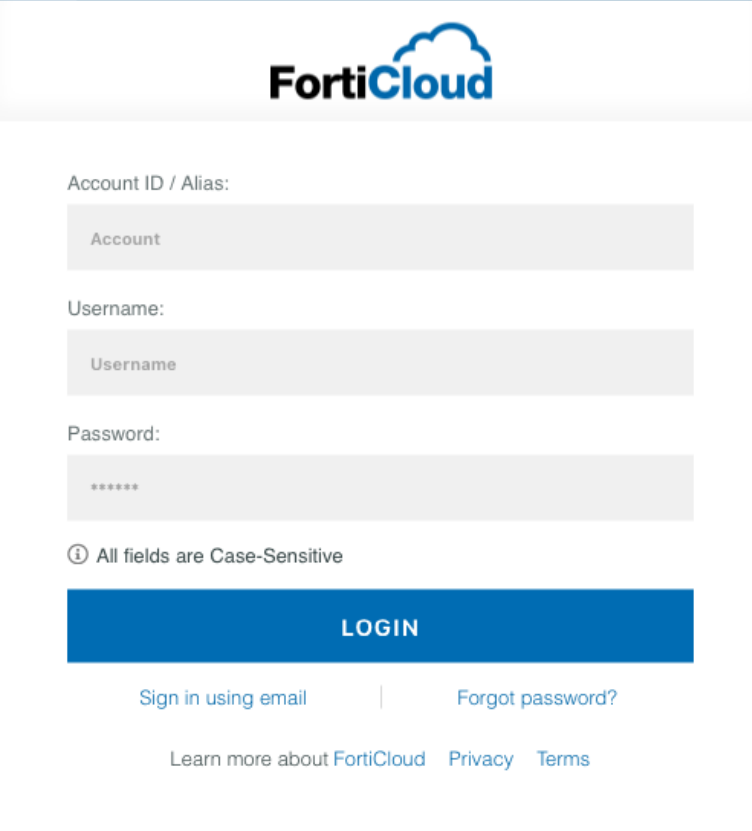
OR

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

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

You can login into FortiCloud using your registered FortiCloud account details, **Email** and **Password** **OR** click **Sign in as IAM user**.

Enter your registered IAM user credentials to login, the **Account ID** is that of the master account.



The image shows the FortiCloud login interface. At the top is the FortiCloud logo. Below it is a form with three input fields: 'Account ID / Alias:' with a placeholder 'Account', 'Username:' with a placeholder 'Username', and 'Password:' with a placeholder '*****'. Below the password field is a note: 'All fields are Case-Sensitive'. At the bottom of the form is a blue 'LOGIN' button. Below the button are two links: 'Sign in using email' and 'Forgot password?'. At the very bottom are three links: 'Learn more about FortiCloud', 'Privacy', and 'Terms'.

External IDP Authentication

FortiPresence supports integration of third-party Identity Provider (IDP) services to log-in for data analytics. This feature is useful for enterprises that need to secure their user credentials and hence provision FortiPresence access through

their own IDP website. The external IDP initiated Security Assertion Markup Language (SAML) assertion consisting of specific IDP attributes is used by FortiCloud/FortiPresence to verify the user account details and grant required access. External IDP authentication is offered in conjunction with FortiCare and FortiAuthenticator. Contact the Fortinet *Customer Support* team to enable external IDP support and raise an enrollment request with the appropriate FortiCare accounts.

Note: Support for SAML 2.0 and IDP initiated assertion response is required.

After successful authentication on your IDP website, you are re-directed to the FortiCloud portal from where you access FortiPresence based on the configured roles. For more information, see [FortiCloud](#) documentation.

Adding External IDP Roles

Access the **Identity & Access Management (IAM)** service from the FortiCloud portal

1. Navigate to **Manage External IdP Roles** and click **Add IDP Role**.
2. Enter a unique **Role Name** and **Description** (optional).
Note: The role name must exactly match the role attribute in the SAML assertion.
3. Select an asset group from the **Asset Permissions** list.
4. Configure the **Effective Portal Permissions** for the required portals. Click on the edit icon against the portal and update the following.

Permission	Description
Allow Portal Access	Toggle Yes to allow access to a portal.
Access Type	Select the Access Type that is defined by the selected portal. The allowed access types can vary for different portals.
Additional Permission	Allow Additional Permission based on the selected access type. The additional permission also varies for different portals.

5. Configure the **Cloud Management & Services** permissions to enable access to FortiPresence. Click add (+) and select **FortiPresence** from the list.
6. Click the edit icon and configure the required permissions for FortiPresence.
 - Toggle **Yes** to allow access to FortiPresence.
 - Select the required **Access Type**, *Admin* or *Read-Only*.

Create External IdP Role

External IdP Role

Role Details

Role Name: *

FortiPresence

Description :

External IDP Authentication for FortiPresence

Asset Permissions*

My Assets

Effective Portal Permissions

Portals	Access	Access Type	Additional Permission
Asset Management		Denied	-
FortiCare		Admin	-

Cloud Management & Service	Access	Access Type	Additional Permission
FortiPresence		Admin	-

< CANCEL

ADD ROLE

7. Click **Add Role**.

After the role is created, it is listed on the on the **Manage External IdP Roles** page. You can enable/disable or delete a created role. Select the role and click on the required option.

Dashboards and Reports

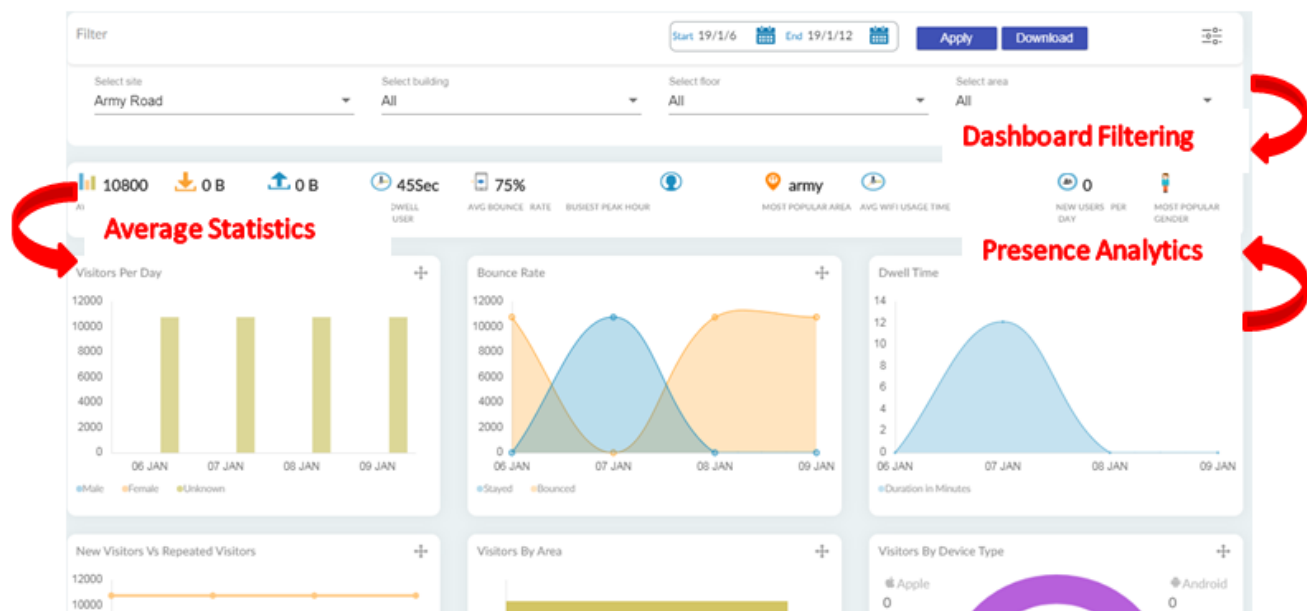
The FortiPresence GUI provides presence analytics in the **Presence** and **Current View** dashboards and downloadable reports.

Presence Dashboard

The Presence dashboard provides a summary view of FortiPresence analytics. The dashboard provides a customizable graphical representation of visitor, device, and site analytics for specific locations and date range. This provides a comprehensive data analytics of the consumer traffic patterns in your establishment.

The aggregate trends depicted in the dashboard panels are recorded over a period of time as configured, by default data is displayed for the current week.

The access points (FortiGate and FortiLAN Cloud) and the FortiWLC controllers send the aggregated client data (station reports) to the cloud analytics engine as per configured time intervals. The analytics engine processes this raw data which is then compiled into summary charts and statistics. This data is fetched and displayed on the Presence dashboard when you access it.



The panels displayed on the dashboard can be rearranged.

The dashboard provides a configurable summary view time and location, you can select the date/time range and also the location to filter and click **Apply** to view corresponding data on the dashboard. You can download the dashboard data in a .pdf and/or .csv format, click **Download**.



Note: For paid tier users, the dashboard retains data for the last 1 year. You can select a time range within this period to view data on the dashboard. See [GUI Data Limits – Dashboards and Reports on page 12](#).

The Presence dashboard is organized into different panels.

Dashboards Filtering

The filtering parameters of the dashboard analyze the related visitor statistics based on the selected time range and the site details. The dashboard generates data at a configured time interval. You can select the time interval from the Date and Time drop-down list. The default is **This Week**.

Average Statistics

The dashboard calculates the average statistics during the selected time range and displays it on the dashboard. The following average values are displayed:

- Average Visitors
- Average Data Usage (uploads and downloads)
- Average Dwell Time
- Average Bounce Rate
- Busiest Peak Hour (with the highest number of visitors)
- Most Popular Area (based on the maximum number of visitors)
- Average Wifi Usage Time
- New Users Per Day
- Most Popular Gender (gender with the highest visits)

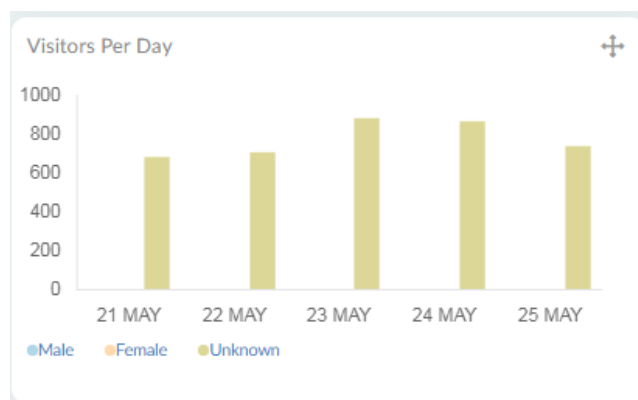
The dashboard provides real time data and analytics based on the following parameters:

- [Visitor Analytics on page 24](#)
- [Device Analytics on page 26](#)
- [Site Analytics on page 27](#)

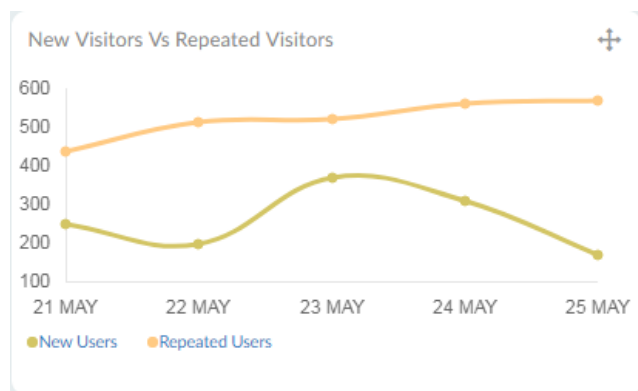
Visitor Analytics

This section provides analytics based on visitor behaviour.

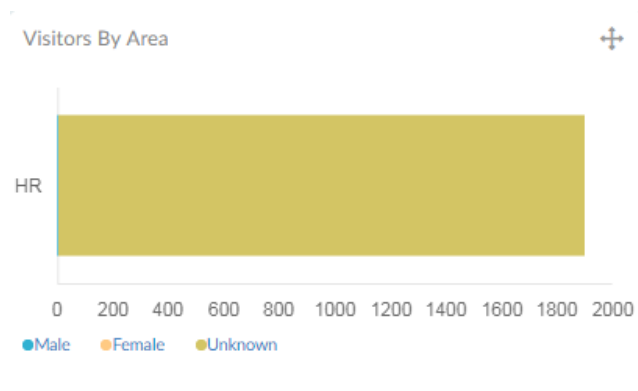
Visitors per day – Provides the total number of visitors per day within the time range selected. The chart displays the visitors categorized and Male, Female, and Unknown (absence of sufficient data for gender classification).



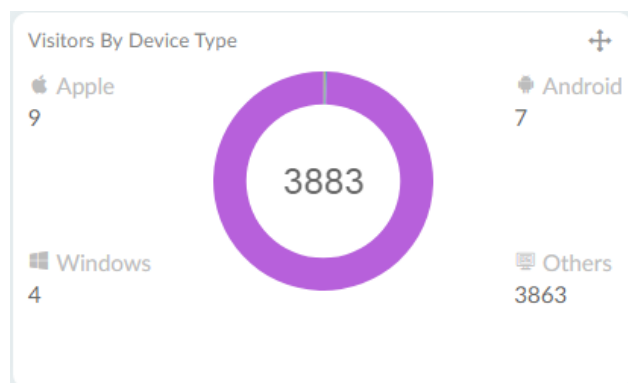
New Visitors vs Repeated Visitors – Provides the total number of new visitors and repeated visitors (visitors who visit more than once) per day. Hover over the lines plotted on the chart to obtain the number of new and repeated visitors.



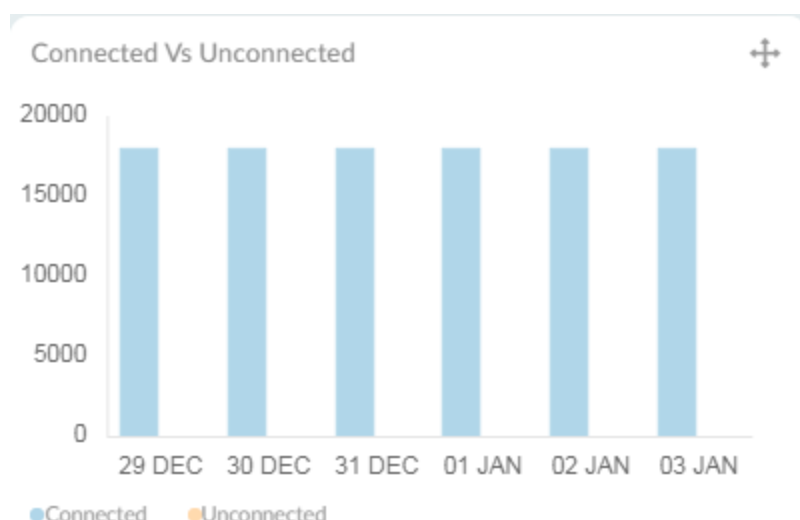
Visitors by area – Provides the total number of visitors for different areas in a particular site. This data is calculated from the start of the data range to the current time. Hover over the bars in the chart to obtain the total number of visitors per area and the categorization as Male, Female, and Unknown.



Visitors by Device Type – Provides the total number of visitors based on the OS used for social network logins. The chart displays the total number of logins from iOS, Android, Windows, and other OS. Hover over the chart to obtain the total number of users per OS.



Connected Vs Unconnected - Provides the total number of **Connected** visitors connected to the Wi-Fi and authenticated via the FortiPresence Captive Portal per day within the time range selected vs the **Unconnected** visitors not authenticated in via the FortiPresence Captive Portal but connected to the Wi-Fi.

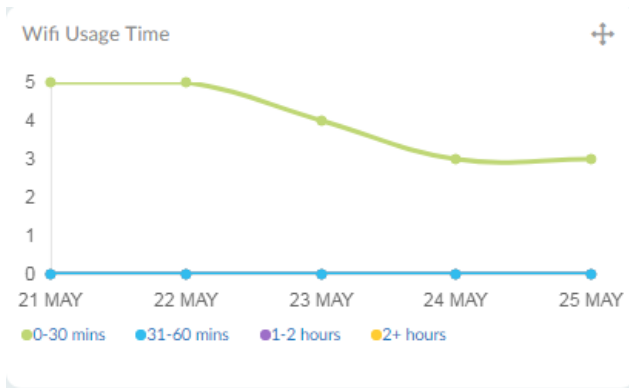


Device Analytics

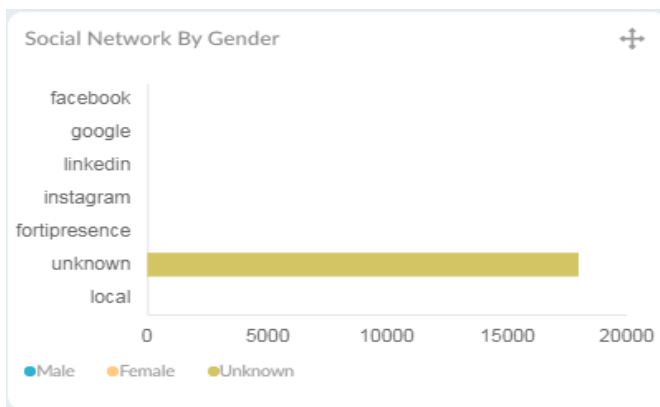
This section provides analytics based on visitor device usage patterns.

Data Usage – Provides the total bandwidth consumption per day. The chart displays the total data upload and downloads per day. Hover over the bars in the chart for the total upload and download size in GB.

Wifi Usage Time – Provides the total wifi usage time per day. The chart categorizes the usage time into different time buckets, **0-30 minutes**, **31-60 minutes**, **1-2 hours**, and **2+ hours**. Hover over the chart to get the number of users against each of the buckets.



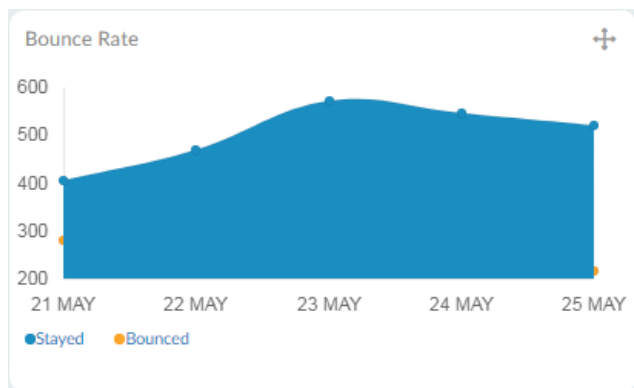
Social Network By Gender – Provides the gender based social network login information. The chart displays the total number of users, categorized as male and female for each authentication type, **Facebook**, **Google**, **Instagram**, **LinkedIn**, and **FortiPresence**. Users authenticated via the FortiPresence Captive Portal but unwilling to share gender details are classified as **Unknown**. Users who login into the network on acceptance of terms and conditions and do not require authentication are classified as **Local**.



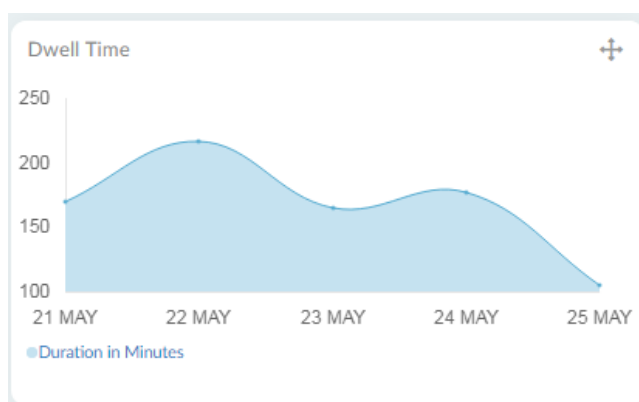
Site Analytics

This section provides analytics based on the site/area that the visitors visit/roam.

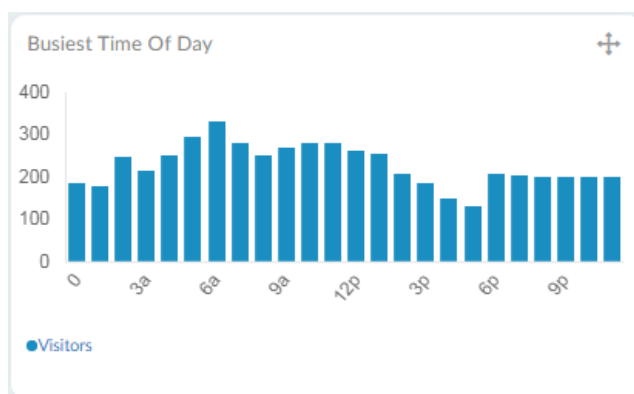
Bounce Rate – Provides the total number of and stayed/engaged visitors based on the bounce rate threshold configured at **Admin > Settings > Threshold**. Visitors who spend more than the configured bounce rate are classified as stayed and the ones less than the bounce rate as bounced.



Dwell Time – Provides the total visitor dwell time in minutes based on the **Dwell Inactive Time Limit** threshold configured at **Admin > Settings > Threshold**. If a visitor is seen after a gap of the configured threshold, it is considered as a new dwelling session for dwell time calculation. If the visitor is seen within the configured threshold, the dwell session continues. Hover over the chart to see the highest dwell time per day.

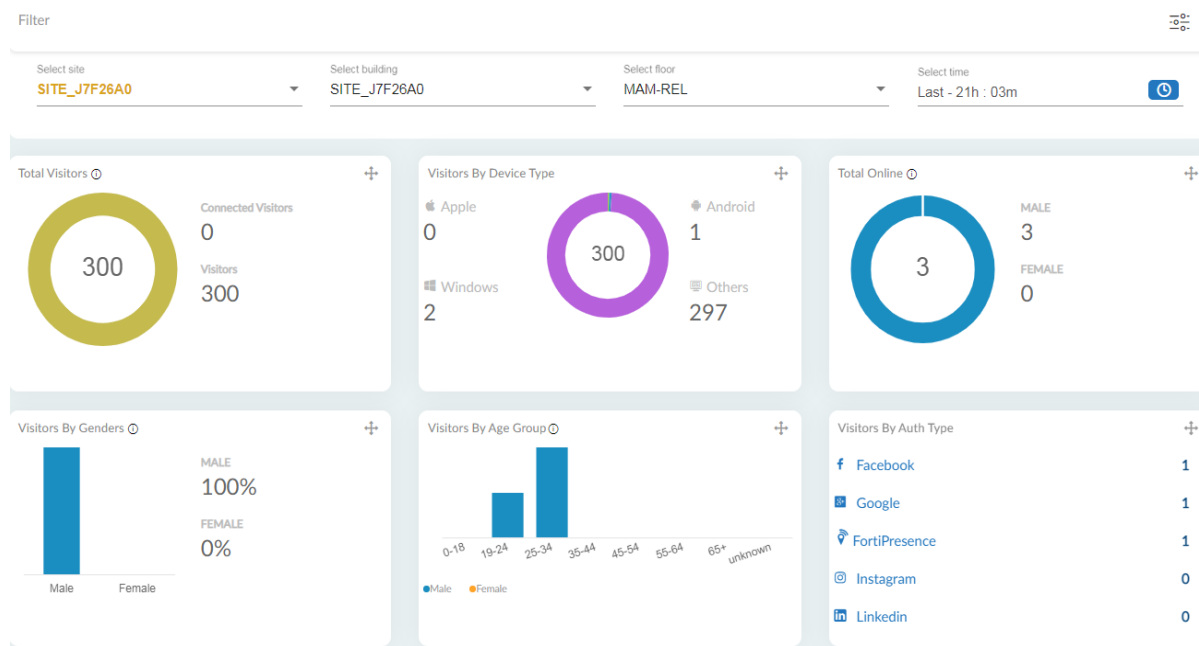


Busiest Time of the Day – Provides the cumulative hours over the different times for the selected time range, for example, if the dashboard is configured to display data for a week then the cumulative visitor hours for the entire week for different times are displayed. Hover over each bar on the chart to view the total number of visitors during that time.



Current View Dashboard

By default, the **Current View** dashboard provides a summary of FortiPresence analytics in the last 15 minutes for the selected floor. Analytics data for a maximum of 24 hours is displayed, you can customize this duration and view analytics for the last few hours, as per the time selected.



Total Visitors – Provides the total number of visitors for the configured view time. The chart categorizes the visitors connected via the FortiPresence Captive Portal and Wi-Fi infrastructure (**Connected Visitors**) and the visitors who are connected to the Wi-Fi but not authenticated via the FortiPresence Captive Portal(**Visitors**).

Visitors By Device Type – Provides the total number of visitors based on the OS used for social network logins. The chart displays the total number of logins from iOS, Android, Windows, and other OS.

Total Online – Provides the total number of social network login information and categorizes them based on the gender (male and female).

Visitors By Gender – Provides the gender based visitor percentage calculated as per the social network login information.

Visitors By Age Group – Provides visitor classification based on the age group as per the social network login information. Connected visitors authenticated via the FortiPresence Captive Portal but unwilling to share their age are classified as **Unknown**.

Visitors By Authentication Type – Provides visitor classification based on social network login information. The chart displays the total number of users for each authentication type, **Facebook**, **Google**, **Instagram**, **LinkedIn**, and **FortiPresence**. Users who login into the network on acceptance of terms and conditions and do not require authentication are classified as **Local**.

Reports

FortiPresence provides customizable standard report types that allow you to generate and analyze visitor data for different time periods. You can create reports to view and download them for further analysis in the **.csv/.pdf** format.

These reports allow you to perform visitor, network, device, and site analysis at different time periods and for different geographic regions.

Select the time period and the site to be covered by the selected report. These fields are supported for all report types. The reports are searchable for specific fields for data that is generated. To configure auto-generation of reports, see [Schedule Configuration on page 64](#).

Click on **Download & Email** to download generated reports and/or email them to the registered email address in a **.pdf** and/or **.csv** format.

Download & Email

-----Format-----

☒ PDF ☒ CSV

-----Action-----

☒ Download ☒ Email

Submit

For more information on the report fields see [Presence Dashboard on page 23](#).

Connected Visitor Reports

The Connected Visitor Reports provides details of the following visitor analytics associated with each visitor name.

NAME	USER KEY	GENDER	AGE RANGE	DEVICE TYPE	EMAIL	PHONE NO	AUTH TYPE	NO OF VISITS	VISITED DATES
demo_3262619105	Copy f0179ad2571f1f6...	male	24	android	demo_7675973699	9194864875	fortipresence	4	2019/1/7 [36 Min:...
demo_6243648132	Copy 164c5180cc9353...	female	25	windows	demo_7986248626	5703097342	fortipresence	4	2019/1/7 [36 Min:47 Sec], 2019/1/8 [22 Min:48 Sec], 2019/1/8 [3 H:31 Min:16 Sec], 2019/1/9 [2 H:8 Min:48 Sec]
demo_885587996	Copy ad39315170509...	female	25	windows	demo_6235531522	6667967713	fortipresence	4	2019/1/7 [36 Min:...
demo_2940252203	Copy 7d83c06af9717c...	female	19	apple	demo_7266680898	5515552541	fortipresence	4	2019/1/7 [36 Min:...
	Copy 7ac8846e7680cf...	unknown		apple			unknown	4	2019/1/7 [36 Min:...

Items per page: 5 1 - 5 of 15 < >

Field	Description
Name	Displays the name of the visitor based on the social network logins.
Gender	Displays the gender, whether male, female, or unknown (in the absence of data), associated with the visitor name based on the social network logins.

Field	Description
Age Range	Displays the age associated with the specific visitor name.
Device Type	Displays the device type or the OS used by the specific visitor, whether iOS, Android, Windows, or Others.
Auth Type	Displays the social network authentication method used by the visitor, whether Facebook, Google, Instagram, LinkedIn, or FortiPresence.
Number of Visits	Displays the number of visits by a specific visitor within the selected time range.
Visited Dates	Displays the dates of visits by a specific visitor within the time range. Hover over the date to view the visitor dwell time on the specific day.
The following fields are applicable only for paid tier users.	
Phone No	Displays the visitor's mobile number.
Email	Displays the visitor's email address.

You can select the fields to include in the downloaded visitor report, click on Download & Email to select the required options.

Download & Email

-----Format-----

☐ PDF
☒ CSV

-----Action-----

☒ Download
☐ Email

-----Display Fields-----

☒ NAME
☒ USER KEY

☒ GENDER
☒ AGE RANGE

☒ DEVICE TYPE
☒ EMAIL

☒ PHONE NO
☒ AUTH TYPE

☒ NO OF VISITS
☒ VISITED DATES

☒ SUBSCRIPTION

Submit

Network Reports

The Network Report provides the details about visitor devices/network based on the MAC address.

NAME	USER KEY	DEVICE TYPE	UPLOAD	DOWNLOAD	WIFI USAGE TIME
Emily Fujihara	Copy dbb1d277acf5831d30d1d616e...	android	0 Bytes	0 Bytes	0 Sec
MIGRATE-0	Copy 3e7652d8775e96dc16b4971d...	others	10.6 MB	21.2 MB	1 Hr
NEWSELENIUM-1	Copy 66413de80c0250a17d72808c...	others	10.6 MB	21.2 MB	1 Hr
SELENIUM-11699	Copy 76585ffc5f5164fdb25256de19...	apple	0 Bytes	0 Bytes	0 Sec
Yong Hayes	Copy d5da184a39a01c268ed4dae0...	windows	0 Bytes	0 Bytes	0 Sec

Field	Description
Name	Displays the name of the visitor based on the social network logins.
User Key	Displays the user key associated with the specific visitor device.
Device type	Displays the device type or the OS used by the specific visitor, whether iOS, Android, Windows, or Others.
Data Usage	Displays the total bandwidth consumption by the specific visitor within the time range selected. The total upload and download size is displayed.
WiFi Usage Time	Displays the total wifi usage time by the specific visitor within the time range selected.

Site Report

The Site Report provides the details about site analytics for each day within the selected time range for report generation.

DATE	BUSY HOUR	SOCIAL LOGIN	NO OF VISITOR	CONNECTED VISITORS	DWELL TIME	BOUNCE RATE
2020-01-05	8-9 PM	4	18000	18000	23 Hr, 54 Min, 27 Sec	0 %
2020-01-06	11-12 AM	4	18000	18000	23 Hr, 51 Min, 51 Sec	0 %
2020-01-07	12-1 PM	4	18000	18000	13 Hr, 59 Min, 48 Sec	0 %

Items per page: 500 1 - 500 of 500 < >

Field	Description
Date	Displays each day within the selected time range.
Busiest hour	Displays the hourly time range on a specific day when the cumulative visits are the highest.

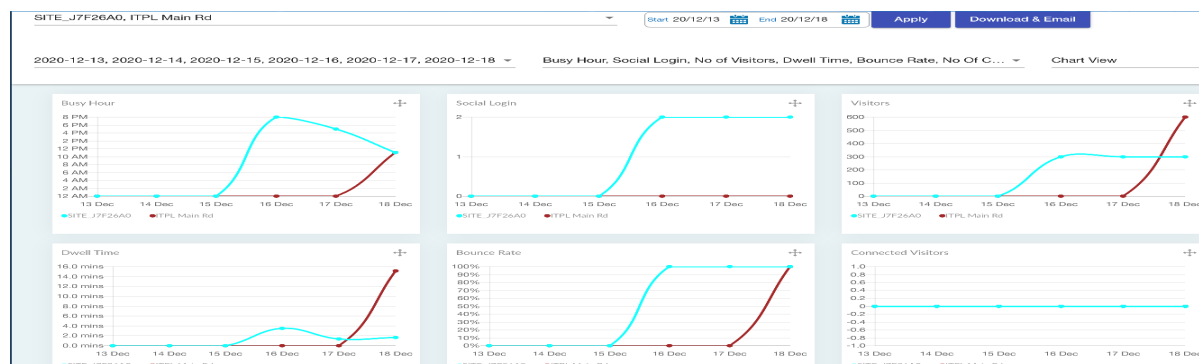
Field	Description
Number of Social Logins	Displays the total number of social network logins on the specific day.
Number of Visitors	Displays the total number of visitors on the specific day.
Connected Visitors	Displays the total number of visitors connected to the Wi-Fi and authenticated via the FortiPresence Captive Portal on a specific day.
Dwell Time	Provides the total visitor dwell time in minutes on the specific day.
Bounce rate	Provides the percentage of stayed/engaged visitors based on the bounce rate threshold configured on each day.

Multi Site Report

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

The Multi Site Report provides data comparison between multiple sites within the selected time range for report generation. The comparison is displayed in a tabular and graphical format. Select the sites, dates, presence data to be compared, and the view (table or chart). A maximum of only 5 sites can be compared.

Data stored up to the last 1 year can be compared.



Field	Description
Busiest hour	Displays the hourly time range on a specific day when the cumulative visits are the highest.
Number of Social Logins	Displays the total number of social network logins on the specific day.
Number of Visitors	Displays the total number of visitors on the specific day.
Dwell Time	Provides the total visitor dwell time in minutes on the specific day.
Bounce rate	Provides the percentage of stayed/engaged visitors based on the bounce rate threshold configured on each day.
Number of Connected Visitors	Displays the total number of connected visitors.

Device Report

The Device Report provides the details about device analytics for each visitor device MAC address.

USER KEY	NEW/REPEATED	CONNECTIVITY STATE	NO OF VISITS	VISITED DATES
Copy 6d84688c8931ba5d852dc9286918b8...	Repeated	Connected	3	2020/1/6 [23 Hr:56 Min:55 Sec], 2020/1/7 [14 Hr:32 Min:53 Sec]
Copy 1809022b04d935ebacdfd164bf55125...	Repeated	Connected	3	2020/1/6 [23 Hr:56 Min:57 Sec], 2020/1/7 [14 Hr:32 Min:53 Sec]
Copy b96c19cf69b50a2cb2b3c2fce7bf7809...	Repeated	Connected	3	2020/1/6 [23 Hr:56 Min:55 Sec], 2020/1/7 [14 Hr:32 Min:53 Sec]
Copy bfe732bcd72fc1bd79ed0abe677cb...	Repeated	Connected	3	2020/1/7 [14 Hr:32 Min:54 Sec], 2020/1/6 [23 Hr:56 Min:55 Sec]
Copy af0377b809fee0cf47dc832c0011766b...	Repeated	Connected	3	2020/1/7 [14 Hr:32 Min:53 Sec], 2020/1/6 [23 Hr:56 Min:55 Sec]
Copy h543rd8d1r2rb1f20f968891778cfe1	Repeated	Connected	3	2020/1/7 [14 Hr:32 Min:53 Sec], 2020/1/6 [23 Hr:56 Min:55 Sec]

Items per page: 500 1 - 500 of 18000 < >

Field	Description
User Key	Displays a unique user key associated with the specific visitor device. You can copy this key and use it or the MAC address to filter reports.
New/Repeated	Displays whether the visitor associated with the user key is a new visitor or a repeat one.
Connectivity State	Displays visitors Connected to the Wi-Fi and authenticated via the FortiPresence Captive Portal or Unconnected visitors not authenticated in via the FortiPresence Captive Portal but connected to the Wi-Fi.
Number of visits	Displays the total number of visits associated with the user key within the time range selected.
Visited Dates	Displays the dates of visits by a specific visitor device user key within the time range selected.

Location Analytics

FortiPresence provides data and analytics based on demographic segmentation and visitor movement between areas. The location analytics delivers data visualization in a customizable format.

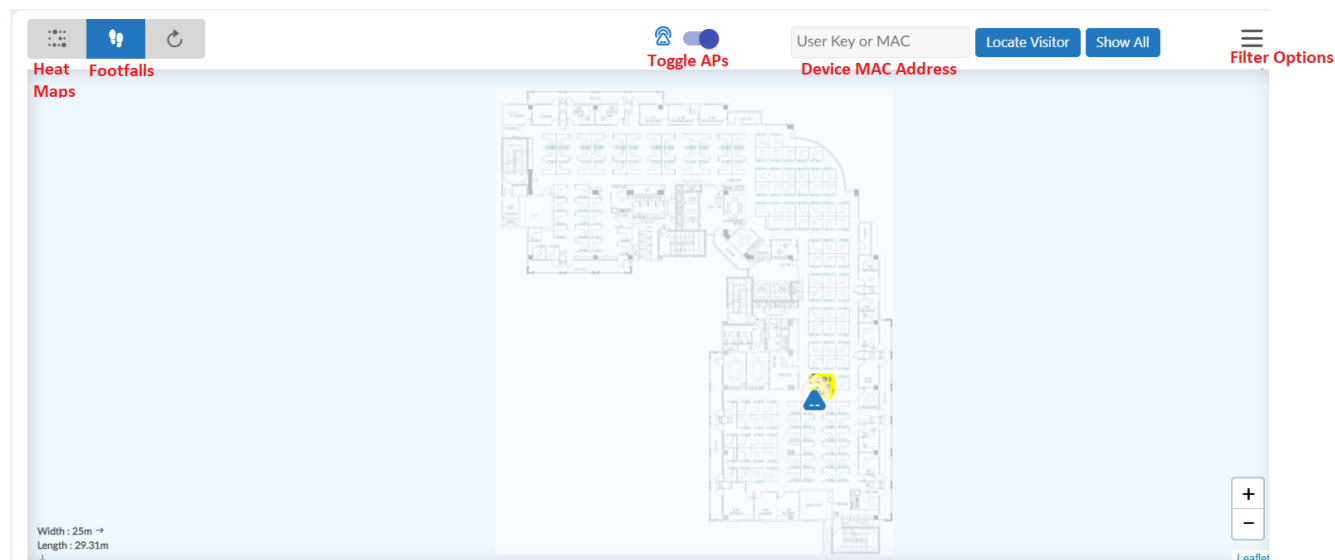
This geographical data analysis provides real-time insights into user behavior. The Location view of the FortiPresence GUI provides analytics for each floor and for each area that the floor is divided into.

The data visualization in location analytics enables you to locate users and track movements.

Floor Analytics

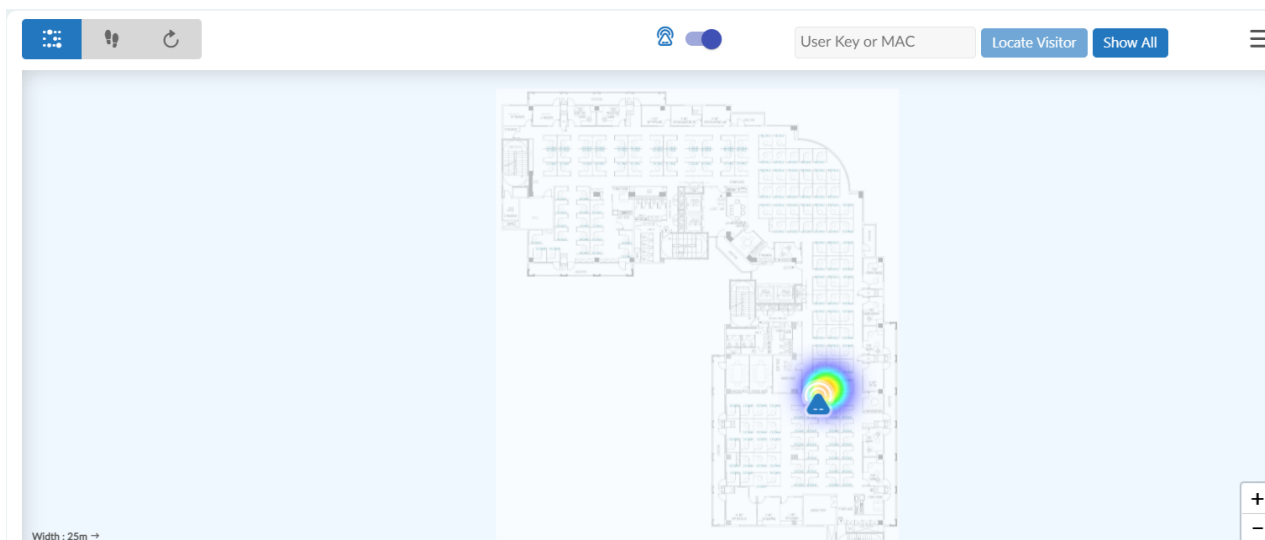
The floor analytics are visualized in the form of drill down heat maps and foot traffic analysis. You can view the current visitor location or view historical data (available only for the last 24 hours). You can select areas on the floor to view localised movements. You can toggle between different forms of data views like **Heatmaps** and **Footfalls**, and also between different APs on the floor map. You can filter down data based specific visitor characteristics. You can customize to view analytics for the last few hours as per the time selected.

Note: Heat maps are NOT supported in this release.



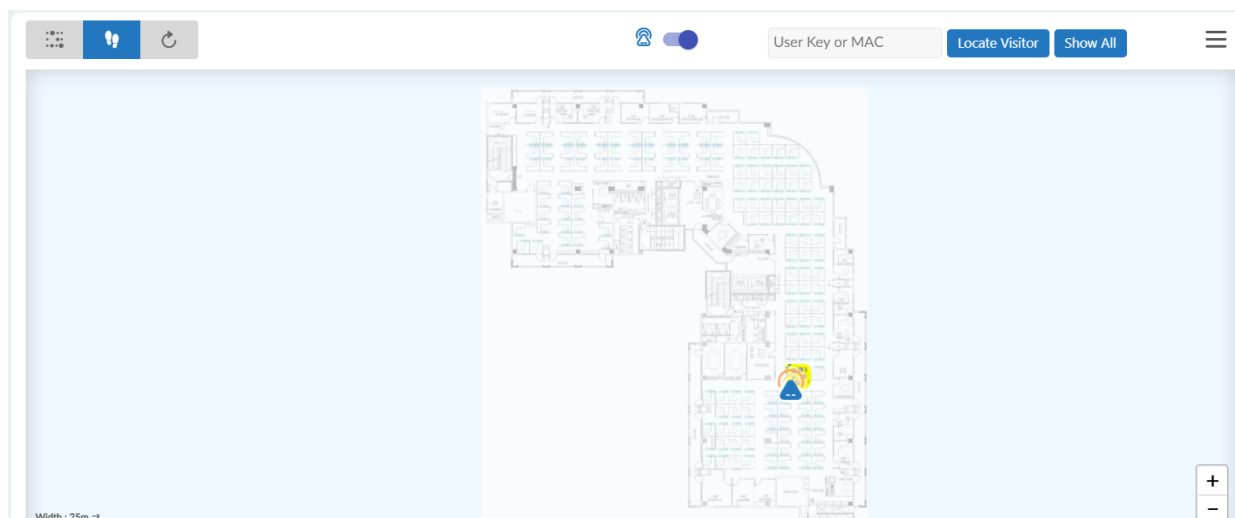
Heat maps

The real-time animated heat maps provide the visitor density and traffic flow analysis. The heat map displays the placement of access points on the selected floor along with the associated MAC addresses. The client density around the access points is calibrated in different colors. Red indicates high density, the density wanes outside the area in the order of, orange, yellow, green, and blue.



Footfall

The footfall view displays the placement of access points on the selected floor along with the associated MAC addresses and the current location of all visitors along with the specific user key.



To know the current location of the visitor, enter the MAC address/user key and click **Locate Visitor**. The related locations and movement is marked on the map. Click **Show All** to view the current location of all visitors in the floor.

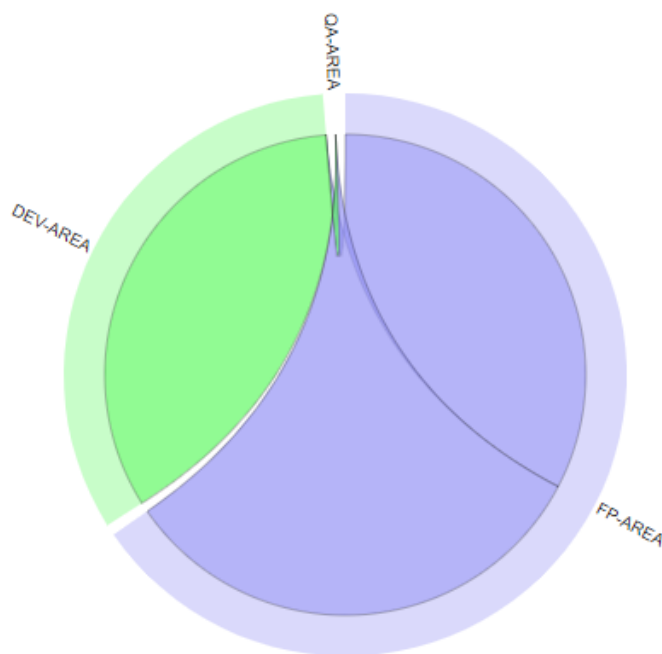
Area Analytics

The area analytics are visualized in the form of charts for different areas that the selected site is divided into. You can track inward and outward visitor movements between areas. You can select specific areas in a site and a specific day to display data.

Visitor Movements

The chart demarcates different areas in different colors and the number of visitors moving between these areas. The color of the path indicates visitors moving from the source area of the same color to a different area. For example, the following image depicts outward visitor movements from **FP-Area** to **Dev-Area** and from **Dev-Area** to **QA-Area**.

Visitor Movements



Visitor Movements Matrix

This matrix displays the statistics from the **Visitor Movements** chart in a tabular form. For example, the following image depicts visitor movement from **FP-Area** to **Dev-Area**, **Dev-Area** to **QA-Area**, and indirect visitor movement from **FP-Area** to **QA-Area**.

Visitor Movements Matrix

→	FP-AREA	DEV-AREA	QA-AREA
FP-AREA	→	300	300
DEV-AREA	0	→	300
QA-AREA	0	0	→


Administering FortiPresence

The FortiPresence GUI provides the administrator with options to manage sites, captive portals, and other settings.

- [Site Management on page 38](#)
- [Portal Management on page 43](#)
- [Administrative Settings on page 49](#)
- [User Management on page 51](#)
- [Configuring Location Services on page 52](#)
- [Configuring Captive Portal on page 56](#)
- [Schedule Configuration on page 64](#)

Site Management

You can manage sites for presence analytics by locating sites on Google maps integrated UI. Once created, the site can be managed by adding buildings, floors, and demarcating floors into areas. You can upload floor maps and place access points and hardware assets on the maps.

1. Navigate to **Admin > Site Management** and search for the geographic location of the site on the Google map and select it.
2. Click the  (**Add Building**) icon on the right side of the map, the mouse pointer turns into a + symbol. Click on the selected site to add a building.
3. Modify the existing default values and enter a unique **Name** and **Description** for the building and site. Click **Save**. The created site with the building details is displayed on the left side menu.

Enter Building Details

BuildingA

Max 32 characters allowed

9/32

CustomerAB

Max 64 characters allowed

10/64

Enter New Site Details :

MySite

Max 32 characters allowed

6/32

CustomerSite

Max 64 characters allowed

12/64

[Save](#)

[Cancel](#)

4. Click on **Add Floor** to upload the floor map for the building.
5. Enter the floor details and browse to the map. Click **Add Floor**.
The floor map is displayed.
6. Adjust the two red pointers on the floor maps and position them across a known distance and specify the **Selected Distance** (feet or meter). This is the reference distance based on which the floor length and width are calculated.

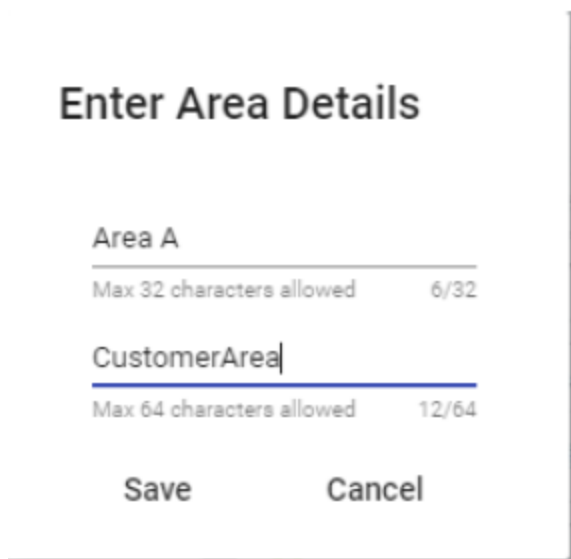
Click **Save**.



7. Click on the (polygon) icon and mark an area on the floor map by drawing a polygon anti-clockwise. Click **Finish**.



8. Enter unique area **Name** and **Description**.



Enter Area Details

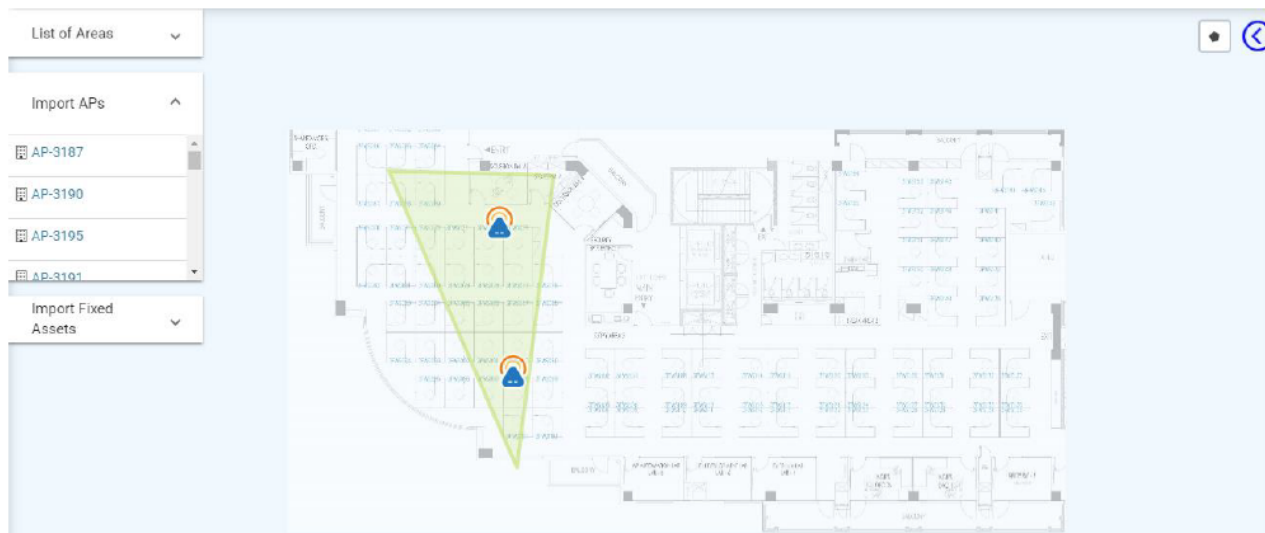
Area A
Max 32 characters allowed 6/32

CustomerArea
Max 64 characters allowed 12/64

Save Cancel

You can create multiple areas on a floor as per your requirement.

9. Select a specific area on the map and click on **Import APs** and place the listed access points on the marked polygon (area) on the floor.



You are prompted to enter the minimum **RSSI** value and required **EIRP** (TX power) of the access point.

Enter Cutoff-RSSI and TX power of AP (EIRP)

18

*TX power value is applicable for the Radio 1

18

*TX power value is applicable for the Radio 2

18

*TX power value is applicable for the Radio 3

-80

.....

This feature is only available in

Save Cancel

Hover over the site to view and edit the MAC address, Tx power, and minimum RSSI of each radio or delete the AP from the site.

AP NAME: GhViuwW ✕

MAC ADDRESS: [REDACTED]

RADIO 1:

TX POWER: 23

MAC ADDRESS: [REDACTED]

RADIO 2:

TX POWER: 23

MAC ADDRESS: [REDACTED]

RADIO 3:

TX POWER: 23

MAC ADDRESS: [REDACTED]

CUTOFF RSSI: -80

Edit Delete

To include Tx power in the ID packets, the enforcement devices and access points must have the supported firmware version.

- Dynamic changes to the Tx power on the FortiPresence GUI takes immediate effect and is overridden when the next ID packet arrives after an hour.
- Dynamic changes to Tx power on the enforcement device (FortiWLC, FortiGate, and FortiLAN Cloud) takes effect within 3 hours.

Add any other fixed assets, for example, printers, cameras, if required.

Go to **Location > Floor Analytics** to view the floor map with the APs.

Notes:

- All access points are listed here only when the location services is configured. See [Configuring Location Services on page 52](#).
- You can view the access points in **Admin > Settings > Discovered APs**.

Portal Management

The portal management operations of FortiPresence enable you to provide limited wireless access to visitors with social media authentication by creating customized portal login pages for your setup/establishment. The look-and-feel features of the portal allow you to choose and add your company logo and color themes. The created portals are managed by specific rules.

Portals are mapped to multiple sites and multiple portals can be created per site.

RADIUS clients are created for Captive Portal authentication and authorization configurations on FortiLAN Cloud/FortiGate/FortiWLC. See [Configuring Captive Portal on page 56](#).

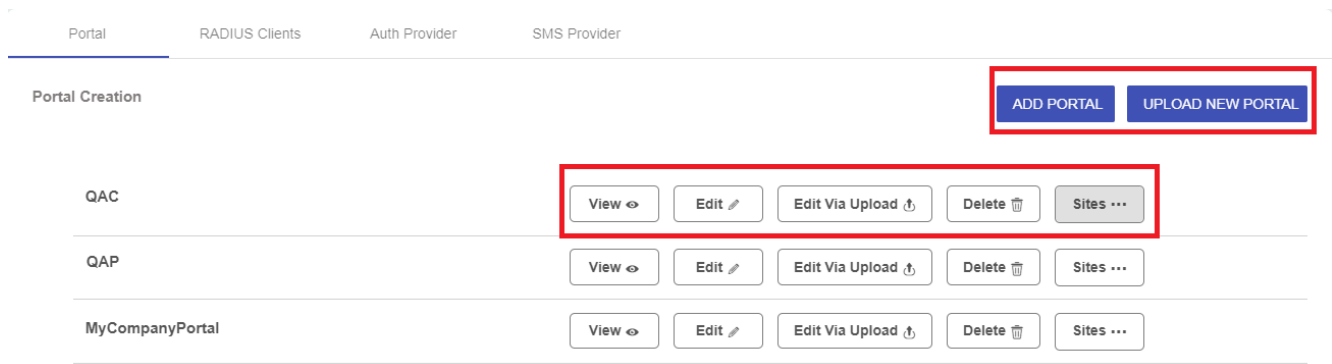
- [Creating a Portal on page 43](#)
- [Configuring Site Rules and Users on page 47](#)
- [RADIUS Configuration on page 48](#)
- [Portal Settings on page 48](#)

Creating a Portal

You can add new captive portals using FortiPresence templates or upload customized captive portals for your sites. The customized files can then be uploaded on the FortiPresence GUI.

- [Adding a New portal on page 44](#)
- [Uploading a New Portal on page 47](#)

Navigate to **Portal > Portal Settings** and perform any of the following operations.



- **Add Portal** - To add a new captive portal. See [Adding a New portal on page 44](#)
- **Upload New Portal** - To upload a new customized captive portal. See [Uploading a New Portal on page 47](#).
- **View** - To preview an existing portal for the supported devices.
- **Edit** - To edit an existing portal.
- **Edit via Upload** - To upload a customized captive portal. See [Uploading a New Portal on page 47](#)
- **Delete** - To delete an existing captive portal. The portal should be detached from all sites to be deleted successfully.
- **Site** - To view the sites that a captive portal is attached to.

Adding a New portal

Perform the steps in this procedure to add a portal.

1. Navigate to **Portal > Portal Settings** and select the site for which the portal is to be created. Click **Add Portal**.
2. Enter a unique **Portal Name** for your site and select a **Theme** and **Color** from the pallet for the portal authentication page. Click **Next**.
3. Upload your **Company Logo** and a **Background Image**. Separate background display images are required for desktop and mobile devices. Images in the JPG and PNG format are supported. Click **Next**.
Note: When upgrading from an older release, the one image uploaded is used for both desktop and mobile devices and first theme is applied by default.
4. Enter the acceptable usage policy for the visitors of your establishment/site and select **Show Policy** to prompt users to accept the policy prior to logging in.
5. Select the supported/permmissible authentication methods.
Portal Login – allows visitors to login using the captive portal. The login credentials are the same as portal users.
Social Login – allows visitors to login using their Facebook, Google, Instagram, or LinkedIn credentials.
No Login - allows visitors to login without any authentication mechanism.
6. Select the **Language** for your portal authentication page. English is the default and the supported languages are, French, Spanish, Romanian, Italian, and Portugese. Click **Next**.
7. Enable **Collect Email** to collect email information during visitor authentication through Captive Portal; enable **Verify Email** to verify the collected email information.
8. For visitors to receive the company's newsletter regularly, enable **Subscribe to the company's newsletter**.
9. Configure the website redirection options for visitors after successful login into the captive portal.
Default Success Page – Visitors are redirected to a successfully logged in portal page.
Original Request URL – Visitors are redirected to the initial URL they tried to browse before authenticating on the portal.
Specific URL – Visitors are redirected to the URL specified while creating the portal, for example <https://www.fortinet.com>.

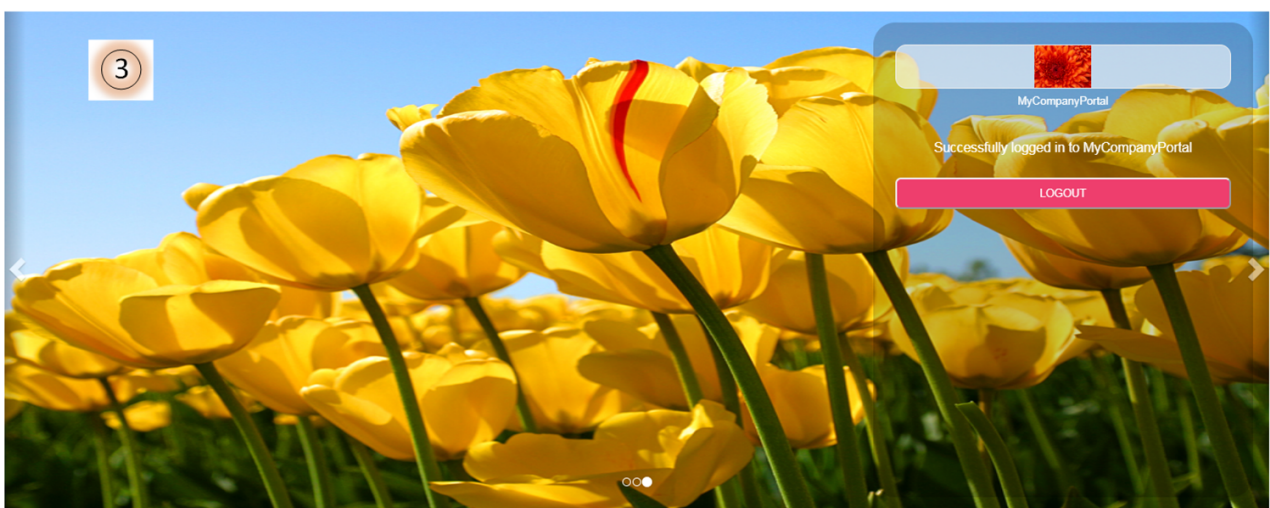
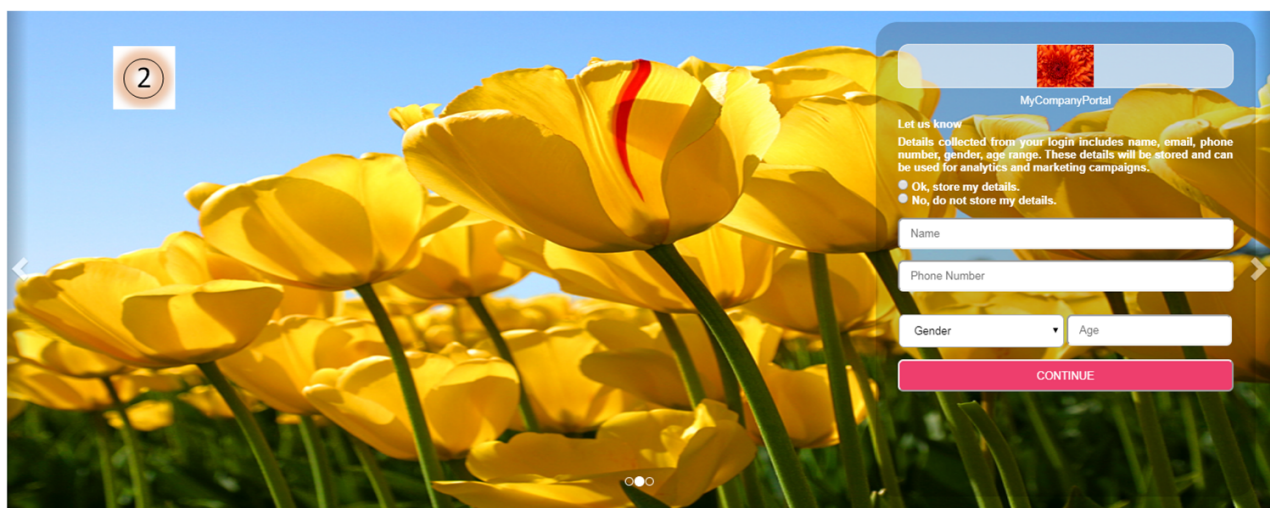
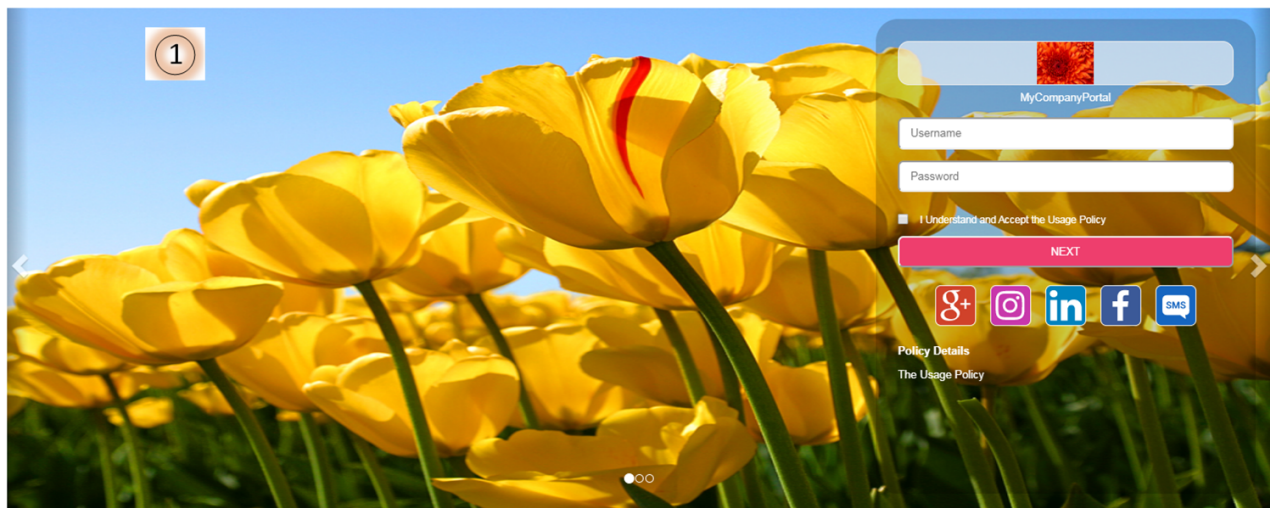
10. To download the portal for customization, click **Download**.

11. Click **Save**.

The portals created can be edited and deleted.

Note: For paid tier users, FortiPresence displays the visitors' e mail address, mobile number, age, and gender on the portal login pages on their devices.

This is a sample captive portal created and viewed on the FortiPresence GUI.



Uploading a New Portal

To upload a customized captive portal, download the portal template files in any of the following ways:

- Add a new portal and download it for customization. See [Adding a New portal on page 44](#).
- Download an existing portal for customization. Click **Edit** on the **Portal Settings** page and navigate to step 4. Click **Download**.

When you download an existing/new portal, *<Portal Name>.zip* is downloaded to your system. Refer to *README.txt* file in the downloaded folder to understand the rules for customization.

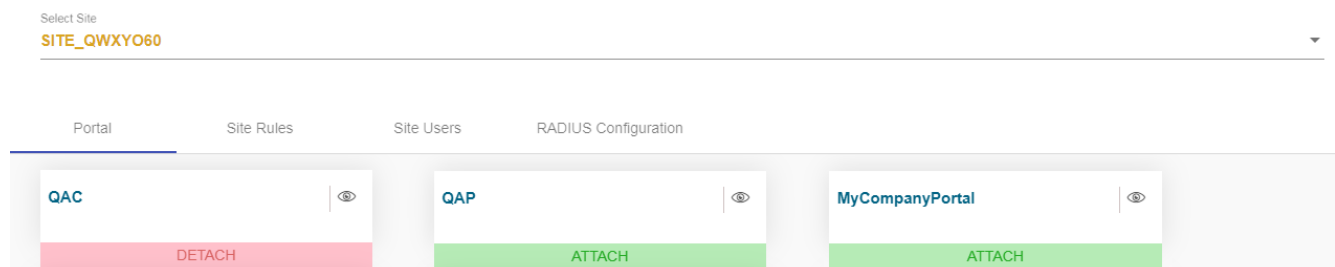
Note: Do not modify the JSON file in the downloaded folder.

You can customize the downloaded portal pages and edit them as per your requirement. After the customization is complete, upload the portal template files in any of the following ways:

- To upload a new portal, click **Upload New Portal** on the **Portal Settings** page and add the *<Portal Name>.zip*.
- To upload an existing customized portal, click **Edit via Upload** on the **Portal Settings** page and add the *<Portal Name>.zip*.

Configuring Site Rules and Users

Navigate to **Portal Management > Portal** to map portals to different sites. Each portal can be attached to multiple sites. All portals are displayed on this page, select the site and click **Attach** to associate a portal with a particular site. Click **Detach** to dis-associate a portal with a particular site.



Navigate to **Portal Management > Site Rules** to configure portal rules for the sites. A default portal rule is created when the first portal is created. Multiple rules can be assigned to different portals attached to a site. The portal rules can be reordered as per priority.

In this example, an area based portal rule is created.

Select Site
SITE_QWXYO60

Portal Site Rules Site Users RADIUS Configuration

Rule Name
AreaBasedAccess

Description
Rule for specific areas

Rules condition *
Area ID

Rules operator *
Equals

Actions option *
QAC

SITE_QWXYO60

☒ Go to Portal
☐ No portal

ADD

Navigate to **Portal Management > Site Users** to configure the **User Name** and **User Password** for the users of the site. You can edit and delete the user details.

RADIUS Configuration

Navigate to **Portal Management > Radius Configuration** to attach the configured RADIUS clients (**Portal > Portal Settings > RADIUS Clients**) to the site. Click **Attach** and the captive portal URL is generated for a specific RADIUS client. Copy this URL and use it while configuring the captive portal on FortiLAN Cloud/ FortiGate/ FortiWLC. See [Configuring Captive Portal on page 56](#).

Portal Settings

This section describes some additional FortiPresence settings.

Navigate to **Portal > Portal Settings**.

Setting	Description
RADIUS Clients	<p>Configure FortiLAN Cloud/FortiGate/ FortiWLC as RADIUS clients for portal authentication. The list of exempted FQDNs for FortiLAN Cloud, FortiGate, and FortiWLC are displayed here. See Creating a Portal on page 43.</p> <p>For existing portals or new ones, you are required to mandatorily add the FQDN, presence-resource.s3.eu-west-1.amazonaws.com to the captive portal exemption list on the enforcement devices (FortiGate, FortiLAN Cloud, FortiWLC).</p> <p>Note: You can edit and delete the RADIUS clients.</p>

Setting	Description
Auth Provider	The authentication provider settings enable you to configure the credentials derived from the Facebook, Google, Instagram, and LinkedIn applications that you use for portal authentication.

Administrative Settings

This section describes some additional FortiPresence settings.

Navigate to **Admin > Settings**.

Setting	Description
Threshold	<p>Select the sites for which to apply thresholds.</p> <p>Bounce Time Limit - This setting aids in collecting bounce rate analytics, that is, total number of stayed/engaged visitors based on the bounce rate threshold configured. Visitors who spend more time than the configured Bounce Time Limit are classified as stayed and the ones less than the bounce rate as bounced. This visitor statistics is reported in Presence Dashboard under Bounce Rate chart.</p> <p>Dwell Inactive Time Limit - This setting aids in collecting dwell time analytics, that is, the visitor dwell time based on the Dwell Inactive Time Limit threshold. If a visitor is seen after a gap of the configured threshold, it is considered as a new dwelling session for dwell time calculation. If the visitor is seen within the configured threshold, the dwell session continues. This visitor statistics is reported in Presence Dashboard under Dwell Time chart.</p> <p>Min Count of Observations - This setting lends accuracy to the visitor data on the dashboards. You can filter out random MAC addresses from devices in and around your establishment by setting the count of observations. Based on this setting visitor is reported only if he is seen more than or equal to Min Count of Observations. Note that the device reporting interval can be set while configuring location services.</p> <p>Organisational Unique Identifier (OUI) – When enabled, this setting filters out the non OUI MAC Addresses and is applicable for all the dashboards.</p> <p>Filter Employees – This setting is enabled by default and filters out the employee MAC addresses added in the Employees tab from site level analytics.</p>

Setting	Description
	<p>Detect Fixed Assets – You can specify threshold parameters that determine fixed assets to be excluded from analytics.</p> <p>The threshold parameters are number of hours and number of days (maximum: 7 days). 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.</p> <p>For example, if the threshold configuration is 5 hours and 3 days, then any device detected for more than 5 hours per day for a period of 3 consecutive days is declared a fixed asset. To view the fixed assets filtered for the configured threshold, select Auto-Detected Fixed Assets in Settings > Fixed Assets.</p> <p>Note: This feature is available only for paid tier users.</p> <p>Site Business Time – You can configure data collection duration for the FortiPresence dashboards. Different operating hours are configured for different days of the week. Configure the Opening Time and Closing Time for each day of the week. This threshold is configured per site.</p> <p>Note: This feature is available only for paid site users.</p>
Discovered APs	<p>Unique project name and secret key is generated for each account on FortiPresence. These are used to configure location services on FortiLAN Cloud/FortiGate/FortiWLC.</p> <p>The AP name, MAC address, serial number, timestamp, site, firmware version, license expiry date, state (Active (identification of packets received in the last 24 hours) or Inactive (no identification of packets received in the last 24 hours)), AP radio details (Tx power and MAC address) and Actions are displayed.</p> <p>If FortiPresence does not receive the Identification (ID) packets for any of the planned APs in the discovered AP list 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.</p> <p>You can sort the displayed column based on the name, timestamp, site, expiry date, and state.</p> <p>The Location server IP and port are also displayed here. The APs with location services enabled are displayed here. See Configuring Location Services on page 52.</p>
Fixed Assets	<p>The fixed assets added to this list are excluded from locationing services and analytics.</p> <p>Add manually or upload in a .csv format (similar to the sample file available for download) the fixed assets, for example, printers, cameras, scanners, in your establishment. You can specify the placement co-ordinates (X and Y Axis) of fixed assets on the map. You can place these assets on the map while creating/editing sites.</p> <p>Select Manual Fixed Assets to view the fixed assets uploaded manually and select Auto-Detected Fixed Assets to view the fixed assets determined by the thresholds configured in Thresholds (Detect Fixed Assets) tab.</p>

Setting	Description
Employees	<p>Select the site and manually add the MAC address or upload the file in the format similar to the sample file available for download.</p> <p>Once the MAC addresses are added, go to the Threshold tab and select the filter (enabled by default).</p>

User Management

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

You can create RBAC users and assign them specific access-based roles.

1. Navigate to **Admin > User Management** and enter a unique **First Name**, **Last Name**, and **Email ID** for each user. Ensure that the account you create here is also registered on *FortiCloud*. For more information on account management see notes on RBAC users in [Accessing FortiPresence](#).
2. Assign each user with either **Admin** or **User** roles. The **User** role is allowed only view access for dashboards and reports. The **Admin** role is allowed to perform administrative operations on the FortiPresence GUI.

3. Click **Add User**.
4. Click **Change Password** to assign a new unique password to the user account.

Once created, you can modify the assigned role and the password. To modify the password, click **Change Password**; an account reset link is sent to the specified e mail address.

To delete a user, click the delete icon against the specific user.

Configuring Location Services

With the completion of FortiPresence registration process, project name and project secret key are generated and are available at **Admin > Settings > Discovered APs**. The project name identifies the account to which the access point belongs. The project secret key is shared password between you and FortiPresence to validate the origin and untampered transmission of the station reports.

The project name and secret key are unique for each account registration; all sites under a particular account use the same project name and secret key.

The project name and secret key are required to be configured on FortiGate/FortiLAN Cloud/FortiWLC to enable Location Services. The location services are configured with location server IP address **34.245.252.61/location.presence.fortinet.com** and server port **4013**.

- [FortiLAN Cloud on page 52](#)
- [FortiGate on page 53](#)
- [FortiWLC on page 54](#)

FortiLAN Cloud

Follow this procedure on the FortiPresence and FortiLAN Cloud GUIs to enable and configure location services.

1. On the FortiLAN Cloud GUI select a configured AP Network and navigate to **Configure > FortiPresence**.
2. Enable **Location Services**; configure the mode as **Foreign Channels Only /Foreign and Home Channels**.
3. Enter the **Location Server IP Address** - 34.245.252.61 and **UDP Listening Port** - 4013, (**Location Server IP and Port** are displayed in the FortiPresence GUI - **Admin > Settings > Discovered APs**).

4. Enter the **Project Name** and **Secret Password**, (**Project Name** and **Project Secret Key** respectively copied from the FortiPresence GUI - **Admin > Settings > Discovered APs**).

The screenshot shows the FortiPresence GUI with the 'Discovered APs' tab selected. The top section contains fields for 'Project Name' (17c7cc003edb40ec), 'Project Secret Key' (81a6a2938dfc4a), 'Location Server IP' (34.245.252.61), and 'Port' (4013). A red arrow points from the 'Project Name' and 'Project Secret Key' fields to the bottom section, which is highlighted with a red box. The bottom section contains fields for 'Server IP Address' (34.245.252.61), 'UDP Listening Port' (4013), 'Project Name' (a9fead721f5549f1), and 'Primary server secret' (masked with dots). Below these fields are 'Report Transmit Frequency' (5), 'Reporting of Rogue APs' (Enable), and 'Reporting of Unassociated Stations' (Enable).

In the FortiPresence GUI, **Admin > Settings > Discovered APs**, refresh to view the access points discovered on FortiLAN Cloud.

FortiGate

Follow this procedure on the FortiPresence and FortiGate GUIs to enable and configure location services.

1. On the FortiGate GUI navigate to **WiFi and Switch Controller > FortiAP Profiles**.
2. Select and double-click a specific FortiAP profile, scroll down to the **FortiPresence** section.
3. Enable **Location Services**; configure the mode as **Foreign Channels Only/Foreign and Home Channels**.
4. Enter the **Project name** and **Password**, (**Project Name** and **Project Secret Key** respectively copied from the FortiPresence GUI - **Admin > Settings > Discovered APs**).

5. Enter the **FortiPresence server IP** - 34.245.252.61 and **FortiPresence server port** - 4013, (**Location Server IP** and **Port** are displayed in the FortiPresence GUI - **Admin > Settings > Discovered APs**).

The screenshot shows the FortiPresence GUI with the 'Discovered APs' tab selected. The 'FortiPresence' profile is highlighted. A red box highlights the 'Project name', 'Password', 'FortiPresence server IP', and 'FortiPresence server port' fields. A red arrow points from the 'Discovered APs' tab to the 'FortiPresence' profile.

RADIUS Clients	Threshold	Auth Provider	Discovered APs	Fixed Assets	My Account
Project Name :	17c7cc003edb40ec	Copy	Project Secret Key :	81a6a2938dfc4a	Copy
Location Server IP :	34.245.252.61	Copy	Port :	4013	Copy

FortiPresence

Mode: ☐ Disable ☐ Foreign Channels Only ☒ Foreign and Home Channels

Project name: 17c7cc003edb40ec

Password:

FortiPresence server IP: 34.245.252.61

FortiPresence server port: 4013

Report rogue APs: ☐

Report unassociated clients: ☒

Report transmit frequency (in seconds): 30

☐ Ekahau blink

☐ AeroScout

Locate WiFi clients when not connected: ☐

[OK](#) [Cancel](#)

In the FortiPresence GUI, **Admin > Settings > Discovered APs**, refresh to view the access points discovered on FortiGate.

Note: Repeat this procedure for every FortiAP profile in case you have multiple profiles.


FortiWLC

Follow this procedure on the FortiPresence and FortiWLC GUIs to enable and configure location services.

1. On the FortiWLC GUI navigate to **Configuration > Devices > Location Services**.
2. Enable **Location Services Feed**; configure the **Report Format** as **FortiPresence**.
3. Enter the **Project Name** and **Secret**, (**Project Name** and **Project Secret Key** respectively copied from the FortiPresence GUI - **Admin > Settings > Discovered APs**).

4. Enter the **Server IP Address** - 34.245.252.61 and **Server Port** - 4013, (**Location Server IP** and **Port** are displayed in the FortiPresence GUI - **Admin > Settings > Discovered APs**).

RADIUS Clients	Threshold	Auth Provider	Discovered APs	Fixed Assets	My Account
Project Name :	17c7cc003edb40ec	Copy	Project Secret Key :	81a6a2938dfc4a	Copy
Location Server IP :	34.245.252.61	Copy	Port :	4013	Copy



Location Services Configuration ?

Location Services Feed Enable ▼

Report Format Forti-Presence ▼

Project Name 17c7cc003edb40ec Enter 1-16 chars.

Secret

Source Type All ▼

Server IP Address/hostname 34.245.252.61 Enter IPv4 or IPv6 Address or FQDN Name.

Server Port 4013 Valid range: [300-65535]

Report Interval (in Seconds) 5 Valid range: [3-3600]

Apply to ALL APs No ▼

AP Groups Select Here ▼

Access Points Select Here ▼

In the FortiPresence GUI, **Admin > Settings > Discovered APs**, refresh to view the access points discovered on FortiWLC.

Configuring Captive Portal

Captive Portal configurations for wireless access to visitors are to be accomplished on both FortiPresence and FortiGate/FortiLAN Cloud/FortiWLC based on the deployed access points. You are required to configure RADIUS profiles for authentication and specify the Fully Qualified Domain Names (FQDN URL) that will be exempted and enabled to process social WiFi login. For example, to allow Facebook login, enter *www.facebook.com*. The list of FQDNs are available on the FortiPresence GUI – **Portal > Portal Settings > RADIUS Clients**.

The RADIUS profiles are configured with RADIUS server IP address **34.245.252.61/radius.presence.fortinet.com** and port **1812** for authentication and **1813** for accounting.

This section describes the Captive Portal configurations on the FortiGate/FortiLAN Cloud/FortiWLC. Prior to configuring Captive Portal ensure the following:

- Sites are created – See [Site Management on page 38](#)
- Portals are configured on FortiPresence – See [Portal Management on page 43](#).

Follow this procedure to create RADIUS clients on FortiPresence.

1. On the FortiPresence GUI navigate to **Portal > Portal Settings > Radius Clients** to create a RADIUS client for the public IP address of the FortiLAN Cloud.
2. Enter the **RADIUS Client Name**, **RADIUS Client IP**, **RADIUS Secret Key**, and select the **Device Type** as FortiGate/FortiLAN Cloud/FortiWLC. Click **Add**.

Portal	RADIUS Clients	Auth Provider	SMS Provider
Exemption List:			
RADIUS Client Name: FortiWLC Max 32 characters allowed			
RADIUS Client IP: 8/32			
RADIUS Secret Key			
Device Type: FortiGate FortiWLC FortiLANCloud			
NAME FORTIWLC SECRET KEY			

For FortiLAN Cloud setups:

Configure the RADIUS Client IP address based on your region. For the latest RADIUS client IP address, navigate to **FortiAP Network > Configure > SSID** on the FortiLAN Cloud GUI.

FortiLAN Cloud Global – 173.243.132.77

FortiLAN Cloud Europe – 81.201.100.238

FortiLAN Cloud Japan – 173.243.132.207

The **Project Secret Key** is **fortipresence**.

3. Navigate to **Portal Management** and select the site to attach the configured RADIUS client.

4. Select **Radius Configuration** and click **Attach** against the RADIUS client created for FortiLAN Cloud. The captive portal URL is generated.

FortiWLC NAME		SecretKey SECRET KEY	Captive Portal URL https://connect.presence.fortinet.com/portal/c7206c9c68f44c069982c...	DETACH
------------------	--	-------------------------	---	--------

- FortiLAN Cloud on page 57
- FortiGate on page 58
- FortiWLC on page 62

FortiLAN Cloud

Follow this procedure on the FortiLAN Cloud GUI to configure captive portal.

1. Select a configured AP Network and navigate to **Configure > My RADIUS Server** to configure a RADIUS profile. Click **Add My RADIUS Server**. Update the configuration parameters as required.
2. Enter the **Primary Server Name/IP** –34.245.252.61/radius.presence.fortinet.com.
3. The **Primary Server Secret** should be the same as the **RADIUS Secret Key** configured on the FortiPresence GUI (**Portal > Portal Settings > Radius Clients**). Click **Apply** and update the configuration parameters as required.
Note: Configure the Project Secret Key to fortipresence for all FortiLAN Cloud setups.

×

Add My RADIUS Server

Name *

RADIUS-AUTH

NAS IP

Primary Server Name/IP *

34.245.252.61

Primary Server Secret *

.....

Show

Secondary Server Name/IP

Secondary Server Secret

Show

Server Port *

1812

CoA Status

☐

Apply

Cancel

4. Navigate to **Configure > SSIDs** to create an SSID. Configure the **Captive Portal** as **My Captive Portal** and enter the **Captive Portal URL**, (Captive Portal URL copied from the FortiPresence GUI – **Portal Management > Radius Configuration**).
5. Set the **Redirect URL** to **Specific URL** and enter <https://connect.presence.fortinet.com/portal/success>. The actual redirect option can be specified while creating the portal on FortiPresence GUI - [Adding a New portal on page 44](#).
6. Enter the FQDN based exclusions in the **Walled Garden** list. A comma separated list with character limitation is supported.
7. Select **My RADIUS Server** and specify the RADIUS profile created earlier in this procedure as the **Sign on Method**.

SSID *	FortiPresence	
Enabled	<input checked="" type="checkbox"/>	Broadcast SSID <input checked="" type="checkbox"/>
MAC Access Control	<input type="checkbox"/>	
Mesh Link	<input type="checkbox"/>	
Authentication	Open ▼	
Captive Portal	My Captive Portal ▼	
Captive Portal URL	https://connect.presence.fortinet.com/portal/2decc69418684202 How to build my captive portal page?	
Redirect URL	<input checked="" type="radio"/> Original Request <input type="radio"/> Specific URL	
Walled Garden	www.google.co.in, www.facebook.com, www.gmail.com	
	<small>* IP address, domain name and sub-network address/mask are allowed.</small> <small>* To enter more than one value, separate the values with a comma.</small>	
Sign on Method	My RADIUS Server ▼	RADIUS_AUTH ▼
	Test the RADIUS Server <small>* Please whitelist FortiCloud server (IP: 208.91.113.117) as a client to access the RADIUS server.</small>	
IP Assignment	<input type="radio"/> NAT <input checked="" type="radio"/> Bridge	
QoS Profile	<Disable> ▼	
VLAN ID	0	

8. Click **Next** and update the configuration parameters as required. Click **Apply**.

FortiGate

Follow this procedure on the FortiGate GUI to configure captive portal.

1. Navigate to **User and Device > RADIUS Servers** and create a new RADIUS server authentication profile. Select **Create New**.
2. Enter the primary RADIUS server details. The **Primary Server IP/Name** - 34.245.252.61/radius.presence.fortinet.com. The **Primary Server Secret** should be the same as the **RADIUS Secret Key** configured on the FortiPresence GUI (**Portal > Portal Settings > Radius Clients**).

3. Enter the **NAS IP** and click **OK**.

New RADIUS Server

Name: RADIUS_AUTH

Primary Server IP/Name: radius.presence.fortinet.com

Primary Server Secret: •••••••• Test Connectivity

Secondary Server IP/Name:

Secondary Server Secret: Test Connectivity

Authentication Method: **Default** Specify

NAS IP: 10.34.110.119

Include in every User Group: ☐

OK Cancel

4. Configure RADIUS server accounting profile via the FortiGate CLI mode. Run the following commands in the same order.
- ```
config user radius
edit <RADIUS profile created in Step 2>
config accounting-server
edit <integer>
set status enable
set server <IP address of the RADIUS server>
set secret <same as the RADIUS Secret Key configured on the FortiPresence GUI (Portal > Portal Settings > Radius Clients)>
```
5. Navigate to **User and Device > User Groups** and create a new user group to map the RADIUS servers to the user group for ease of configuration. Select **Create**

6. Click **Add** in the **Remote Groups** section and select the configured RADIUS authentication server. Click **OK**.

**Edit User Group**

Name: FortiPresence\_UserGroup

Type: **Firewall**

Members: +

Remote Groups

+ Add Edit Delete

Remote Server

**RADIUS\_AUTH**

OK Cancel

7. Navigate to **Policy and Objects > Addresses** to create individual addresses for exemption FQDNs. Select **Create New > Addresses** and update the configuration parameters as required.
8. Select **Type** as **FQDN** and enter the exempt FQDN. Click **OK**.

**New Address**

Name: FortiPresence\_Connect

Color: [Change]

Type: **FQDN**

FQDN: connect.presence.fortinet.com

Interface: any

Show in Address List: ☒

Static Route Configuration: ☐

Comments: 0/255

OK Cancel

9. Repeat Steps 7 and 8 to create exclusion based addresses for all FQDNs.
10. Create address groups to easily map the individual FQDNs. Select **Create New > Address Group** and update the configuration parameters as required and populate the FQDN entries in the Members field. The FQDN entries are displayed in the right-side panel.

New Address Group

Group Name

Color [Change]

Members

- google
- google-drive
- google-play
- 

Show in Address List ☒

Static Route Configuration ☐

Comments  0/255

OK Cancel

You can create a single address group or multiple groups based on your requirement.

11. Navigate to **WiFi and Switch Controller > SSID** to create an SSID. Click **Create New > SSID** and update the configuration parameters as required.
12. Select the **Security Mode** as **Captive Portal** and the **Authentication Portal** type as **External**.
13. Enter the **Authentication Portal**, (**Captive Portal URL** copied from the FortiPresence GUI – **Portal Management > Radius Configuration**) and select the created **User Group**.
14. Select the address groups created for exempted FQDNs in **Exempt Destination/Services**. Click **OK**.
15. Set the **Redirect After Captive portal** to **Specific URL** and specify <https://connect.presence.fortinet.com/portal/success>. The actual redirect option can be specified while creating the portal on FortiPresence GUI - [Adding a New portal on page 44](#)
16. Navigate to **Policy & Objects > IPv4 Policy** to configure Firewall policies. Select **Create New**. You are required to create the following three Firewall policies:
  - a. Policy to allow access to the DHCP and DNS services before authentication.
  - b. Policy to allow access to the exempted FQDNs for authentication.
  - c. Policy to allow access to the internet after authentication.

The following is an example of a policy to allow access to the exempted FQDNs for authentication.

New Policy

|                    |                                                                                                         |             |
|--------------------|---------------------------------------------------------------------------------------------------------|-------------|
| Name               | CaptivePortal-PermitAuth                                                                                |             |
| Incoming Interface | ESS-CLOUD (ESS-CLOUD)                                                                                   | X           |
| Outgoing Interface | port1                                                                                                   | X           |
| Source             | all                                                                                                     | X           |
| Destination        | FortiPresence_Connect<br>FB OAUTH GROUP<br>GOOGLE OAUTH GROUP                                           | X<br>X<br>X |
| Schedule           | always                                                                                                  |             |
| Service            | ALL                                                                                                     | X           |
| Action             | <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN |             |

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☐

OK Cancel

## FortiWLC

Follow this procedure on the FortiWLC GUI to configure captive portal.

1. Navigate to **Configuration > Security > RADIUS** to configure a RADIUS profile. Click **Add**. Create one RADIUS profile for authentication and one for accounting. Update the configuration parameters as required.

**Note:** The FortiWLC SSID must be configured in the tunnel mode; SSIDs in the bridge mode are NOT supported for Captive Portals.

2. Enter the **RADIUS IP** - 34.245.252.61 and the **RADIUS Secret** should be the same as the **RADIUS Secret Key** configured on the FortiPresence GUI (**Portal > Portal Settings > Radius Clients**). Click **Save**.

### RADIUS Profiles - Add ?

|                       |                                            |                           |
|-----------------------|--------------------------------------------|---------------------------|
| RADIUS Profile Name * | <input type="text" value="RADIUS-AUTH"/>   | Enter 1-16 chars.         |
| Description           | <input type="text"/>                       | Enter 0-128 chars.        |
| RADIUS IP *           | <input type="text" value="34.245.252.61"/> | Enter 0-127 chars.        |
| RADIUS Secret *       | <input type="password" value="*****"/>     | Enter 1-64 chars.         |
| RADIUS Port           | <input type="text" value="1812"/>          | Valid range: [1024-65535] |

3. Navigate to **Configuration > Security > Captive Portal** and create a **Captive Portal Exemptions** profile. Click **Add** and update the configuration parameters as required. Enter the FQDN based exclusions in the **FQDN** list.

#### Add Captive Portal Exemptions

|                |                                                         |                               |
|----------------|---------------------------------------------------------|-------------------------------|
| Profile Name * | <input type="text" value="Authentication-Exemptions"/>  | Enter 1-32 chars.             |
| Description    | <input type="text" value="Exempted FQDNs for FortiPi"/> | Enter 0-128 chars.            |
| FQDN           | <input type="text"/>                                    | Enter 1-256 chars. <b>ADD</b> |

| Added FQDN               |                               |
|--------------------------|-------------------------------|
| <input type="checkbox"/> | FQDN                          |
| <input type="checkbox"/> | graph.facebook.com            |
| <input type="checkbox"/> | facebook.com                  |
| <input type="checkbox"/> | fbcdn.net                     |
| <input type="checkbox"/> | google.com                    |
| <input type="checkbox"/> | www.googleapis.com            |
| <input type="checkbox"/> | gstatic.com                   |
| <input type="checkbox"/> | googleusercontent.com         |
| <input type="checkbox"/> | youtube.com                   |
| <input type="checkbox"/> | connect.presence.fortinet.com |

**DELETE**

4. Create a **Captive Portal** profile. Click **Add** and in **User Authentication** enter the RADIUS profiles created for authentication and accounting.
5. Configure the **External Portal Settings**, Select **Fortinet-Presence** as the **External Server**.

6. Select the **Captive Portal Exemption Profile** created in Step 7 enter the **Captive Portal URL**, (**Captive Portal URL** copied from the FortiPresence GUI – **Portal Management > Radius Configuration**). Click **Save**.

Add Captive Portal Profile

CP Name \*  Enter 1-32 chars.

**User Authentication**

Authentication Type

**Radius Authentication**

Primary Authentication

Secondary Authentication

**Radius Accounting**

Primary Accounting

Secondary Accounting

Accounting Interim Interval  Valid range: [ 60-36000 ].

**External Portal Settings**

External Server

Captive Portal Exemption Profile

External Portal URL  Enter 0-255 chars.

Public IP of Controller  Enter IPv4 or IPv6 Address.

7. Navigate to **Configuration > Security > Profile**. Click **Add** and update the configuration parameters as required.
8. Configure the **Captive Portal Settings**. Select **WebAuth** as the **Captive Portal** and select the created **Captive Portal profile** in Step 8 and the **Captive Portal Authentication Method** as **External**.
9. Enter the Captive Portal profile name as the **Passthrough Firewall Filter ID**. Click **Save**.

CAPTIVE PORTAL SETTINGS

Captive Portal

Captive Portal profile

Captive Portal Authentication Method

Passthrough Firewall Filter ID  Enter 0-16 chars.

10. Navigate to **Configuration > Wireless > ESS** to create an ESS profile. Click **Add** and update the configuration parameters as required.
11. Select the **Security Profile** created in Step 10. Click **Save**.

## Schedule Configuration

You can schedule auto-generation of reports and logs for ease-of-use instead of downloading them manually. Navigate to **Admin > Schedule Configuration**.

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



## Schedule Reports

In this tab, enter a unique **Configuration Name** to configure and save the report delivery schedule.

Schedule Reports
Schedule Logs

Configuration Name  
TestReport

Add Users

@fortinet.com X

Reports  
Network Report

Select site  
SITE\_QO5F200

Select building  
SITE\_QO5F200

Select floor  
SITE\_QO5F200

Select area  
SITE\_QO5F200

Fortinet
Everyday at 1:00
Apple
4-5 GB
4-5 GB
30-60 Min

RESET

Report Format  
PDF

Schedule Date\Time  
Every Tuesday at 3:00

RESET

SAVE

- **Add Users** - The auto-generated reports are delivered to email addresses that are specified here. A maximum of 25 email addresses are supported for each configuration.
- **Reports** - Select one or multiple types of reports to generate and configure the data filters to include in the report.
- **Report Format** - Select the report generation format, *PDF* or *CSV*.
- **Schedule Date/Time** - Select the time interval to generate the report, **Daily**, **Weekly**, or **Monthly**.

Click **Save**, the configure auto-generation schedule is saved. You can edit or delete this configuration.

| Name       | Actions |
|------------|---------|
| TestReport |         |

To view the list of historically generated reports and download them, click **Schedule Logs**.

Schedule Reports
Schedule Logs

| Reports       | Users         | Report Format | Schedule Date/Time | Actions |
|---------------|---------------|---------------|--------------------|---------|
| Device Report | @fortinet.com | PDF           | Everyday at 14:38  |         |
| Device Report | @fortinet.com | CSV           | Everyday at 14:38  |         |

