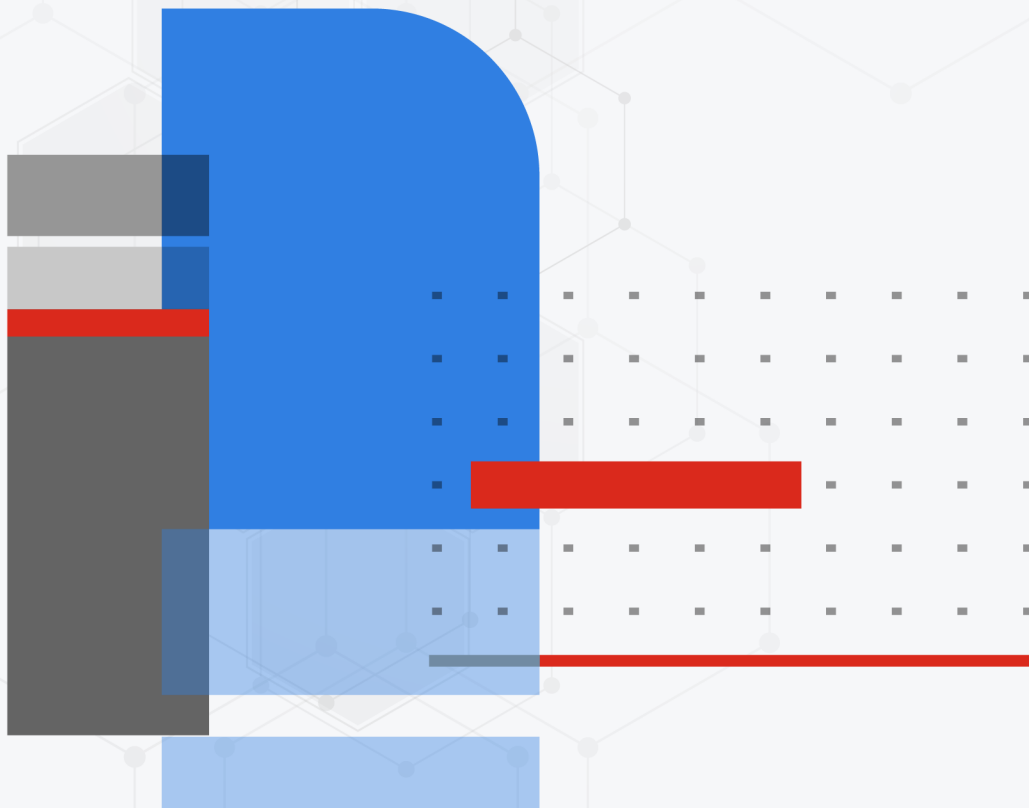




Administration Guide

FortiPresence 23.4



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

February 12, 2024

FortiPresence 23.4 Administration Guide

69-234-865552-20240212

TABLE OF CONTENTS

Change log	5
Overview	6
How FortiPresence Works	8
FortiPresence User Interface overview	10
Licensing	11
Viewing License Information	12
Signing-on for FortiPresence	13
Registering on FortiCloud	13
Accessing FortiPresence	13
External IDP Authentication	14
Dashboards and Reports	15
Dashboard	15
Creating a Dashboard	15
Adding Widgets	16
Editing and Deleting Dashboards	17
Statistics	18
Reports	20
Site Report	20
Visitor Reports	21
Schedule Configuration	22
Download Reports	23
Captive Portal Management	24
Creating a Captive Portal	24
Adding a New Captive Portal	25
Uploading a New Captive Portal	27
Configuring Captive Portal Rules and Users	27
Attaching RADIUS Clients	28
Configuring Authentication Provider	28
Configuring RADIUS Clients	29
Site Management	30
Sites	30
Resources	31
Settings	32
Administering FortiPresence	35
AP Management	35
License Details	36
Email Notifications	36
Configuring Location Services	38
FortiLAN Cloud	38
FortiGate	39
FortiWLC	39

Configuring Captive Portal	41
FortiLAN Cloud	41
FortiGate	43
FortiWLC	47

Change log

Date	Change description
2023-12-07	FortiPresence version 23.4 release document.
2024-02-12	Content format updates.

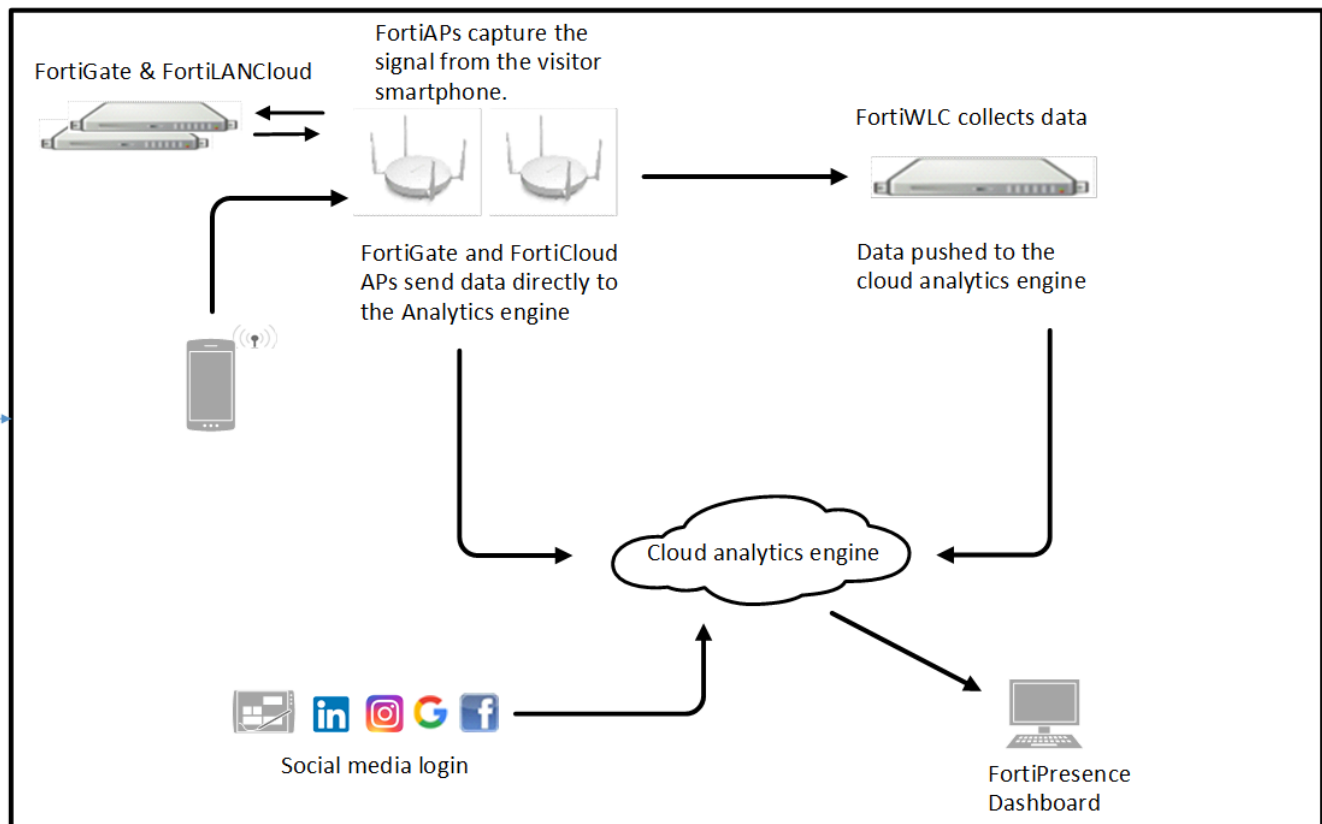
Overview

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.

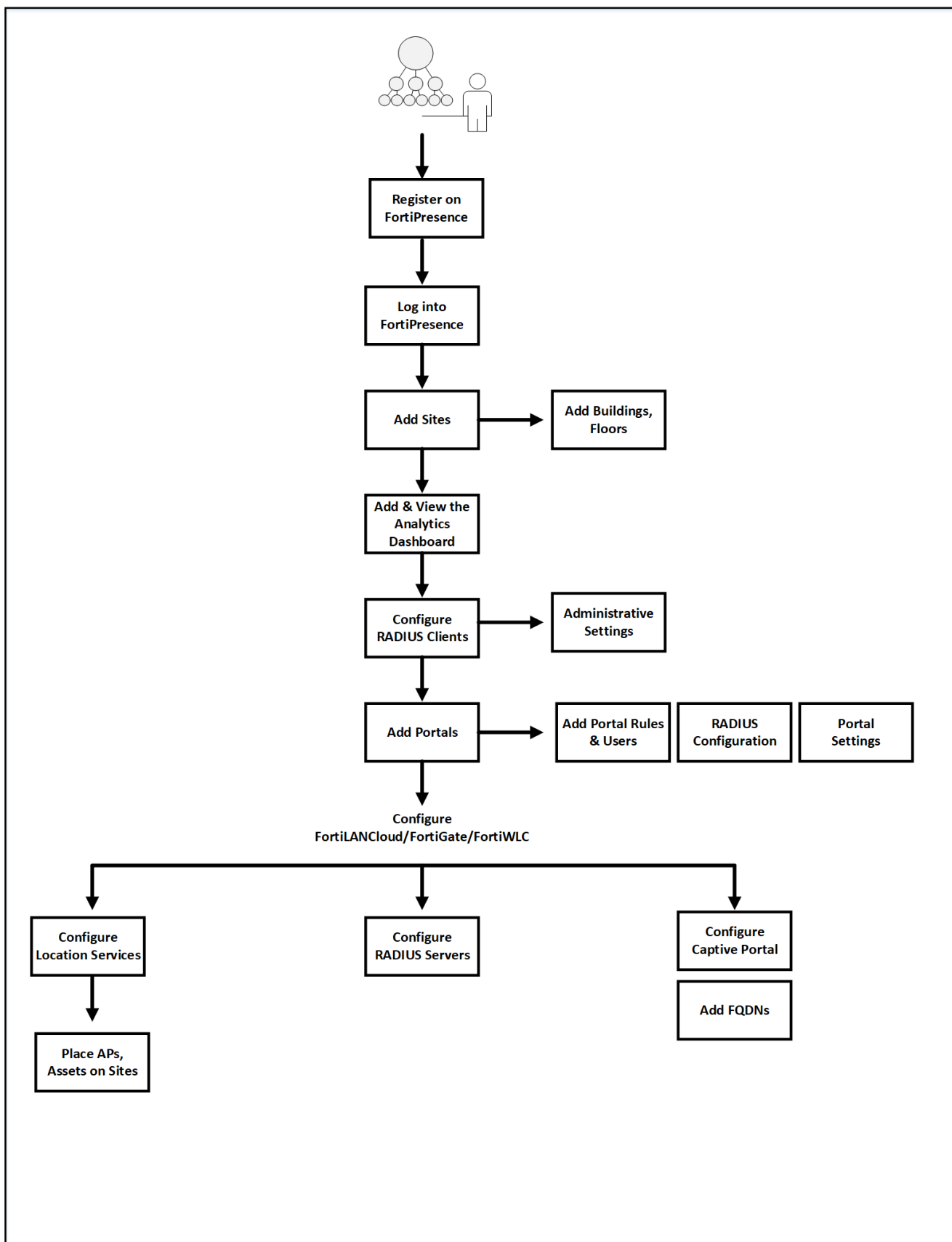
FortiPresence is **General Data Protection Regulation (GDPR)** compliant.

- 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

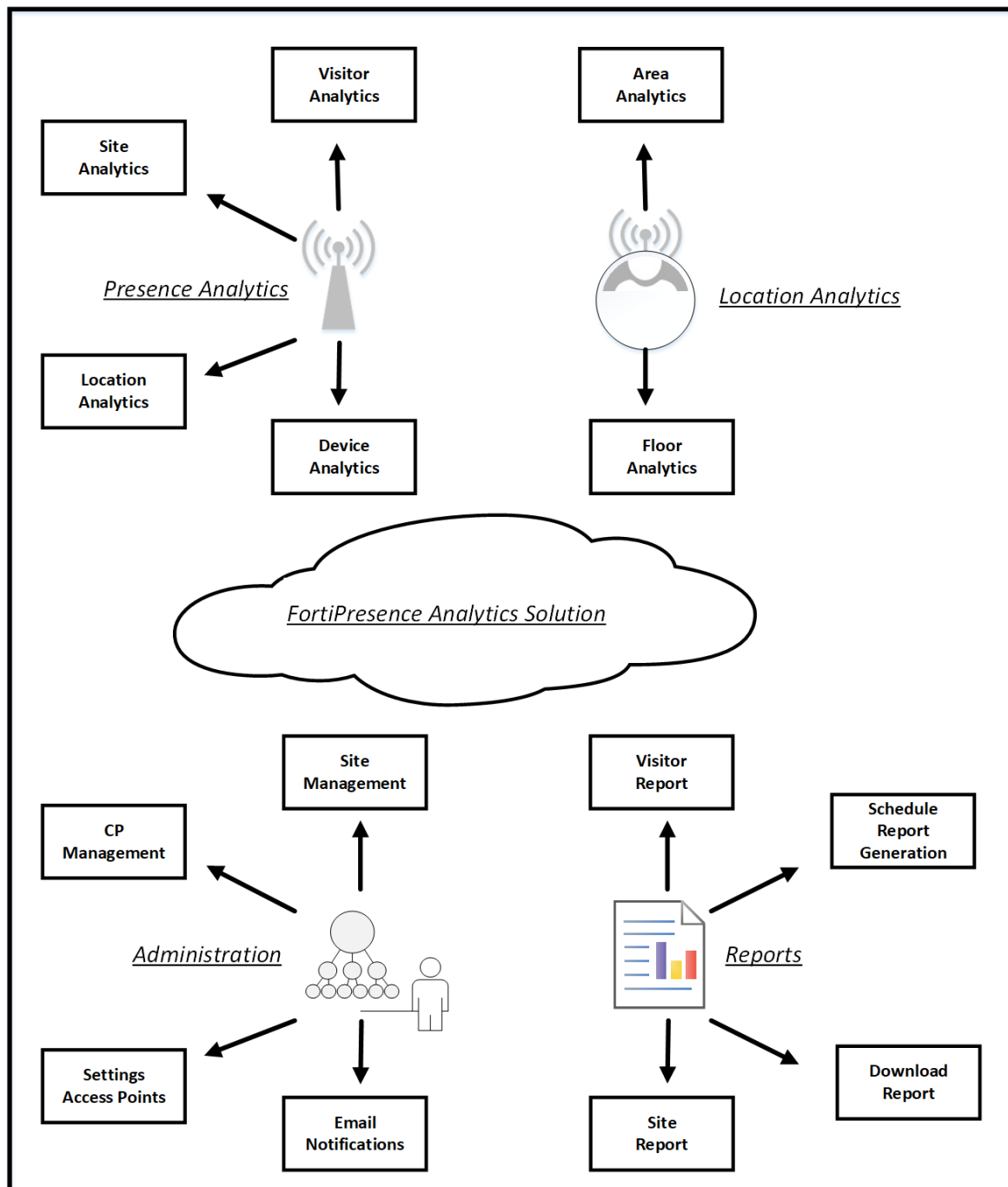
This document describes the configurations and management operations on FortiPresence, FortiLANCloud, FortiGate, and FortiWLC to enable location services for location analytics and Captive Portal configurations for social media logins and internet access. You can add and manage sites using the integrated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



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 a Freemium version. Data retention for Freemium 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 Freemium 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.
- Freemium 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 Freemium users are described in this table.




Feature	Licensed	Freemium
Number of Sites	Unlimited	1
Number of access points	Unlimited	15
Data Retention	1 year	7 days
Number of concurrent Captive Portal sessions	Unlimited	200
Specifying the RSSI of the AP while adding it in a site.	Yes	Yes
RSSI Threshold	Yes	Yes
Email notification for inactive APs	Yes	Yes

Feature	Licensed	Freemium
Captive Portal customization	Yes	Yes
Themes and images for captive portal	Yes	Yes
Language support for captive portal	Yes	Yes
Schedule Configuration (Reports)	Yes	No
Collect email and phone number for portal users.	Yes	No
Automatic exclusion of fixed assets	Yes	No
Email verification	Yes	No
Social authentication via Instagram and linkedIn	Yes	No
Fixed employees	Yes	No

Note: Only 30 days of data is stored for area movement, floor data and heat maps

Viewing License Information

To view licensing information for access points navigate to **Administration > AP Management**.

Access Points License Details									
 Delete	 Search								
<input type="checkbox"/>	Status	Name	Mac Address	Serial No	Timestamp	Site	Firmware Version	Expiry	AP Radio
<input type="checkbox"/>	Active	AP-1			2023/08/18 10:58:26	Demo Site 1	8.3-3dev-25	2024/06/23 11:01:19	AP Radio 1 AP Radio 2 AP Radio 3
<input type="checkbox"/>	Active	AP-2			2023/08/18 10:58:26	Demo Site 1	8.3-3dev-25	2024/06/23 11:01:19	AP Radio 1 AP Radio 2 AP Radio 3

- 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

Single sign-on support is available 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	<ol style="list-style-type: none"> 1. Registering on FortiCloud on page 13 2. Accessing FortiPresence on page 13
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.	<ol style="list-style-type: none"> 1. Accessing FortiPresence on page 13

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.

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 FortiLAN Cloud account. To configure IAM users, see [Adding IAM users](#).

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.

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 to add external IDP roles. See [Adding external IdP roles](#).

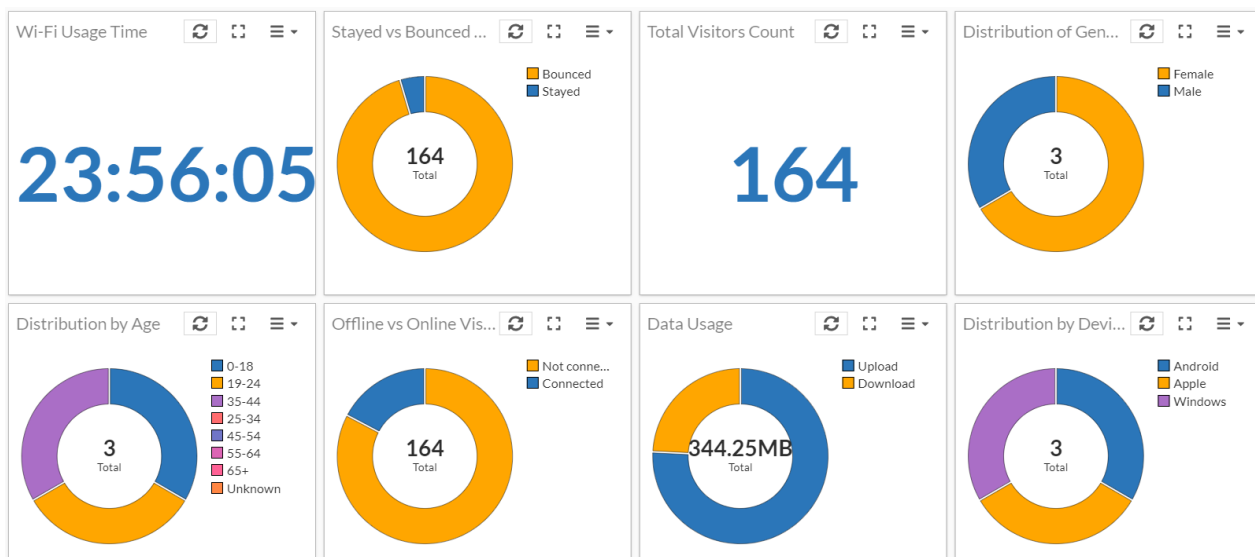
Dashboards and Reports

The FortiPresence GUI provides presence analytics in customizable dashboards and downloadable reports.

Dashboard

The 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.

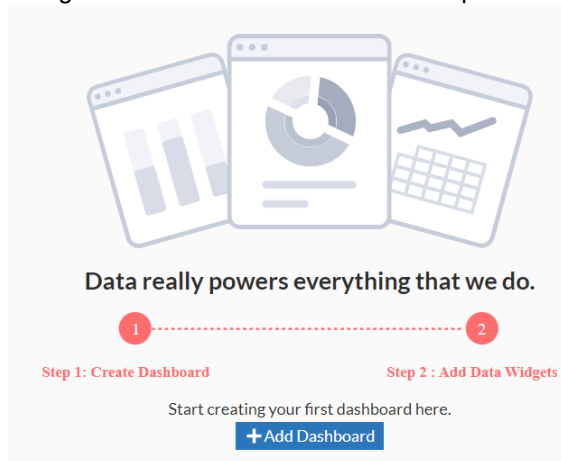
The access points (FortiGate and FortiLAN Cloud) and the FortiWLC controllers send the aggregated client data (station reports) to the cloud analytics engine as per configured time intervals. The analytics engine processes this raw data which is then compiled into summary charts and statistics. This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



Creating a Dashboard

You can create a dashboard tailored to your own requirements with specific data widgets.

1. Navigate to **Dashboards** on the left-side panel of the GUI and click **+ Add Dashboard**).



2. Enter a unique **Dashboard Name** and select any of the following data ranges.

Create Dashboard

Dashboard

Today's Data

Cancel

Create

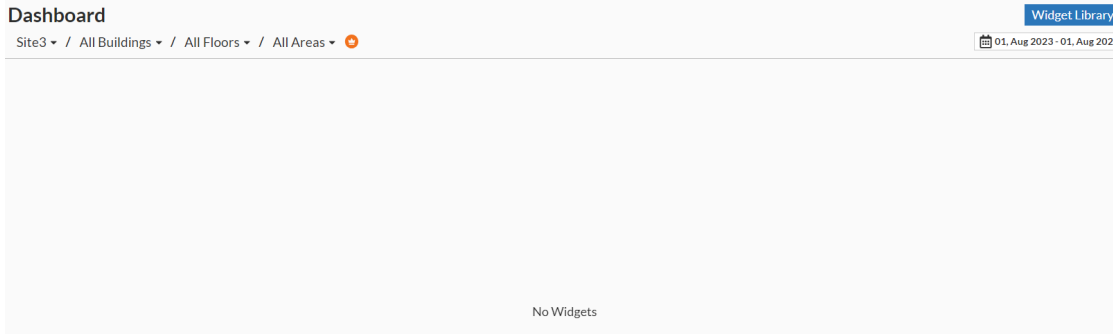
- **Today's Data** - The data generated in the last 24 hours.
- **Historic Date wise Data** - A calendar option is provided in the dashboard that allows you to select a specific date for viewing FortiPresence data.
- **Historic DateRange wise Data** - A calendar option is provided in the dashboard that allows you to select a specific date range for viewing FortiPresence data or view weekly (current and last)/monthly (current and last) data.

This Month	<	August, 2023							September, 2023							>
Last Month		Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	
This Week			1	2	3	4	5	6					1	2	3	
Last Week		7	8	9	10	11	12	13	4	5	6	7	8	9	10	
		14	15	16	17	18	19	20	11	12	13	14	15	16	17	
		21	22	23	24	25	26	27	18	19	20	21	22	23	24	
		28	29	30	31				25	26	27	28	29	30		
2023/08/01 → 2023/08/01																

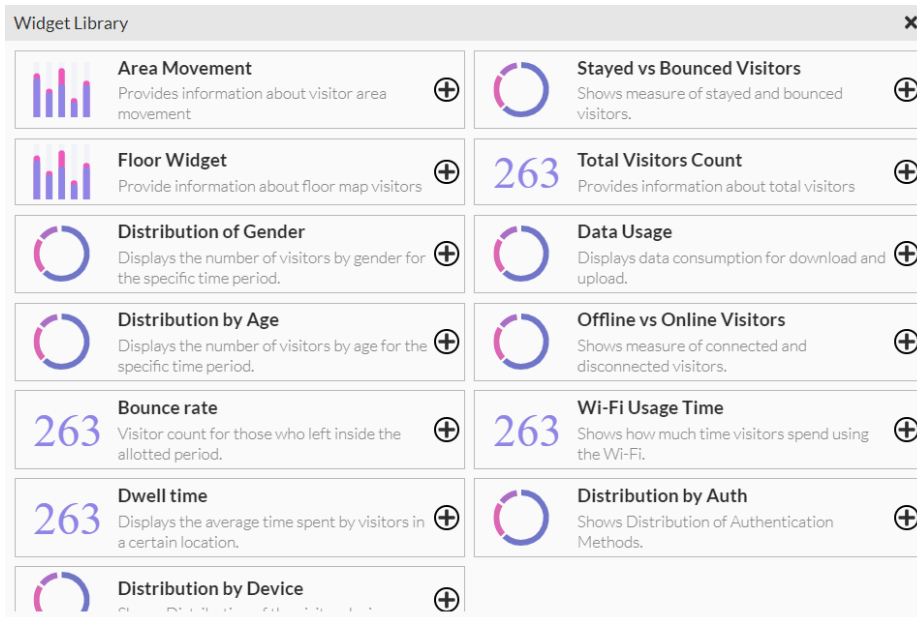
3. Click **Create**. A new dashboard is created.

Adding Widgets

FortiPresence allows you to select and manage the various widgets displaying data on the dashboards. A new dashboard does not contain any widgets. Click the **Widget Library** to add widgets.

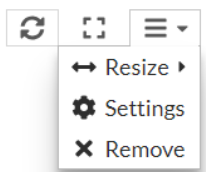


Select the widgets you want on your dashboard and click **Add**. The selected widgets are displayed in the dashboard.



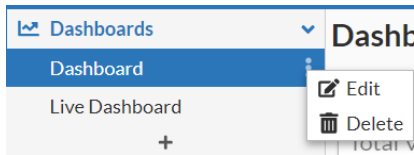
- **Floor Widget** - This widget is available only in the **Today's Data** and **Historic Date wise Data** dashboards.
- **Area Movement** - This widget is available only in the **Historic Date wise Data** dashboard.
- **Busiest Time** - This widget is available only in the **Historic Date Range wise Data** dashboard.

Click on the right-side menu on a widget and you can re-size, remove, and re-name (**Settings**) the widgets as required.



Editing and Deleting Dashboards

To edit and delete an existing dashboard, click on the  icon on the left-side menu and select **Edit** or **Delete**.



Note: The edit operation allows you to change the name of the dashboard.

Statistics

The dashboard calculates the average statistics during the selected time range and displays it on the dashboard. The dashboard provides real time data and analytics based on the following parameters:

- [Visitor Analytics on page 18](#)
- [Device Analytics on page 18](#)
- [Site Analytics on page 19](#)
- [Location Analytics](#)

Visitor Analytics

This section provides analytics based on visitor behaviour.

- **Total Visitors Count** – Provides the total number of visitors for the configured view time.
- **Distribution By Device** – 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.
- **Offline vs Online Visitors** – 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**).
- **Distribution of Gender** – Provides the gender based visitor percentage calculated as per the social network login information.
- **Distribution By Age** – 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**.
- **Distribution by Auth** – 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**.

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. Hover over the chart to get the number of users against each of the buckets.

Site Analytics

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

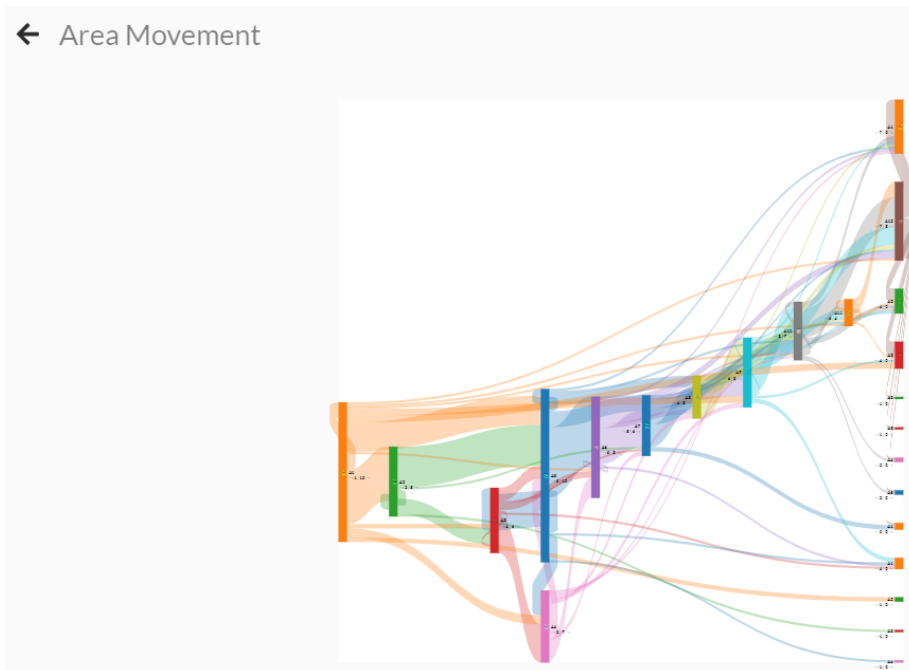
- **Bounce Rate** – Provides the total number of and stayed/engaged visitors based on the bounce rate threshold configured at **Site Management > Settings**. Visitors who spend more than the configured bounce rate are classified as stayed and the ones less than the bounce rate as bounced.
- **Dwell Time** – Provides the total visitor dwell time in minutes based on the **Dwell Inactive Time Limit** threshold configured at **Site Management > Settings**. 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.

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 floor/area widgets of the dashboard 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.

Area Analytics

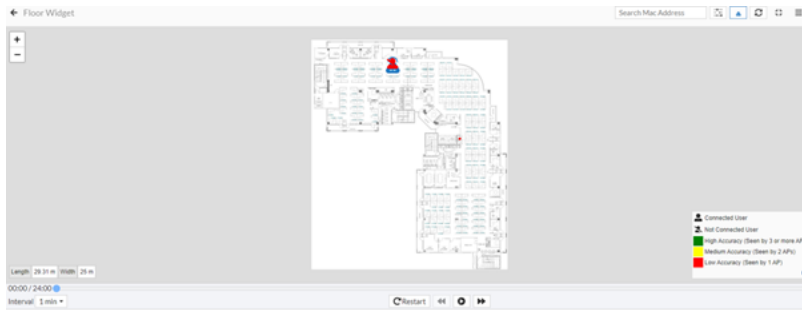
The area analytics are displayed in the **Area Movement** widget for different areas that the selected site is divided into. You can track inward and outward visitor movements between areas. The table lists the number of visitors moving between these areas.



Note: The **Area Movement** widget in the dashboard will not have any historical data, that is, data prior to upgrading to the current release. The maximum data this widget displays is that of 1 year.

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.



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.

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. The related locations and movement is marked on the map.

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

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 22](#).

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

Site Report

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

Date ▾	Site Name ▾	Busy Hour ▾	No. of Visitors ▾	Connected Visitors ▾	Dwell Time ▾	Bounce Rate ▾
2023/08/01 05:30:00		23:00	183	0	05:01:39	1%
2023/08/02 05:30:00		13:00	281	0	13:51:35	2%
2023/08/03 05:30:00		12:00	268	0	14:05:15	1%
2023/08/04 05:30:00		12:00	189	1	11:55:50	0%

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

Visitor Reports

The Visitor Reports provides details of the following visitor analytics associated with each visitor user key.

Date ▾	User Key (Mac) ▾	Connected Status ▾	Age ▾	Device Type ▾	Wifi Usage Time ▾	Email
2023-11-26		Connected	Unknown			
2023-11-26		Connected	Unknown			
2023-11-26		Connected	Unknown			
2023-11-26		Connected	Unknown			

Field	Description
Date	Displays each day within the selected time range.
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.
Connected Status	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.
Upload and Download	Displays the total bandwidth consumption by the specific visitor within the time range selected. The total upload and download size is displayed.

Field	Description
WiFi Usage Time	Displays the total wifi usage time by the specific visitor within the time range selected.
Age and Gender	Displays the age and gender of each visitor.
Email/Phone Number	Displays the email address/phone number of the visitor.
Auth Type	Displays the authentication method used by the visitor to login into the captive portal.
First Seen/Last Seen	Displays the time stamp of when the visitor logged in first and last.
Site Name	Displays the name of the site the associated with the visitor.

Schedule Configuration

You can schedule auto-generation of reports and logs for ease-of-use instead of downloading them manually.

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

Click **Schedule Report** and enter a unique **Report Name** to configure and save the report delivery schedule.

Schedule Report
✕

Report Type
Site Report ▾

Report Name
Site-Report

Add Users
User Email
+

Select Sites
site
+

Report Format
PDF ▾

Select Timezone
Asia/Calcutta ▾

Daily ✓ ▾

Time 11:00 ⌚

Weekly >

Monthly >

- **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.
- **Report Type** - Select the type of report to generate.
- **Report Format** - Select the report generation format, *PDF* or *CSV*.
- **Schedule Timezone** - Select the time zone and select the time interval to generate the report, **Daily**, **Weekly**, or **Monthly**.

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

	Reports Type ↕	Report Name ↕	Users	Format ↕	Created On ↕	Scheduled Date/Time
<input checked="" type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/04 15:46:54	Daily at 15:48
<input type="checkbox"/>	Visitor	Weekly Visitor Report CSV 15:50	@fortinet.com	pdf	2023/07/04 15:48:22	Weekly on Tuesday at 15:50
<input type="checkbox"/>	Site	Montly Site Report CSV 16:00	@fortinet.com	csv	2023/07/04 15:50:03	4 of every Month at 16:00

Download Reports

This page displays all the generated reports, you can download only one report at a time. Select the report and click **Download Report**.

	Reports Type ↕	Reports Name ↕	Users	Format ↕	Generation Date/Time ↕
<input type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/20 15:54:05
<input type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/21 16:04:29
<input checked="" type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/22 17:27:19
<input type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/22 17:44:56
<input type="checkbox"/>	Site	Site Report Daily PDF 15:48	@fortinet.com	pdf	2023/07/22 17:51:02

Captive 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 41](#).

- [Creating a Captive Portal on page 24](#)
- [Configuring Captive Portal Rules and Users on page 27](#)
- [Attaching RADIUS Clients on page 28](#)
- [Configuring Authentication Provider on page 28](#)
- [Configuring RADIUS Clients](#)

Creating a Captive 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 Captive Portal on page 25](#)
- [Uploading a New Captive Portal on page 27](#)

Navigate to **Captive Portal > My Portals** and perform any of the following operations.

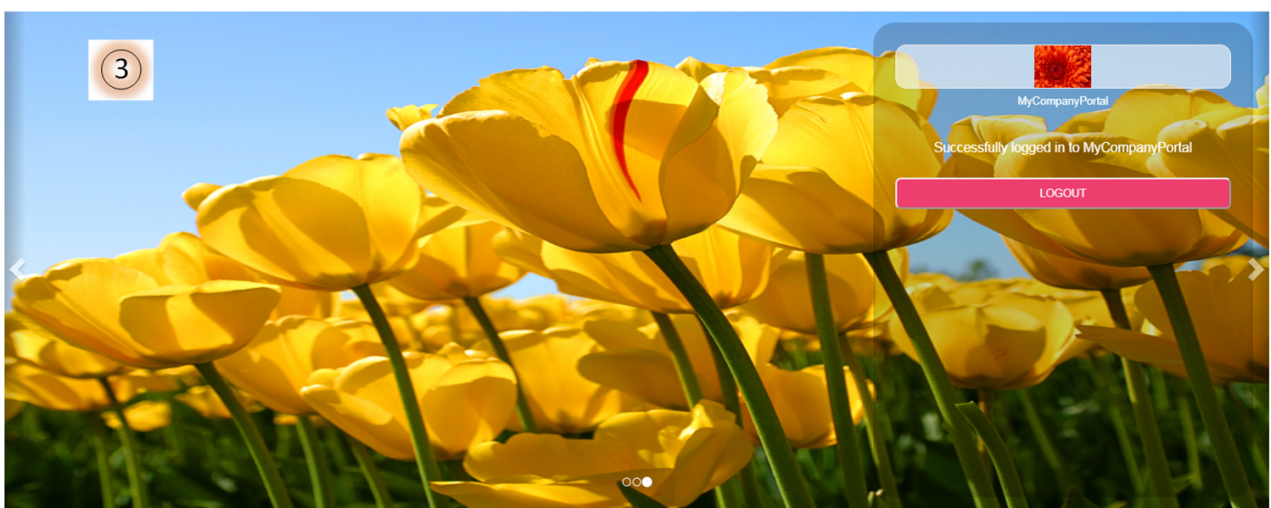
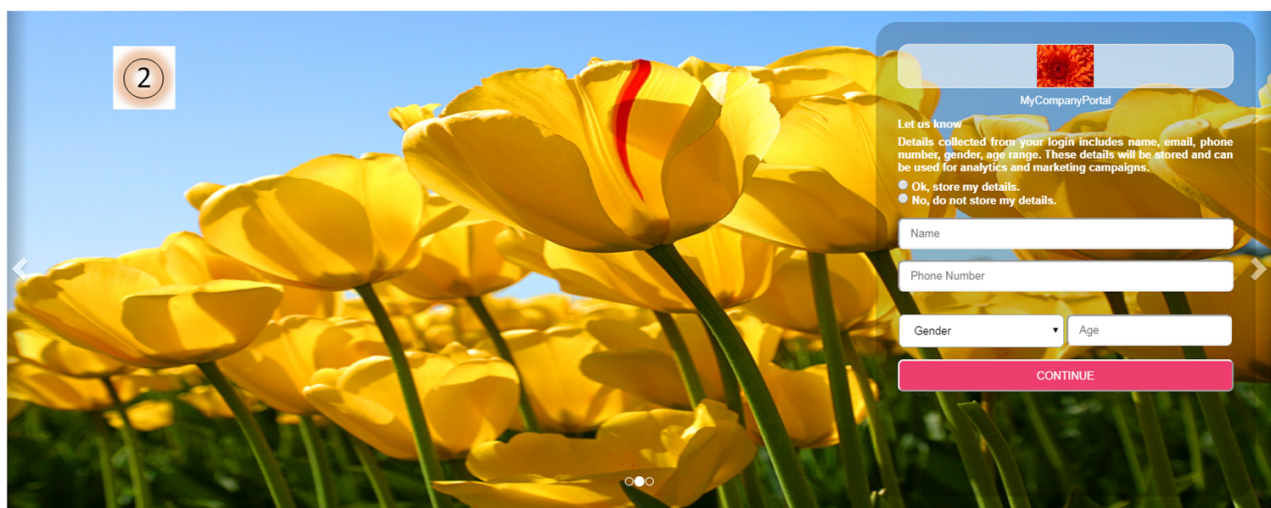
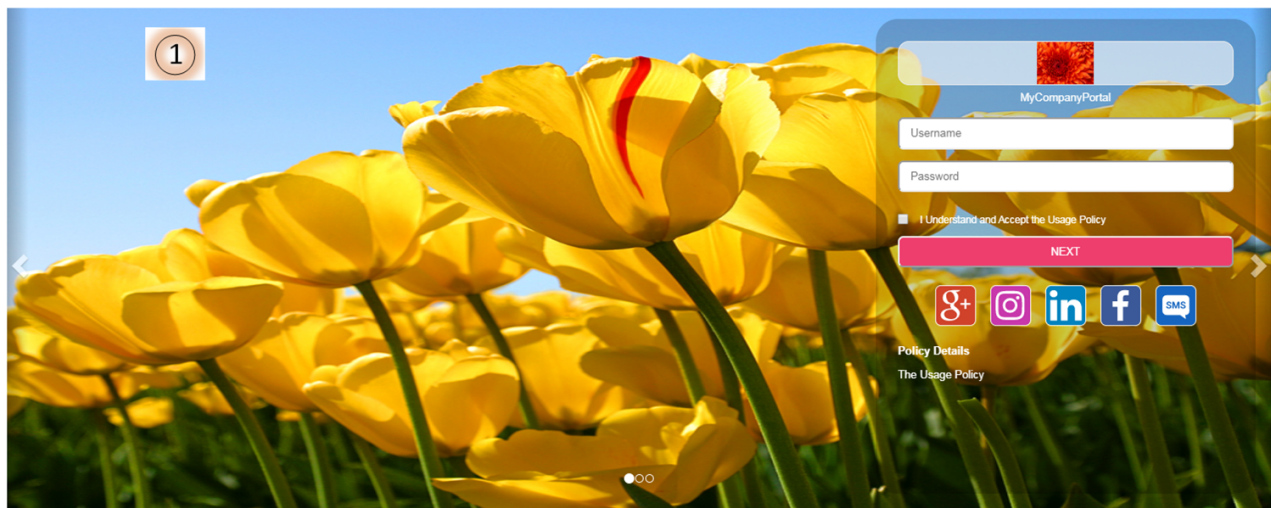
My Portals	
Here you can create, edit and delete your captive portals with ease.	
<div> + Create portal Upload new Portal Preview Edit by Upload Edit Delete <input type="text" value="Search"/> </div>	
Portal Name	Associated Sites
<input type="checkbox"/> Testing	3 sites
<input type="checkbox"/> FGT_Portal	5 sites
<input type="checkbox"/> 999 Portal1	0 sites

- **Add Portal** - To add a new captive portal. See [Adding a New Captive Portal on page 25](#)
- **Upload New Portal** - To upload a new customized captive portal. See [Uploading a New Captive Portal on page 27](#).
- **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 Captive Portal on page 27](#)
- **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 Captive Portal

Perform the steps in this procedure to add a portal.

1. Navigate to **Captive Portal > My Portals** and select the site for which the portal is to be created. Click **Create Portal**.
2. Enter a unique **Portal Name** for your site and select a **Layout** and **Theme Color** from the pallet for the portal authentication page. Click **Next**.
3. Upload your **Logo** and a **Mobile Background** or a **Desktop Background**. 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 **Policy Statement** to prompt users to accept the policy prior to logging in.
5. Select the supported/permmissible authentication methods.
Email Password – 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.
One Tap 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 Portuguese. Click **Next**.
7. Enable **Email** to collect email information during visitor authentication through Captive Portal; enable **Verify Email** to verify the collected email information. In case of **One Tap Login**, you can optionally select additional user data collection such as, phone number, gender, and age.
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 Captive 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 Captive Portal on page 25](#).
- Download an existing portal for customization. Click **Edit** on the **My Portals** page and navigate to step 5. 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 **My Portals** page and add the *<Portal Name>.zip*.
- To upload an existing customized portal, click **Edit by Upload** on the **My Portals** page and add the *<Portal Name>.zip*.

Configuring Captive Portal Rules and Users

Navigate to **Captive Portal > Site-Portal Config** 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.

The screenshot displays the 'Site-Portal Config' interface for the 'California' site. At the top, there is a 'Choose site' dropdown menu set to 'California' with an orange plus icon. Below this are four tabs: 'Assign portal' (active), 'Portal Rules', 'Site Users', and 'RADIUS config'. The main content area is divided into two sections: 'Available portals' and 'Attached portals'. In the 'Available portals' section, there are three portal cards: 'Testing', 'FGT_Portal', and '999 Portal1'. Each card has a 'Preview' button with an eye icon and an 'Attach' button. In the 'Attached portals' section, there are three portal cards: 'Testing', 'Asha_CP', and 'portal1reg'. Each card has a 'Preview' button with an eye icon and a 'Detach' button. A 'Show less' link is located at the top right of the 'Available portals' section.

Navigate to **Portal Rules** to configure portal rules for the portal. 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.

Create new rule

Rule Name

Rule Description

Rule Conditions

Configure rules for what happens if the conditions you specify are met.

Conditions

SSID

Contains

Forti

×

AND

Rules conditions*

Rules Operators*

Select a value

×

+

Perform action

Go to Portal

Portal123

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

Create new user

User name

Password

👁

Confirm password

👁

Attaching RADIUS Clients

Navigate to **Captive Portal > Site-Portal Config > RADIUS Config** to attach the configured RADIUS clients (**Captive Portal > Site-Portal Config > 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 41](#).

Choose site		Demo Site 1			
Assign portal	Portal Rules	Site Users	RADIUS config		
Server Name	Server IP	Password	Captive portal URL		Action
WLC	192.168.1.1	*****	https://connect.presence.fortinet.com/portal/192.168.1.1:8080/fortinet.com		Detach
RobotRadius	192.168.1.1	*****	https://connect.presence.fortinet.com/portal/192.168.1.1:8080/fortinet.com/		Detach

Configuring Authentication 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. Navigate to **Captive Portal > Auth Provider Config**.

Add Authentication Provider

Provider	Google ▼
Name	Google-auth
Client ID	1003054041393-
Secret Key	60QrC41xbk

Configuring RADIUS Clients

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 Captive Portal on page 24](#).

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).

Follow this procedure to create RADIUS clients on FortiPresence.

1. On the FortiPresence GUI navigate to **Captive Portal > 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**.

Add RADIUS Client

Device Type	FortiWLC ▼
RADIUS Client Name	WLC
RADIUS Secret Key	●●●●●●●●
RADIUS Client IP	10.1.1.1

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 – 173.243.132.75, 173.243.132.76, 173.243.132.77, or 173.243.132.78

FortiLAN Cloud Europe – 154.52.2.173, 154.52.2.174, or 154.52.2.175

FortiLAN Cloud Japan – 154.52.29.78

FortiLAN Cloud US – 38.21.192.17

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

3. Navigate to **Site-Portal Config** and select the site to attach the configured RADIUS client.
4. Select **Radius config** and click **Attach** against the RADIUS client created for FortiLAN Cloud. The captive portal URL is generated.

Note: Any updates to an existing RADIUS secret key take effect in an hour (approximately).

Site Management

You can create and manage sites for presence analytics by locating sites on Google maps integrated GUI. Once created, the site can be managed by adding buildings, floors, and demarcating floors into areas.

- [Sites](#)
- [Resources](#)
- [Settings](#)

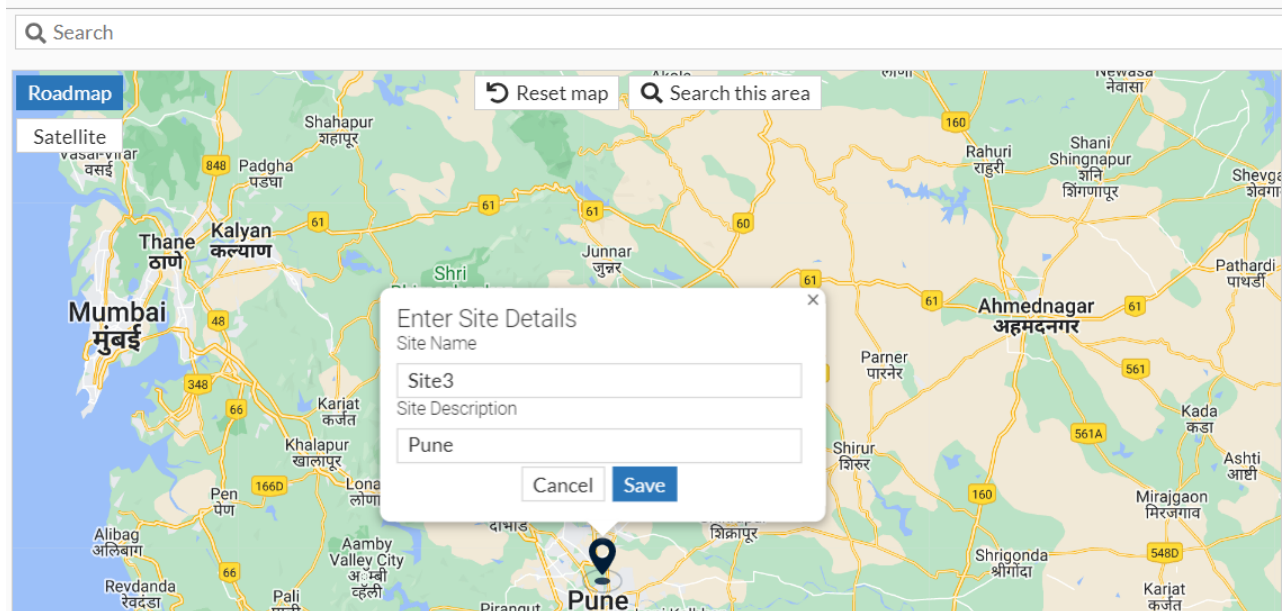
Sites


You can upload floor maps and place access points and hardware assets on the maps.

1. Navigate to **Site Management > Sites** and search for the geographic location of the site on the Google map and select it.
2. Click **Add Site** and enter the **Site Name** and **Site Description**. The new site is listed on the right side of the page.

Sites Map

All Sites



3. To add buildings in a site, click the  (**Details**) icon against a particular site, and click **Add Building**.
4. Enter a unique **Name** for the building and site. Click **Ok**.

Enter Building Details
✕

Building Name




Building 1

The created building is displayed.

Buildings in Site3

All Sites / Site3


Add Building

	Building 1	0 Floors	 
---	------------	----------	---

5. Click on building name and then click **Add Floor** to upload the floor map for the building.
6. Enter the floor details and browse to the map. Click **Add Floor**.
The floor map is displayed.
7. 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**.

Site Management

Drag two red pointer on floor map and position them across a known distance and enter the distance below. Based on this known distance, Floor Width and Height will be calculated automatically.

Selected Distance Unit Floor Width & Height X 

8. 7. Click on the floor name and then **Draw Area** to mark the area on the floor map by drawing a polygon anti-clockwise. Click **Finish**.
9. Enter unique area **Name** and **Description**.
You can create multiple areas on a floor as per your requirement.
10. 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.

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.

Notes:

- All access points are listed here only when the location services is configured. See [Configuring Location Services on page 38](#).
- You can view the access points in **Administration > AP Management**.

Resources

This section describes configuring additional FortiPresence resources such as, fixed assets and employees. Navigate to **Site Management > Resources**.

- [Fixed Assets](#)
- [Fixed Employees](#)

Fixed Assets

The fixed assets added to this list are excluded from locationing services and analytics. 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.

Select **Manual Added Assets** to view the fixed assets uploaded manually and select **Auto-Detected Assets** to view the fixed assets determined by the thresholds configured in **Detect Fixed Assets** in the [Settings](#) tab.

Site Resources

Fixed Assets

Fixed Employees

3P68+J7X / Site123 / flr1

+ Create

Upload List

Edit

Delete

Show Only

Manual Added Assets

Auto-detected Assets

	Asset Name	MAC address	X-Axis	Y-Axis
<input type="checkbox"/>	Printer-1	00:00:00	-1	-1

Fixed Employees

Select the site and manually add the MAC address or upload the file in the format similar to the sample file available for download. Once the MAC addresses are added, go to the **Employees Filter** in the [Settings](#) tab and select the filter (enabled by default).

Fixed Assets

Fixed Employees

California

+ Create

Upload List

Edit

Delete

	Employee Name	Employee Device MAC address	Description
<div><div></div><div></div></div>	Employee1	00:1B:44: [REDACTED]	

Settings

This section describes some additional FortiPresence settings. Navigate to **Site Management > Settings** and select the site. After configuring the settings, click **Apply Changes**.

- [Bounce Time Limit](#)
- [Dwell Inactive Time Limit](#)
- [Min Count of Observations](#)
- [Employees Filter](#)
- [Non \(OUI\) MAC address](#)
- [Detect Fixed Assets](#)

Settings

Choose site

site

Apply Changes

Bounce Time Limit

0 Hours: 5 Minutes

This setting helps in collecting Bounce Rate Analytics. A visitor has to be seen more than **Bounce Time Limit**, for him to be considered as an **Stayed or Engaged Visitor**. Otherwise he will be considered as a **Bounced Visitor**.

Dwell Inactive Time Limit

1 Hours: 0 Minutes

This setting helping in collecting dwell time analytics. If a visitor is seen after a gap of **Dwell Inactive Time Limit**, it is considered as a new dwelling session (Dwell time calculation). If the visitor is seen within this time limit the dwell session continues.

Min Count of Observations

1 Observations

This setting helps in reducing random MAC addresses. Based on this setting visitor is reported only if he is seen more than or equal to Min Count of Observations. This setting is applicable for **all the dashboards**

Available in only for FortiPresence - Paid Site

Employees Filter

Enabled

This filter allows for excluding analytics for the devices belonging to employees. To configure employee devices site wise, navigate to [Site Settings --> Employees](#)

Non OUI MAC address

Disabled

This filter allows for excluding analytics for the devices belonging to organization. This setting is applicable for all the dashboards. To configure organization devices site wise, navigate to [Site Settings --> Fixed assets](#)

Detect Fixed Assets

Enabled

HH Hours : DD Days

Device MAC address detected for more then the configured number of hours per day for the configured number of (consecutive) days will be declared a fixed asset.

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.

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.

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.

The following settings are available only for **paid site** users.

Employees Filter

This setting is enabled by default and filters out the employee MAC addresses added in the Employees tab from site level analytics.

Non (OUI) MAC address

When enabled, this setting filters out the non Organizational Unique Identifier (OUI) MAC Addresses and is applicable for all the dashboards.

Detect Fixed Assets

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

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.

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 Assets** in [Resources on page 31](#).

Administering FortiPresence

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

- [AP Management](#)
- [License Details](#)
- [Email Notifications](#)

AP Management

This page displays the AP details. 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.

Access Points Management						
Access Points		License Details				
Delete		Search				
Status	Name	Mac Address	Serial No	Timestamp	Site	F
Inactive	4KS4OPZ			2023/01/17 22:08:50	5th Main Rd	8.
Inactive	83x_3F_FortiPresence			2023/02/15 13:09:34	Corp-Bengaluru	FI

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.

You can filter data on this page using the filter options of the displayed columns. For example, data is filtered and displayed only for APs *AP113* and *AP114*.

Access Points

License Details

Delete

Search

	Status	Name
<input type="checkbox"/>	Inactive	AP113
<input type="checkbox"/>	Inactive	AP114

Resize to Contents

Filter

Contains

Exact Match

NOT

AP113, AP114,

Suggestions

AP113

AP114

Access Points License Details									
<div> <div>Delete</div> <div>Name = ap113, ap114 X Search</div> </div>									
	Status	Name	Mac Address	Serial No	Timestamp	Site	Firmware Version	Expiry	AP Radio
<input checked="" type="checkbox"/>	Inactive	AP113			2023/06/21 13:58:03	Udupi	8.3-3dev-25	1970/01/01 05:30:00	AP Radio 1 AP Radio 2 AP Radio 3
<input type="checkbox"/>	Inactive	AP114			2023/06/21 13:58:03	Udupi	8.3-3dev-25	1970/01/01 05:30:00	AP Radio 1 AP Radio 2 AP Radio 3
<input type="checkbox"/>	Inactive	AP114			2023/06/21 13:58:03	Udupi	8.3-3dev-25	1970/01/01 05:30:00	AP Radio 1 AP Radio 2 AP Radio 3
<input type="checkbox"/>	Inactive	AP113			2023/06/21 13:58:03	Udupi	8.3-3dev-25	1970/01/01 05:30:00	AP Radio 1 AP Radio 2 AP Radio 3

License Details

With the completion of FortiPresence registration process, project name and project secret key are generated and are available at **Administration > AP Management > License Details**. A 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. 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 38](#).

Access Points Management

Access Points	License Details
Project ID	<div></div>
Project Secret Key	<div></div>
Port	4013
Location Server FQDN	<div></div> .com
Sync Licensed APs	<p>This syncs the FortiPresence licensing information from FortiCare for all the APs listed in discovered APs. For APs whose license has expired and has subsequently been renewed in FortiCare, the user needs to sync for the change to reflect in FortiPresence.</p> <div>Sync Licensed APs</div>

Email Notifications

You can enable notifications on your registered email address for the following events.

- **AP Down** - An email alert is sent when the AP experiences an outage and when it is available again.
- **AP License Expiry** - You receive email reminders on license renewals as the expiry date draws near.
- **Account Pause** - You receive a email alert if there is no activity/logins in your account for 23 days or more.

Email Notifications

In this section, you can set your email notification preferences.

AP Down

☒ Enabled

An email notification will be sent when the access point experiences an outage.

AP License Expiry

☒ Enabled

An email notification will be sent when the AP license is about to expire.

Account Pause

☒ Enabled

An email notification will be sent when your account is not used for 23 days and more.

Configuring Location Services

With the completion of FortiPresence registration process, project name and project secret key are generated and are available at **Administration > AP Management**. 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 38](#)
- [FortiGate on page 39](#)
- [FortiWLC on page 39](#)

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 **Configuration > Connectivity Profiles > 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 - **Administration > AP Management**).

FortiPresence ⓘ

Mode	Foreign and Home Channels ▼
* Background or foreground (dedicated) scanning radio should be enabled.	
Server Address (IPv4/FQDN)	34.245.252.61
UDP Listening Port	4013 0 to 65535
Project Name	2ce0655f64d847ff
Primary server secret	***** Show Password
Report Transmit Frequency	5 5 to 65535 sec
Reporting of Rogue APs	<input checked="" type="checkbox"/> Enable
Reporting of Unassociated Stations	<input checked="" type="checkbox"/> Enable

In the FortiPresence GUI, **Administration > AP Management**, 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 - **Administration > AP Management**).
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 - **Administration > AP Management**).

The screenshot shows the FortiGate GUI configuration page for FortiAP Profiles. The left sidebar contains a menu with options: Managed FortiAPs, SSID, FortiAP Profiles (selected), WIDS Profiles, Log & Report, and Monitor. The main content area displays the configuration for a selected FortiAP profile. The 'FortiPresence' section is highlighted with a red box, containing the following fields:

- Project name: 17c7cc003edb40ec
- Password: [masked with dots]
- FortiPresence server IP: 34.245.252.61
- FortiPresence server port: 4013

Below these fields are several checkboxes and a text input:

- Report rogue APs: [unchecked]
- Report unassociated clients: [checked]
- Report transmit frequency (in seconds): 30
- Ekahau blink: [unchecked]
- AeroScout: [unchecked]
- Locate WiFi clients when not connected: [unchecked]

At the bottom right, there are 'OK' and 'Cancel' buttons.

In the FortiPresence GUI, **Administration > AP Management**, 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 - **Administration > AP Management**).

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 - **Administration > AP Management**).

Location Services Feed	<input type="button" value="Enable"/>
Report Format	<input type="button" value="Forti-Presence"/>
Project Name	<input type="text" value="17c7cc003edb40ec"/> Enter 1-16 chars.
Secret	<input type="password" value="*****"/>
Source Type	<input type="button" value="All"/>
Server IP Address/hostname	<input type="text" value="34.245.252.61"/> Enter IPv4 or IPv6 Address or FQDN Name.
Server Port	<input type="text" value="4013"/> Valid range: [300-65535]
Report Interval (in Seconds)	<input type="text" value="5"/> Valid range: [3-3600]
Apply to ALL APs	<input type="button" value="No"/>
AP Groups	<input type="button" value="Select Here"/>
Access Points	<input type="button" value="Select Here"/>

In the FortiPresence GUI, **Administration > AP Management**, 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 – **Captive Portal > 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.

- [FortiLAN Cloud on page 41](#)
- [FortiGate on page 43](#)
- [FortiWLC on page 47](#)

FortiLAN Cloud

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

1. Select a configured AP Network and navigate to **Configuration > User Access Control > 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 (**Captive Portal > 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 *

NAS IP

Primary Server Name/IP *

Primary Server Secret * [Show](#)

Secondary Server Name/IP

Secondary Server Secret [Show](#)

Server Port *

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 – **Captive Portal Site-Portal Config > RADIUS config**).
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 Captive Portal on page 25](#).
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 *	<input type="text" value="FortiPresence"/>	
Enabled	<input checked="" type="checkbox"/>	Broadcast SSID <input checked="" type="checkbox"/>
MAC Access Control	<input type="checkbox"/>	
Mesh Link	<input type="checkbox"/>	
Authentication	<input type="text" value="Open"/>	
Captive Portal	<input type="text" value="My Captive Portal"/>	
Captive Portal URL	<input type="text" value="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	<input type="text" value="www.google.co.in, www.facebook.com, www.gmail.com"/>	
	<small>* IP address, domain name and sub-network address/mask are allowed. * To enter more than one value, separate the values with a comma.</small>	
Sign on Method	<input type="text" value="My RADIUS Server"/>	<input type="text" value="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	<input type="text" value="<Disable>"/>	
VLAN ID	<input type="text" value="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 (**Captive Portal > 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 (Administration > AP Management)>
```
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 – **Captive Portal > Site-Portal Config > RADIUS config**) 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 Captive Portal on page 25](#)
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)                                                                                   |
| Outgoing Interface | port1                                                                                                   |
| Source             | all                                                                                                     |
| Destination        | FortiPresence_Connect<br>FB OAUTH GROUP<br>GOOGLE OAUTH GROUP                                           |
| Schedule           | always                                                                                                  |
| Service            | ALL                                                                                                     |
| 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.

- 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 (**Captive Portal > 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] |

- 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"/> | fbcnd.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**

- Create a **Captive Portal** profile. Click **Add** and in **User Authentication** enter the RADIUS profiles created for authentication and accounting.
- 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 – **Captive Portal > Site-Portal Config > RADIUS Config**). 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**.

