FortiPresence VM - Administration Guide

Version 1.1.0

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

August 20, 2021
FortiPresence VM 1.1.0 Administration Guide

TABLE OF CONTENTS

Change log

Date	Change description
2021-07-14	FortiPresence VM 1.1.0 document release version.
2021-07-26	Updated section Upgrading FortiPresence VM on page 18.
2021-08-20	Updated section Upgrading FortiPresence VM on page 18.

Introduction

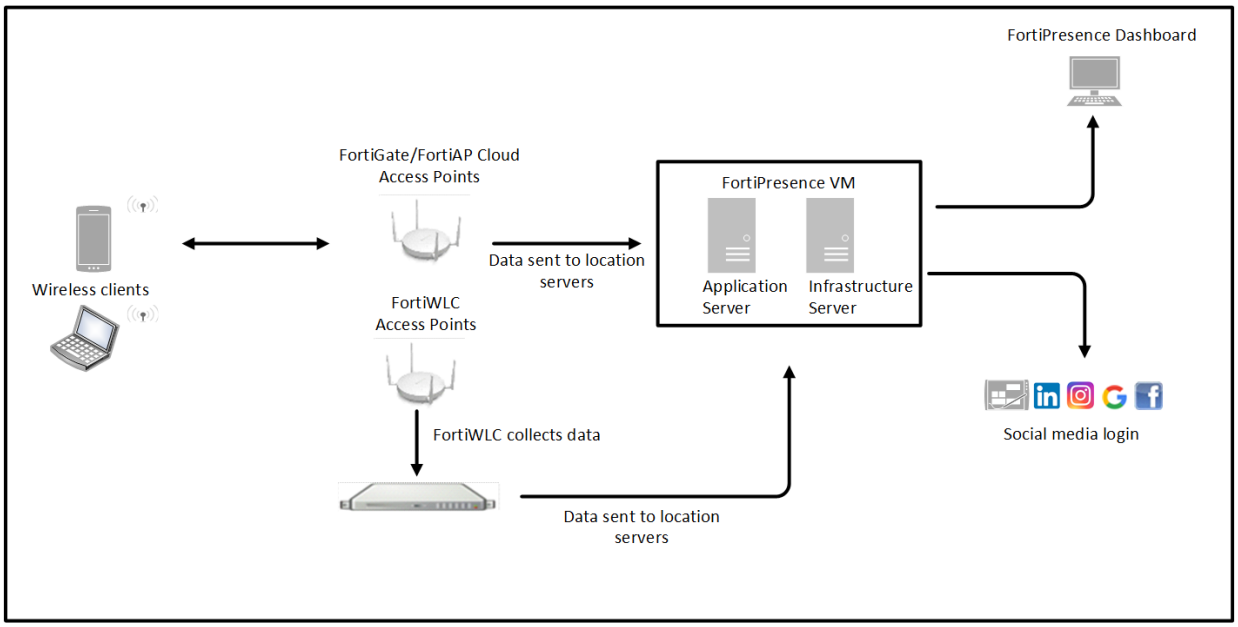
FortiPresence VM is a comprehensive data analytics solution designed for analyzing user traffic and deriving usage patterns. By capturing analytics of consumer traffic patterns, businesses can learn more about their customers. FortiPresence VM combines WiFi and analytics to deliver end-to-end solution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

FortiPresence VM is deployed locally on your site and consists of two virtual machines. All the analytics data collected and computed resides locally on the VMs.

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 VM 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 by the VMs and presented on the customizable dashboards on the FortiPresence VM GUI.

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

- **Infrastructure Server** — This server hosts all the infrastructure related services for SQL, NoSQL databases, Message Broker and a Local Simple Storage Service.
- **Applications Server** — This server hosts all the FortiPresence VM application related services like GUI and locationing services.
- **Access Point Support** — The FortiPresence VM solution supports all Fortinet wireless access points. FortiGate, FortiAPCloud wireless access points (send visitor data in the form of station reports directly to FortiPresence VM), and FortiWLC wireless access points (send visitor data in the form of station reports to the FortiWLC controller which redirects data to FortiPresence VM).
- **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, SMS-OTP authentication, or a customized visitor portal.



This is an example of FortiPresence VM 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 VM analytics engine receives data via a secure SSL connection and processes it.

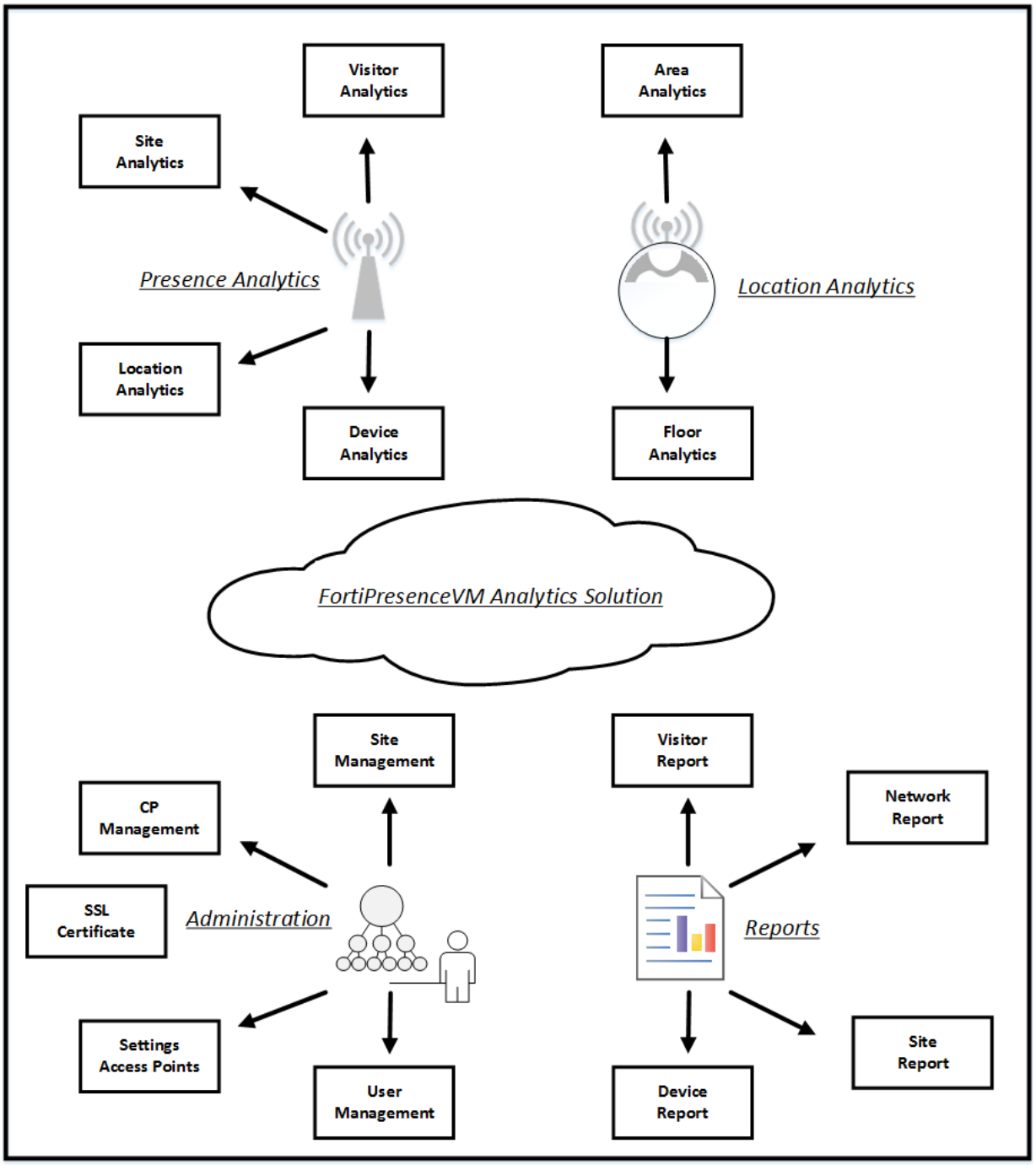
FortiPresence is **General Data Protection Regulation (GDPR)** compliant.

- 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 the WiFi network, 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.

User Interface Overview

The FortiPresence VM 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.

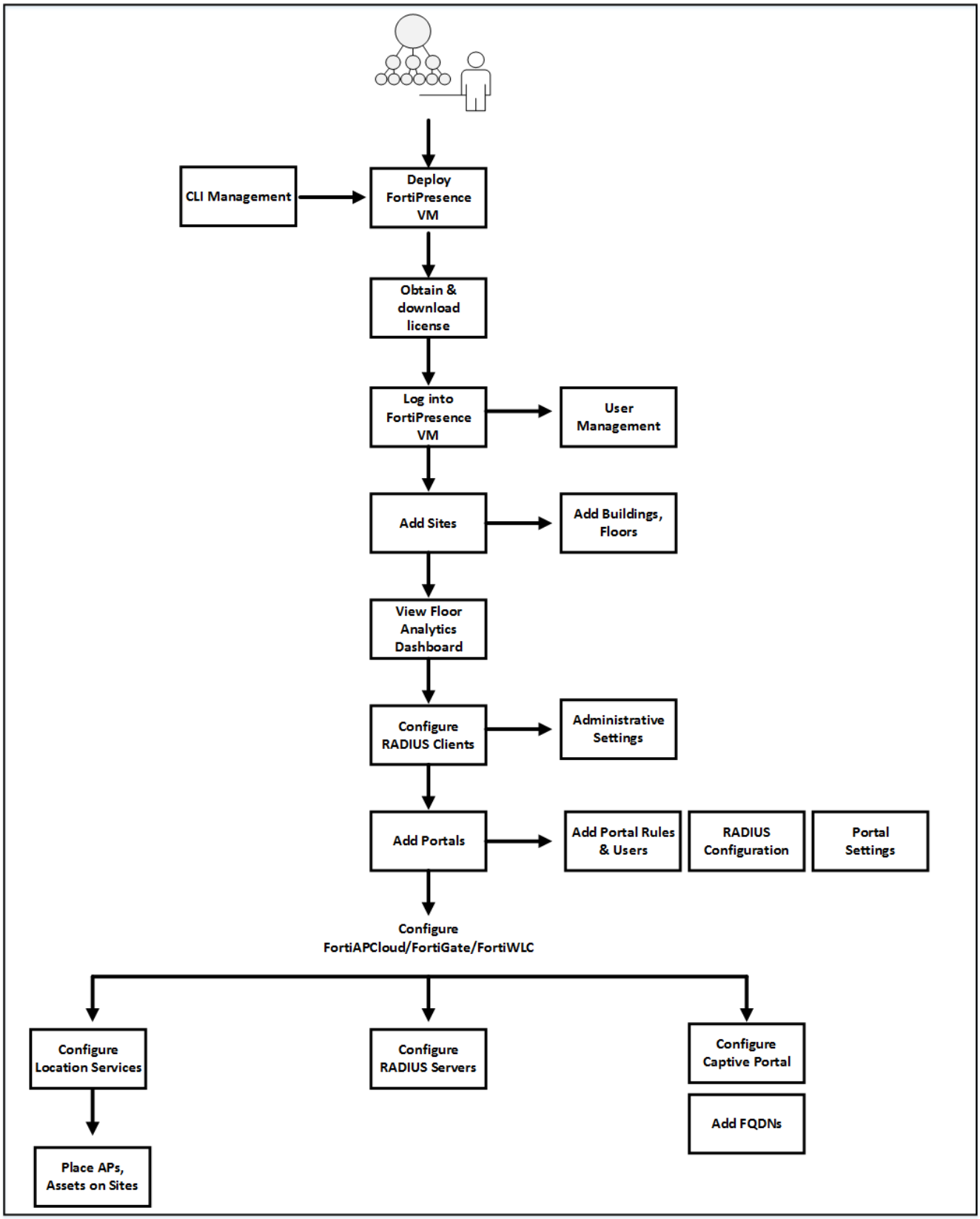
The components of the GUI are explained in the subsequent chapters of this document.


Visitor Analytics
Area Analytics
Site Analytics
Presence Analytics
Location Analytics
Location Analytics
Device Analytics
Floor Analytics
FortiPresenceVM Analytics Solution
Site Management
Visitor Report
CP Management
Network Report
SSL Certificate
Administration
Reports
Settings Access Points
Site Report
User Management
Device Report

How FortiPresence VM Works

This section outlines the configurations and management operations on FortiPresence VM, FortiAPCloud, 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 FortiAPCloud, see the respective *product documentation.*


CLI Management
Deploy FortiPresence VM
Obtain & download license
Log into FortiPresence VM
User Management
Add Sites
Add Buildings, Floors
View Floor Analytics Dashboard
Configure RADIUS Clients
Administrative Settings
Add Portals
Add Portal Rules & Users
RADIUS Configuration
Portal Settings
Configure FortiAPCloud/FortiGate/FortiWLC
Configure Location Services
Place APs, Assets on Sites
Configure RADIUS Servers
Configure Captive Portal
Add FQDNs

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 800000 devices	NA
Presence Dashboard	Up to 800000 devices	Up to 800000 devices
Device Report	Up to 500000 devices	Up to 500000 devices
Site Report	Up to 500000 devices	Up to 500000 devices
Visitor Report	Up to 7500 devices (tested)	Up to 7500 devices (tested)
Network Report	Up to 7500 devices (tested)	Up to 7500 devices (tested)
Multisite Report	Up to 85000 devices	Up to 85000 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

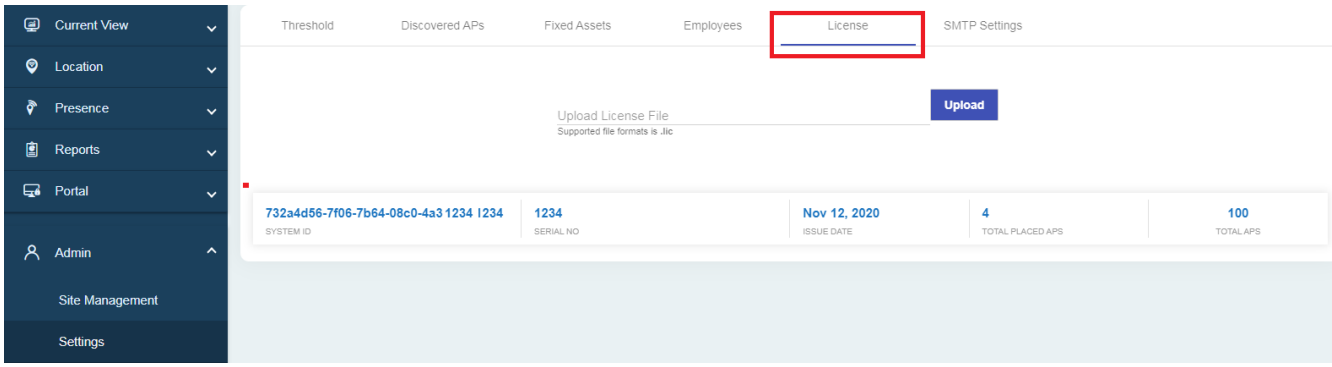
FortiPresence VM requires a perpetual license. Contact the *Fortinet Customer Support* at **support@fortinet.com** with the following detais to obtain a license.

- System ID of the Applications server. Run the **presence-apps --info** command to obtain the system ID.
- Number of APs

The generated license file is available for download on https://support.fortinet.com. Navigate to **Admin > Settings > License** in the GUI and upload the license file.

Viewing License Information

Run the **presence-apps --info** command to view the licensing information or navigate to **Admin > Settings > License** in the GUI.



Deploying FortiPresence VM

This section describes deploying FortiPresence VM. The following two servers are available in this solution. Both these servers use Docker engine services to communicate with each other.

Infrastructure server runs the following infrastructure related services.

- LocalstackS3
- MongoDB
- Redis
- PostgreSQL
- Scheduler

Applications server runs the following application related services.

- Presence
- JobWorker
- AnalyticsWorker
- LocationWorker
- RADIUS
- Connect
- LocationParser
- LocationEpoll
- RestApi

Note: The Application server is also termed as the *Apps Server* or *Apps Host* and the Infrastructure server is also termed as the *Infra Server* or *Infra Host*.

Recommended Hardware and Software

The following are the recommended for deploying FortiPresence VM.

Hardware	For 1000 MAC/sec system, the following minimum resources are required. • **RAM**: 16 GB (for both Infrastructure and Applications servers) • **Disk Space**: 500 GB (for Infrastructure server) and 100 GB (for Applications server) • **Number of Processors**: 8 (for both Infrastructure and Applications servers) For 3000 MAC/sec system, the following minimum resources are required. • **RAM**: 32 GB (for both Infrastructure and Applications servers) • **Disk Space**: 1 TB (for Infrastructure server) and 100 GB (for Applications server) • **Number of Processors**: 16 (for both Infrastructure and Applications servers)
Software	• **Operating System**: Centos Linux 7 (Core)

	• A non-root user **presence** configured on both the servers (default password: **presence**). • A **root** user configured on both the servers (default password: **root@123**).

Notes:

- Data retention is for 1 year on both 3000 MAC/sec and 1000 MAC/sec systems.
- [Test environment] On a 3000 MAC/sec system, with 30000 daily visitors for 100 days, the disk usage is 34 GB in the Infrastructure server and 10 GB in the Applications server.

Pre-requisites

This table describes the pre-requisites for installing FortiPresence VM.

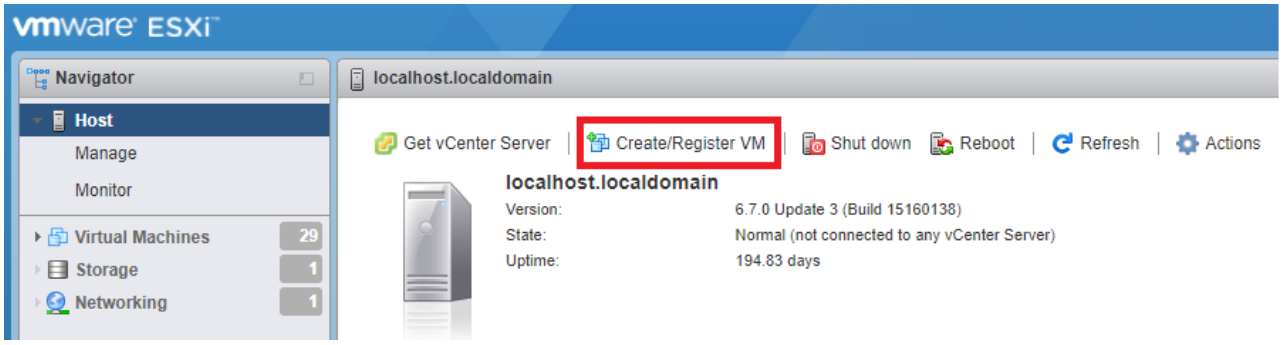
Category	Requirements
Resources	VMware ESXi 6.7.0 and above. **Notes**: • If using a version above ESXi 6.7.0, modify the required hardware (vmx) in the *.ovf* installation files for both Infrastructure and Application servers. See https://kb.vmware.com/s/article/1003746. **<vssd:VirtualSystemType>vmx-14</vssd:VirtualSystemType>** • If you are using vSphere web client (on ESXi host of version less than 6.7.0), edit the *.ovf* files of both VMs and ensure all lines containing **nvram** are removed. See https://kb.vmware.com/s/article/67724. **Example** Remove the following lines from the Application server *.ovf*. **<File ovf:href="presence-apps.nvram" ovf:id="file2" ovf:size="0"/> <vmw:ExtraConfig ovf:required="false" vmw:key="nvram" vmw:value="ovf:/file/file2"/>** Remove the following lines from the Infrastructure server *.ovf*. **<File ovf:href="presence-infra.nvram" ovf:id="file2" ovf:size="0"/> <vmw:ExtraConfig ovf:required="false" vmw:key="nvram" vmw:value="ovf:/file/file2"/**
Network	It is recommended to install both the Infrastructure and Applications servers on the same ESXi host as they need to communicate with each other. **Note**: If the IP addressing mode is changed from **DHCP** to **static**, by default, IPv4 forwarding gets disabled. Enable IPv4 forwarding before starting the installation process. See IPv4 Forwarding on page 21. The Applications server must have internet connectivity for social media and SMS authentications for captive portal.
FQDNs	An FQDN is required for GUI access and additionally by FortiPresence Connect to facilitate captive portal social authentication. Navigate to **Admin > SSL Certificate** to generate a CSR and the certificate should be signed by a CA. The FQDNs can be configured on the Application server during initial setup or later using the `presence-apps --basics` command.

Category	Requirements
	Note: Use port 8443 to access the FortiPresence VM GUI.

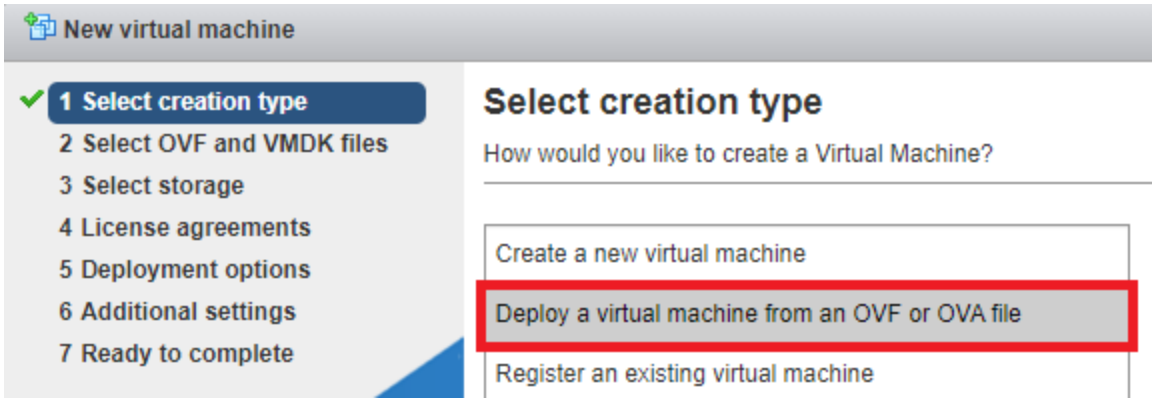
Installing FortiPresence VM

Follow this procedure to create the Infrastructure and Application servers for the FortiPresence VM setup.

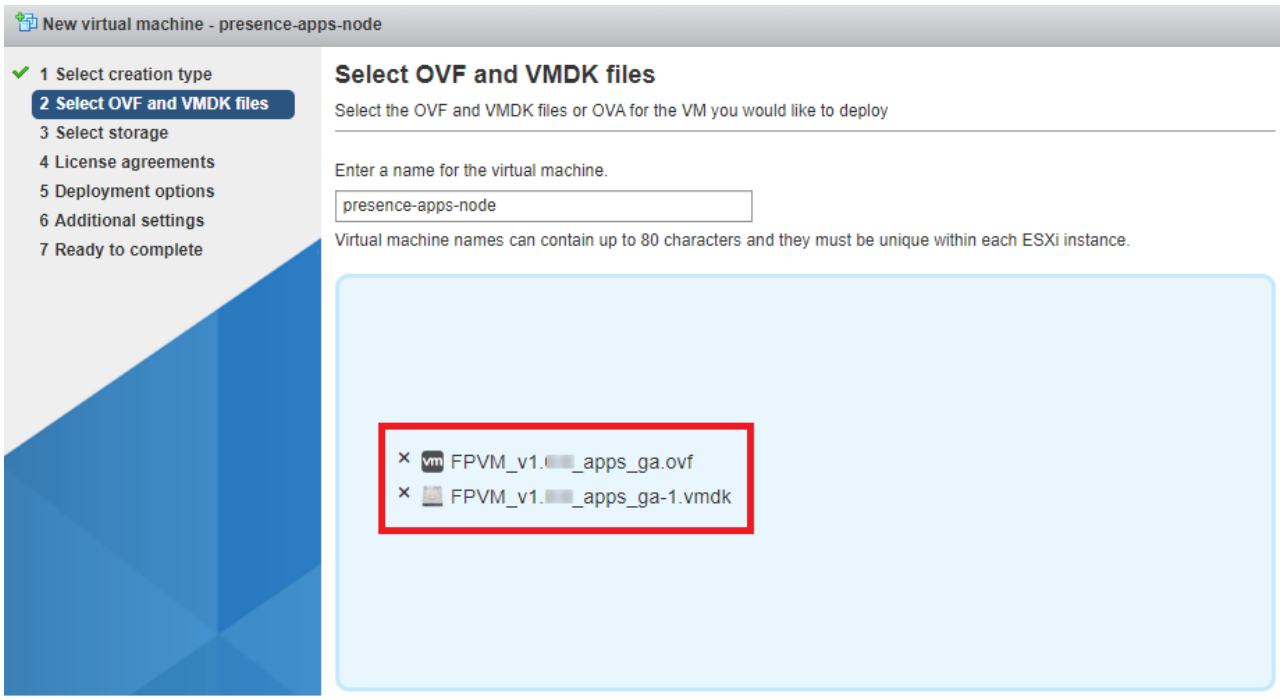
1. Download the installation files from the *Fortinet Support* portal.
2. Log in into VMWare ESXi.
3. Select **Create/Register VM** in the **Host** tab.



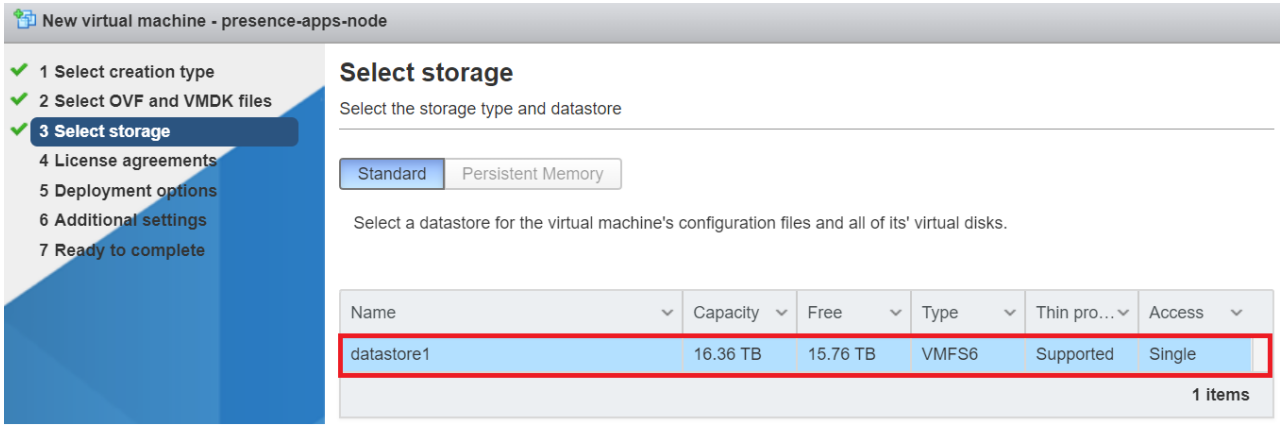
4. Select **Deploy a virtual machine from an OVF or OVA file** as the creation type.



5. Browse and select the downloaded *.ovf* and *.vmdk* files and enter a suitable hostname.



6. Select the appropriate storage and deployment options.



7. Click **Finish**.

Repeat this procedure for creating both the servers.

Configuring FortiPresence VM

Perform the following steps to access and configure the VMs after successful installation.

Note: If the hardware recommended for 3000 MACs/sec scaling is deployed, the `presence-apps` command displays an additional option to select the scale configuration between 1000 MACs/sec (default) and 3000 MACs/sec.

1. Log in into the newly created VMs as **root** user with the username **root** and password **root@123**. Modify the password after the first login.
   Note: **root** credentials must be used by an administrator only. **Login with appropriate user permissions to**

ensure that the installation is successful.

2. Ensure that the IP addresses of both the VMs are configured appropriately. Run the `ifconfig` command, the IP address is displayed after **inet** in the section beginning with **ens192:**.
3. Ensure that the date and time are updated correctly. Run the following commands to manage the time-zone settings.
   - `timedatectl`: To view the system's current time-zone.
   - `timedatectl list-timezones`: To list the available time-zones.
   - `timedatectl set-timezone <time_zone>`: To set to a new time-zone. For example, `timedatectl set-timezone America/Toronto`.
4. Run the `source ~/.bash_profile` command on both the VMs prior to using the CLI mode.
5. Logout as the **root** user and login as **presence** user with the username and password **presence**.
   Note: This ensures appropriate permissions to files and folders and system upgrades. **Login with appropriate user permissions to ensure that the installation is successful**.
6. Extract the appropriate CLI script from the tar on both the servers.
   Infrastructure server: `tar -xzf FPVM-cli-vx.y.z-buildxxxx.tar presence-infra`
   Application server: `tar -xzf FPVM-cli-vx.y.z-buildxxxx.tar presence-apps`
7. Run the `presence-infra --init` command in the */presence/ directory* on the Infrastructure server to initialize the infrastructure services and follow the instructions.
8. Run the `presence-apps --init` command in the */presence/* directory on the Application server and use the displayed options to manage or check the status of the application services.
9. Update the IP addresses for Infrastructure and Applications hosts, and optionally the FortiPresence VM FQDN for GUI access and the FortiPresence Connect FQDN for captive portal usage.
10. Enter the required details to create an account, for example, email address and password to access the FortiPresence VM GUI.
11. Run the `presence-apps` command to display options to manage or view the services.

Additional Commands

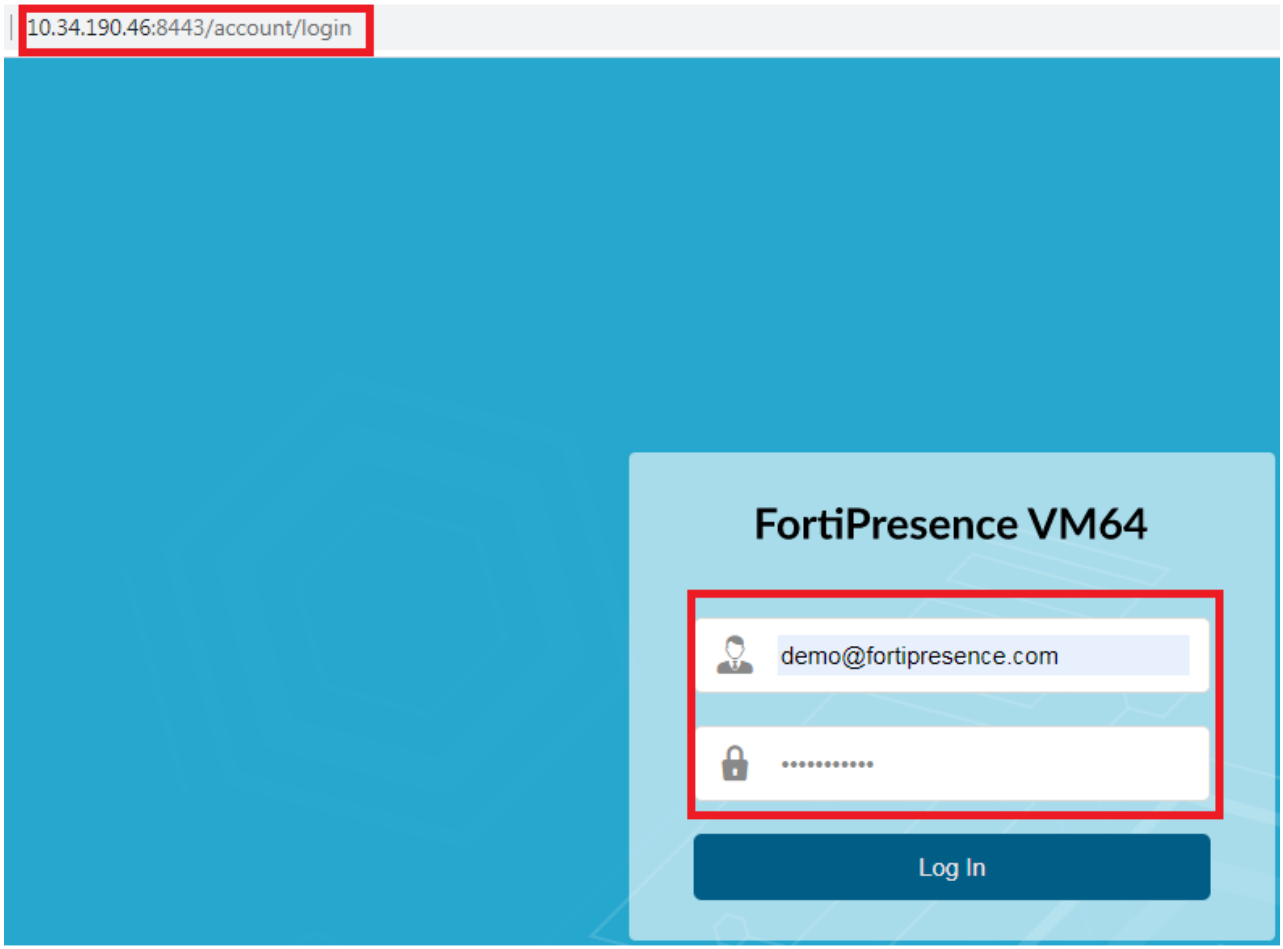
These are details on some commands for FortiPresence VM.

Command	Description
`presence-infra`	Displays general options to manage the infrastructure services.
`presence-apps --help`	Displays presence-apps script usage details with various available options.
`presence-infra --info`	Displays information on the infrastructure services.
`presence-infra --init`	Initializes the infrastructure services for the first time.
`presence-apps --init`	Initializes the application services for the first time.
`Get Status`	Displays the status of the services.
`Start Services`	Starts the services.
`Stop Services`	Stops the services.
`Show Logs`	Displays services' logs.

Accessing FortiPresence VM

After successfully completing the initial configuration on FortiPresence VM, you can access the GUI.

1. To access the FortiPresence VM GUI, enter the FortiPresence VM FQDN or Applications server IP address in a web browser. Port 8443 is used for GUI access.
2. To log in into FortiPresence VM enter the email address and password configured in the CLI.



3. In the FortiPresence VM GUI, navigate to **Admin > Settings > License** to upload the license file.

Upgrading FortiPresence VM

This section describes the upgrade to the latest version of FortiPresence VM.

Notes:

- Upgrade Infrastructure services **before** Application services.
- Both Infrastructure and Application servers should have the same version.
- Pre-upgrade version specific tars **must be** available on both the servers.
- Use release specific CLI scripts for upgrade.

- Logs are generated on the Application server when an upgrade is unsuccessful. You can share this with *Customer Support* teams if required.
- The system is reverted to the pre-upgrade version if the upgrade is unsuccessful.

Perform these steps to upgrade the Infrastructure and application services,

1. Download these files from the *Fortinet Support* portal.
   Infrastructure server: *FPVM-infra-x.x.x-buildXXXX* and *FPVM-cli-x.x.x-buildxxxx*
   Application server: *FPVM-apps-x.x.xbuildxxx* and *FPVM-cli-x.x.x-buildxxxx*
2. Login as **presence** user and copy the downloaded files to the VM servers. Use the following commands.
   `sftp username@<SFTP_server_IP>:<filename.tar>`
   OR
   `scp username@<SCP_server_IP>:<filename.tar> /presence`
3. Extract the latest CLI script on the Infrastructure server (as **presence** user).
   `tar -xzf FPVM-cli-x.x.x-buildxxx presence-infra`
4. Run the `presence-infra --upgrade` command on the Infrastructure server to upgrade the services and follow the instructions.
   After successful upgrade of the Infrastructure services, upgrade the Application services.
5. Extract the latest CLI script on the Application server (as **presence** user).
   `tar -xzf FPVM-cli-X.X.X-buildXXXX presence-apps`
6. Run the `presence-apps --upgrade` command on the Application server to upgrade the services and follow the instructions.
7. After successful upgrade, login into FortiPresence VM to use the services.

Note: After successful upgrade, retain the tars of the latest version and delete the tars of older versions.

Changing Dynamic to Static IP Address

Perform these steps to change the default dynamic IP address to static IP address.

1. Stop the Application services **before** the Infrastructure services.
2. Login into the Infrstructure server (as **root** user) and edit the */etc/sysconfig/network- scripts/ifcfg-ens192* file.
   Change the value of **BOOTPROTO** to **static** and add the below entries.
   IPADDR=x.x.x.x
   NETMASK=x.x.x.x
   GATEWAY=x.x.x.x
   This example depicts the */etc/sysconfig/network- scripts/ifcfg-ens192* file with dynamic and static IP addresses

configured.

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="dhcp"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192"
UUID="dc8f70dd-c261-4e65-ba16-3a89e8d9cc32"
DEVICE="ens192"
ONBOOT="yes"
```

```
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192"
UUID="dc8f70dd-c261-4e65-ba16-3a89e8d9cc32"
DEVICE="ens192"
ONBOOT="yes"
IPADDR="XX.XX.XX.XX"
NETMASK="XX.XX.XX.X"
GATEWAY="X.X.X.X"
```

3. Run the `service network restart` command to restart network services.
   The **ifconfig ens192** output has the newly added details.
4. Run the `sysctl -w net.ipv4.ip_forward=1` command to enable IPv4 Forwarding. See IPv4 Forwarding on page 21.
5. Repeat the previous steps on the Application server.
6. Login into the Infrastructure server (as **presence** user) and run the `presence-infra --basics` command to update the new IP address of the Application server.
7. [As **presence** user] Start the Infrastructure services.
8. Login into the Application server (as **presence** user) and run the `presence-apps --infra_host` command to update the new IP address of the Infrastructure server and the `presence-apps --basics` command to update new IP address of Application server.
9. [As **presence** user] Start the Application services.

Changing Default Subnet For Containers

Docker uses the default 172.17. 0.0/16 subnet for container networking. If this is already used in the network, perform the following steps to change the Docker subnet.

1. Stop the Application services and the Infrastructure services.
2. Login into the Infrastructure server (as **root** user) and edit the */etc/docker/daemon.json* file to add the highlighted content.

```
{
        "log-driver": "json-file",
        "log-opts": {
        "max-size": "10m",
        "max-file": "3",
        "labels": "production_status",
        "env": "os,customer"
        },
        "default-address-pools" : [
                {
                "base" : "X.X.X.X/16",
                "size" : 24
                }
        ]
}
```

Note: Replace x.x.x.x/16 with the desired subnet range.

3. Run the `systemctl restart docker` command to restart the Docker services.
4. Repeat the previous steps on the Application server.
5. [As **presence** user] Start the Infrastructure services **before** the Application services.
6. Login into FortiPresence VM. If the dashboard data is not displayed, disable and enable the location services on FortiWLC or FortiGate.

IPv4 Forwarding

IPv4 forwarding is required for the Application and Infrastructure servers to communicate. If the IP addressing mode is changed to static from DHCP (default), IPv4 forwarding gets disabled. In this case, verify the status of IPv4 forwarding and enable it before the initialization process starts.

Note: IPv4 forwarding is enabled by default.

Enable IPv4 forwarding on both the Application and Infrastructure servers before initializing the docker engine services required for communication. Login as **root** user.

1. Edit the */etc/sysctl.conf* file to add **net.ipv4.ip_forward=1** and save the file.

```
# sysctl settings are defined through files in
# /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
#
# Vendors settings live in /usr/lib/sysctl.d/.
# To override a whole file, create a new file with the same in
# /etc/sysctl.d/ and put new settings there. To override
# only specific settings, add a file with a lexically later
# name in /etc/sysctl.d/ and put new settings there.
#
# For more information, see sysctl.conf(5) and sysctl.d(5).
net.ipv4.ip_forward=1
```

2. Run the `systemctl restart network` command to restart the network services.
3. Run the `sysctl net.ipv4.ip_forward` to check the status of IPv4 forwarding. The expected output is **net.ipv4.ip_forward=1**.

Dashboards and Reports

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

FortiPresence VM 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.

Presence Dashboard

The Presence dashboard provides a summary view of FortiPresence VM 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.

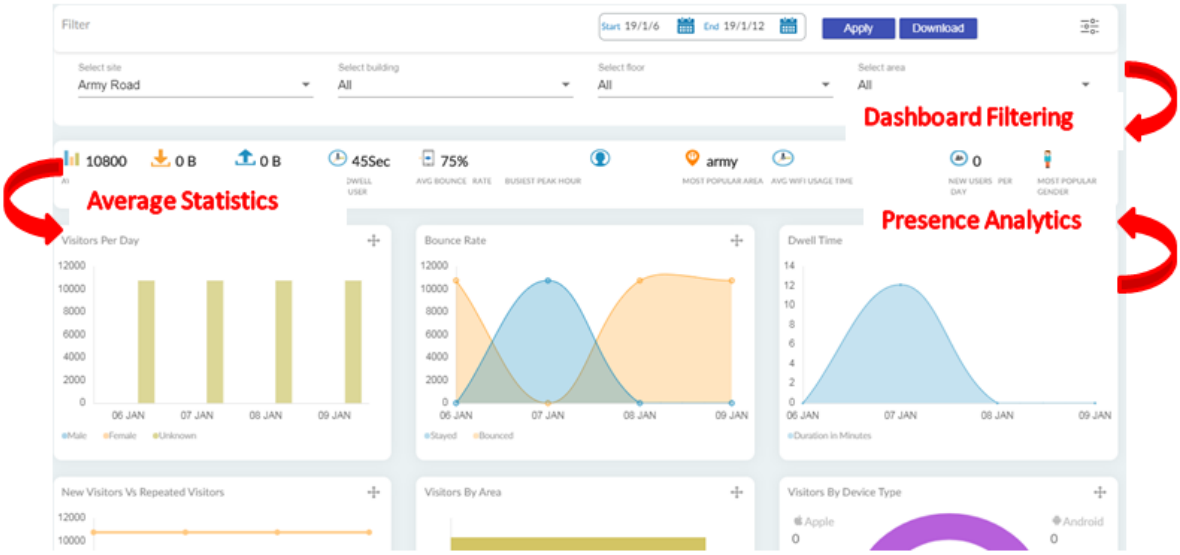
The access points (FortiGate and FortiAPCloud) and the FortiWLC controllers send the aggregated client data (station reports) to the cloud analytics engine as per configured time intervals. The analytics engine processes this raw data which is then compiled into summary charts and statistics. This data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

The 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. To download the dashboard data in *.pdf* format, click **Download**.

The panels displayed on the dashboard can be rearranged.

Note: You can select a time range within a specific period to view data on the dashboard. See GUI Data Limits – Dashboards and Reports on page 11.

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)

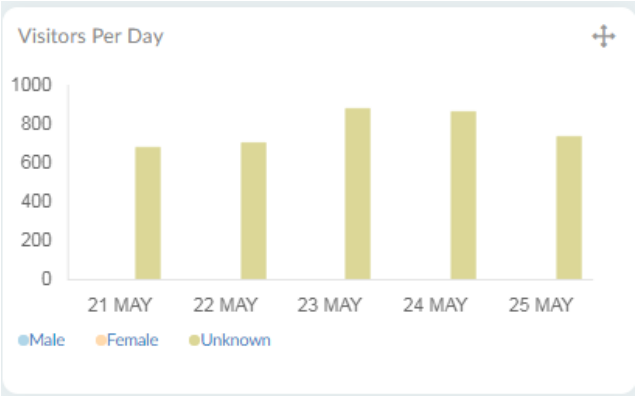
The dashboard provides real time data and analytics based on the following parameters:

- Visitor Analytics on page 24
- Device Analytics on page 26
- Site Analytics on page 27

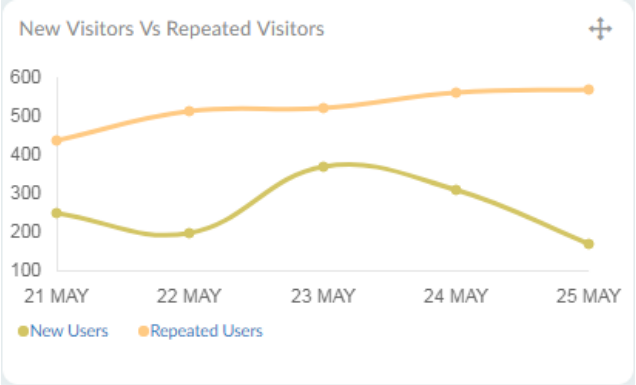
Visitor Analytics

This section provides analytics based on visitor behaviour.

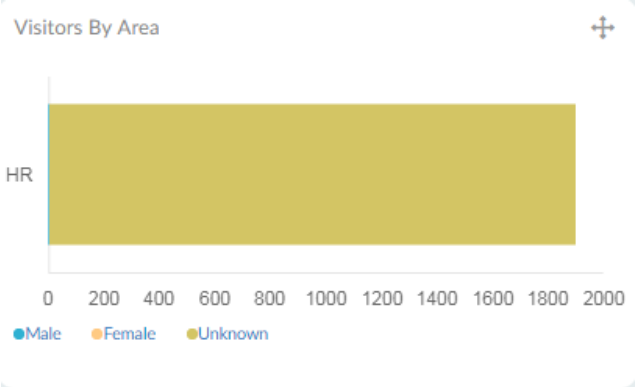
Visitors per day – Provides the total number of visitors per day within the time range selected. The chart displays the visitors categorized and Male, Female, and Unknown (absence of sufficient data for gender classification).



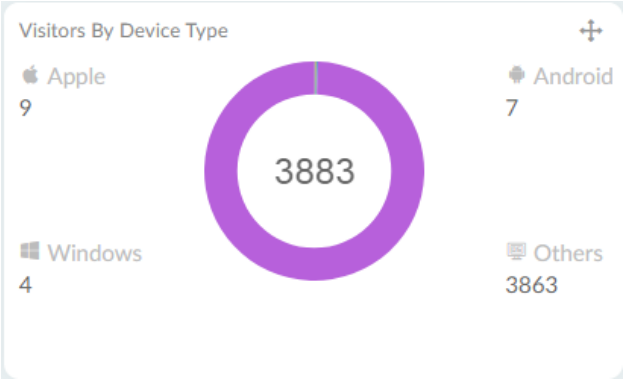
New Visitors vs Repeated Visitors – Provides the total number of new visitors and repeated visitors (visitors who visit more than once) per day. Hover over the lines plotted on the chart to obtain the number of new and repeated visitors.



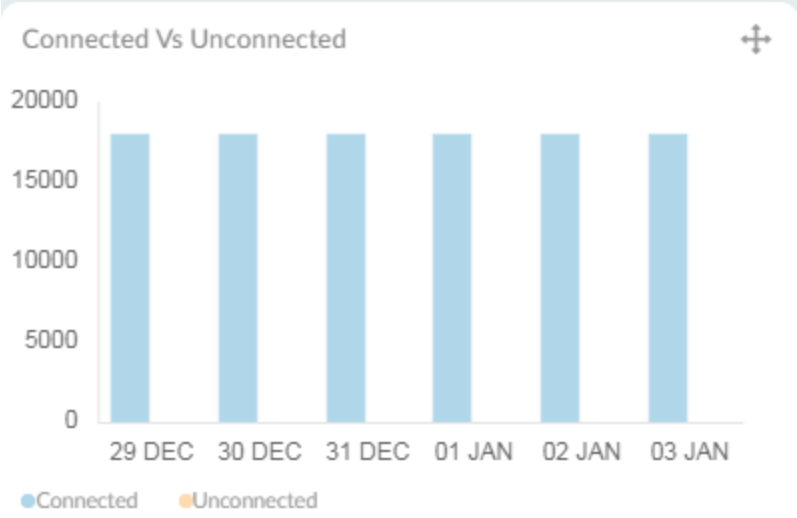
Visitors by area – Provides the total number of visitors for different areas in a particular site. This data is calculated from the start of the data range to the current time. Hover over the bars in the chart to obtain the total number of visitors per area and the categorization as Male, Female, and 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 VM Captive Portal per day within the time range selected vs the **Unconnected** visitors not authenticated in via the FortiPresence VM Captive Portal but connected to the Wi-Fi.

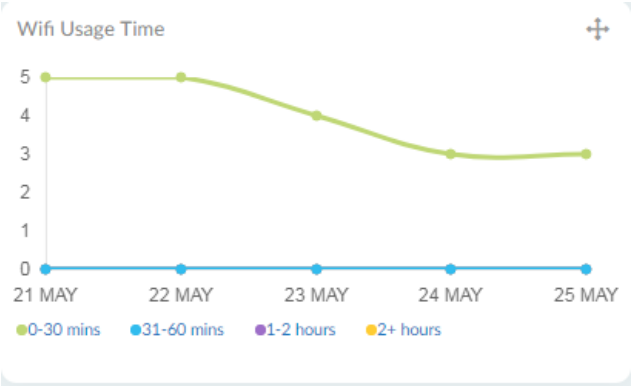


Device Analytics

This section provides analytics based on visitor device usage patterns.

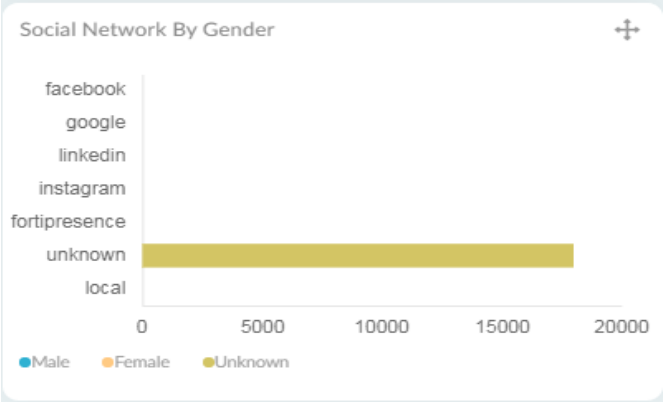
Data Usage – Provides the total bandwidth consumption per day. The chart displays the total data upload and downloads per day. Hover over the bars in the chart for the total upload and download size in GB.

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 VM Captive Portal but unwilling to share

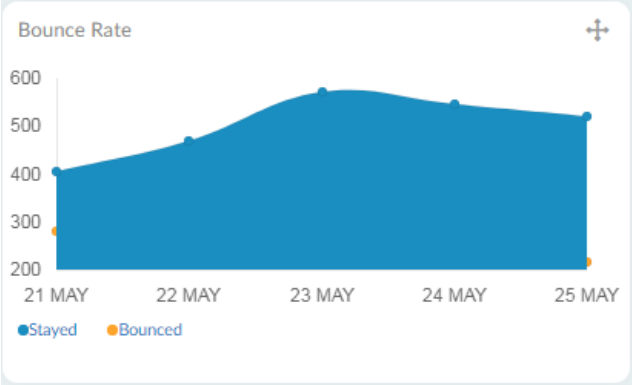
gender details are classified as **Unknown**. Users who login into the network on acceptance of terms and conditions and do not require authentication are classified as **Local**.



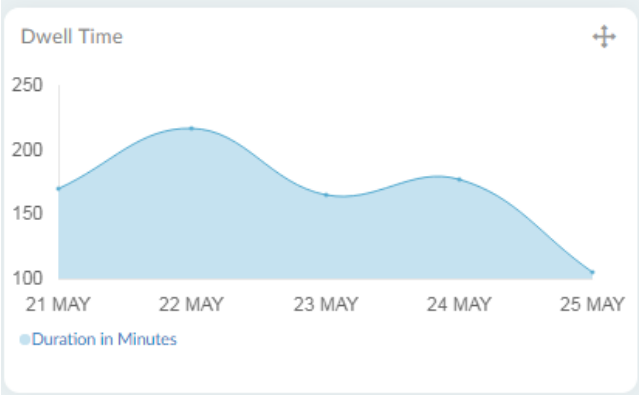
Site Analytics

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

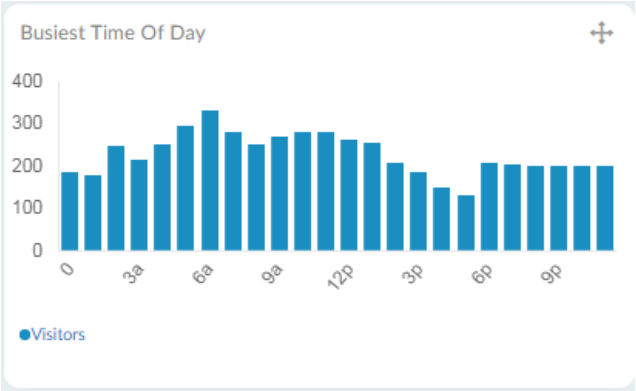
Bounce Rate – Provides the total number of and stayed/engaged visitors based on the bounce rate threshold configured at **Admin > Settings > Threshold**. Visitors who spend more than the configured bounce rate are classified as stayed and the ones less than the bounce rate as bounced.



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.

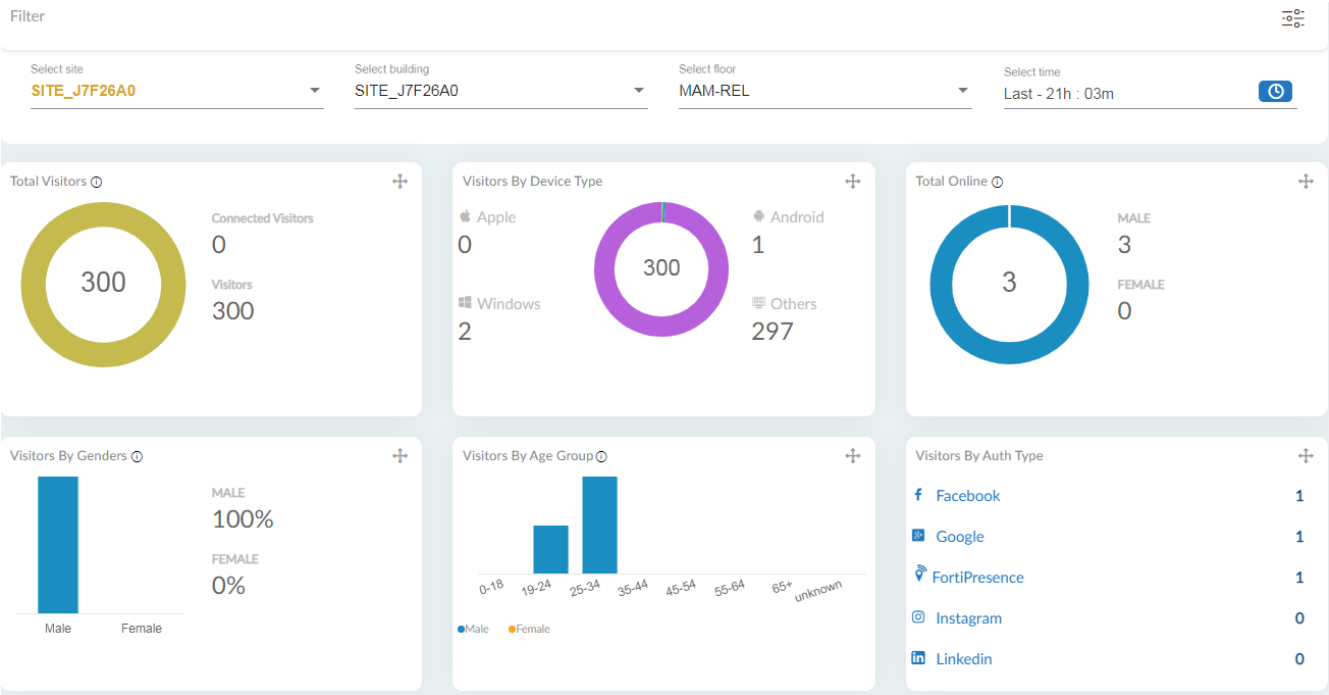


Busiest Time of the Day – Provides the cumulative hours over the different times for the selected time range, for example, if the dashboard is configured to display data for a week then the cumulative visitor hours for the entire week for different times are displayed. Hover over each bar on the chart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



Current View Dashboard

By default, the **Current View** dashboard provides a summary of FortiPresence VM analytics in the last 15 minutes for the selected floor. Analytics for a maximum of 24 hours can be viewed, 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 VM Captive Portal and Wi-Fi infrastructure (**Connected Visitors**) and the visitors who are connected to the Wi-Fi but not authenticated via the FortiPresence VM 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 VM 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**. SMS OTP based logins are included in the **FortiPresence** authentication type. Users who login into the network on acceptance of terms and conditions and do not require authentication are classified as **Local**.

Reports

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

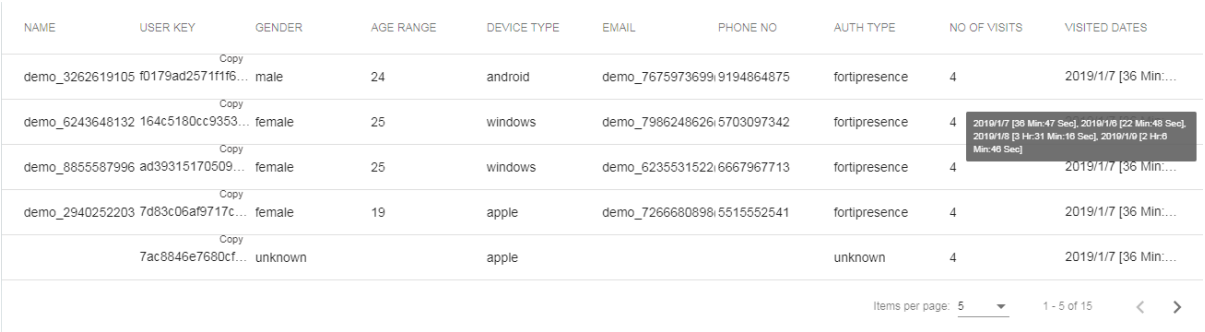
Select the time period and the site to be covered by the selected report. These fields are supported for all report types. The reports are searchable for specific fields for data that is generated.

Click on **Download & Email** to download generated reports and email them to the registered email address.

For more information on the report fields see Presence Dashboard on page 23.

Visitor Reports

The 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], 2019/1/6 [22 Min:48 Sec], 2019/1/8 [3 Hr:31 Min:16 Sec], 2019/1/9 [2 Hr:6 Min:46 Sec]
demo_8855587996	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:...

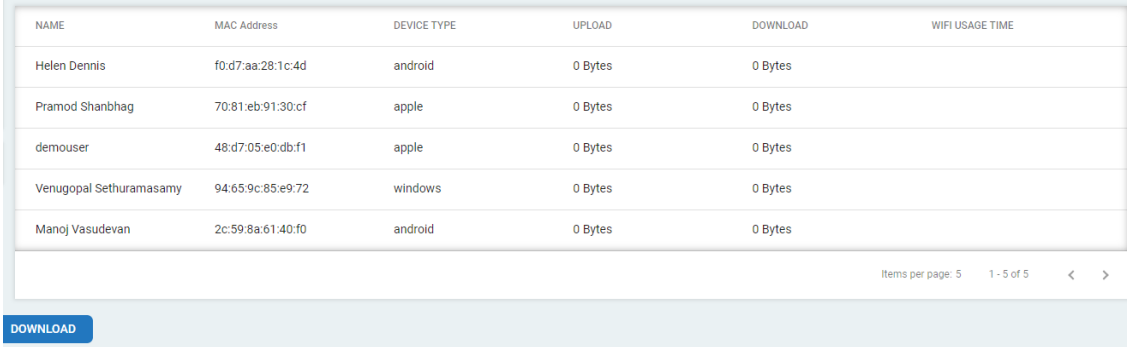
Items per page: 5 1 - 5 of 15

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.
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. SMS OTP based logins are included in the FortiPresence authentication type.
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.

Field	Description
Phone No	Displays the visitor's mobile number.
Email	Displays the visitor's email address.

Network Reports

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



NAME	MAC Address	DEVICE TYPE	UPLOAD	DOWNLOAD	WIFI USAGE TIME
Helen Dennis	f0:d7:aa:28:1c:4d	android	0 Bytes	0 Bytes	
Pramod Shanbhag	70:81:eb:91:30:cf	apple	0 Bytes	0 Bytes	
demouser	48:d7:05:e0:db:f1	apple	0 Bytes	0 Bytes	
Venugopal Sethuramasamy	94:65:9c:85:e9:72	windows	0 Bytes	0 Bytes	
Manoj Vasudevan	2c:59:8a:61:40:f0	android	0 Bytes	0 Bytes	

Items per page: 5 1 - 5 of 5

DOWNLOAD

Field	Description
Name	Displays the name of the visitor based on the social network logins.
MAC address	Displays the MAC address 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 %

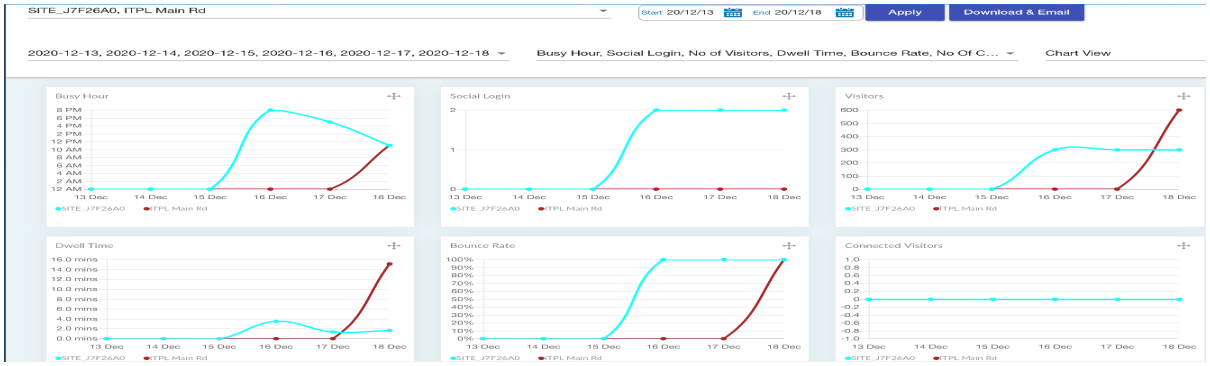
Items per page: 500 1 - 500 of 500

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.
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 VM 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

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.

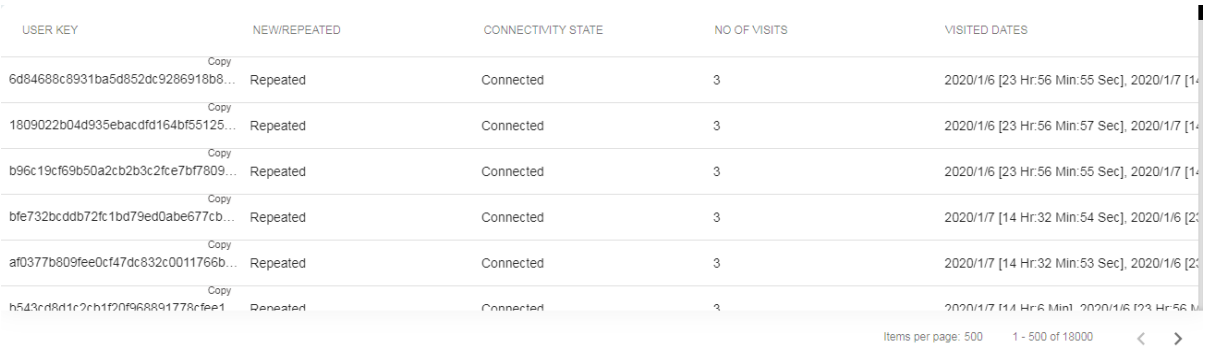
Data stored up to the last 1 year can be compared.



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.

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
Copy 1809022b04d935ebacdfd164bf55125...	Repeated	Connected	3	2020/1/6 [23 Hr:56 Min:57 Sec], 2020/1/7 [14
Copy b96c19cf69b50a2cb2b3c2fce7bf7809...	Repeated	Connected	3	2020/1/6 [23 Hr:56 Min:55 Sec], 2020/1/7 [14
Copy bfe732bcddb72fc1bd79ed0abe677cb...	Repeated	Connected	3	2020/1/7 [14 Hr:32 Min:54 Sec], 2020/1/6 [23
Copy af0377b809fee0cf47dc832c0011766b...	Repeated	Connected	3	2020/1/7 [14 Hr:32 Min:53 Sec], 2020/1/6 [23
Copy b543cd8d1c2cb1f20f968891778cfee1	Repeated	Connected	3	2020/1/7 [14 Hr:6 Min], 2020/1/6 [23 Hr:56 M

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 VM Captive Portal or **Unconnected** visitors not authenticated in via the FortiPresence VM 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

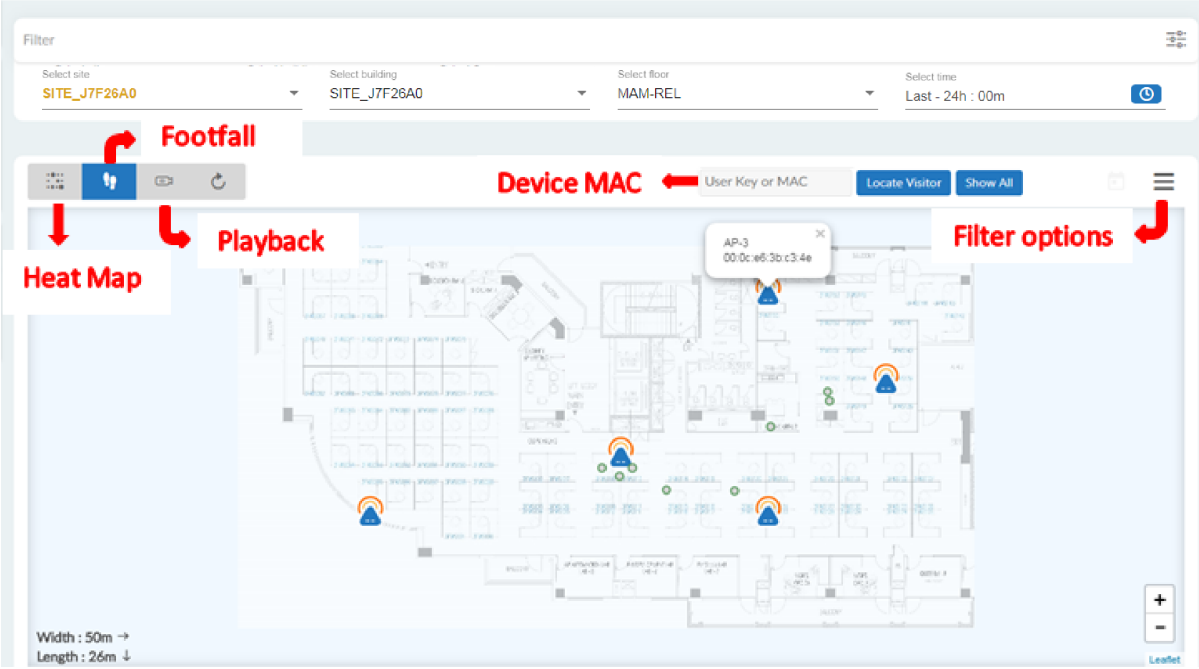
FortiPresence VM provides data and analytics based on demographic segmentation and visitor movement between areas. The location analytics delivers data visualization in a customizable format.

This geographical data analysis provides real-time insights into user behavior. The Location view of the FortiPresence VM 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**, **Footfalls**, and **Playback**. 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.



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

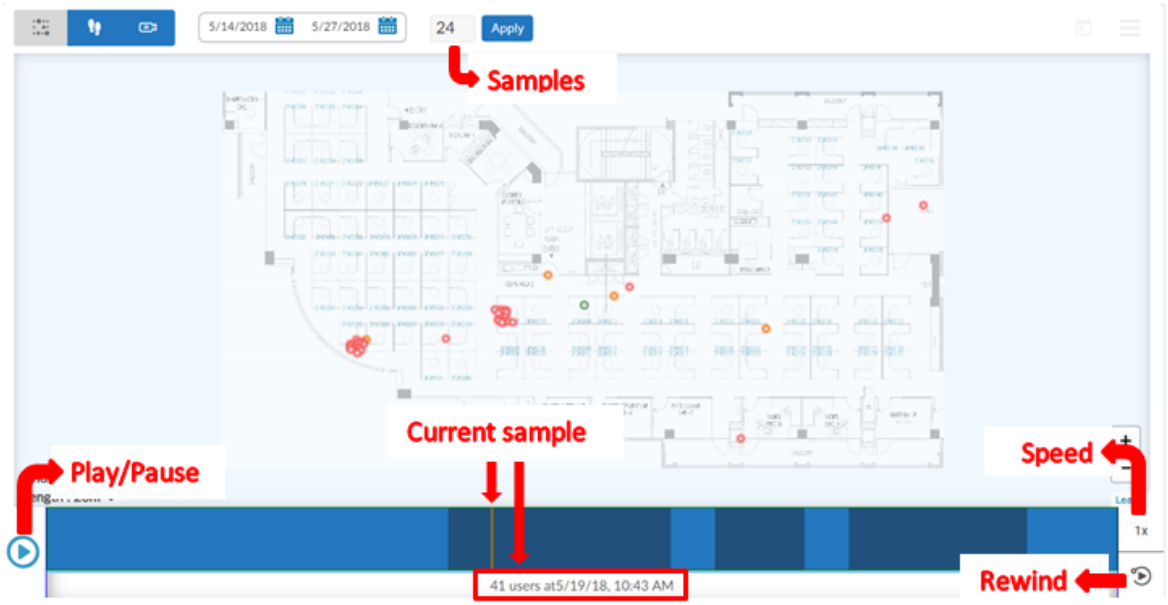
The footfall view displays the placement of access points on the selected floor along with the associated MAC addresses and the current location of all visitors along with the specific user key.

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.

Playback

The **Open Player** option visualizes visitor data/footfalls on a timescale. Select the date range to view historical data and select the number of samples, that is, frames of equal duration into which data over the selected range is broken into. Click **Apply**.

The progress bar of the playback option segregates data into time samples. Samples which contain visitor information are marked in dark blue while the absence of such information is marked in lighter blue. You can pause, play, and rewind the data visualization. The rewind option works per sample, that is, each click on **Rewind** takes you to the previous sample. You can also control the speed of the playback, reduce it to half (**0.5x**) or double it (**2x**). Click on the **Open Player** icon to exit this mode.



The **Footfall**, **Heat Map**, and **Playback** data visualization options for floor analytics can be filtered for **WiFi** and **BLE** users based on the following criteria. Hover over the icons visitor icons displayed on the map to view details based on the filter criteria.

Filter	Description
Visitors	Filters the data based on the gender classification of the visitors. The maps display the visitors categorized as **Male**, **Female**, and **Unknown** (absence of sufficient data for gender classification). The total number of visitors is also displayed in the filter tab.
Accuracy	Filters the data based on the accuracy of the device signals/user presence detected by the number of access points. The accuracy is classified as, **Good accuracy**, when detected by 3 or more access points, **Medium**, when detected by 2 access points, and **Low** when detected by 1 access point.
Device Type	Filters the data based on the OS used for social network logins. The map displays the total number of logins from iOS, Android, Windows, and other OS. The total number of visitors per device type is also displayed in the filter tab.
Connectivity State	Filters data based on users connected to the Wi-Fi but authenticated (**Connected**) not authenticated (**Unconnected**) via the Captive Portal.

Filter	Description
Age group	Filters data based on the age group classification of the visitors. Select the require age group as provided in the filter options.
Authentication Type	Filters the data based on social network login information. The map displays the total number of users for each authentication type, **Facebook**, **Google**, **Instagram**, **LinkedIn**, and **FortiPresence**.
Area	The areas the floor is divided into are displayed, click on an area to highlight it on the map. You can select the area to view localized movements.

The **Visitors** tab lists the visitors along with the associated MAC address, you can **Track** and **Locate User**.

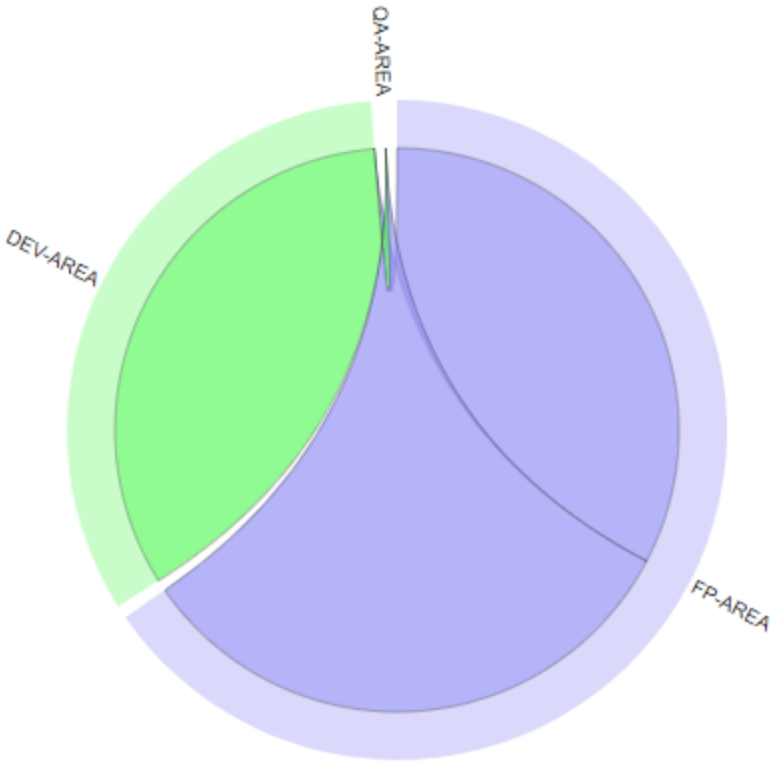
Area Analytics

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**.

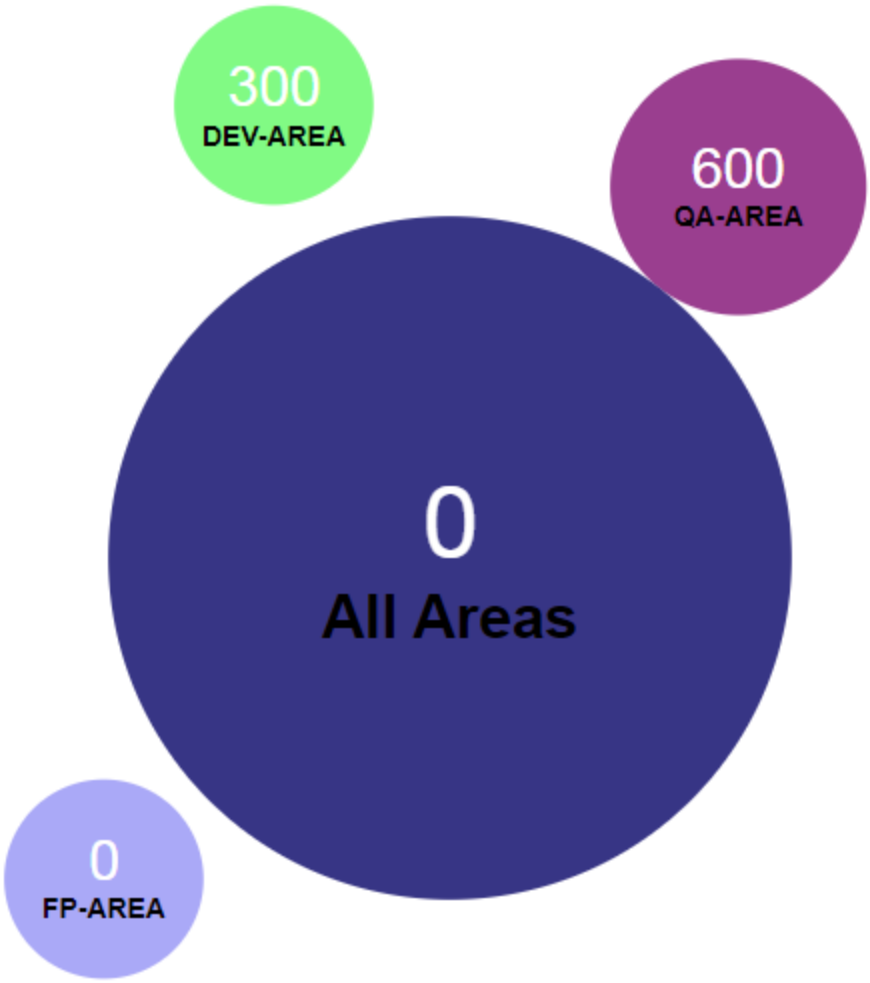
Visitor Movements Matrix

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

Top 10 Visitor Movements by Area

This chart displays the top 10 areas (by visitor movement) and the number of visitors in each area. The **All Areas** bubble indicates the total number of visitors who visited all the areas.

Top 10 Visitor Movements By Area



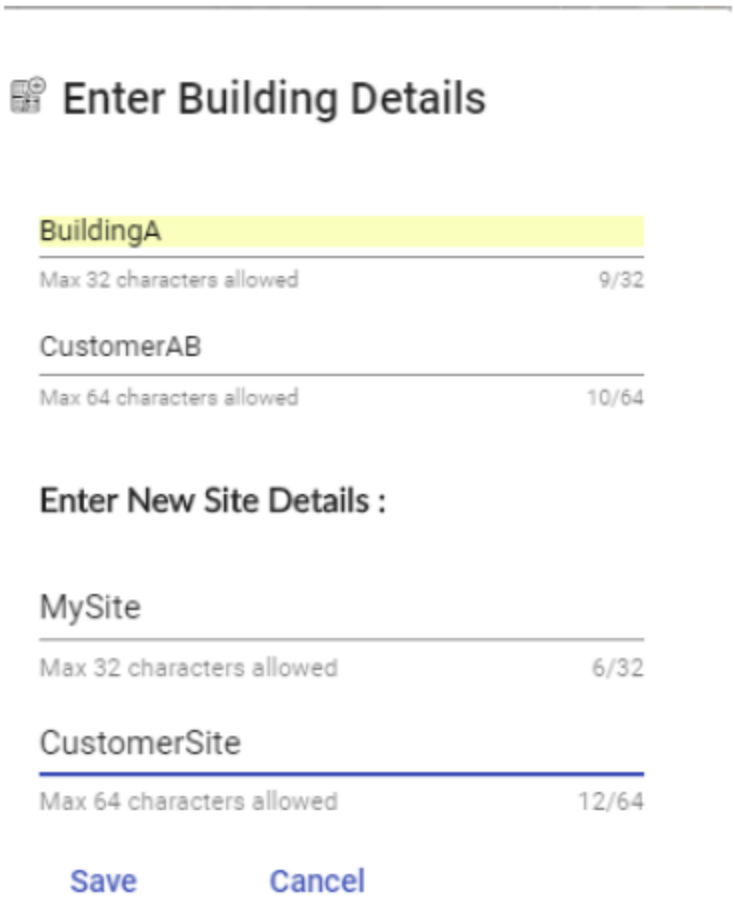
Administering FortiPresence

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

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.

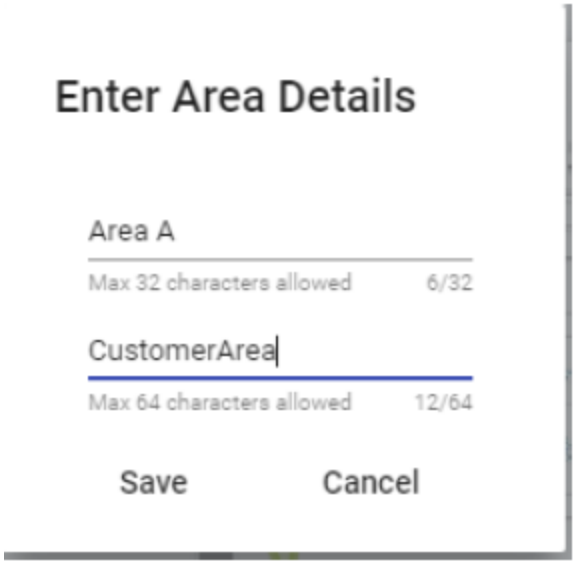


4. Click on **Add Floor** to upload the floor map for the building.
5. Enter the floor details and browse to the map. Click **Add Floor**.
   The floor map is displayed.
6. Adjust the two red pointers on the floor maps and position them across a known distance and specify the **Selected Distance** (feet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

Click **Save**.

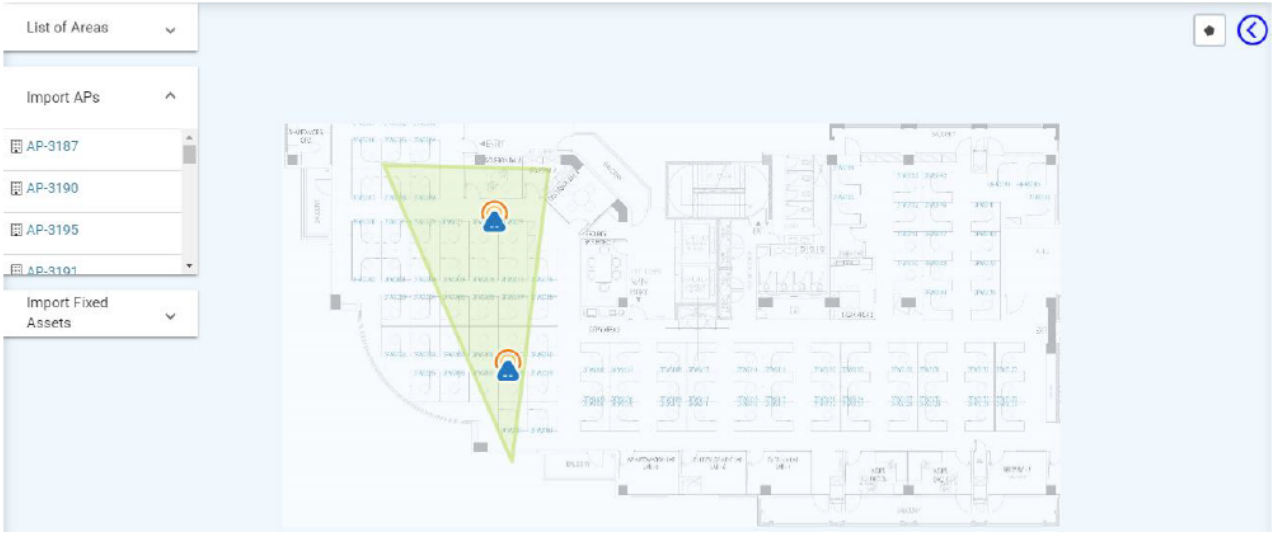
7. 7. Click on the (polygon) icon and mark an area on the floor map by drawing a polygon anti-clockwise. Click **Finish**.

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

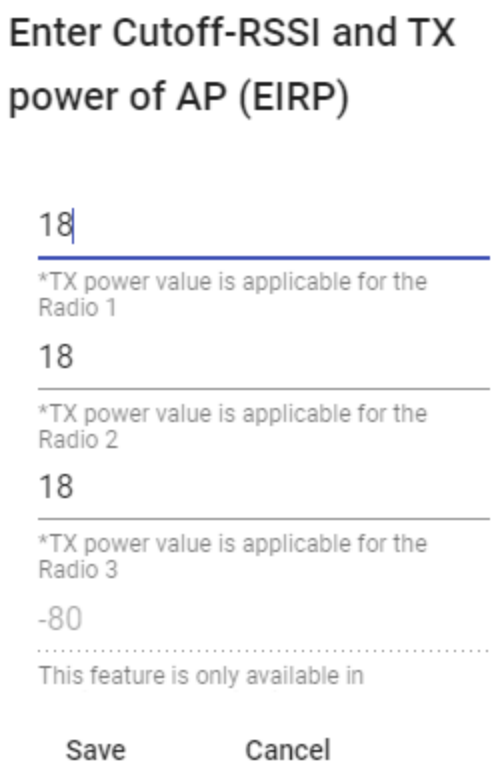


You can create multiple areas on a floor as per your requirement.

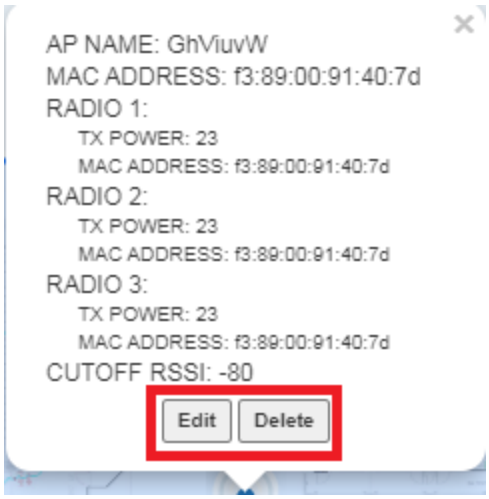
9. Select a specific area on the map and click on **Import APs** and place the listed access points on the marked polygon (area) on the floor.



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



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.



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 overidden when the next ID packet arrives after an hour.
- Dynamic changes to Tx power on the enforcement device (FortiWLC, FortiGate, and FortiAP 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 56.
- You can view the access points in **Admin > Settings > Discovered APs**.

Portal Management

The portal management operations of FortiPresence VM 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.

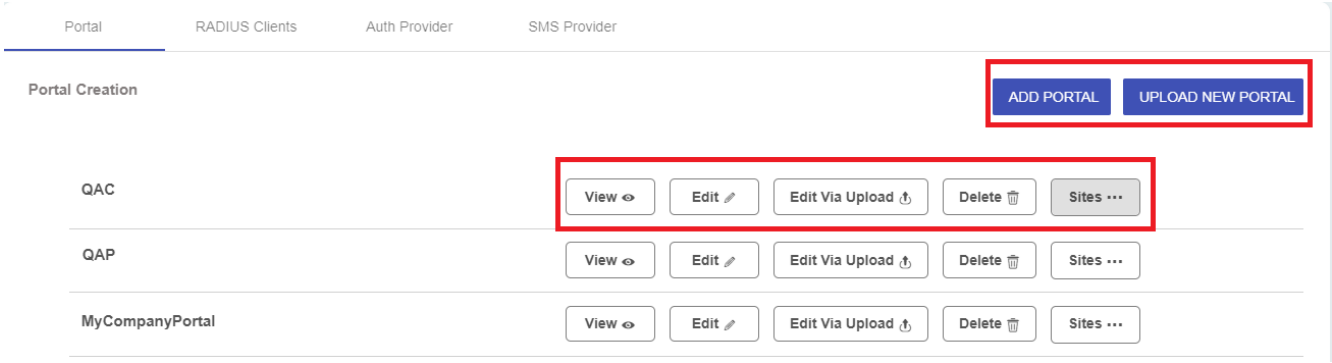
Portals are mapped to multiple sites and multiple portals can be created per site.

RADIUS clients are created for Captive Portal authentication and authorization configurations on FortiAPCloud/FortiGate/FortiWLC. See Configuring Captive Portal on page 59.

Creating a Portal

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

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 46.
- **Upload New Portal** - To upload a new customized captive portal. See Uploading a New Portal on page 49.
- **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 49.
- **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.

Navigate to **Portal > Portal Settings** and select the site for which the portal is to be created. Click **Add Portal**.

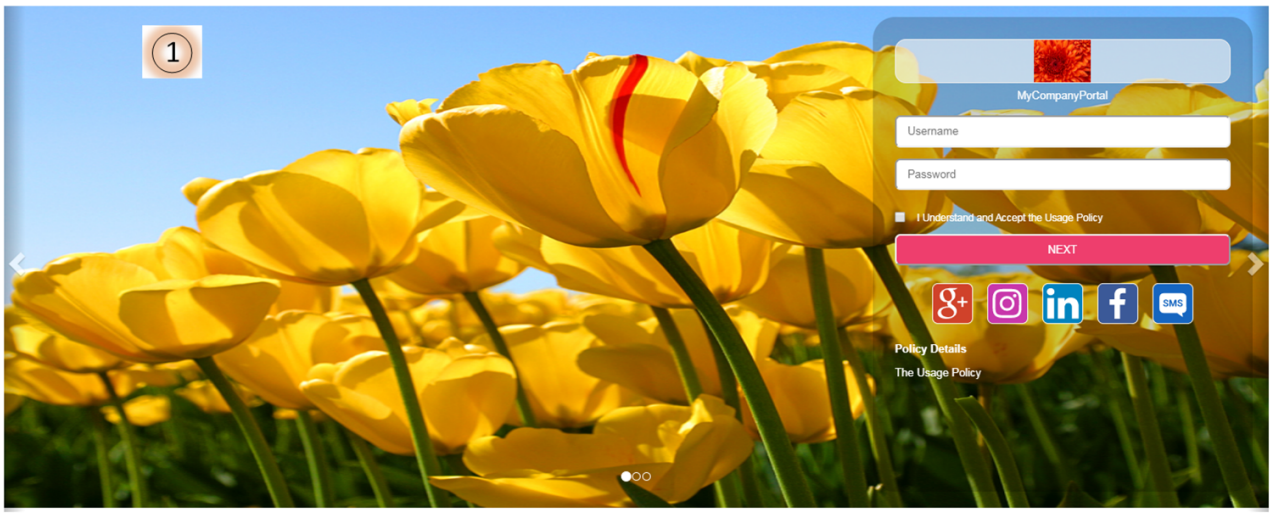
1. Enter a unique **Portal Name** for your site and select a **Theme** and **Color** from the pallet for the portal authentication page. Click **Next**.
2. Upload your **Company Logo** and a **Background Image**. Separate background display images are required for desktop and mobile devices. Images in 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.
3. 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.
4. Select the supported/permissible 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.
   SMS Login – allows visitors to login using a One Time Password (OTP) sent via SMS on the user provided mobile number. Attach a specific SMS provider to this portal. To configure the SMS provider, see Portal Settings.

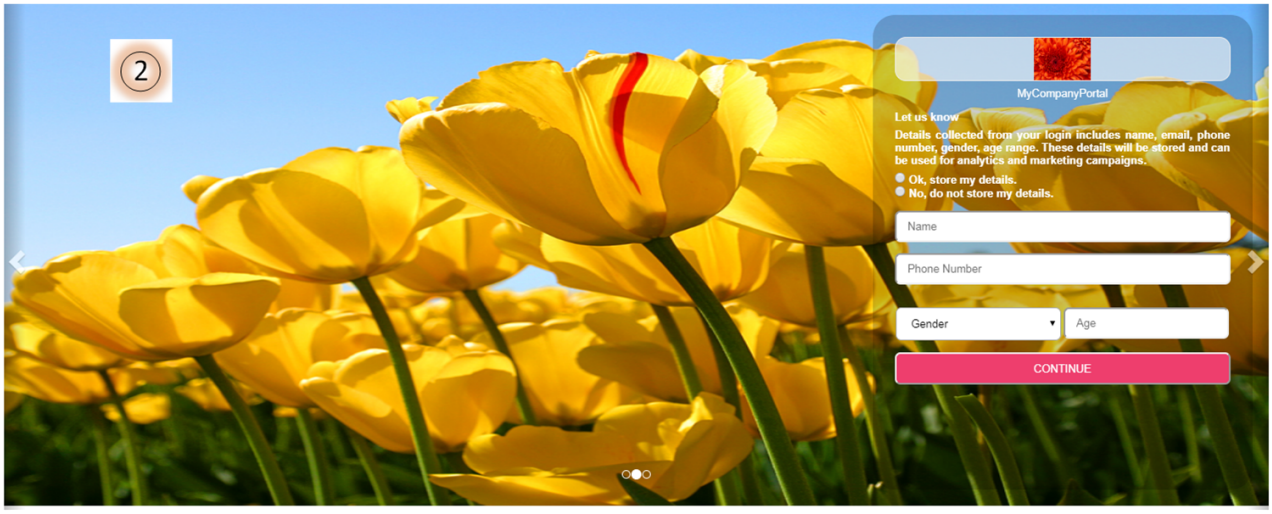
   Click on the **SMS Template Settings** ( ) icon to customize the default SMS text. The %OTP% variable MUST be a part of the SMS text, irrespective of whether the default SMS text is customized or not.
   The %OTP% variable translates to the actual OTP in the text message sent to the user provided mobile number.
   The user will not be able to save the message if the %OTP% variable is not present.
   Note: This feature is available only for paid tier users.
   If you do not select any of the above options, the portal authenticates the visitor without any credentials.
5. 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**.

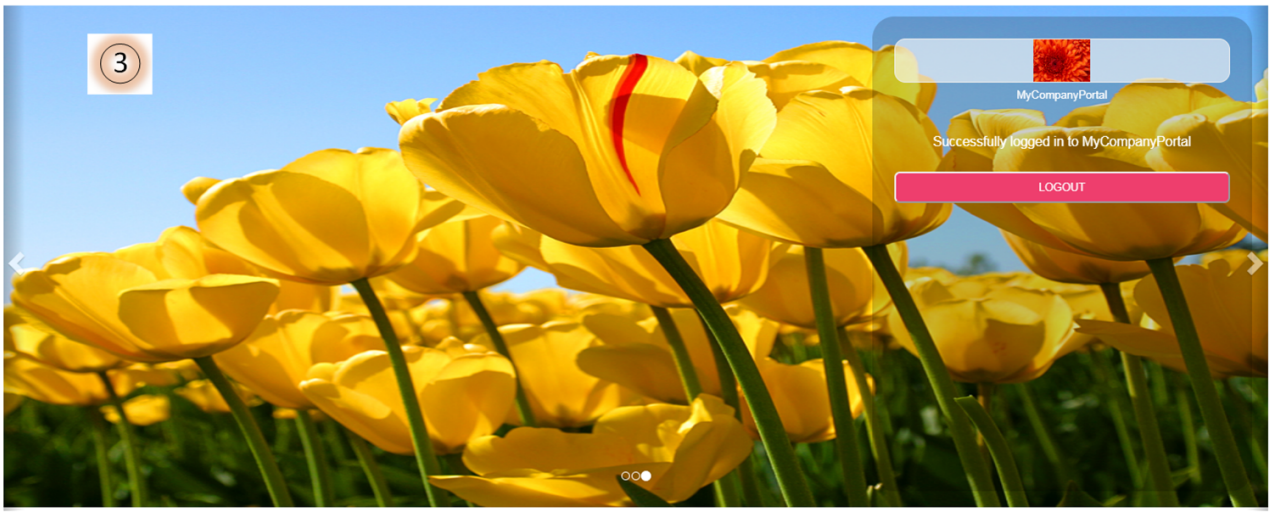
6. Enable **Collect Email** to collect email information during visitor authentication through Captive Portal; enable **Verify Email** to verify the collected email information.
7. Configure the website redirection options for visitors after successful login into the captive portal.
   Default Success 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.
8. To download the portal for customization, click **Download**.
9. Click **Save**.
   The portals created can be edited and deleted.

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 46.
- 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.

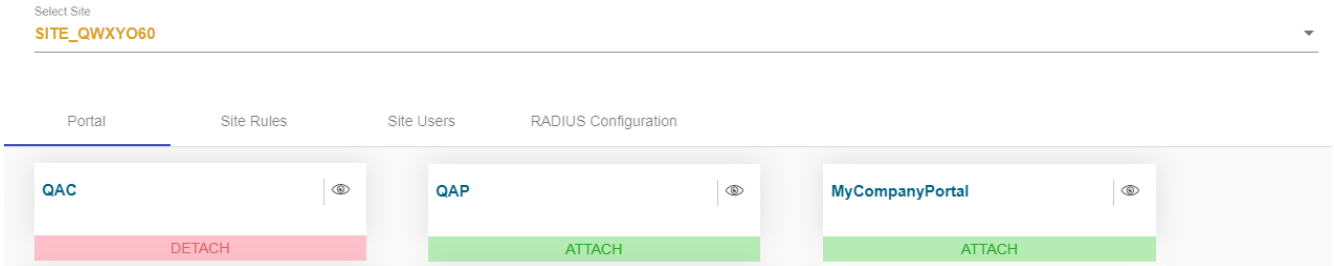
Note: Do not modify the JSON file in the downloaded folder.

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*.

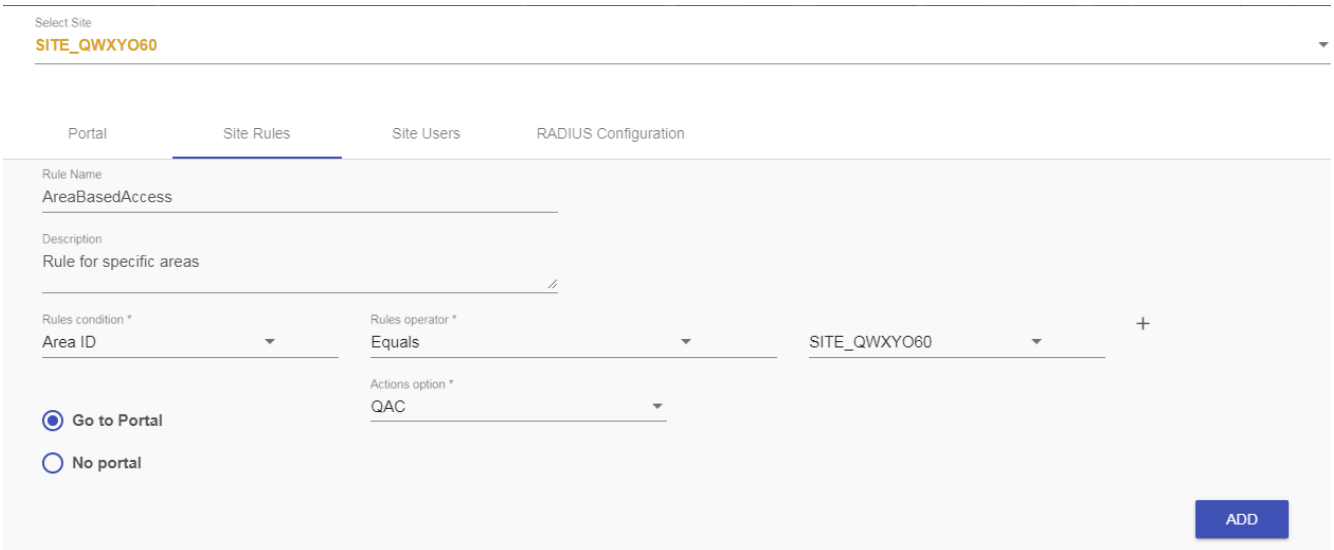
Configuring Site Rules and Users

Navigate to **Portal > 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 > 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.



Navigate to **Portal > 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 > 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 FortiAPCloud/ FortiGate/ FortiWLC. See Configuring Captive Portal on page 59.

Portal Settings

This section describes some additional FortiPresence VM settings.

Navigate to **Portal > Portal Settings**.

Setting	Description
RADIUS Clients	Configure FortiAPCloud/FortiGate/ FortiWLC as RADIUS clients for portal authentication. The list of exempted FQDNs for FortiAPCloud, FortiGate, and FortiWLC are displayed here. See Configuring Captive Portal. **Note**: You can edit and delete the RADIUS clients.
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.
SMS Provider	You can add multiple SMS providers to set up SMS OTP login support for captive portals.

Setting	Description

	Specify the name and description of the SMS provider. The supported SMS service type is HTTP API and the HTTP GET and POST methods are permitted.
	When defining the HTTP API call for both GET and POST methods, **%PHONENUMBER%** and **%MESSAGE%** variables MUST be included. These variables act as place holders and get their data from the portal which is used by the user to login to the captive portal enabled SSID.
	• **%PHONENUMBER%** - The mobile number provided by the user trying to authenticate to the captive portal enabled SSID. This number receives the OTP details.
	• **%MESSAGE%** - The SMS text that is sent along with the OTP to the user provided mobile number.
	The SMS text can be customised through the SMS template while creating a portal.
	Consider the following example:
	1. Resource **URL** is *https://api.textlocal.in/send/* and **data** = *urllib.parse.urlencode({'apikey': apikey, 'numbers': numbers,'message' : message, 'sender': sender})*
	2. Then the API URL will be *https://api.textlocal.in/send/?apikey=<API KEY provided by the SMS provider>&numbers=numbers&message=message&sender=sender*
	3. Replace the numbers and message variables in the API URL *https://api.textlocal.in/send/?apikey=a12344rewrwreoi89&numbers=**%PHONENUMBER%**&message=**%MESSAGE%**&sender=TXTLCL*
	Notes:
	• FortiPresence VM encodes only the **%PHONENUMBER%** and **%MESSAGE%** variables.
	Note: The requirement for parameters and their encoding varies based on the SMS provider. You are required to obtain information regarding the API, parameters and their encoding from the SMS providers.
	Encode all other variables based on the SMS provider requirements.
	• For the HTTP GET method, **%PHONENUMBER%** and **%MESSAGE%** variables are always encoded by FortiPresence; for the HTTP POST method, **%PHONENUMBER%** and **%MESSAGE%** variables are encoded by FortiPresence VM only when the HTTP header is defined as follows:
	  • **Key**: Content-Type
	  • **Value**: *application/x-www-form-urlencoded*
	Once the SMS provider is configured, the providers can either be attached to new or existing portals.
	Navigate to **Portal > Portal Management** (add new portal or edit an existing portal). See Portal Management on page 45.

s

Administrative Settings

This section describes some additional FortiPresence VM settings.

Navigate to **Admin > Settings**.

Setting	Description
Threshold	Select the sites for which to apply thresholds. **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. **Current View Time** - This setting applies to the visitor data displayed in the Current View Dashboard and Location Floor Analytics. The default is 24 hours. You can customize the view time using this option. **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. **Organisational Unique Identifier (OUI)** – When enabled, this setting filters out the non OUI MAC Addresses and is applicable for all the dashboards. **Filter Employees** – This setting is enabled by default and filters out the employee MAC addresses added in the Employees tab from site level analytics. **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 Fixed Assets** in **Settings > Fixed Assets**. **Site Business Time** – You can configure data collection duration for the FortiPresence VM 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.

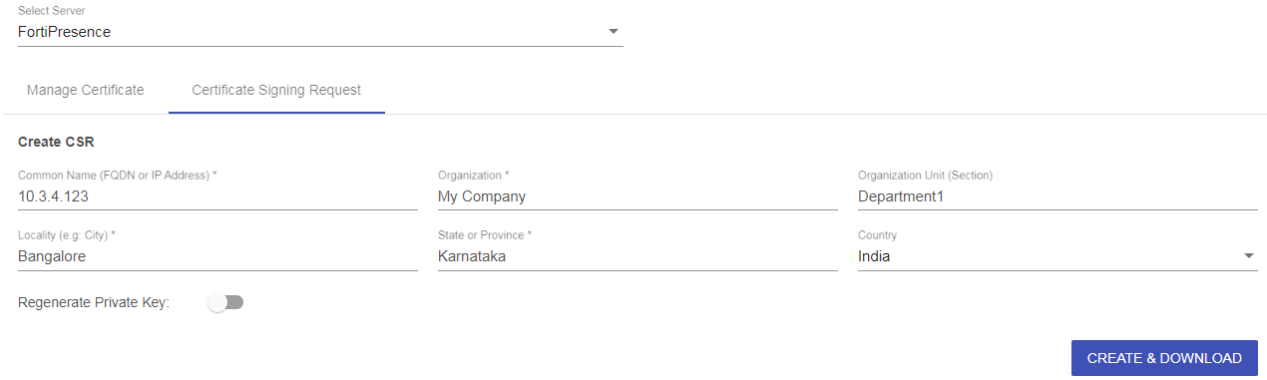
Setting	Description
Discovered APs	Unique project name and secret key is generated for each account on FortiPresence VM. These are used to configure location services on FortiAPCloud/ FortiGate/FortiWLC. The AP name, MAC address, serial number, timestamp, site, firmware version, license expiry date, location, and state (**Active** (identification of packets received in the last 24 hours) or **Inactive** (no identification of packets received in the last 24 hours)) are displayed. If FortiPresence VM 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 VM 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 sort the displayed column based on the name, timestamp, site, expiry date, and state. The Location server IP (**App Server IP**) and port are also displayed here. The APs with location services enabled are displayed here. See Configuring Location Services on page 56.
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 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.
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 **Threshold** tab and select the filter (enabled by default).
License	The valid license files are uploaded in the *.lic* format. The existing license details are also displayed.
SMTP Settings	Configure the SMTP settings to send FortiPresence related emails. The emails are configured using the Plain/CRAM-MD5/Login SMTP authentication methods and SSL/TLS authentication encryption methods.

SSL Certificate

Certificates provide security assurance validated by a Certificate Authority (CA). Server certificates are generated based on a specific Certificate Signing Request (CSR). The CSR is a request sent from an applicant to a CA in order to apply for a digital identity certificate. When a CSR is generated, the associated private key to sign and/or encrypt connections is also generated.

By default, the FortiPresence VM is equipped with self signed certificates to use with the FortiPresence GUI and FortiPresence Connect services. However, you can replace the default self signed (with internal CA) SSL certificates with externally signed SSL certificates for your domains.

1. Navigate to **Admin > SSL Certificate** and select the server to generate the certificate.
2. In the **Certificate Signing Request** tab, enter the following.
   - **Common Nam**e - The FQDN or IP address of the server.
   - **Organization** - The name of your establishment or organization.
   - **Locality** - The city or area where your organization is located.
   - **State or Province** - The state or province of the above mentioned area.
   - Optionally, you can enter the **Organization Unit** and the **Country**.
3. Click **Create & Download** to download the CSR.



4. Select **Regenerate Private Key** to generate a new private key. Since the new key replaces the existing one, default/current certificates stop working. Note that creating a temporary certificate automatically replaces default/current certificates.
5. In the **Manage Certificate** tab, you can generate a temporary certificate with the existing private key and replace the default/current certificates. Download and upload the externally signed SSL certificate.

User Management

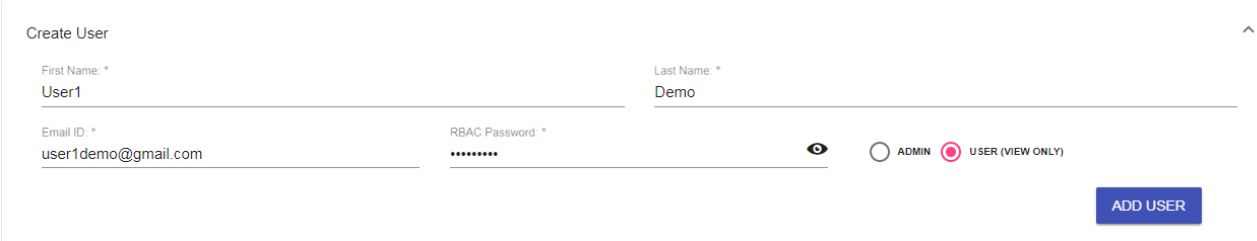
You can manage RBAC users and generate API user credentials.

- User Account on page 55
- API Users on page 55

User Account

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**, **Email ID**, and **RBAC Password** for each user.
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.



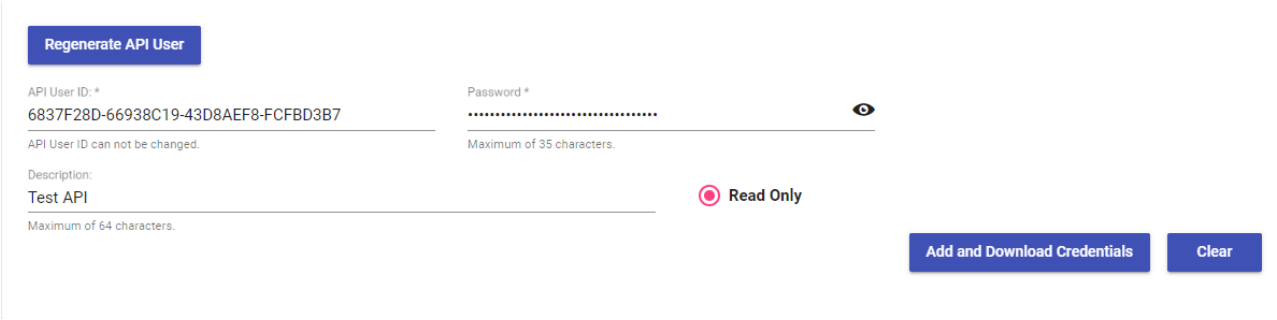
3. Click **Add User**.

You can modify the assigned role and the password by clicking on **Change Password**. To delete a user, click the delete icon against the specific user.

API Users

You can access REST APIs in the Swagger interface using the configuration defined in this section. *Read Only* APIs are only supported.

1. Click **Generate API User** to generate a unique API User ID and provide a (optional) **Password**. The API user credentials are created.
2. Enter an optional **Description** for the API user.
3. Click **Add and Download Credentials** to add the API details to FortiPresence VM and download them.



4. Modify the API user access type to **Active**.
5. Run the following command to generate an access token.
```
$ curl -X POST -k 'https://{Application server FQDN/IP}:7443/api/token/' -H
'Content-Type: application/json' -H 'Accept: application/json' -d '
{"username":"API User ID","password":"API User password" }'
```
6. Access the Swagger interface, *https://{Application server FQDN/IP}:7443/swagger* and authorize using the access token.

Configuring Location Services

With the completion of FortiPresence VM 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 VM to validate the origin and un-tampered 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.

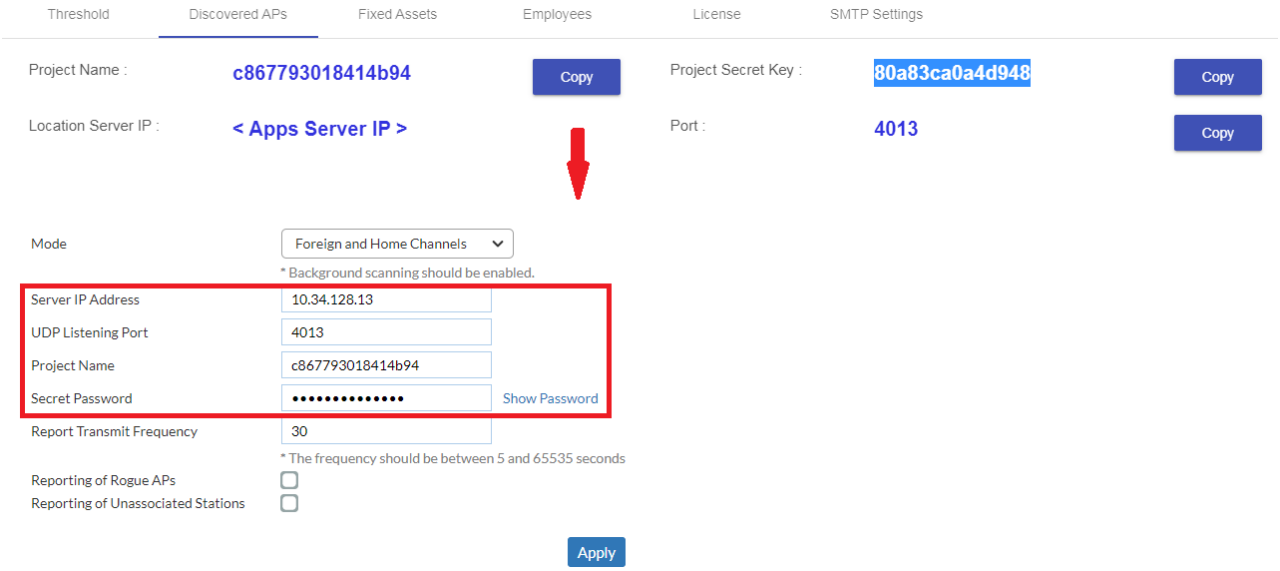
The project name and secret key are required to be configured on FortiGate/FortiAPCloud/FortiWLC to enable Location Services. The location services are configured with location server IP address which is the Application server IP address and server port **4013**.

- FortiAPCloud on page 56
- FortiGate on page 57
- FortiWLC on page 57

FortiAPCloud

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

1. On the FortiAPCloud 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 Server IP Address - (Application server IP address) and the **UDP Listening Port** - 4013.
4. Enter the **Project Name** and **Secret Password**, (**Project Name** and **Project Secret Key** respectively copied from the FortiPresence VM GUI - **Admin > Settings > Discovered APs**).

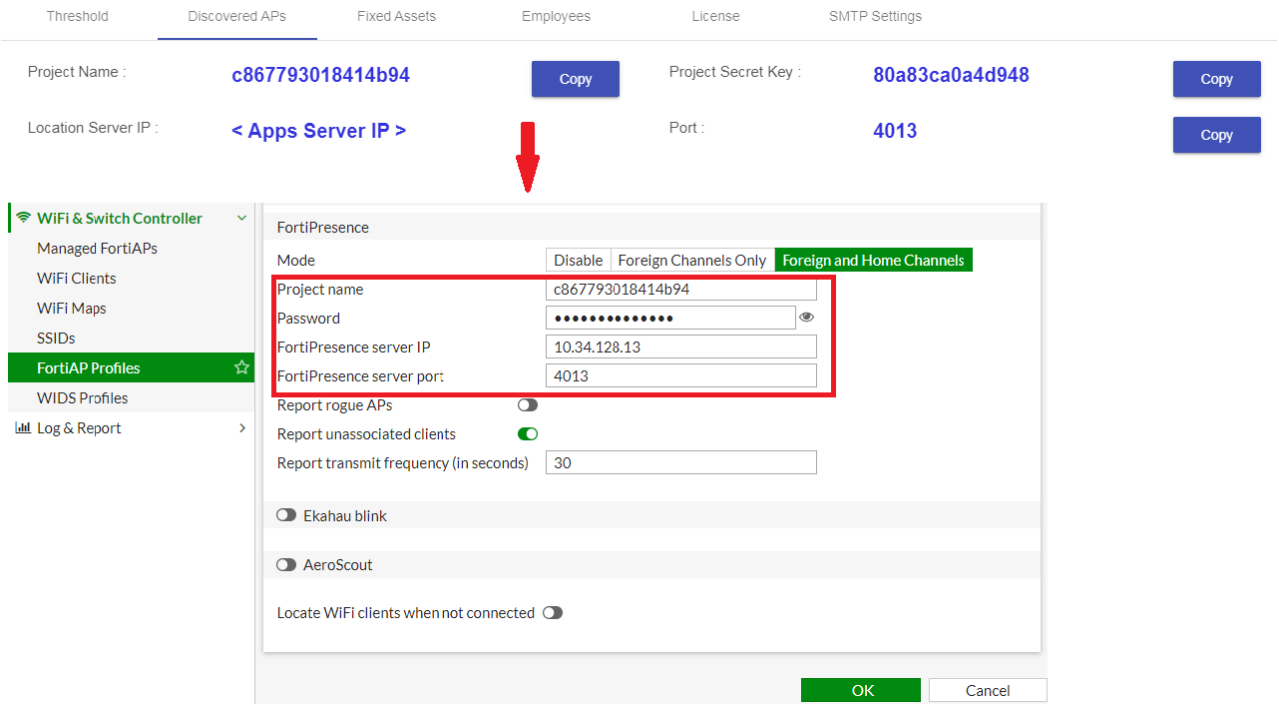


In the FortiPresence VM GUI, **Admin > Settings > Discovered APs**, refresh to view the access points discovered by FortiAPCloud.

FortiGate

Follow this procedure on the FortiPresence VM 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 VM GUI - **Admin > Settings > Discovered APs**).
5. Enter the **FortiPresence server IP** - (Application server IP address) and **FortiPresence server port** - 4013.



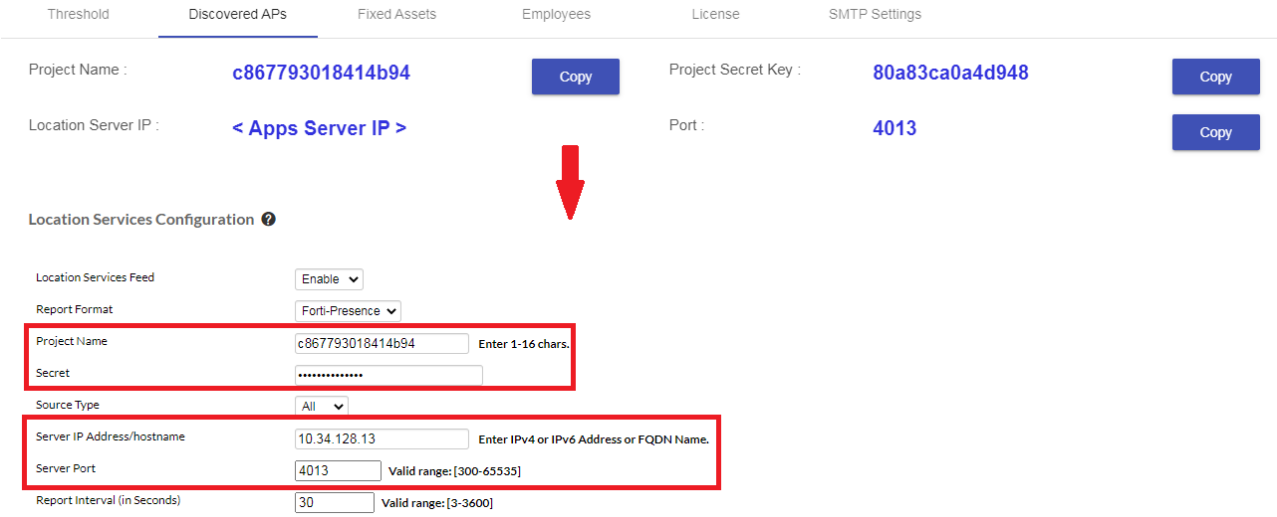
In the FortiPresence VM GUI, **Admin > Settings > Discovered APs**, refresh to view the access points discovered by FortiGate.

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

FortiWLC

Follow this procedure on the FortiPresence VM 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 VM GUI - **Admin > Settings > Discovered APs**).
4. Enter the **Server IP Address** - (Application server IP address) and **Server Port** - 4013.



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

Configuring Captive Portal

Captive Portal configurations for wireless access to visitors are to be accomplished on both FortiPresence VM and FortiGate/FortiAPCloud/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 VM GUI – **Portal > Portal Settings > RADIUS Clients**.

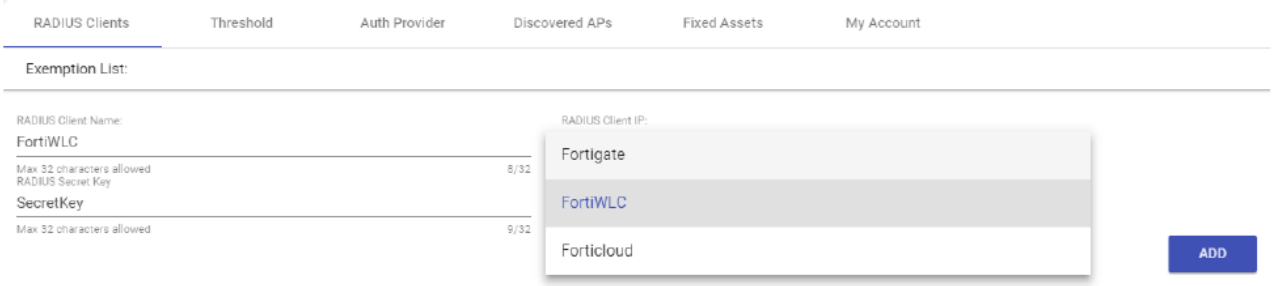
Note: The RADIUS server/FortiPresence Connect IP address is the Application server IP address. Port **1812** is used for authentication and **1813** for accounting.

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

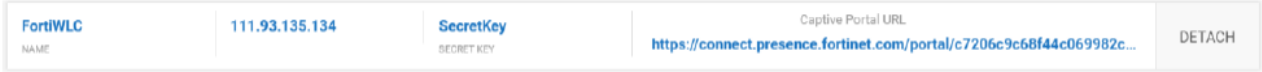
- Sites are created – See Site Management on page 40
- Portals are configured on FortiPresence VM – See Portal Management on page 45.

Follow this procedure to create RADIUS clients on FortiPresence VM.

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



   For FortiAPCloud 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 FortiAPCloud GUI.
   FortiAPCloud Global – 173.243.132.77
   FortiAPCloud Europe – 81.201.100.238
   FortiAPCloud Japan – 173.243.132.207
   Configure the **Project Secret Key** to **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 FortiAPCloud. The captive portal URL is generated.



- FortiAPCloud on page 60
- FortiGate on page 62

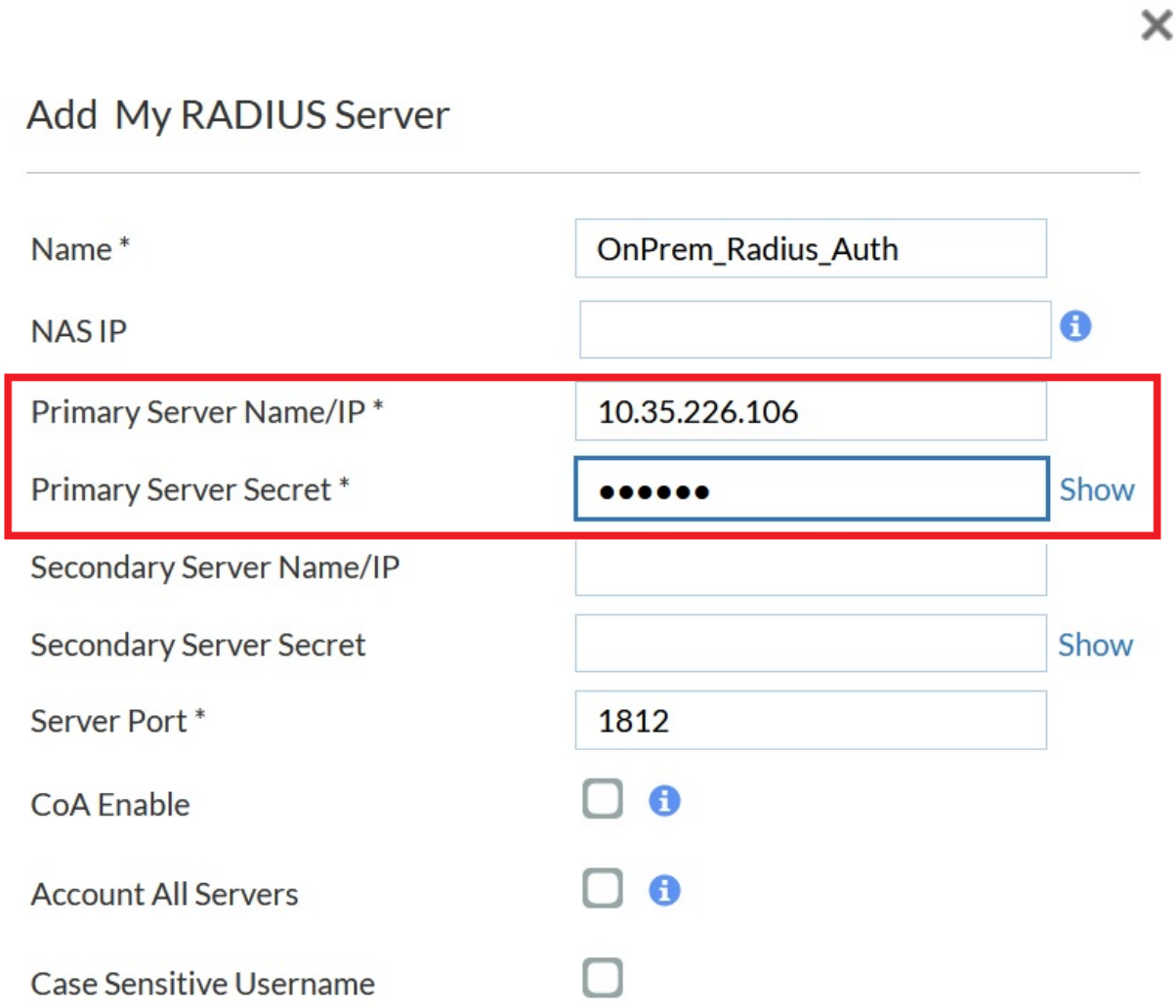
- FortiWLC on page 66

FortiAPCloud

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

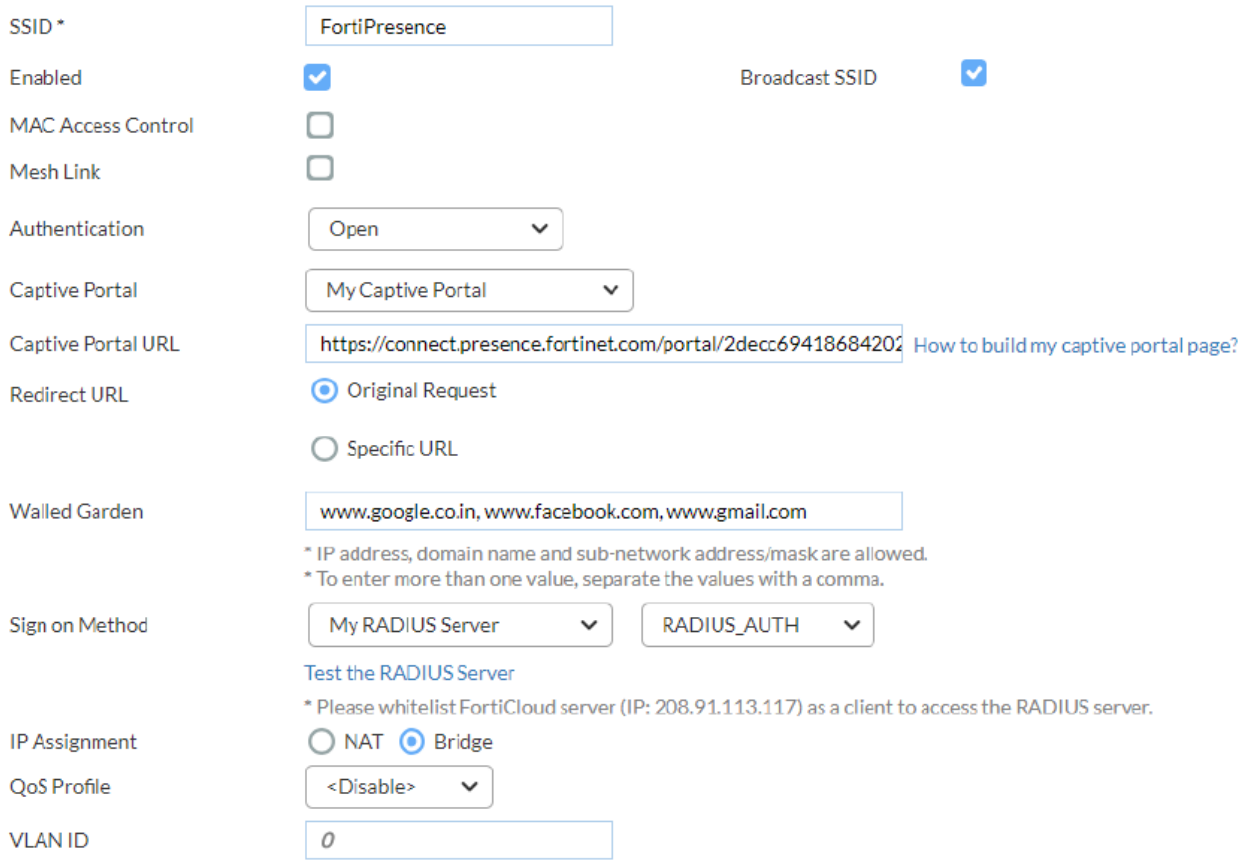
1. Select a configured AP Network and navigate to **Configure > My RADIUS Server** to configure a RADIUS profile. Click **Add My RADIUS Server**.
   Update the configuration parameters as required.
2. Enter the **Primary Server Name/IP** – (Application server IP address).
3. The **Primary Server Secret** should be the same as the **RADIUS Secret Key** configured on the FortiPresence VM 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 FortiAPCloud setups.



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 VM GUI – **Portal Management > Radius Configuration**).
5. Set the **Redirect URL** to **Specific URL** and enter *https://<FortiPresence Connect FQDN>/portal/success*. The actual redirect option can be specified while creating the portal on FortiPresence VM GUI - Adding a New portal on page 46.
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**.



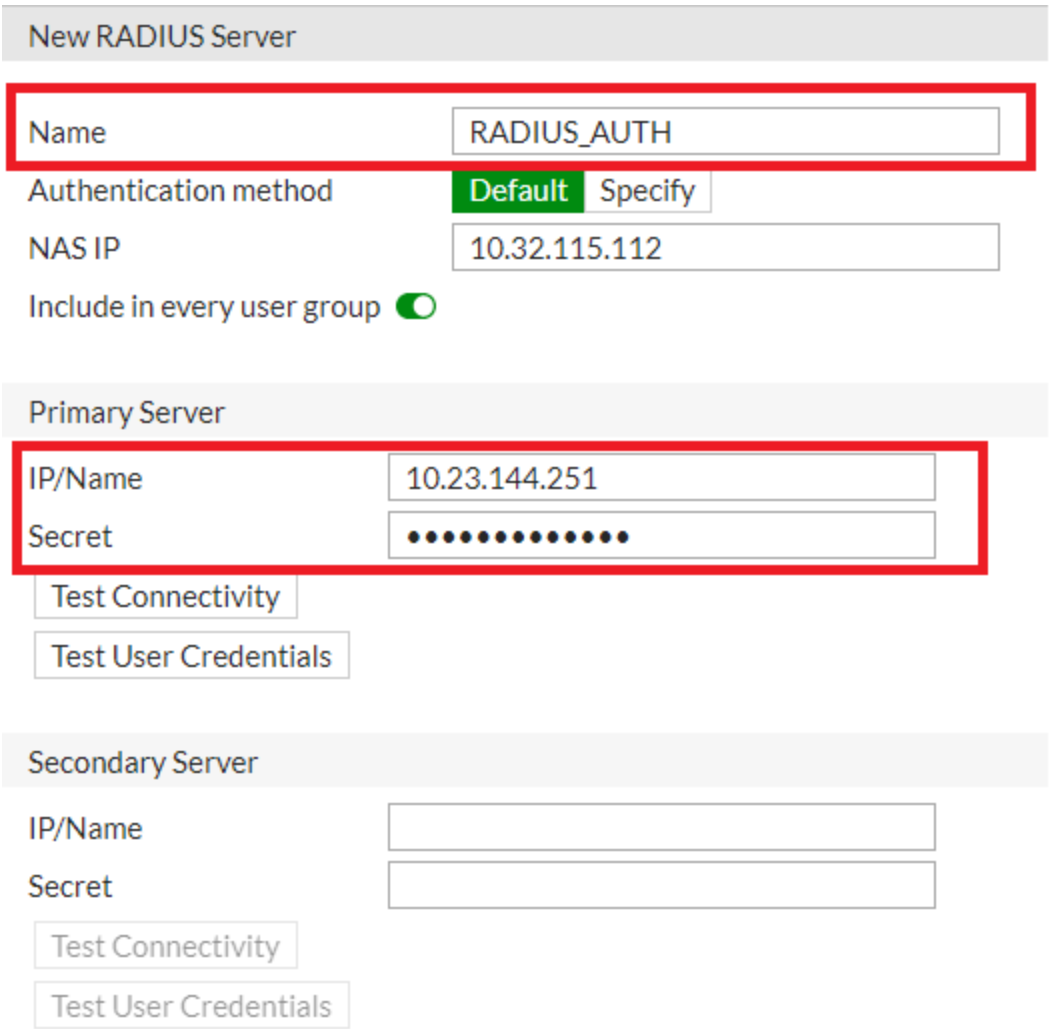
8. Click **Next** and update the configuration parameters as required. Click **Apply**.

FortiGate

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

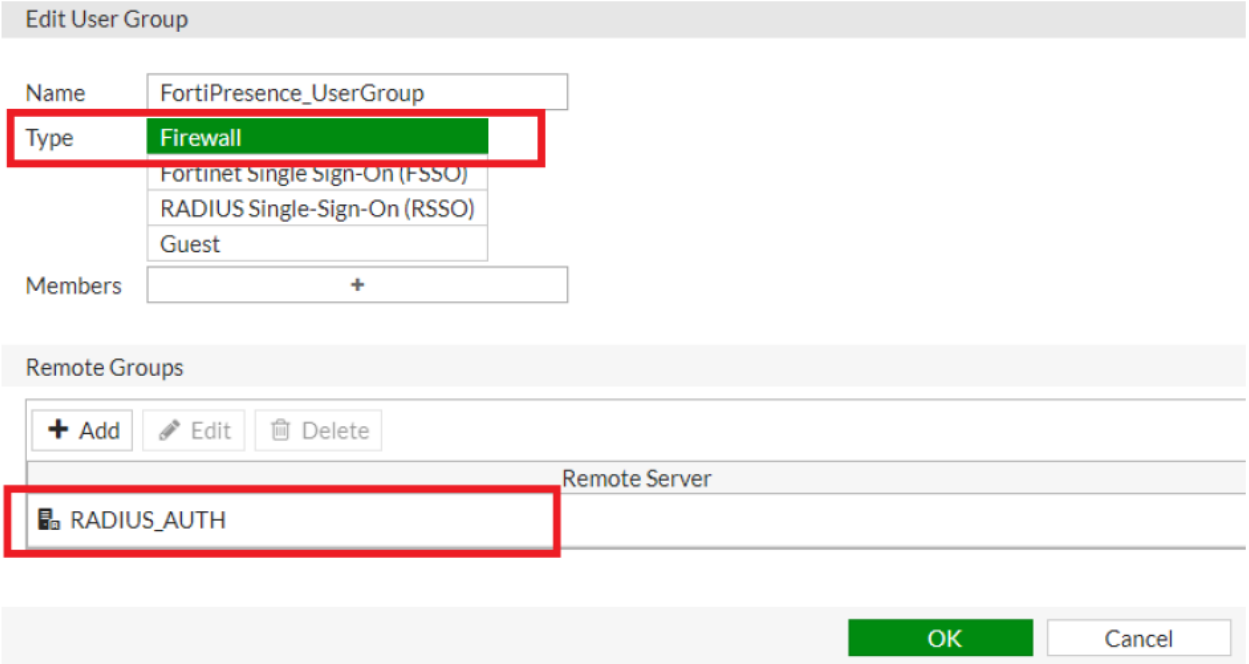
1. Navigate to **User and Device > RADIUS Servers** and create a new RADIUS server authentication profile. Select **Create New**.
2. Enter the primary RADIUS server details. The **Primary Server IP/Name** - (Application server IP address). The **Primary Server Secret** should be the same as the **RADIUS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

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

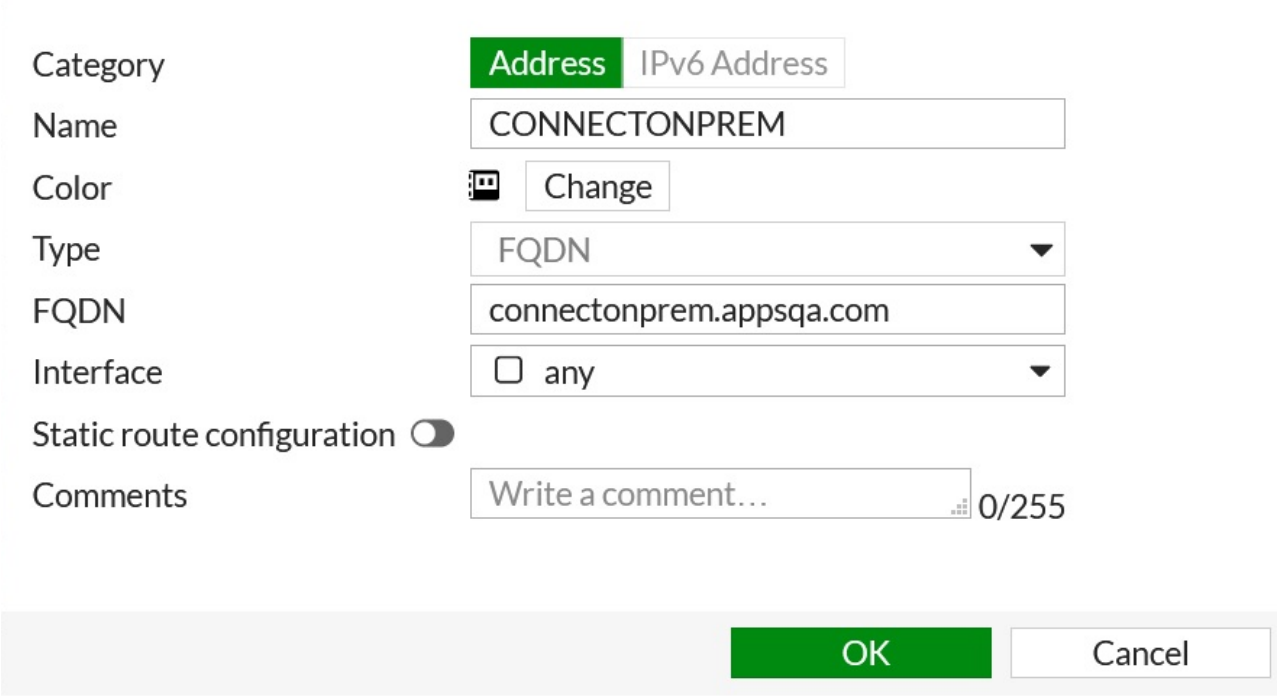


4. Configure RADIUS server accounting profile via the FortiGate CLI mode. Run the following commands in the same order.
   config user radius
   edit <RADIUS profile created in Step 2>
   config accounting-server
   edit < integer>
   set status enable
   set server <IP address of the RADIUS server>
   set secret <same as the **RADIUS Secret Key** configured on the FortiPresence VM 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**

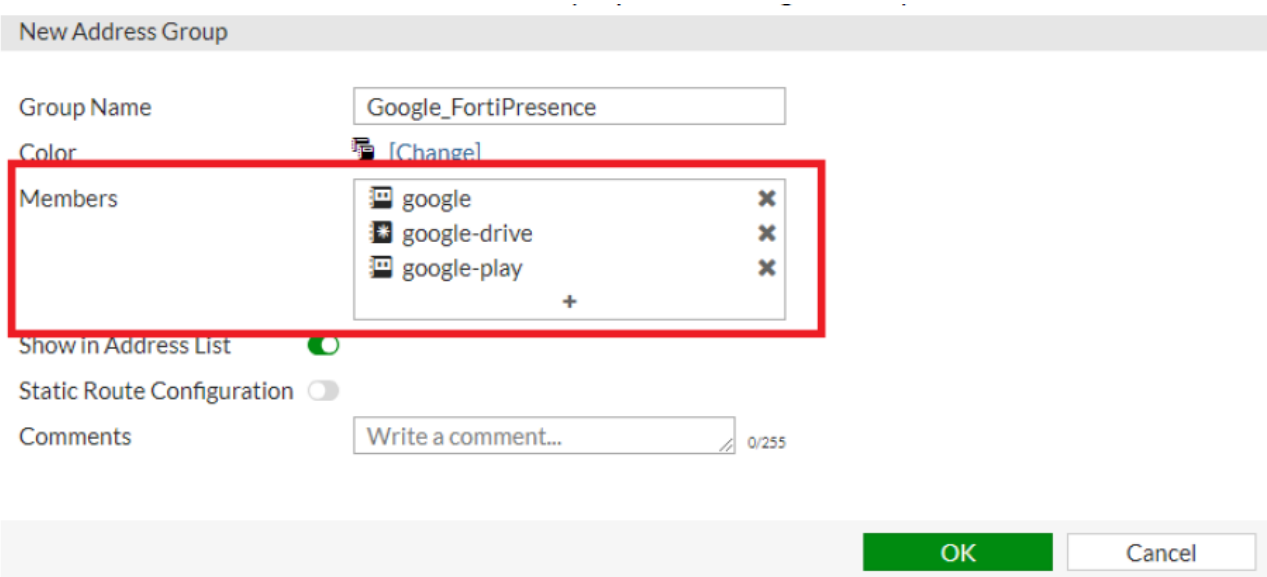
6. Click **Add** in the **Remote Groups** section and select the configured RADIUS authentication server. Click **OK**.



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**.



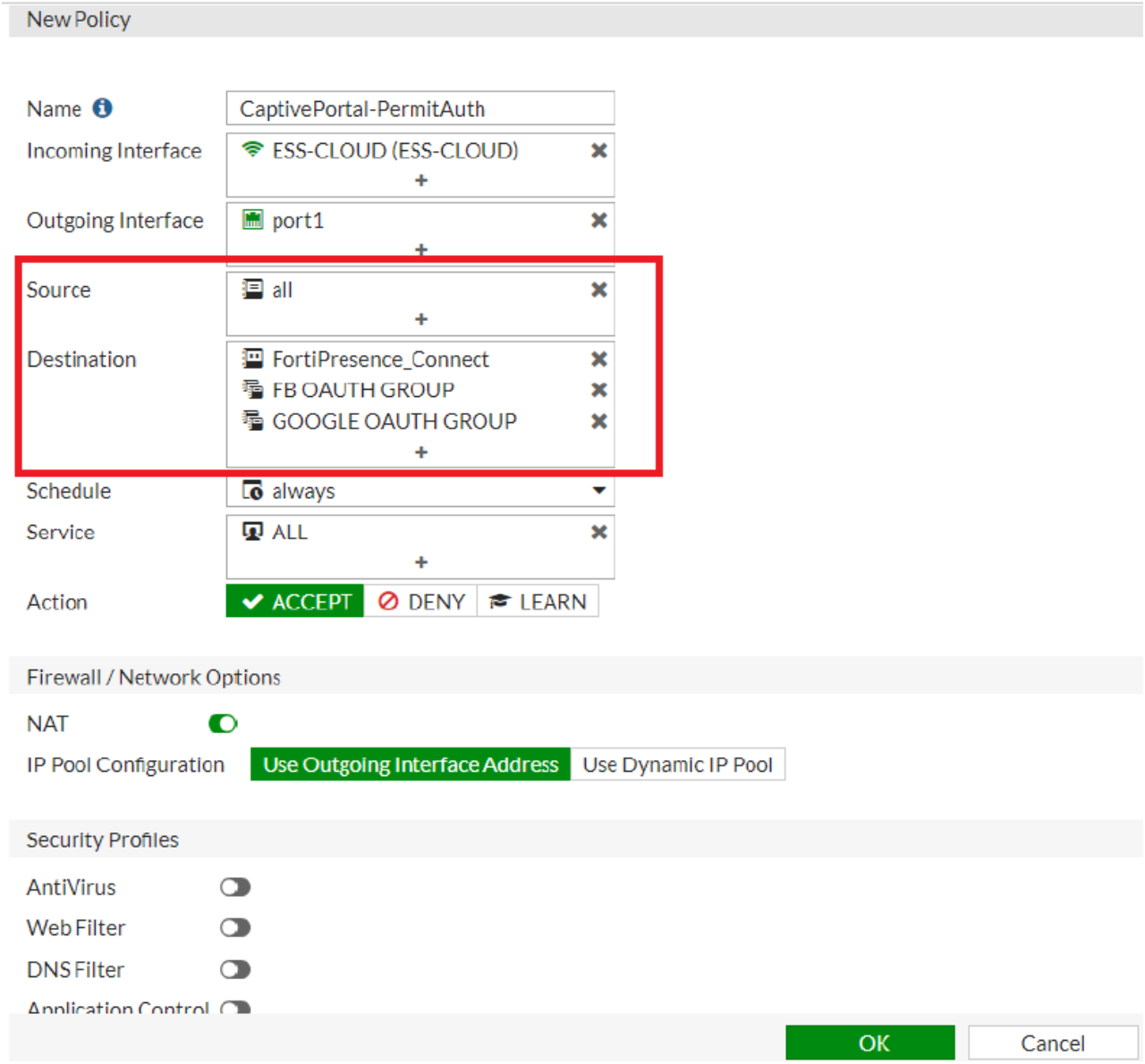
9. Repeat Steps 7 and 8 to create exclusion based addresses for all FQDNs.
10. Create address groups to easily map the individual FQDNs. Select **Create New > Address Group** and update the configuration parameters as required and populate the FQDN entries in the Members field. The FQDN entries are displayed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



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 VM 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://<FortiPresence Connect FQDN>/portal/success*. The actual redirect option can be specified while creating the portal on FortiPresence VM GUI - Adding a New portal on page 46
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.

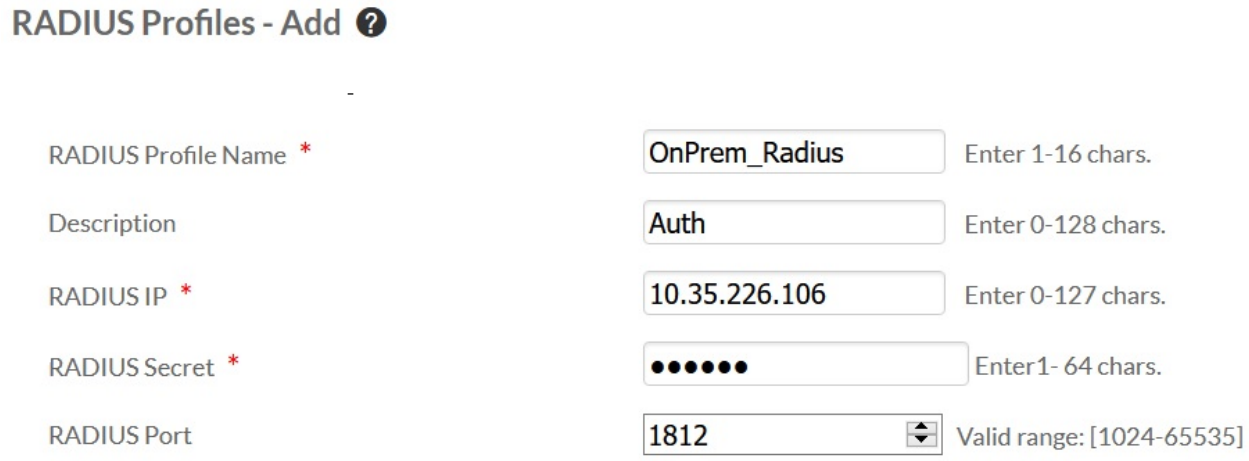


FortiWLC

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.

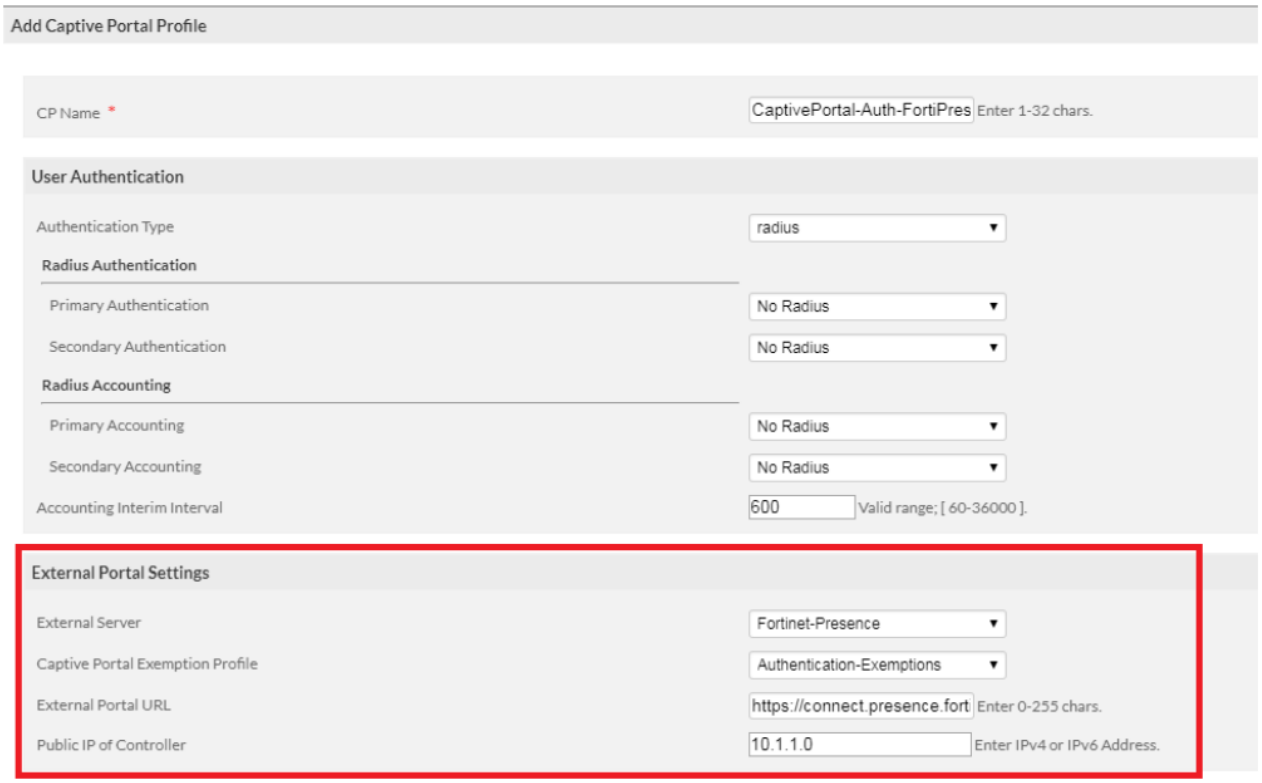
2. Enter the **RADIUS IP** - (Application server IP address), the **RADIUS Secret** should be the same as the **RADIUS Secret Key** configured on the FortiPresence VM GUI (**Portal > Portal Settings > Radius Clients**). Click **Save**.



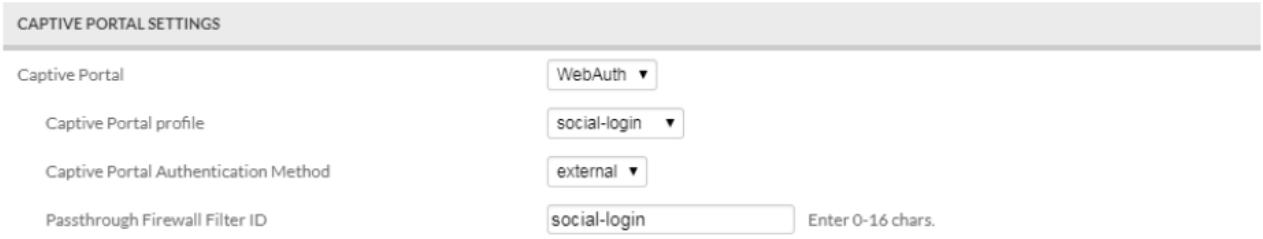
3. Navigate to **Configuration > Security > Captive Portal** and create a **Captive Portal Exemptions** profile. Click **Add** and update the configuration parameters as required. Enter the FQDN based exclusions in the **FQDN** list. Add the FQDN for FortiPresence Connect server to the exemption list.

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 VM GUI – **Portal Management > Radius Configuration**). Click **Save**.



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**.



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**.