FortiPresence
Administration Guide
Release 2.0.0
# Table of Contents

- **Overview** ................................................................. 2
- **Signing-on for FortiPresence** ........................................... 4
  - **Registering on Fortinet One** ........................................ 6
  - **Accessing FortiPresence** ............................................. 6
- **Administering FortiPresence** ........................................... 8
  - **Site Management** ..................................................... 8
  - **Portal Management** .................................................. 11
    - **Adding a Portal** .................................................... 11
    - **Configuring Portal Rules and Users** ............................ 13
    - **RADIUS Configuration** .......................................... 13
  - **Settings** ..................................................................... 14
  - **User Management** .................................................... 16
- **Configuring Location Services** ......................................... 17
  - **FortiGate** .................................................................. 18
  - **FortiCloud** .................................................................. 19
  - **FortiWLC** ................................................................... 20
- **Configuring Captive Portal** ............................................. 21
  - **FortiGate** .................................................................. 22
  - **FortiCloud** .................................................................. 27
  - **FortiWLC** ................................................................... 29
Overview

This document describes the configurations and management operations on FortiPresence, FortiCloud, 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.

This document is to be used in conjunction with the FortiPresence Getting Started Guide.

For configuration details on FortiWLC, FortiGate, and FortiCloud, see the respective product documentation.
### Signing-on for FortiPresence

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

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

Your FortiPresence account is migrated to the [https://support.fortinet.com](https://support.fortinet.com) registered email ID.
Registering on *Fortinet One*

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

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

Accessing FortiPresence

Any user registered on [https://support.fortinet.com](https://support.fortinet.com) can access FortiPresence. Once you log in to *Fortinet One*, click on your email ID, a banner with Fortinet products is displayed. Select *FortiPresence*. You are redirected to the FortiPresence GUI - [https://presence.fortinet.com](https://presence.fortinet.com).
Notes:

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

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

OR

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

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

Enter Building Details

<table>
<thead>
<tr>
<th>Building1</th>
<th>Max 32 characters allowed</th>
<th>6/32</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerAB</td>
<td>Max 64 characters allowed</td>
<td>10/64</td>
</tr>
</tbody>
</table>

Enter New Site Details:

<table>
<thead>
<tr>
<th>MySite</th>
<th>Max 32 characters allowed</th>
<th>6/32</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomerSite</td>
<td>Max 64 characters allowed</td>
<td>12/64</td>
</tr>
</tbody>
</table>

Save      Cancel

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. 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.

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

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

**NOTE:**

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

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

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

Adding a Portal

1. Navigate to Admin > Portal Management > Portal and select the site for which the portal is to be created. Click Add Portal.
2. Enter a unique Portal Name for your site and a Description.
3. Upload your Company Logo and a Background Image. Images in the JPG, GIF, and PNG format are supported.
4. Enter the acceptable usage policy for the visitors of your establishment/site and select Show Policy to prompt users to accept the policy prior to logging in.
5. Select the supported/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 or Google credentials.
   - If you do not select any of the above options, the portal authenticates the visitor without any credentials.
6. 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.
7. Click **Save**.

The portals created can be edited and deleted.

**Note**: For paid tier users, FortiPresence displays the visitors’ e-mail address, mobile number, age, and gender on the portal login pages on their devices.
**Configuring Portal Rules and Users**

Navigate to Admin > Portal Management > Portal Rules to configure rules for the portals. A default portal rule is created when the first portal is created. Multiple rules can be added as and when portals are created. The portal rules are applied per site and can be reordered as per priority.

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

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

**RADIUS Configuration**

Navigate to Admin > Portal Management > RADIUS Configuration to attach the configured RADIUS clients (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 FortiCloud/ FortiGate/ FortiWLC. See [Configuring Captive Portal](#).
## Settings

This section describes some additional FortiPresence settings.

Navigate to Admin > Settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Clients</strong></td>
<td>Configure FortiCloud/FortiGate/ FortiWLC as RADIUS clients for portal authentication. The list of exempted FQDNs for FortiCloud, FortiGate, and FortiWLC are displayed here. See Configuring Captive Portal. Note: You can edit and delete the RADIUS clients.</td>
</tr>
<tr>
<td><strong>Threshold</strong></td>
<td>Select the sites for which to apply thresholds. <strong>Bounce Time Limit</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Dwell Inactive Time Limit</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Current View Time</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Min Count of Observations</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Organisational Unique Identifier (OUI)</strong> – When enabled, this setting filters out the non OUI MAC Addresses and is applicable for all the dashboards.</td>
</tr>
<tr>
<td><strong>Auth Provider</strong></td>
<td>The authentication provider settings enable you to configure the credentials derived from the Facebook and</td>
</tr>
<tr>
<td>Google applications that you use for portal authentication.</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Discovered APs</td>
<td>Unique project name and secret key is generated for each account on FortiPresence. These are used to configure location services on FortiCloud/ FortiGate/FortiWLC. The AP name, MAC address, timestamp, planning status, location, and state <em>(Active</em> (identification of packets received in the last 24 hours) or <em>Inactive</em> (no identification of packets received in the last 24 hours)) are displayed. The Location server IP and port are also displayed here. The APs with location services enabled are displayed here. See Configuring Location Services.</td>
</tr>
<tr>
<td>Fixed Assets</td>
<td>Add manually or upload in a .csv format 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.</td>
</tr>
<tr>
<td>My Account</td>
<td>Configure your FortiPresence account credentials. Upload the login and logout files, so that FortiWLC redirects to these FortiPresence pages and not display/bring up its own login and logout pages.</td>
</tr>
</tbody>
</table>
User Management

This feature is available only for paid tier users.

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

1. Navigate to Admin > User Management and enter a unique First Name, Last Name, and Email ID for each user. Ensure that the account you create here is also registered on Fortinet One. For more information on account management see Notes on RBAC users.

2. Assign each user with either Admin or User roles. The User role is allowed only view access for dashboards and reports. The Admin role is allowed to perform administrative operations on the FortiPresence GUI.

3. Click Add User.

4. Click Change Password to assign a new unique password to the user account.

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

To delete a user, click the delete icon against the specific user.
Configuring Location Services

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

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

The project name and secret key are required to be configured on FortiGate/FortiCloud/FortiWLC to enable Location Services. The location services are configured with location server IP address 34.245.252.61/location.presence.fortinet.com and server port 4013.
Follow this procedure on the FortiPresence and FortiGate GUIs to enable and configure location services.

1. On the FortiGate GUI navigate to WiFi and Switch Controller > FortiAP Profiles.
2. Select and double-click a specific FortiAP profile, scroll down to the FortiPresence section.
3. Enable Location Services; configure the mode as **Foreign Channels Only/Foreign and Home Channels**.
4. Enter the **Project name** and **Password**, (Project Name and Project Secret Key respectively copied from the FortiPresence GUI - Admin > Settings > Discovered APs).
5. Enter the **FortiPresence server IP** - 34.245.252.61 and **FortiPresence server port** - 4013, (Location Server IP and Port are displayed in the FortiPresence GUI - Admin > Settings > Discovered APs).

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

**Note:**
Repeat this procedure for every FortiAP profile in case you have multiple profiles.
FortiCloud
Follow this procedure on the FortiPresence and FortiCloud GUIs to enable and configure location services.

1. On the FortiCloud GUI select a configured AP Network and navigate to Configure > FortiPresence.
2. Enable Location Services; configure the mode as Foreign Channels Only /Foreign and Home Channels.
3. Enter the Location Server IP Address - 34.245.252.61 and UDP Listening Port - 4013, (Location Server IP and Port are displayed in the FortiPresence GUI - Admin > Settings > Discovered APs).
4. Enter the Project Name and Secret Password, (Project Name and Project Secret Key respectively copied from the FortiPresence GUI - Admin > Settings > Discovered APs).

Note:
Configure the Project Secret Key to fortipresence for all FortiCloud setups.

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

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

1. On the FortiWLC GUI navigate to **Configuration > Devices > Location Services**.
2. Enable **Location Services Feed**; configure the **Report Format** as **FortiPresence**.
3. Enter the **Project Name** and **Secret**, (**Project Name** and **Project Secret Key** respectively copied from the FortiPresence GUI - **Admin > Settings > Discovered APs**).
4. Enter the **Server IP Address** - **34.245.252.61** and **Server Port** - **4013**, (**Location Server IP** and **Port** are displayed in the FortiPresence GUI - **Admin > Settings > Discovered APs**).

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

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

The RADIUS profiles are configured with RADIUS server IP address 34.245.252.61/radius.presence.fortinet.com and server port 4031.

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

- Sites are created – See Site Management.
- Portals are configured on FortiPresence – See Portal Management.

Follow this procedure to create RADIUS clients on FortiPresence.

1. On the FortiPresence GUI navigate to Admin > Settings > Radius Clients to create a RADIUS client for the public IP address of the FortiCloud.

2. Enter the RADIUS Client Name, RADIUS Client IP, RADIUS Secret Key, and select the Device Type as FortiGate/FortiCloud/FortiWLC. Click Add.

   For FortiCloud 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 FortiCloud GUI.
     - FortiapCloud Global – 173.243.132.77
     - FortiapCloud Europe – 81.201.100.238
   - 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 FortiCloud.

The captive portal URL is generated.
FortiGate

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

1. Navigate to User and Device > RADIUS Servers and create a new RADIUS server authentication profile. Select Create New.

2. Enter the primary RADIUS server details. The Primary Server IP/Name - 34.245.252.61/ radius.presence.fortinet.com. The Primary Server Secret should be the same as the RADIUS Secret Key configured on the FortiPresence GUI (Admin > 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.
   a. config user radius
   b. edit <RADIUS profile created in Step 2>
   c. config accounting-server
   d. edit < integer>
   e. set status enable
   f. set server <IP address of the RADIUS server>
   g. set secret <same as the RADIUS Secret Key configured on the FortiPresence GUI (Admin > 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 New and update the configuration parameters. Select Firewall as the Type of the user group.
6. Click **Add** in the **Remote Groups** section and select the configured RADIUS authentication server. Click **OK**.

   ![Remote Group Configuration](image1.png)

7. Navigate to **Policy and Objects > Addresses** to create individual addresses for exemption FQDNs. Select **Create New > Addresses** and update the configuration parameters as required.

8. Select **Type** as **FQDN** and enter the exempt FQDN. Click **OK**.

   ![New Address Configuration](image2.png)

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.

![Address Group Members](image)

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

11. Navigate to WiFi and Switch Controller > SSID to create an SSID. Click Create New > SSID and update the configuration parameters as required.
12. Select the **Security Mode** as **Captive Portal** and the **Authentication Portal** type as **External**.
13. Enter the **Authentication Portal**, (Captive Portal URL copied from the FortiPresence GUI – Portal Management > Radius Configuration) and select the created **User Group**.
14. Select the address groups created for exempted FQDNs in **Exempt Destination/Services**. Click **OK**.
16. Navigate to Policy & Objects > IPv4 Policy to configure Firewall policies. Select **Create New**.
   You are required to create the following three Firewall policies:
   - Policy to allow access to the DHCP and DNS services before authentication.
   - Policy to allow access to the exempted FQDNs for authentication.
   - 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.
FortiCloud

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

1. Select a configured AP Network and navigate to Configure > My RADIUS Server to configure a RADIUS profile. Click Add My RADIUS Server.

   Update the configuration parameters as required.

2. Enter the Primary Server Name/IP – 34.245.252.61/radius.presence.fortinet.com.

3. The Primary Server Secret should be the same as the RADIUS Secret Key configured on the FortiPresence GUI (Admin > Settings > Radius Clients). Click Apply and update the configuration parameters as required.

   **Note:**
   Configure the Project Secret Key to fortipresence for all FortiCloud setups.


5. Set the Redirect URL to Specific URL and enter https://connect.presence.fortinet.com/portal/success. The actual redirect option can be specified while creating the portal on FortiPresence GUI - Adding a Portal.

6. Enter the FQDN based exclusions in the Walled Garden list. A comma separated list with character limitation is supported.
7. Select **My RADIUS Server** and specify the RADIUS profile created earlier in this procedure as the **Sign on Method**.

   - **SSID**: FortIPresence
   - **Enabled**: Checked
   - **Broadcast SSID**: Checked
   - **MAC Access Control**: Not checked
   - **Mesh Link**: Not checked
   - **Authentication**: Open
   - **Captive Portal**: My Captive Portal
   - **Captive Portal URL**: https://connect.presence.fortinet.com/portal/2decc6941868a4205
   - **Redirect URL**: Original Request
   - **Sign on Method**: My RADIUS Server
   - **Test the RADIUS Server**: Untitled
   - **IP Assignment**: NAT, Bridge
   - **QoS Profile**: <Disable>
   - **VLAN ID**: 0

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

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

5. **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.

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

   ![RADIUS Profile Configuration](image)

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

   ![Add Captive Portal Exemptions](image)

8. **Create a Captive Portal profile. Click Add and in User Authentication enter the RADIUS profiles created for authentication and accounting.**

9. **Configure the External Portal Settings, Select Fortinet-Presence as the External Server.**

10. **Select the Captive Portal Exemption Profile created in Step 7 enter the Captive Portal URL, (Captive Portal URL copied from the FortiPresence GUI – Portal Management > Radius**
11. Navigate to Configuration > Security > Profile. Click Add and update the configuration parameters as required.

12. 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.

13. Enter the Captive Portal profile name as the Passthrough Firewall Filter ID. Click Save.

14. Navigate to Configuration > Wireless > ESS to create an ESS profile. Click Add and update the configuration parameters as required.

15. Select the Security Profile created in Step 10. Click Save.
Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.