ECW7210-L

Enterprise Cloud Based Indoor Access Point

User Guide

www.edge-core.com

Contents

Overview

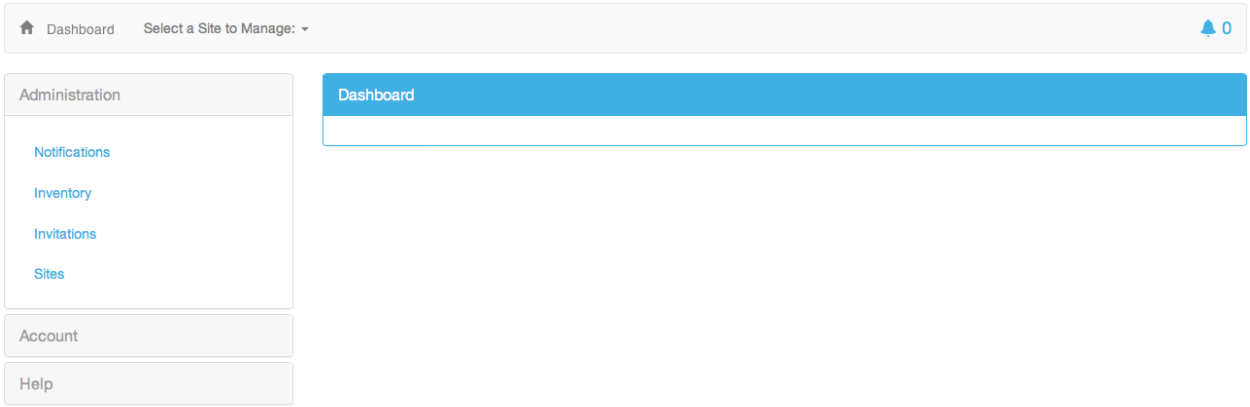
Welcome to Tallac Networks. This user guide will get you acquainted with the Tallac Cloud System where you can setup and manage your Wi-Fi networks. Let's start with a few key terms:

- **Tallac Cloud Service**
  - This is where you setup and manage your Wi-Fi networks. Access the Tallac Cloud Service through the web interface at **https://cloud.tallac.com**.
  - **In addition to the web interface, the cloud service also provides an API, or application programming interface, where software from simple scripts to complex business solutions can interact with your network. Through a network of expert partners Tallac can assist you in developing tailored solutions for your business.**
- **Access Point**
  - **An access point or AP is a device with radio hardware to broadcast a Wi-Fi service (SSID). This is the device that allows users to wirelessly connect to your network. Depending on the location size and configuration, multiple APs may be required for proper wireless coverage.**
- **Site**
  - **A site is a set of access points that share a common configuration. A site might be one physical location with one or more access points, or multiple physical locations with access points that all share the same configuration.**
- **User Roles**
  - **Managed Service Provider (MSP)**
    - The MSP is the user or company that provides fully managed network services to their customers. This is the main administrative account on the cloud service. MSPs have the ability to create additional sites and to create user accounts, known as **operators**, for their customers.
  - **Operators**
    - User accounts on the cloud service with restricted permissions allowing for self service and self provisioning of customer portals.

Getting Started

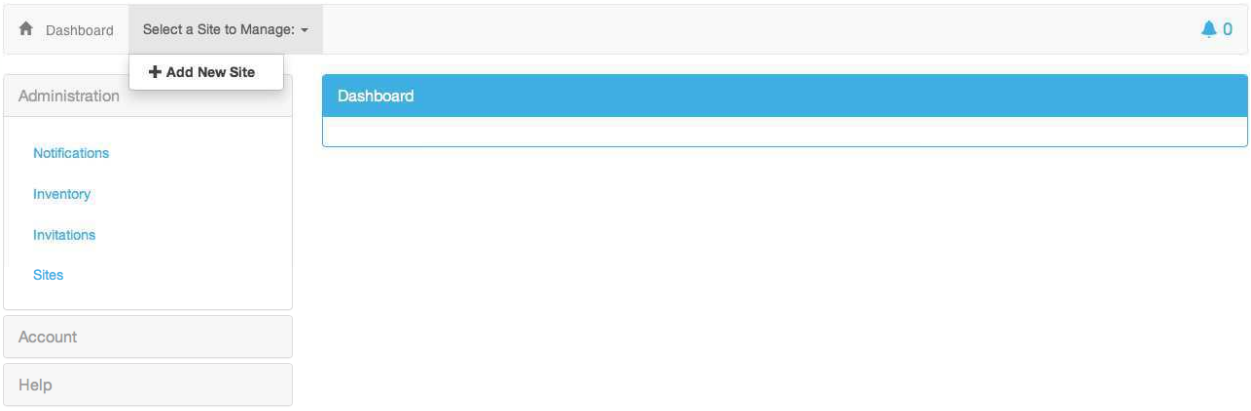
Tallac Network Systems are managed through the Tallac Cloud Services Platform, which can be accessed with a web browser at **https://cloud.tallac.com**. Login with your credentials or click Join our Trial for a free trial.

After entering your credentials, you will get forwarded to the dashboard window, showing you an overview of the resources associated with your account.



To get started you need to create a site. A **site** is a set of access points that share a common configuration. A site might be one physical location with one or more access points, or multiple physical locations with access points that all share the same configuration.

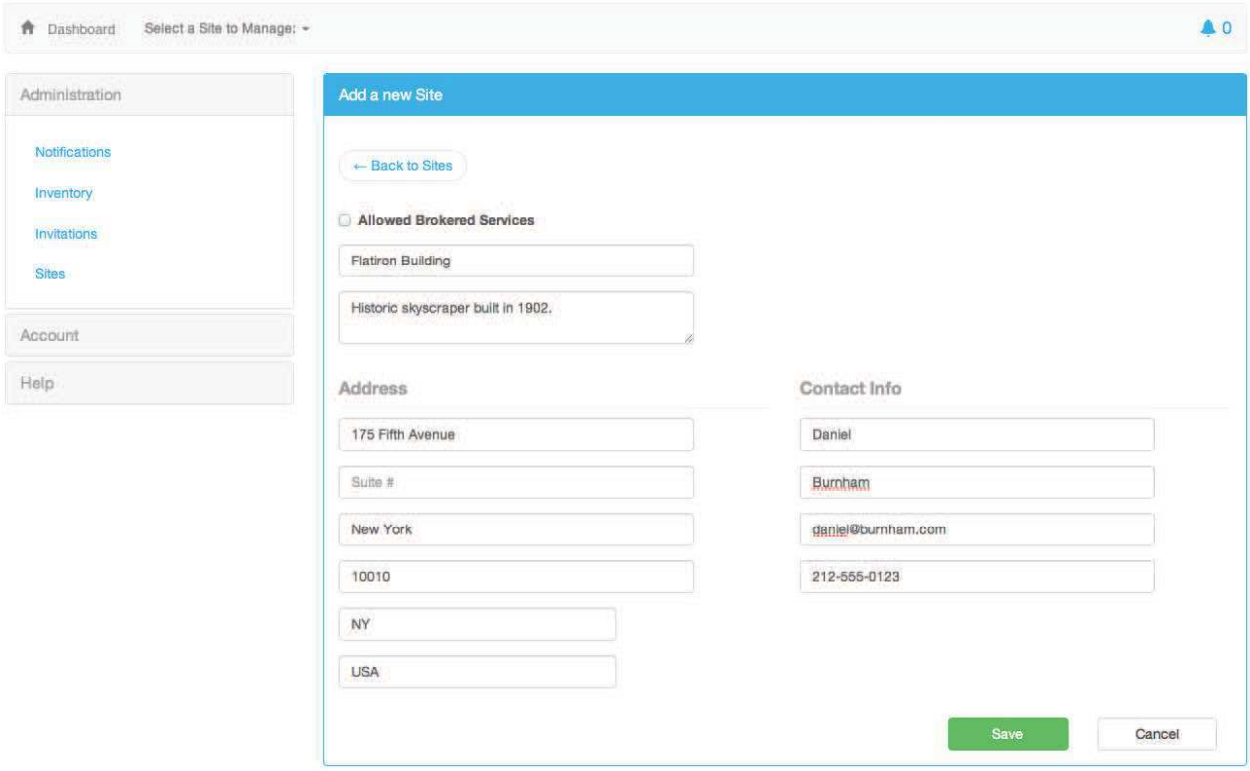
On the top-left is the **Select a Site to Manage** menu, which contains the **Add New Site** button.



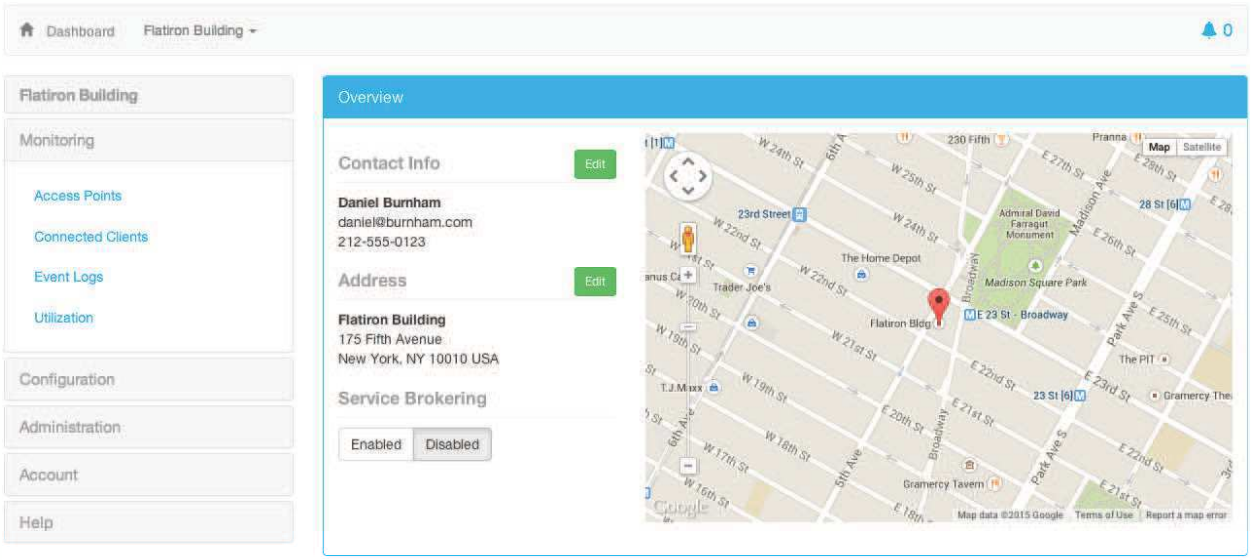
When creating a site, you will be asked for the following basic information:

- **Site Name & Description**: Information about the site
- **Address**: The location of the site.
- **Contact Info**: Contact information for the site.

The address and contact information for the site will be used as default shipping information in the event of additional hardware orders.



After entering the needed information and saving, you will see the site overview window showing the site you just created.



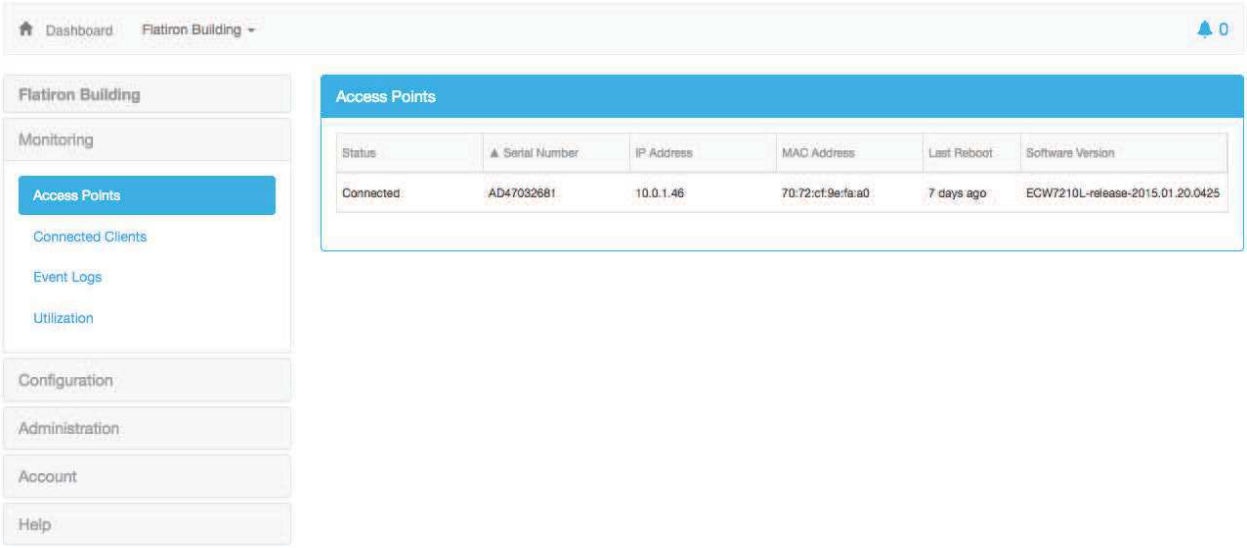
Your site can now be managed through the site menu tabs on the left side. The tabs for this site include **Monitoring**, **Configuration**, and **Administration**. There are also tabs for your **Account** and **Help**. This guide will go through the tabs in order, but if you want to create a Wireless Service (SSID) now, jump ahead to the **Configuration** Tab. To order APs or invite operators to manage sites see the **Administration** tab.

Monitoring

Monitoring allows you to get detailed information about the current selected site including access points, event logs, connected clients, and utilization. You can change the selected site with the site select menu at the top of the screen.

Monitoring ▸ Access Points

The Access Points page displays a list of APs available at this site.



The following information is available for each access point:

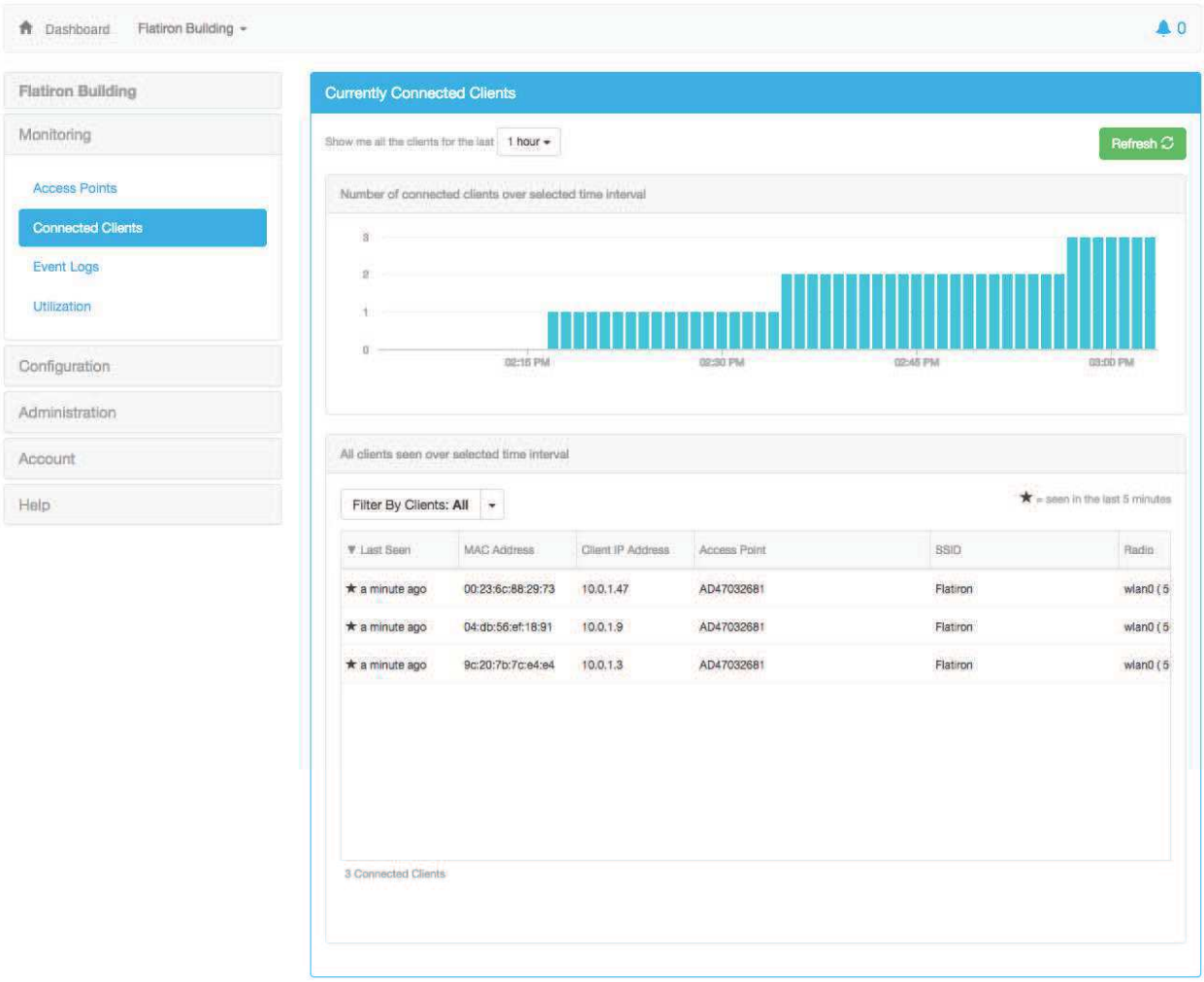
- Status
  - *Connected* if the AP is currently registered with the cloud service; *Disconnected* otherwise.
- Serial Number
  - The serial number of the access point.
- IP Address
  - The IP address seen at the last registration of the access point.
- MAC Address
  - The MAC address of the eth0 interface.
- Last Reboot
  - The duration since the last reboot of the access point.
- Software Version
  - The current firmware version of the access point.

Clicking on an AP will display the following tabs:

- Status
  - Displays the current AP connection status.
  - Displays the date and time of the last reboot and allows you to reboot the device.
    - Note that rebooting a device is a serious operation that will result in all connected clients experiencing a momentary loss of connectivity. Rebooting takes about 2 minutes.
  - Displays whether the AP is connected to the Tallac Management VPN. The Management VPN provides a direct connection to the AP, even if the AP is behind a NAT.
- Info
  - Displays the AP info including site, serial number, IP address, VPN IP address, software version, short name, and description.
  - The short name and description can be modified by clicking on the Edit button.
  - Clicking download diagnostics will download a diagnostic archive from the device.
- Radio Settings
  - This tab allows you to view and edit radio settings including status, band, mode, channel, power, and bandwidth for the available radios.
  - A note on channel options:
    - For 2.4GHZ, the options are auto, 1, 2, ... 11. We strongly recommend only using the channels 1, 6 and 11; all other channels overlap with these and may massively impede stability and performance. For more information see http://en.wikipedia.org/wiki/List_of_WLAN_channels.
    - For 5GHZ, the channels are auto or 36, 40, 44, 48, 149, 153, 157, 161
- Logs
  - Provides access to AP log entries.
  - Log entries can be filtered by
    - recent time range or custom date range.
    - MAC address (of client). The MAC address should be entered in the format 01:02:03:04:05:06. Click the refresh button to update the results.
    - search term.
  - Also, the following buttons are available:
    - **Copy** selected entries to the clipboard.
    - **Toggle** selected entries.
    - **Download as CSV** the selected log entries.
    - **Refresh** the displayed entries.
- Clients
  - Displays the total number of connected clients over various time windows.
  - Note: Hovering over the graph will display detailed information for that time slice.
- Usage
  - View average usage over time per vNet
    - Note: Hovering over the graph will display detailed information for that time slice.
  - View average radio usage (Tx + Rx) over time for each radio

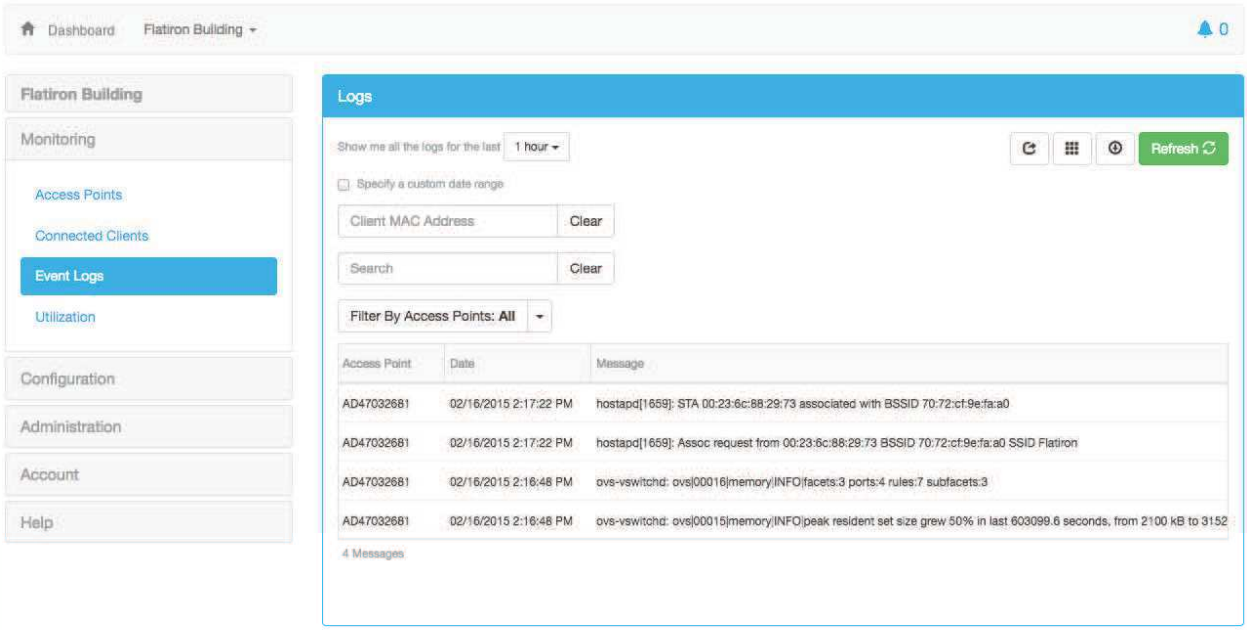
Monitoring ▸ Connected Clients

The Connected Clients page shows a time based graph giving you the number of clients connected at the site. You can zoom in and out as needed by changing the timeframe to view the number of connected clients at the top. Below the graph of connected clients is a list of the actual clients at the site. Clicking on an individual client will open a window that displays further detail about the particular client such as which AP they are connected to, the IP address, last known signal strength and frequency they are using.



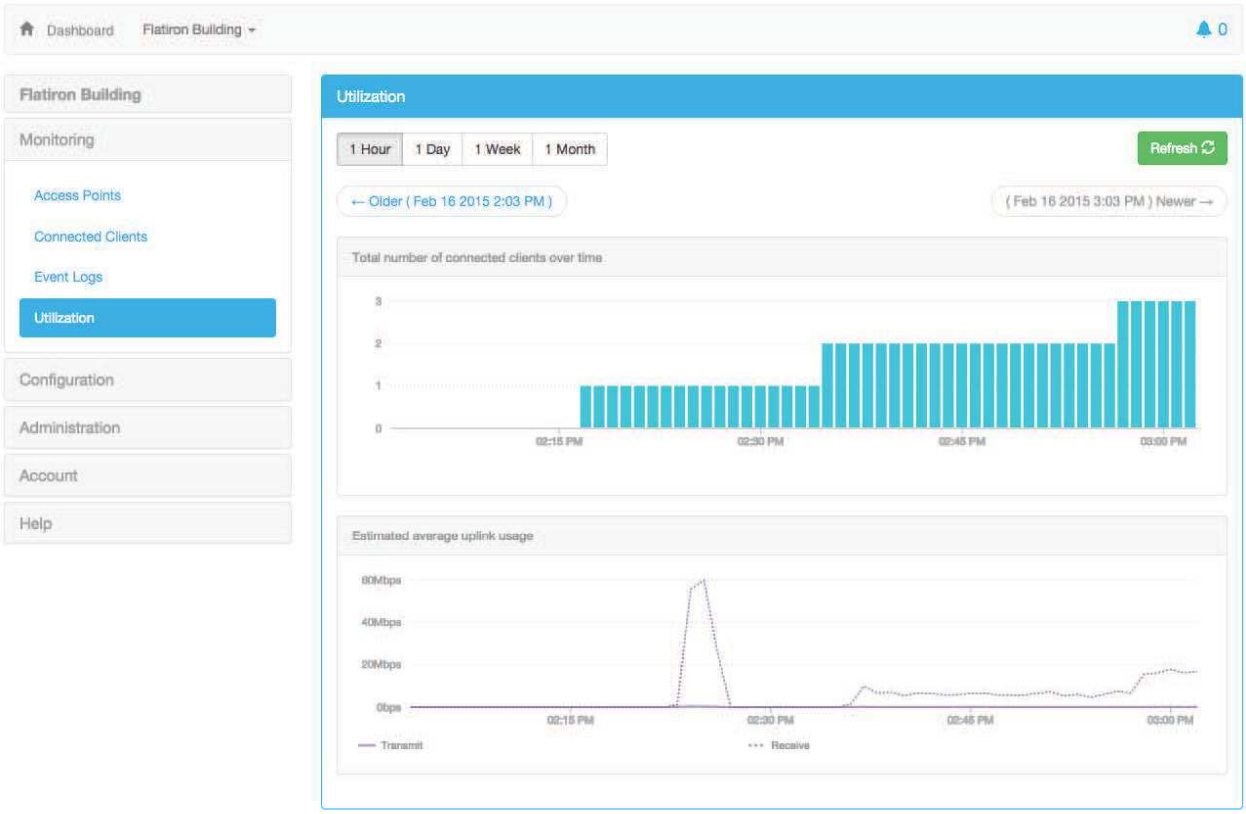
Monitoring ▸ Event Logs

The Event Logs page shows the aggregated event logs from all devices at this site. It is possible to filter the event log by time, AP, client or search term.



Monitoring ▸ Utilization:

The Utilization page shows the total number of connect clients over various time intervals and the estimated average uplink usage in Mbps.

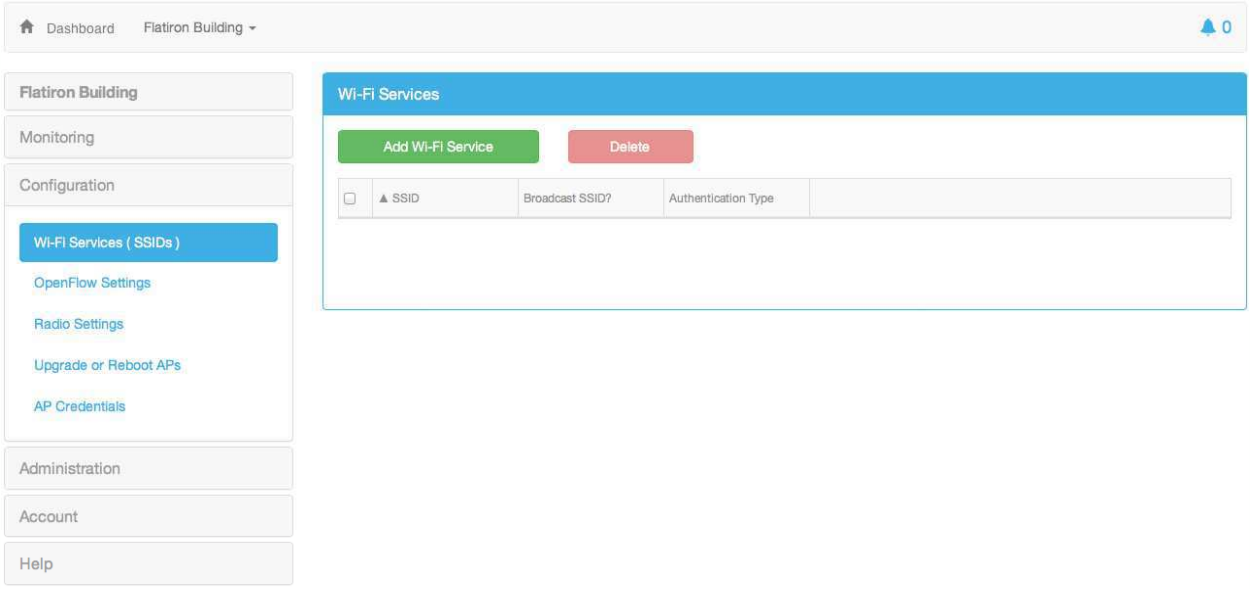


Configuration

The configuration tab allows you to define a Wi-Fi service and other site specific options.

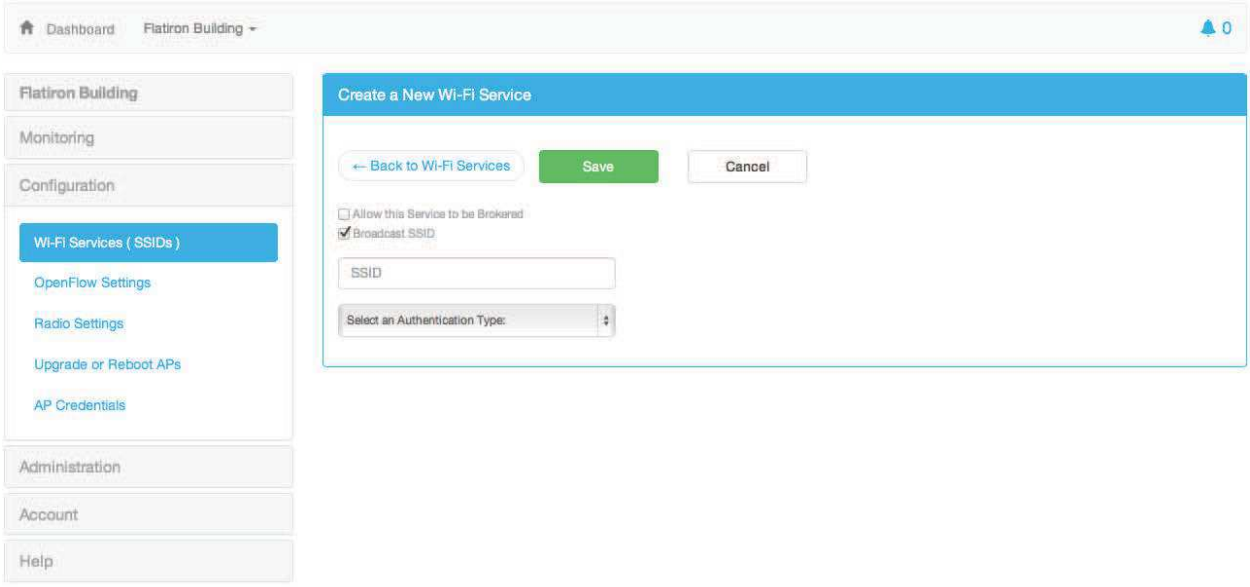
Configuration ▸ Wi-Fi Services (SSIDs)

The Wi-Fi Services (SSIDs) page displays the list of defined SSIDs and allows you to create a new Wi-Fi network. You can add and remove Wi-Fi services (SSIDs) from here as well as check configuration settings such as the password for the selected service. By selecting an existing Wi-Fi service you can see more detailed information about the wireless network. If no Wi-Fi services have been created yet, the list will be empty.



To create your first Wi-Fi service (SSID), click on the **Add Wi-Fi Service** button.

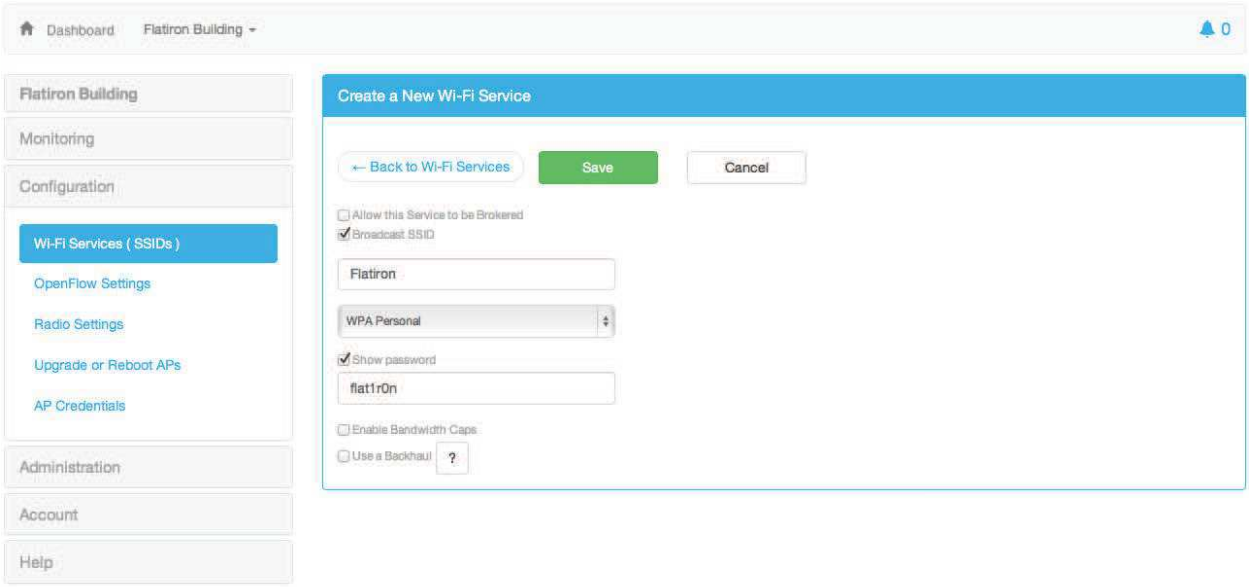
This opens a screen that allows you to enter configuration details for the network.



Enter an SSID for the service and select an **Authentication Type**. The following authentication type options are available:

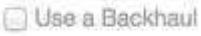
- **Open**
  - No authentication required. Anyone will be able to connect to this network without a password.
- **WPA Personal**
  - Appropriate for home and small office networks, WPA Personal or pre-shared key mode does not require an authentication server. Each user connects to the network using the same password.
- **WPA Enterprise**
  - Appropriate for enterprise networks, WPA Enterprise requires a RADIUS authentication server. Each user connects to the network by authentication with the RADIUS server.
- **Captive Portal**
  - A captive portal is a dedicated web page a user must visit before obtaining network access. Typically the portal presents a login page where users can enter authentication information, payment information, etc.

Once you select an authentication type, additional security configuration options will appear. For example, if you select WPA Personal, you will need to specify a password.



You have the option to **Enable Bandwidth Caps** for this SSID. Checking this box will display a form where you can specify distinct caps for upload and download bandwidth ranging from 64Kbps to 10 Gbps.

You also have the option to have this Wi-Fi service use a backhaul.



A **backhaul** connects your Wi-Fi wireless LAN to another physical or virtual network. If no backhaul is selected, your Wi-Fi wireless LAN will be connected to the default Ethernet port of the access point. The following backhaul types are supported:

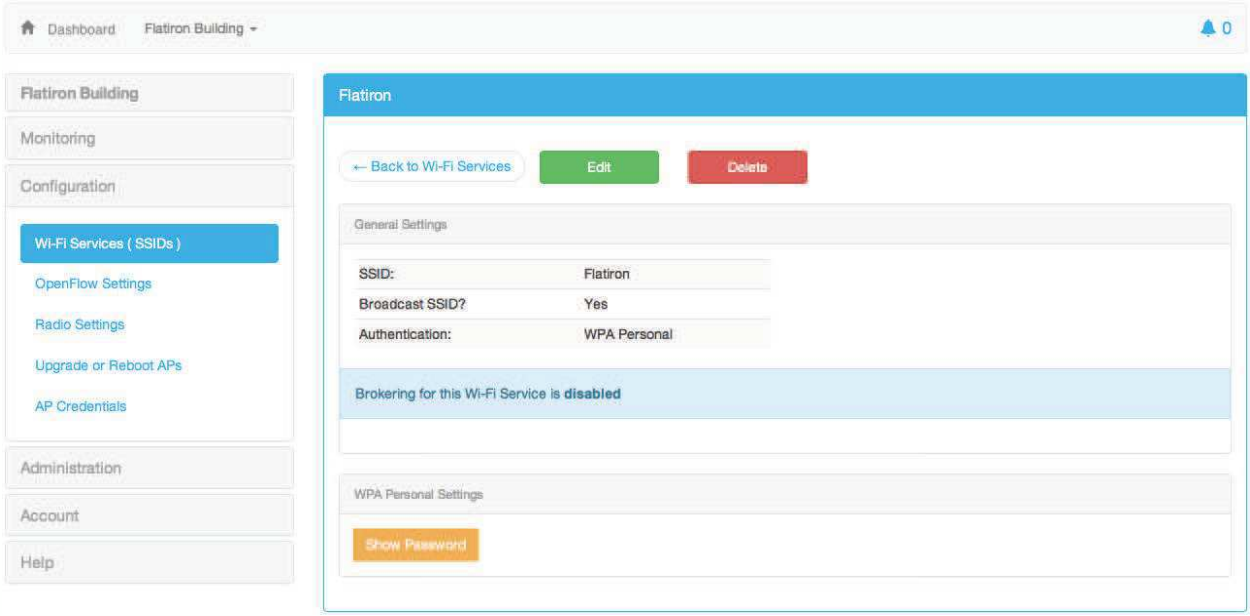
Virtual LANs (VLANs):

- **Default Untagged VLAN**: The default Ethernet port of the access point. Packets are sent and received on the Ethernet port in standard untagged Ethernet format.
- **Tagged VLAN**: An IEEE 802.1Q VLAN on the Ethernet port of the access point. Packets are sent and received on the Ethernet port with an IEEE 802.1Q VLAN tag included.

Tunnels:

- **SSL VPN**: A Secure Sockets Layer (SSL) VPN connection to a remote network via an OpenVPN server. The SSL VPN backhaul requires an OpenVPN (.ovpn) configuration file to be imported.
  - An .ovpn file is an OpenVPN 2.1 or later configuration file that concatenates all the necessary configuration parameters and certificates required to connect to the VPN into a single file. The file can be generated by software provided by the OpenVPN community at http://openvpn.net/index.php/open-source/downloads.html.
- **GRE**: A Generic Routing Encapsulation (GRE) connection to a remote network via a GRE Layer-2 tunnel.
- **VXLAN**: A Virtual Extensible LAN (VXLAN) connection to a remote network via a VXLAN Layer-2 tunnel.

After entering the necessary information and clicking the save button the Wi-Fi service will deployed to all access points at the site and will be available for users to use.

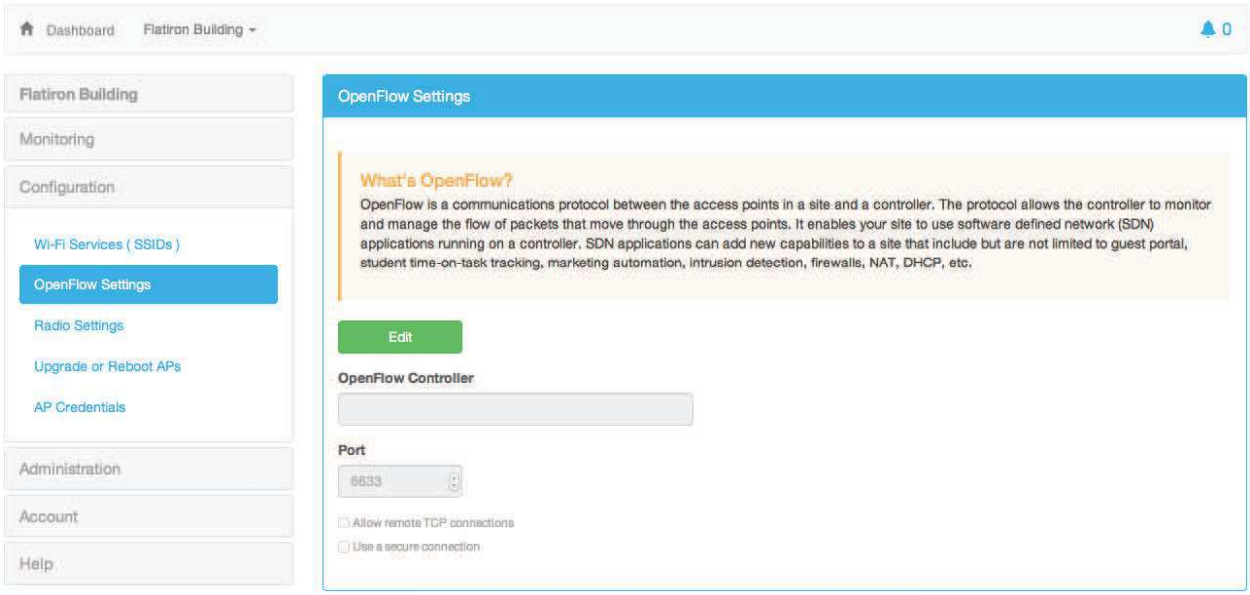


For public sites that might need to provide a large number of different SSIDs, **brokering** provides a mechanism to dynamically provide the needed networks on request and remove them when they are no longer needed.

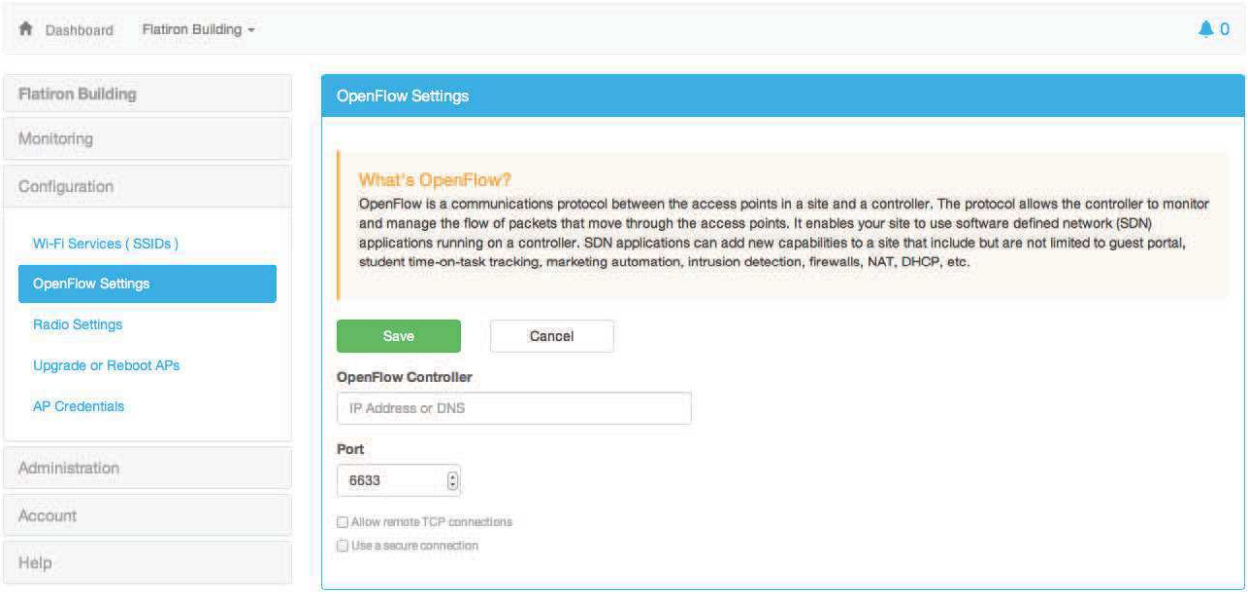
Configuration ▸ OpenFlow Settings

OpenFlow is a communications protocol between the access points in a site and an external software controller. OpenFlow allows the controller to monitor and manage the flow of packets that move through the access points. It enables your site to use software defined network (SDN) applications running on a controller, e.g. OpenDaylight. SDN applications can add new capabilities to a site that include but are not limited to guest portal, student time-on-task tracking, marketing automation, intrusion detection, firewalls, NAT, DHCP, etc.

The OpenFlow controller can be specified by IP address or fully qualified DNS name. Using an OpenFlow controller is optional; it is not necessary to have an OpenFlow controller associated with the APs at a site for basic WLAN operation.



To change an OpenFlow setting, we first need to click the edit button, then provide the new configuration.

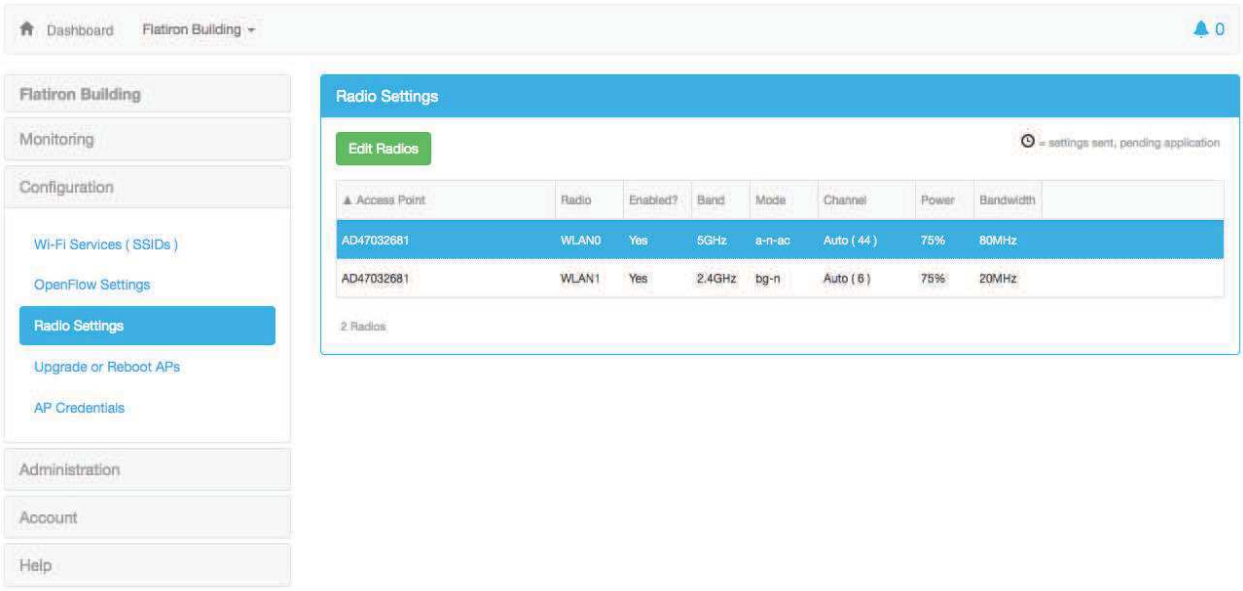


Specify the following parameters to connect an OpenFlow controller:

- OpenFlow Controller
  - The IP address or DNS name of the controller
- Port
  - The TCP port number
  - Standard port numbers are 6633 or 6653
- Allow remote TCP connections
  - In standard OpenFlow, the AP/Switch builds the connection to the controller. There is also the option to have the controller connect to the AP, which can be activated by setting this checkbox. This is also needed for using tools like ovs-vsctl remotely against the switch. Before allowing these connections, a sound security analysis should be done to prevent unauthorized access to the network devices.
- Use a secure connection
  - To secure the OpenFlow link the access points will validate the certificate of the OpenFlow controller by inspecting the signature chain and the contents. The AP validates that the OpenFlow Controller certificate was signed and verified by a trusted root certificate authority (CA). You must provide the certificate of the trusted root CA. The PEM file must contain the trusted root CA as well as any issuer certificates.

Configuration ▸ Radio Settings

Displays a list of all the radios deployed at this site.

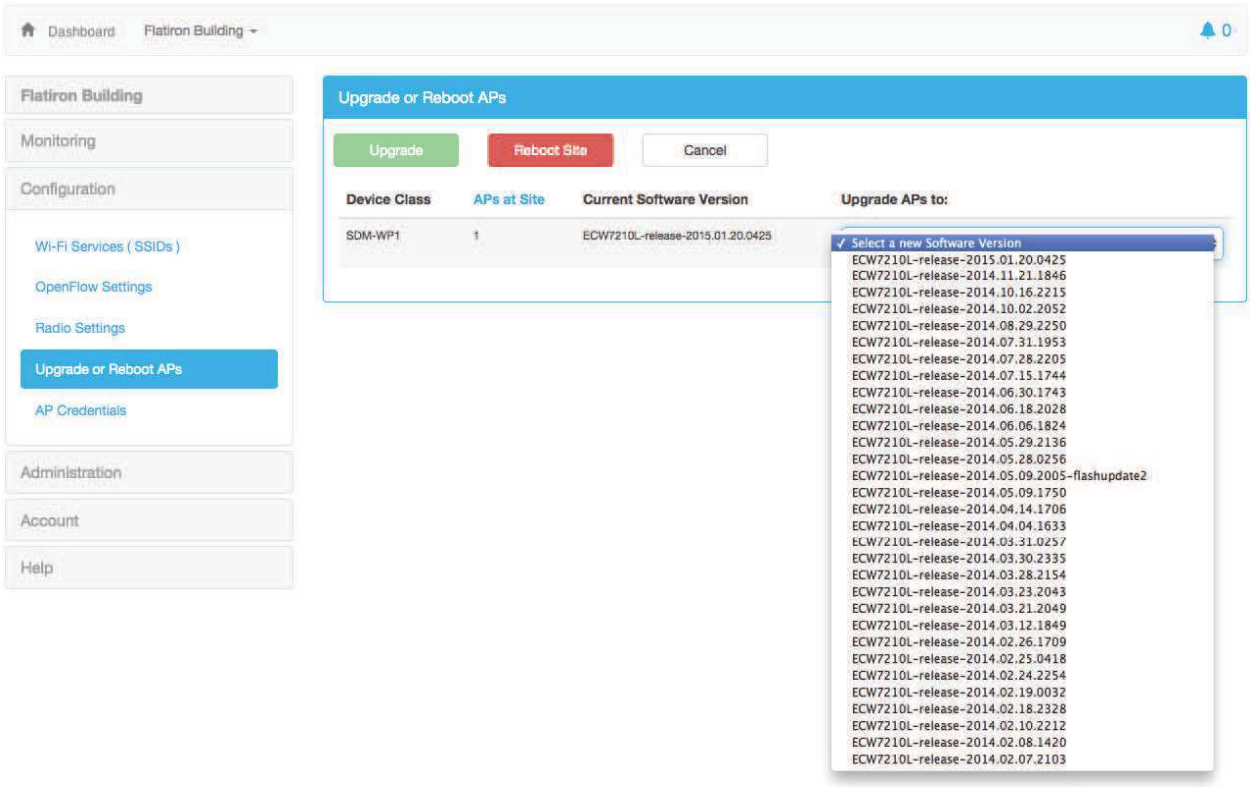


Clicking the **Edit Radios** button will allow you to change the settings.

See Monitoring ▸ Access Points ▸ Radio Settings for more information.

Configuration ▸ Upgrade or Reboot APs

The Upgrade or Reboot APs page shows the software versions installed on each AP. It also allows you to select a new firmware version for your APs.



- **Reboot Site** will reboot all access points at this site. To reboot individual APs see Monitoring ▸ Access Points ▸ Status.
- **Upgrade** will upgrade all access points at this site to the selected firmware version. All matching hardware at a site must be running the same firmware version.
    - Note: If you just setup your site and APs, you should update now.

Configuration ▸ AP Credentials

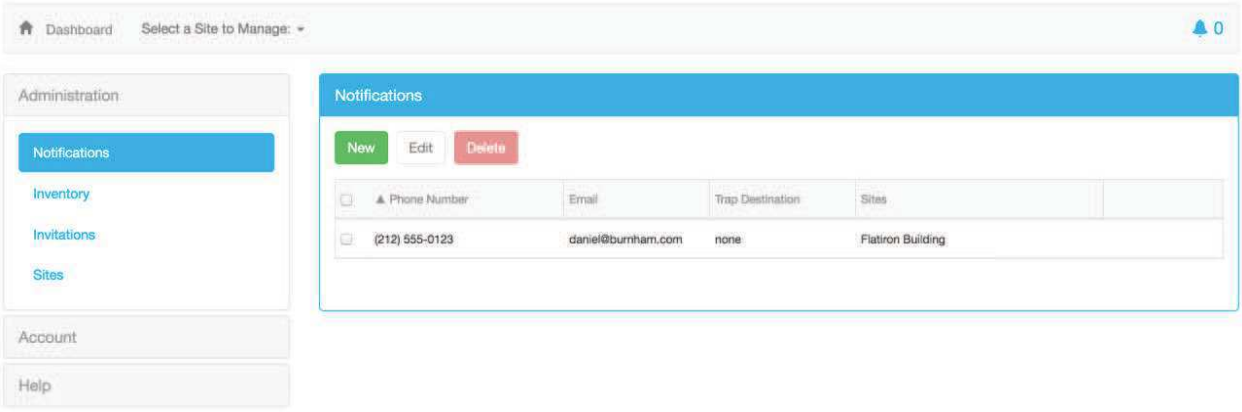
The AP Credentials page enables administration of usernames and passwords for AP Web GUI and SSH.

Administration

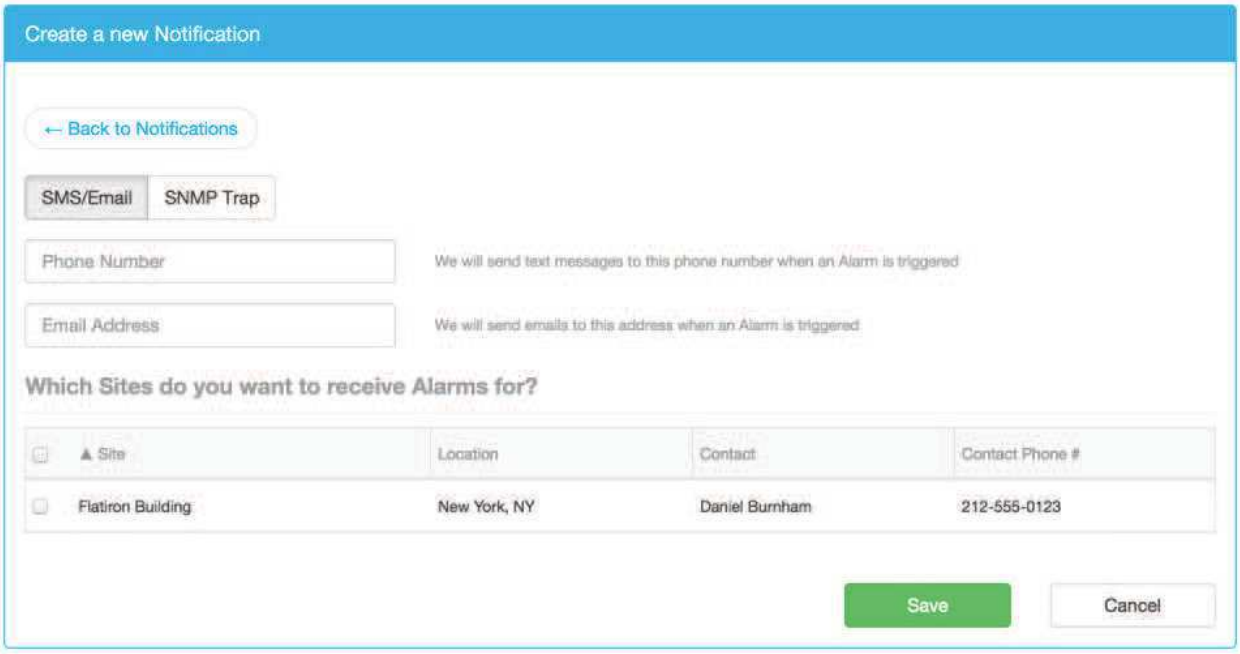
The administration tab allows you to manage your site.

Administration ▸ Notifications

The notifications system allows you to be notified of site alarms via SMS/Email or SNMP trap. The notifications page displays a list of configured notifications.



From here you can create **New** notifications, or **Edit** and **Delete** existing notifications.

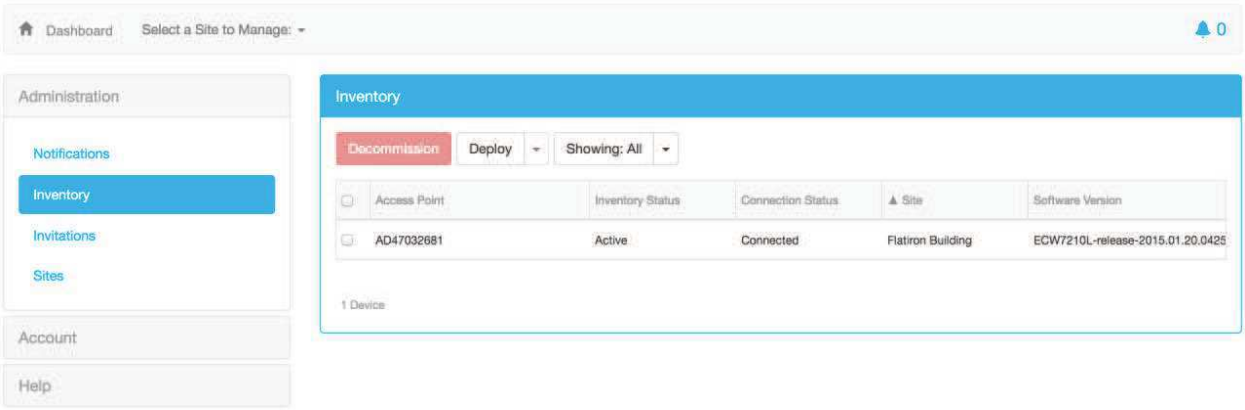


To create a new notification specify the recipient and the sites be included. Two types of categories of notifications are possible:

- SMS/EMAIL: When this is selected, alarms will be sent as text messages to mobile phones and/or as emails, depending on the contact information provided.
  - Phone number
  - Email Address
- SNMP Trap: Traps use the SNMPv2c format. To download the management information base (MIB) see Help ▸ Download MIBs.
  - SNMP Trap Destination: This field takes the IP or FQDN of the traps receiving server.
  - Trap Port Number: When empty, the default port 162 is used.

Administration ▸ Inventory

Displays a detailed list of access points belonging to the user including AP serial number, inventory status,connection status, attached site and software version.



The Decommission button can be used to disassociate the selected access points from a site or sites.

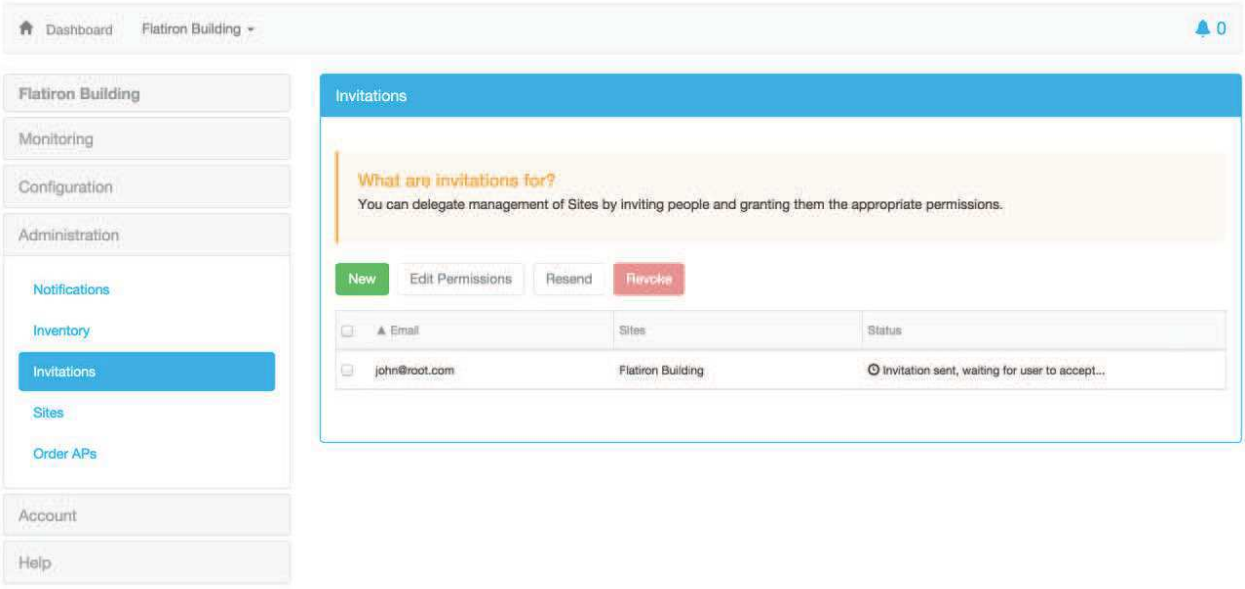
The Deploy button can be used to to assign the selected access points to a site.

The Showing filter can be used to display access points based on deployment status:

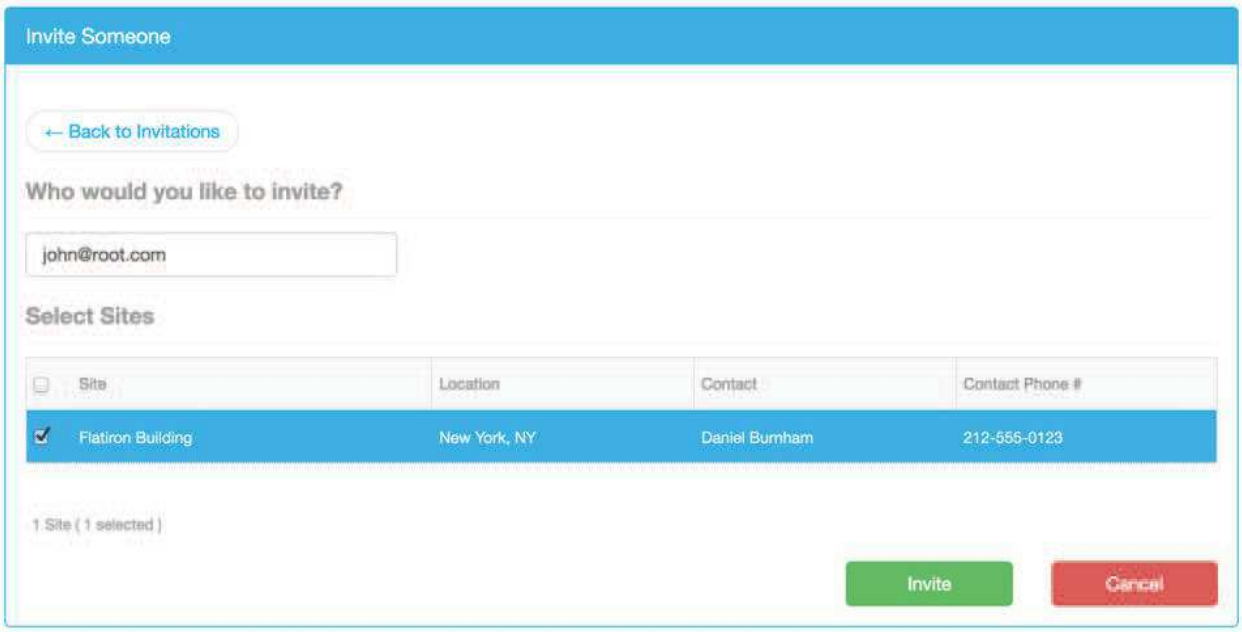
- All
- Active: AP is currently deployed to a site.
- Decommissioned: AP is not deployed to a site.
- Decommissioning: AP is in the process of being disassociated from a site.
- Provisioning: AP is in the process of being deployed to a site.

Administration ▸ Invitations

The Invitations page allows a MSP to assign management of a site to another person (operator). This page will display a list of operators including email address, sites, and invitation status.



The **New** button can be used to create an invitation for a new operator.



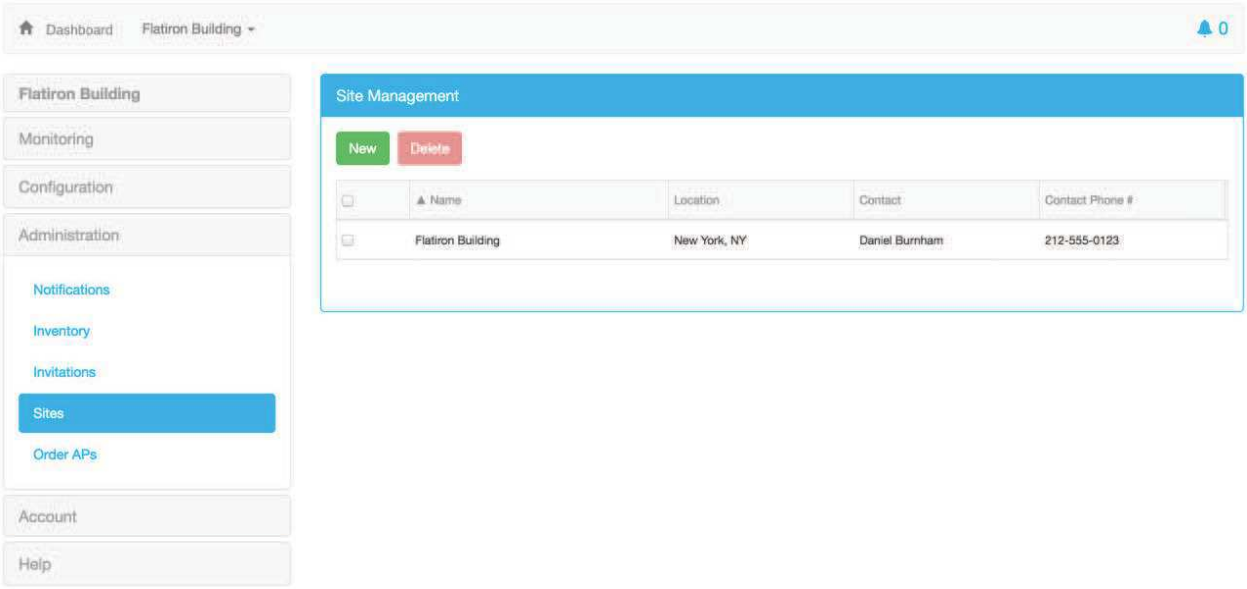
Enter the email address and select the sites for this operator to manage, then click **Invite** to complete the invitation. The operator will receive an invitation email enabling them to activate their account.

After selecting an operator from the invitations page the following buttons are also available:

- The **Edit Permissions** button can be used to add or remove sites from the selected operator's management privileges.
- The **Resend** button can be used to resend the invitation email.
- The **Revoke** button can be used to revoke the operator's account.

Administration ▸ Sites

The sites page displays your list of sites and allows you to create new sites or delete existing sites.



For information on creating a new site see Add New Site in Getting Started.

Administration ▸ Order APs

The Order APs page allows you to order additional devices to be installed at your sites. Through this page you will have the ability to

- View a detailed product list.
- Select hardware and subscription plans
- Review and modify the shipping address
- Enter special delivery instructions or questions
- Complete your order

Account

The account tab allows you to manage your account settings.

Account ▸ Account Settings

From this page you can:

- Change your email address
- Change your password

Help

The help tab links you to downloads and feedback resources

Help ▸ Developer Documentation

Download developer documentation.

Help ▸ Download MIBs

Download the management information base for SNMP trap notifications.

Help ▸ Feedback

Send feedback to Tallac.