Aruba Beacons
Validated Reference Design

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

The Aruba Validated Reference Design (VRD) series is a collection of technology deployment guides that include descriptions of Aruba technology, recommendations for product selections, network design decisions, configuration procedures, and best practices for deployment. Together these guides comprise a reference model for understanding Aruba technology and designs for common customer deployment scenarios. Each Aruba VRD network design has been constructed in a lab environment and thoroughly tested by Aruba engineers. Our customers use these proven designs to rapidly deploy Aruba solutions in production with the assurance that they will perform and scale as expected.

About This Document

This VRD describes *Aruba beacons,* small, low-power wireless transmitters that broadcast Bluetooth Low-Energy (BLE) signals that can be heard and interpreted by iOS and Android devices. Aruba beacons integrate with Meridian-powered apps for more granular mobile engagement, such as providing directions with a glowing blue dot or sending push-notifications based on a visitor's real-time location.

This guide provides an overview of Aruba beacon technology, and describes the different types of Aruba beacons, beacon use cases and deployments, as well as predeployment configuration and testing workflows.

Additional Reference Material

This guide helps a wireless engineer deploy and configure Aruba beacons in a path or area model deployment. It is a base design guide for Aruba beacons and therefore it will not cover the fundamental wireless concepts. Readers should have a good understanding of wireless concepts and the Aruba technology.

For more information on Aruba beacons, refer to the following documents, available for download from the Aruba Networks website:

- Aruba Location Services datasheet
- Mobile Engagement Solution Overview
- Aruba LS-BT1 Location Beacon Installation Guide

For more information on the Meridian mobile app platform, refer to the Meridian documentation set at http://docs.meridianapps.com/help/intro_meridian.

Mobile Engagement with Aruba Networks

Aruba beacons are small, low-power wireless transmitters that broadcast Bluetooth Low-Energy (BLE) signals that can be heard and interpreted by iOS and Android devices that have Bluetooth enabled. Aruba beacons offer increased reliability and accuracy of indoor positioning for apps created with Meridian's AppMaker and SDKs. When you use Aruba beacons in conjunction with the Meridian mobile app platform, the beacons allow public-facing enterprises like large retail spaces, hospitals, hotels, stadiums, museums, schools and airports to infuse their mobile apps with innovative, location-based services.

The Meridian Mobile App Platform

When a mobile device with a Meridian-powered mobile app is within range of Aruba beacons, guests using that app can receive personalized, proximity-aware push notifications, and view a glowing blue dot that shows their real-time location on a venue's map.

The Meridian mobile app platform includes the following features:

- Meridian Editor: A cloud-based content management system that serves as the online hub for Meridian-powered tools. Beacons are monitored and managed through the Meridian Editor.
- AppMaker: A module in the Meridian Editor that lets you build a mobile app for your venue. Beacons can work in conjunction with a Meridian-powered app to provide customers using that app with push notification and location services.
- Mapping and self-guided wayfinding : This Meridian feature lets venues use data from Aruba beacons to incorporate location- specific mapping and turn-by-turn directions into their Meridian-powered mobile app.

You can order a customized (white-label) iOS and Android app from Meridian, create your own app using the Meridian SDK tools, or use the SDK tools to add mapping and wayfinding (NavKit), indoor positioning on a map (BluDotKit), and proximity-based notifications (ZoneKit) to an existing app built by a third-party developer.

Integration with ClearPass Guest

Aruba Networks' ClearPass Guest is a scalable, easy-to-use visitor management solution that delivers secure guest access for customers, contractors, and partners using any type of mobile device. If your network deployment includes ClearPass Guest, a customized ClearPass Guest login portal prompts customers and guests to download your custom-branded Meridian mobile app after logging in to your network. Note, however, that ClearPass is not required for a beacon deployment.

Integration with Aruba Wi-Fi

Communication between the beacons and the client devices is not dependent upon an active Wi-Fi connection. However, you may choose to integrate your beacon deployment with an Aruba Wi-Fi network to simplify beacon management.

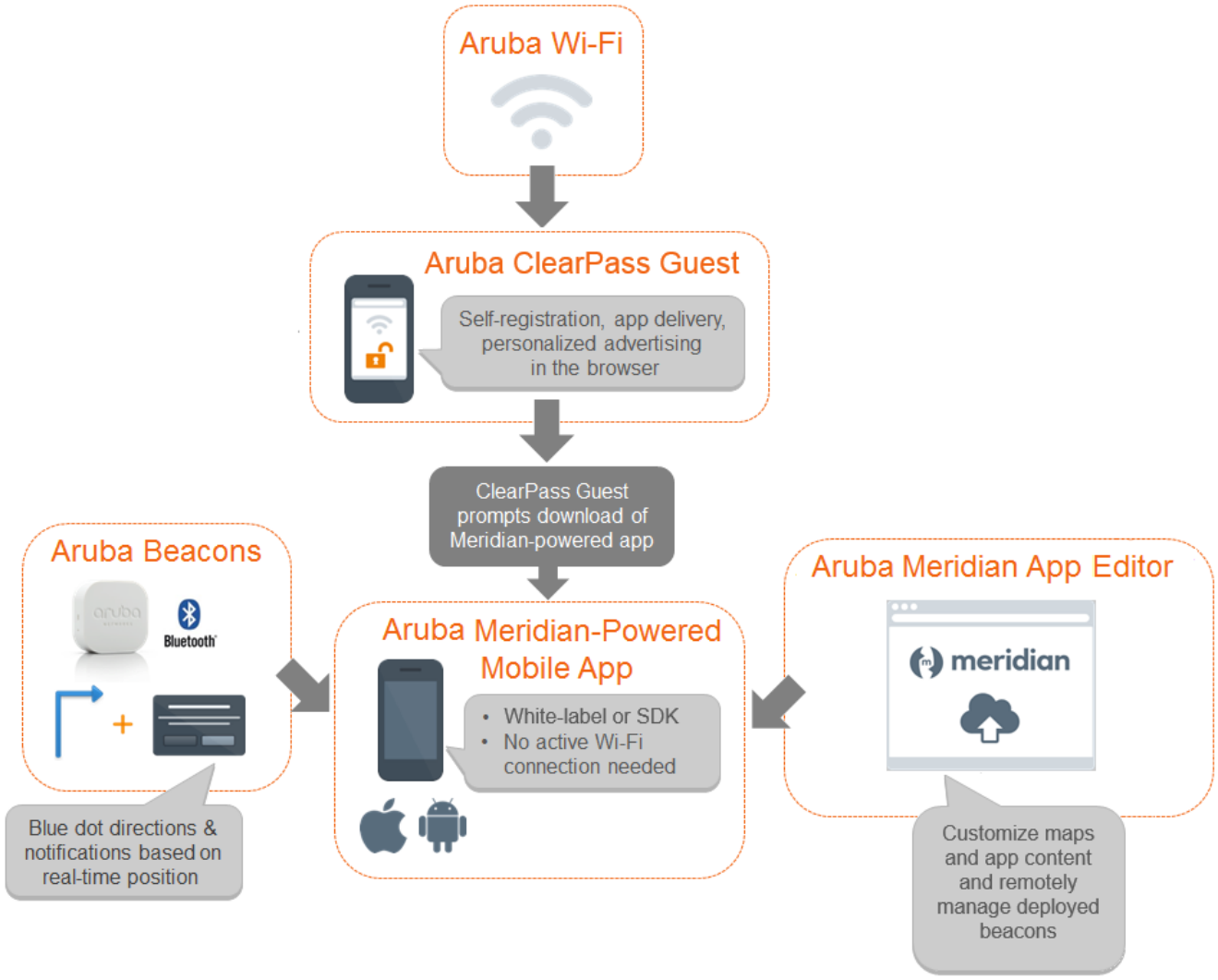
Beacons also work in a non-Aruba wireless network, although deploying them in an Aruba WLAN allows you to benefit from the beacon management capabilities that the combination of Meridian and Aruba APs provide.

Beacons that are user-installed or factory-installed into an Aruba AP can monitor other Aruba Beacons within range and send relevant management data back to the Meridian Editor. This allows you to efficiently manage

the content on your Meridian-powered mobile apps as well as Aruba Beacons from one user-friendly, cloud-based location. Edits made to the Meridian Editor are instantly applied to Aruba Beacons in your venue.

The following graphic shows how beacons, the Meridian app, and the optional integration with Aruba Wi-Fi and ClearPass software work together in an coordinated solution. ClearPass Guest allows visitors to log in to your Aruba Wi-Fi network, register with your enterprise, then download your customized, Meridian-powered mobile app. The Aruba beacons deployed at your site send signals to your customers' iBeacon-compatible mobile devices, which are used by the Meridian mobile app to identify the device's location. The mobile app provides real-time wayfinding and generates push notifications based on instructions from your cloud-based Meridian account.

Figure 1 *Integrating Aruba Wi-Fi and ClearPass Guest into a Beacon Deployment*



Beacon-Compatible Devices

Aruba beacons support the iBeacon standard, an Apple protocol supported by Bluetooth-enabled smart devices, including mobile devices running iOS 7 or later, or Android devices that support Bluetooth 4.0. An Aruba beacon transmits a unique identifier that can be detected by beacon-compatible smart devices in its area. When smart devices are in close proximity to an Aruba beacon, software on these devices can perform actions based on the beacon identifier, such as show the location of the device on a floor map, or trigger push notifications about nearby items for sale.

NOTE

Aruba beacons do not send push notifications directly to devices, just information about the beacon identity. The Meridian-powered app sends push notification directly to devices, based upon instructions it receives from your Meridian account.

A smart device running a Meridian-powered app can use Aruba beacons to pinpoint the location of visitors with a high level of accuracy. Optimal deployments allow smart devices to identify their locations within less than three meters. Communication between the beacons and the client devices is not dependent upon an active Wi-Fi connection, although the client must have Bluetooth enabled. These low-latency communications have a delay of less than two-seconds, providing accurate and timely wayfinding for clients devices, as well as highly targeted push notifications.

Aruba Beacon Types

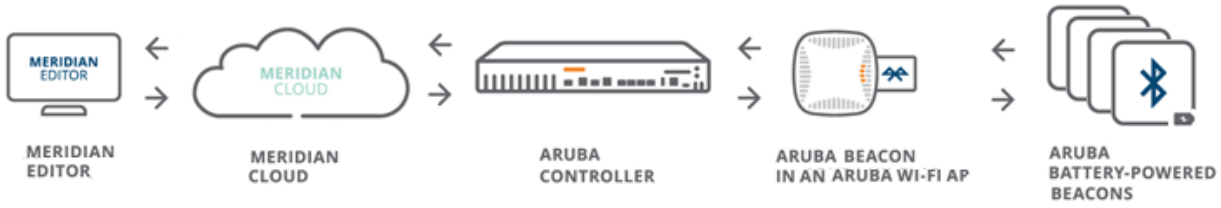
Aruba offers the following different types of beacons:

- **Battery-Powered Beacons**: The standalone battery-powered beacon can be mounted using an adhesive sticker, an indoor mounting bracket, or an outdoor enclosure box.
- **USB-Powered Beacons**: The smaller USB-powered beacon can be inserted into the USB port of an Aruba access point or any other device with an available USB port. Note that plugging a USB beacon into a supported Aruba AP adds beacon management capabilities. The battery-powered beacon can communicate only with iBeacon-compatible devices and beacons in an Aruba AP. A USB-powered beacon in an AP communicates with clients and battery-powered beacons, but can also send information about the beacon's status, battery level, power level and firmware to the Aruba controller and Meridian Editor.
- **Beacons in APs**: AP-320 series access points include a built-in beacon that operates in a manner similar to a USB-powered beacon, in that the beacon built in to the AP communicates with clients and battery-powered beacons, but can also send information about the beacon's status, battery level, power level and firmware to the Aruba controller and Meridian Editor.

Figure 2 *An Aruba USB Beacon and Battery-powered beacon*

As shown in Figure 3 below, an enterprise customer can view and configure Aruba beacon settings from within the Meridian Editor. Meridian pushes configuration changes down through the Aruba controller to beacons installed into an AP USB port or built in to an AP-320 series AP. The beacon in the AP then sends this information directly to the battery-powered beacons on the network.

Figure 3 *Beacon Management Topology*



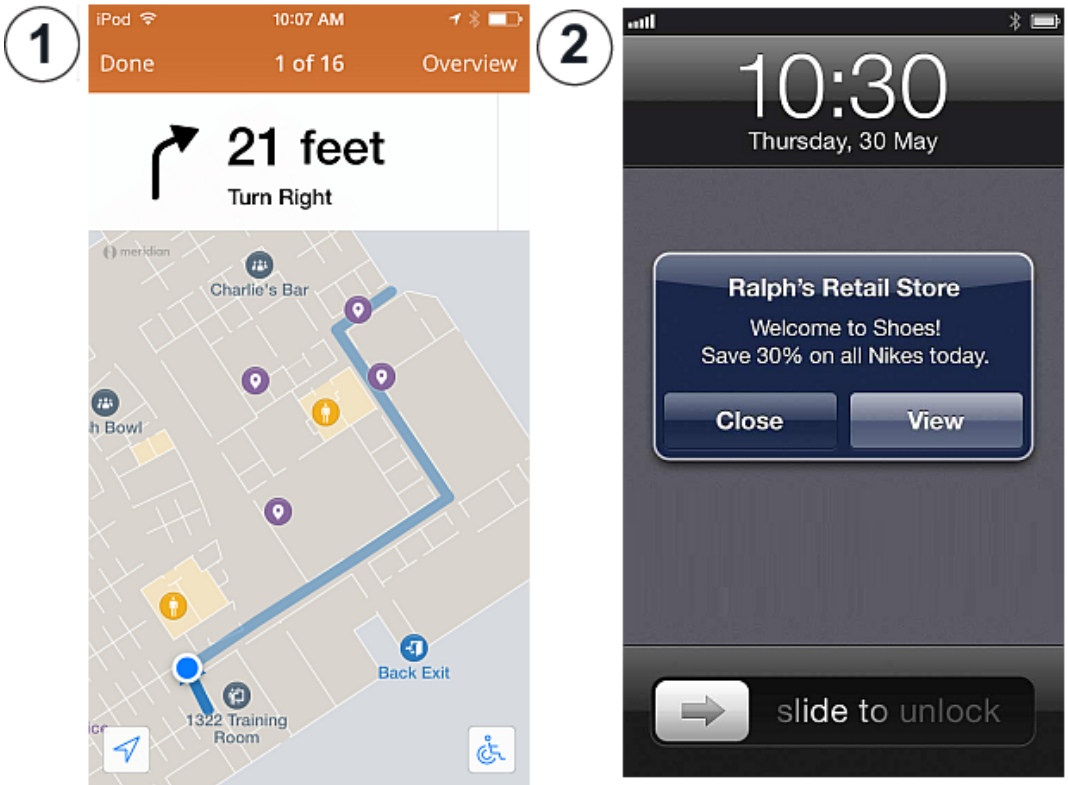
Beacon Configuration Modes

Aruba beacons can be deployed in one of two modes, as a *location* beacon or a *proximity* beacon.

- **Location beacons** support location-based wayfinding using a Meridan app. Beacons deployed in this mode can show mobile app users their indoor location with a glowing blue dot, allowing the users to search for and locate nearby products and services. You can fully configure location beacons using only the Beacons app.
- **Proximity beacons** allow a Meridian app to send push notifications to mobile devices that come within signal range of that beacon. Proximity beacons are also configured using the Aruba Beacons app, but you must use the Meridian editor to define and manage push notifications for those devices. For more information on defining push notification campaigns for location beacons, see Configuring and Testing Campaigns on page 30.

The first image in the figure below shows an example of blue-dot wayfinding using location beacons and a Meridian-powered app. The second image shows a push notification that is triggered when a customer using a Meridian app comes within range of a proximity beacon. In this second image, the campaign notifies customers using a Meridian-powered app about a sale on shoes when the user enters the shoe department.

Figure 4 *Pathfinding and Push Notifications using a Meridian-powered App*



The layout of your floor and the type of location tracking required determines the type of deployment used in a particular venue. There is no single deployment design that is perfectly suitable for every environment, but there are two primary models for deploying Aruba Beacons; a **path** model, and an **area** model.

- Path model: applicable in settings where straight line location accuracy is required. This model is suitable for blue dot tracking in areas such as narrow hallways or corridors.
- Area model: best used in larger areas such as wide rooms or hallways. An area model deployment is applicable for settings where two-dimensional location accuracy is required.

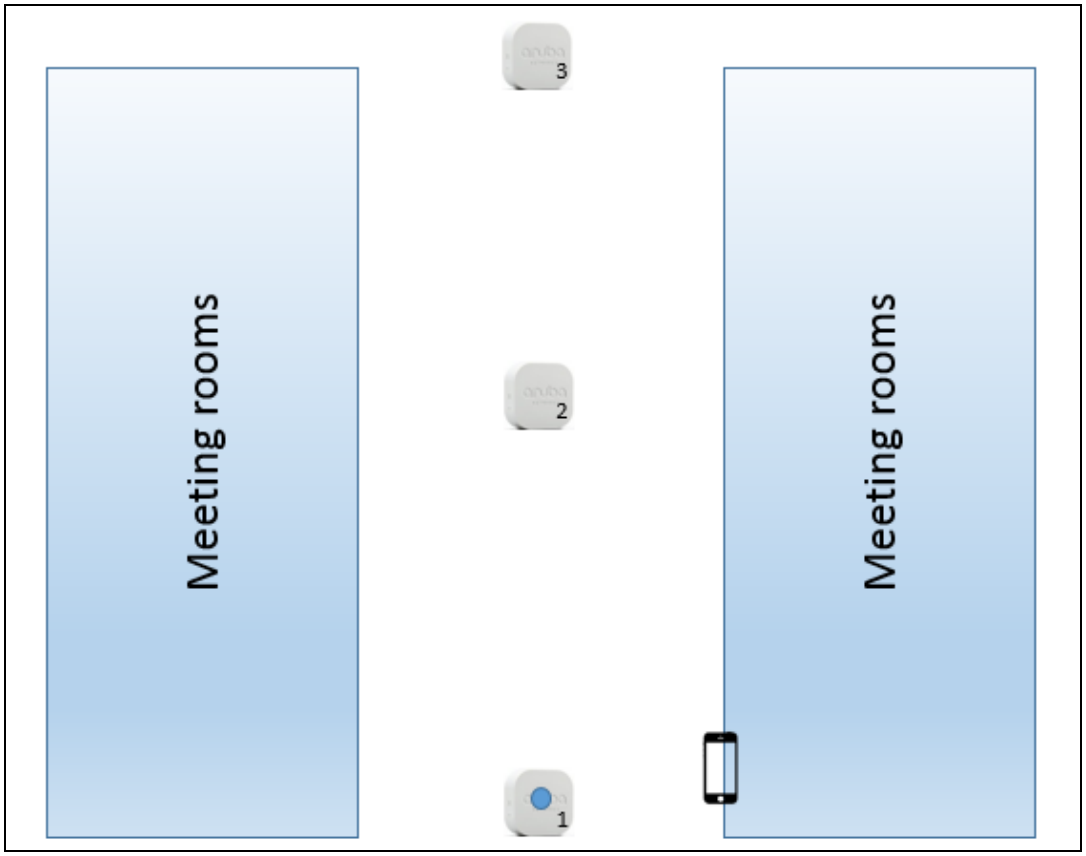
NOTE

For a list of other factors to consider while deploying beacons, refer to Deployment Considerations on page 12.

Path Model

In the example shown in Figure 5, the beacons are ceiling-mounted in a narrow corridor between two meeting rooms. As the client device (represented by the smart phone icon) moves through the corridor, the blue dot moves in a straight line following the beacons. The blue dot will move in a straight line regardless of the client device's actual position in the corridor.

Figure 5 *Path Model*

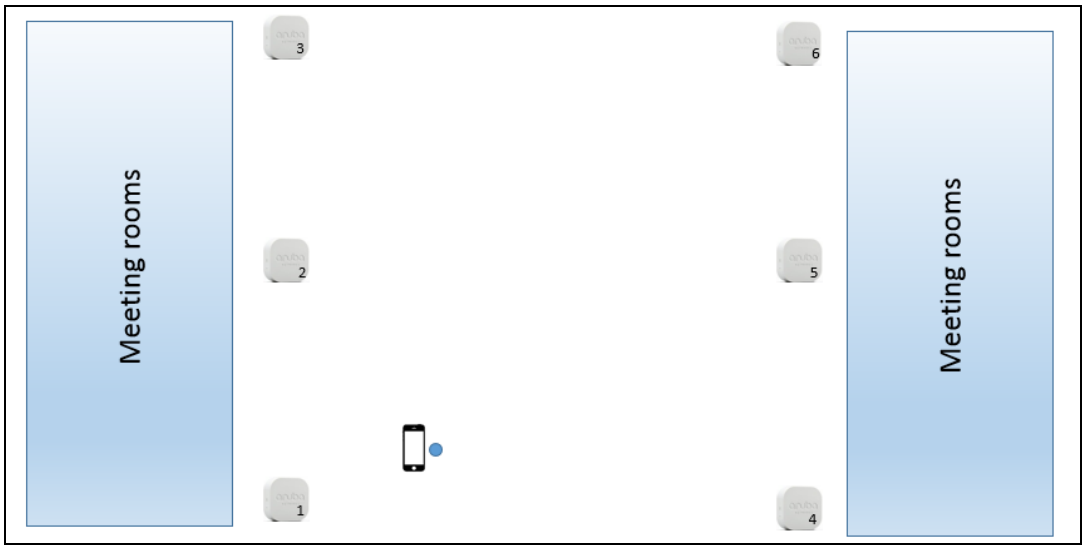


Area Model

The example illustrated in Figure 6 shows six ceiling-mounted beacons installed in a wide hallway. As the client device moves throughout the corridor, the blue dot follows the client along both the x-axis and y-axis. Since this deployment allows for two-dimensional location tracking, the blue dot displays the client's actual location.

If ceiling-mounting is not a feasible option, you can achieve similar two-dimensional location accuracy by wall-mounting beacons in a zig-zag fashion across the hallway .

Figure 6 *Area Model*



Deployment Considerations

Before installing Aruba Beacons, consider the items described in the following sections. The following factors should be considered when determining the placement of beacons to ensure the performance required by your deployment.

Beacon Sizing

For better location accuracy, ensure that successive beacons are placed no more than 40 feet apart. Closer beacon placement provides the best indoor positioning experience by reducing blue dot jumpiness. However, the optimal distance between beacons may vary based on factors such as the deployment model, variations in ceiling height, reflective vs. non- reflective environments, etc.

The no-more-than-40-feet statement is a guideline and your actual deployment may differ. For example, a smaller distance between beacons may be needed to provide tighter location accuracy. However, in larger open areas, a wider spread of beacons might be sufficient.

Beacon Mounting

Battery-powered beacons have multiple mounting options and techniques. The two most common mounting techniques are wall mounting and ceiling mounting. Three mounting options are available for battery-powered beacons:

- Adhesive on the back of the beacon
- Indoor mounting bracket (useful for replacing beacons in the future)
- Outdoor mounting enclosure

The options and techniques used in your deployment will depend on the factors described in the following sections.

Wall Mounting

Wall mounting can be used in open-roof areas or areas with very high ceilings where installation might be a challenge. Wall mounting is easier than ceiling mounting and all three mounting options are useable. However, the beacons are more conspicuous.

Ceiling Mounting

Ceiling mounting is ideal for environments with aesthetics concerns, since it allows beacons to be installed discreetly and out of line of sight. Additionally, ceiling mounting keeps beacons out of reach from curious people and prevents tampering. Since the beacons are placed above the tracked devices, ceiling mounting provides more resiliency to attenuation from crowds.

Keep the following in mind when installing ceiling-mounted beacons:

- Ensure that beacons are mounted far enough from heat generated by light bulbs.
- Beacons must be mounted below ceiling tiles, as some types of tiles may impair beacon signal transmission if the beacons are mounted above the tiles.
- Ensure that the beacon's power level is high enough for the client app to hear and configure the beacon when necessary. NOTE: Only proximity beacons power levels can be adjusted.
- For environments with different ceiling heights, ensure that beacons are placed on the lower ceiling height to prevent the blocking of beacon signal from different locations.
- Ceiling mounting may require a personnel lift or mounting stick. Take proper safety precautions when using such equipment.

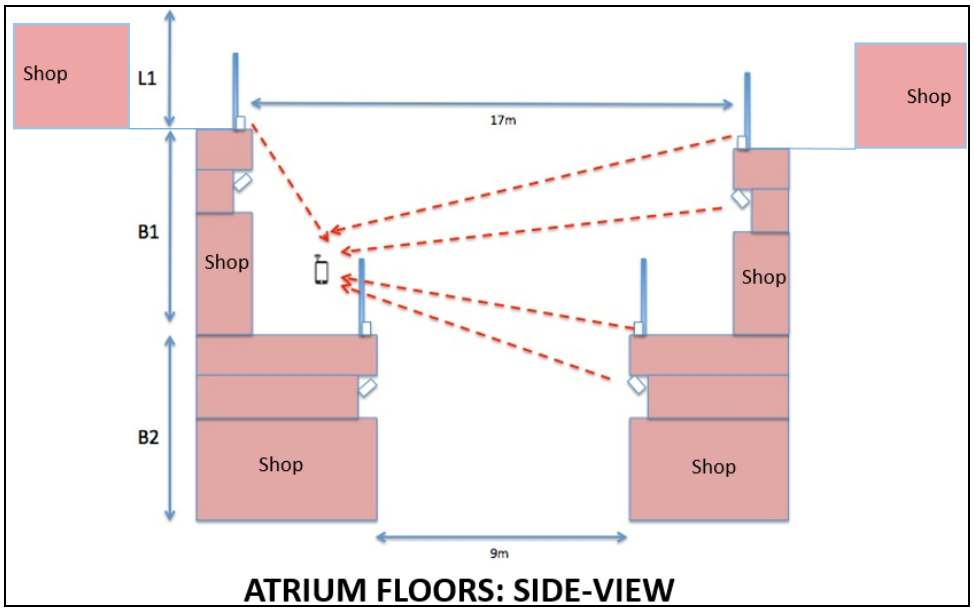
Reflective Environments

Reflective environments, such as areas with marble floors, may result in jumpiness of the blue dot. Carpeted areas have shown better blue dot stability than areas with marble floors. In locations where reflective surfaces are unavoidable, consider using the path model instead of the area model.

Atrium Deployments

Due to beacon signal bleed, deploying beacons in environments such as mall with an open atrium requires proper planning. Without proper planning, blue dot location tracking may be inaccurate and may even report the blue dot on the wrong floor. As seen in Figure 7, the client device receives a signal from beacons on multiple floors.

Figure 7 *Atrium Deployment -Side View*

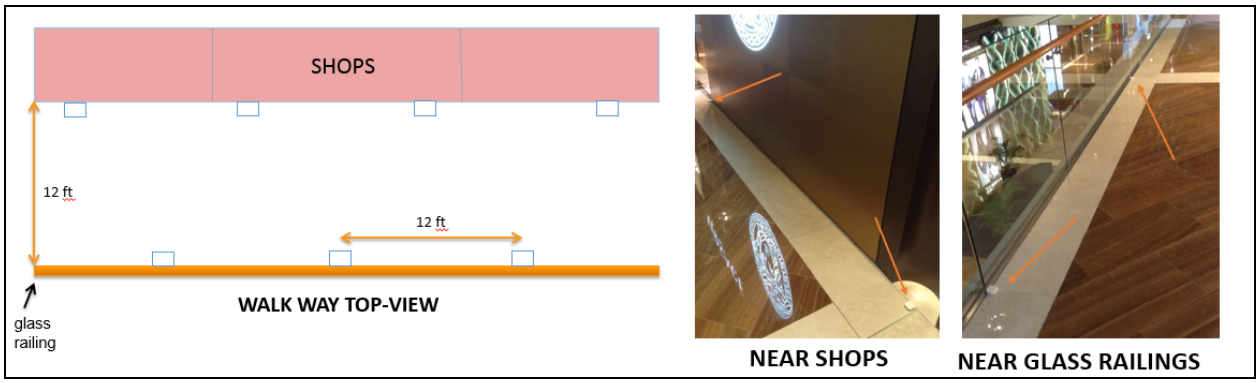


Beacon Placement

Although places like malls are often made up of walkways and corridors, the path model is not recommended. Installing beacons in the center of a ceiling, using the path model, would typically work in a corridor. However, in an atrium with open air between floors, the beacon signal can bleed down to lower floors. This results in blue dot appearing on the wrong floor.

Using the area model provides better blue dot location accuracy. The best blue dot experience is found when beacons are placed closer to the ground (less than or equal to three feet) and facing upwards, reducing signal bleed to the lower floors.

Figure 8 *Atrium Deployment - Beacon Placement*

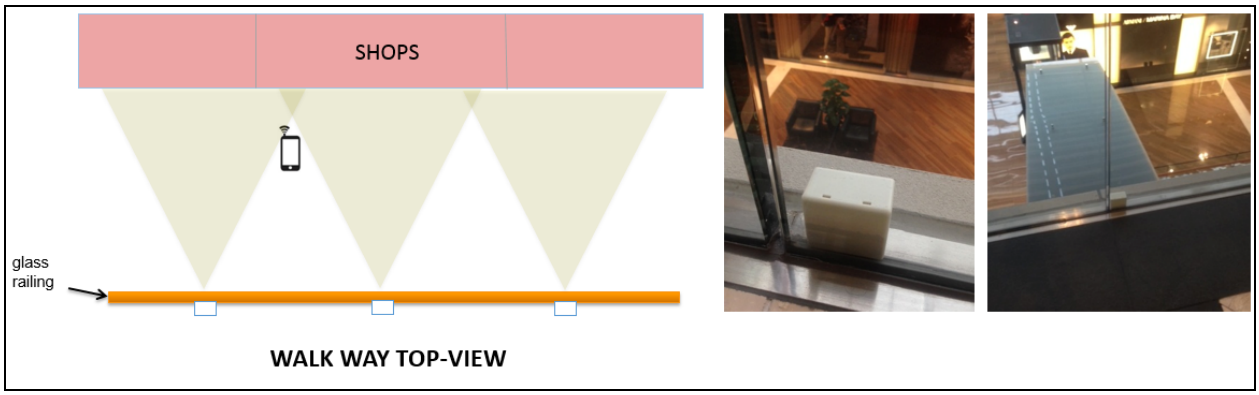


Securing Beacons

Placing beacons on or close to the floor may not be secure or realistic but some measures can be taken to keep beacons out of the reach of people.

Consider the example shown in Figure 8. In this deployment, the beacons could be placed on the opposite side of the glass to prevent tampering. The beacons could be placed on the outside of the glass railing or inside the shop's window. Keep in mind that the thickness of the glass might attenuate the beacon's signal but the power level can be adjusted for proximity beacons.

Figure 9 *Atrium Deployment - Securing Beacons*



Hardware and Software Requirements

Aruba Networks offers three types of beacons, a battery-powered beacon, a USB-powered beacon, and the beacon built in to an AP-320 series AP. The hardware and software configuration requirements vary between these different model types.

Battery-Powered Beacons

Before you begin to configure a battery-powered beacon, you'll need the following items:

- One or more Aruba battery-powered beacons.
- An iBeacon-compatible mobile device running iOS 7 or later with Wi-Fi or 3G/4G internet connectivity, such as an iPhone 4S or later, iPod touch 5 or later, or iPad 3 or later.
- The Aruba Beacons app installed on the iOS mobile device.
- An active Meridian Editor account configured with floor maps of your deployment site.

Log in to the Beacons app using your Meridian Editor credentials. To configure these devices as *location beacons*, your Meridian account only needs to be configured with floor maps of each deployment site. To configure *proximity beacons* and send push notifications, you must also define a push notification campaign in the Meridian Editor. For more information, see Configuring and Testing Campaigns on page 30.

USB-Powered Beacons and Beacons in an AP-320 Series Access Point

A beacon connected to the USB port of an Aruba AP or built into an AP-320 series AP communicates with battery-powered beacons in the area, then sends information about those beacons through the Aruba controller to the Meridian editor in the cloud.

USB-powered beacons are supported by AP-220 series, AP-210 series and later model access points associated with a 7200 Series or 7000 Series controller running ArubaOS 6.4.3.2 or later. If the AP uses PoE, ensure it is using 802.3at, as the USB port will be disabled on 802.3af.

To use the beacon within an AP-320 series AP, that AP must be associated with a 7200 Series or 7000 Series controller running ArubaOS 6.4.4.0 or later .

To configure a USB-powered beacon or a beacon in an AP-320 series AP to communicate with battery-powered beacons, you'll need the following items:

- An iBeacon-compatible mobile device running iOS 7 or later with Wi-Fi or 3G/4G internet connectivity, such as an iPhone 4S or later, iPod touch 5 or later, or iPad 3 or later.
- The Aruba Beacons app version 2.1.1 or later, installed on the iOS mobile device.
- An active Meridian Editor account configured with floor maps of your deployment site.
- One or more Aruba battery-powered beacons running version 1.1-4 or later.

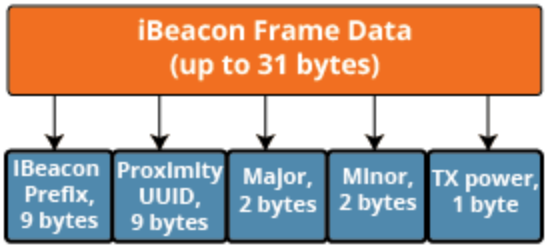
Beacon IDs

Every Aruba beacon is identified by a name and a unique MAC address. When you configure a beacon, the Beacons app also assigns a unique identifier to each beacon comprised of a Universal Unique Identifier (UUID), and major and minor values. A UUID contains 32 Hexadecimal digits, and major and minor values are integers between 1 and 65535 used to better identify the devices within your organization.

The Meridian editor allows you to edit the name of a beacon, but the preset UUID, major and minor values cannot be changed.

The iBeacon advertisement messages transmitted by Aruba beacons are sent in a specific format defined by Apple, and include data about the beacon UUID, major and minor values. Figure 10 below describes the format of an iBeacon advertisement packet.

Figure 10 *iBeacon Frame Data Components*



Beacon Power Levels

The Beacons app allows you to deploy a proximity beacon at the power level that best suits your deployment needs and environment. By default, a proximity beacon sends signals at a Level 14 signal strength (0 dBm). Informal testing shows that in open-air environments with minimal interference, a proximity beacon transmitting at this default power level can be detected with an RSSI of -94 dBm by a client mobile device 25 meters away.

NOTE

For more information on signal strength from beacons at different power levels and the perceived signal power seen by clients at varying distances from the beacon, see Appendix A: Transmission Power Levels.

If you want your proximity beacon to be heard within a larger area, or your environment contains elements like walls or doors that can limit a bluetooth signal, consider increasing the signal strength to a higher level. Similarly, if you want to limit push notifications to within a smaller radius of your beacon, you can reduce the signal strength, so a client mobile device must be closer to the beacon to hear the bluetooth signal.

Use the Beacons app to configure the power level for a proximity beacon, view the location beacon signal range, and test your push notification campaigns to ensure that they are triggered at the appropriate locations. Power levels can then be adjusted through the Beacons app or your Meridian editor account.

Use the following procedures to download and install the Aruba Beacons application, add and configure a new beacon, and place it on the location map.

NOTE

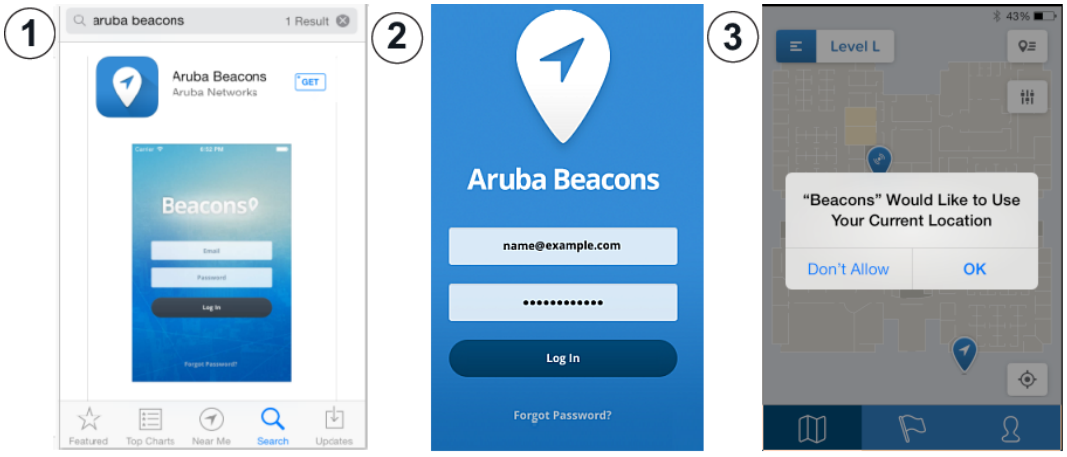
You and your mobile device must be physically present in the location where you are deploying the beacon.

Install the Beacons App

To download, install, and log into the Beacons app:

1. Enable Bluetooth on your iOS mobile device.
2. From your iOS device, access the Apple App store and search for **Aruba Beacons**.
3. Download and launch the Beacons App
4. Log in to the app using your existing Meridian login credentials.

Figure 11 *Install the Beacons App*



Add a New Beacon

Use the following procedure to add a new location or proximity beacon to a location in your Meridian account.

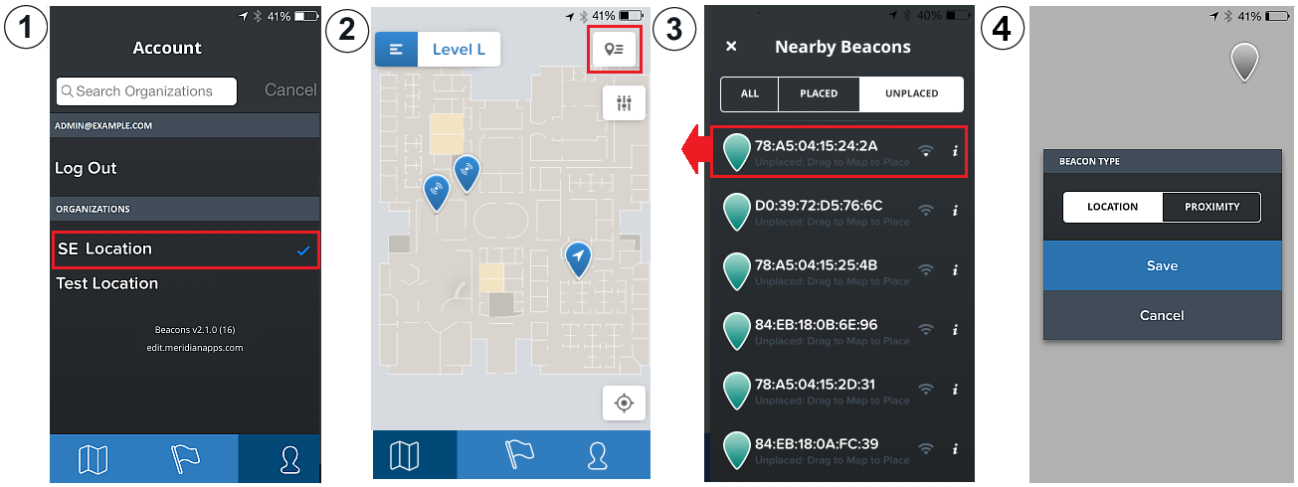
1. Tap the accounts icon ( ) at the bottom of the screen to open the **Accounts** tab. The site locations from your Meridian account appear in the tab.
2. Tap an organization to select the site for the new beacon.
3. Tap the maps icon ( ) to open the **Maps** tab.
4. Click the menu icon ( ) in the upper left corner of the screen, and select the floor on which the beacon is located.
5. Bring the iOS mobile device close to the beacon and click the beacons ( ) icon to open the beacons list.

   Data from nearby beacons are uploaded into the Beacons app. A green icon ( )next to a beacon indicates

it is currently unplaced and available. A gray icon ( )indicates that the beacon is associated with a different location in your Meridain account. A lock icon ( ) means the beacon is part of a different account and you do not have access privileges to edit that beacon.

6. Tap the **Unplaced** button to view unconfigured beacons that are not yet placed on the map. You can identify the beacon to be placed by its MAC address.
7. Tap and hold the beacon icon for the beacon you want to add, then drag the icon to the left side of the screen. The floor map appears.
8. Drop the beacon icon on the appropriate place on the map.
9. The **Beacon Type** pop-up window prompts you to identify the beacon as a location beacon or a proximity beacon. Tap **Proximity** or **Location**.
   - If you select **Location**, the beacon is configured as a location beacon, and placed on the map. The location beacon is represented by the blue location ( ) icon.
   - If you select **Proximity**, you are prompted to select a power level for the beacon before the beacon is placed on the map. Refer to the table below for details on proximity beacon power levels. The proximity beacon is represented by the blue proximity ( ) icon.
10. Tap **Save**.

Figure 12 *Add a New Beacon*



The following table describes the power levels available for proximity beacons. By default, a proximity beacon sends signals at a Level 14 signal strength (0 dBm). For more information on managing proximity beacon power levels, see Beacon Power Levels.

Table 1: *Proximity Beacon Power Levels*

Beacon Power Level	TX power (dBm)
0	-29
1	-27
2	-25

Beacon Power Level	TX power (dBm)
3	-23
4	-21
5	-18
6	-16
7	-14
8	-12
9	-10
10	-8
11	-6
12	-4
13	-2
14	0
15	4

View Beacon Signal Strength and Density

The beacon signal strength seen by a mobile device is determined by a beacon's power setting and the location where the beacon is installed. Follow the procedure below to view the signal strength of a location beacon, as seen by an iBeacon-enabled client.

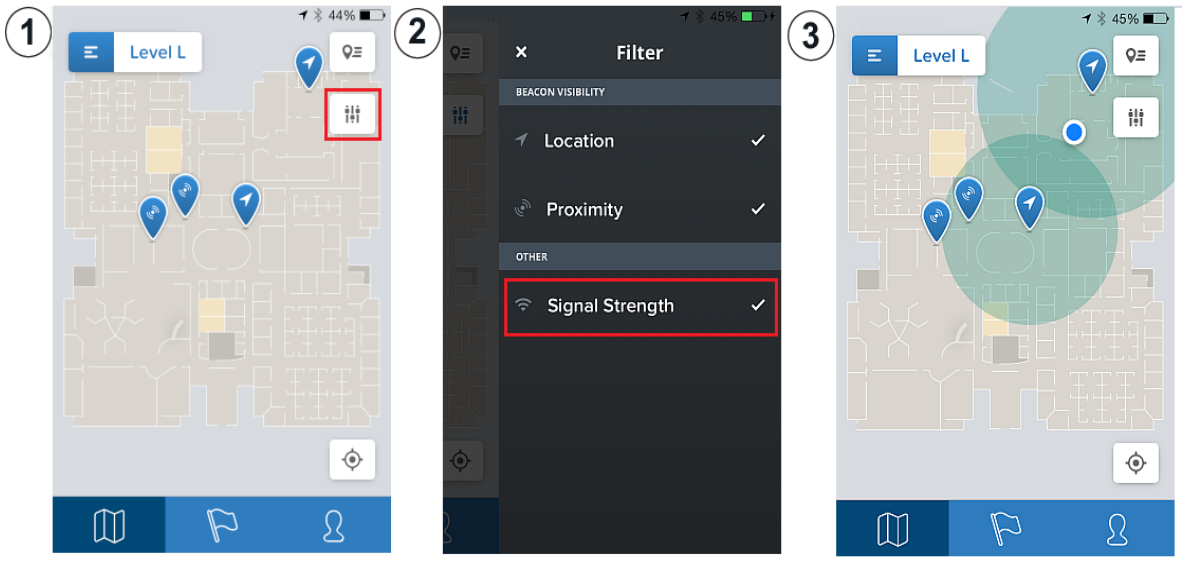
The signal strength display is not meant for precise fine-tuning of beacon placement or beacon signal strength levels, but to give you a general idea of signal density and coverage areas.

1. Open the Aruba Beacons app.
2. From the **Maps** tab, click the filters icon ( ) icon
3. Tap **Location**
4. Tap **Signal Strength** to view the signal density for location beacons.

As shown in Figure 13 , the map displays the beacon signals detected by the mobile device. If the circle between your device and the beacon is large, that indicates that the beacon is farther away from the mobile device and has a weaker signal. If the circle between your device and the beacon is small, that beacon is closer and has a stronger signal.

Note any areas on the map that are not covered by a beacon signal. If your deployed beacons do not fully cover the desired area for your venue with location beacon signals, consider adding beacons, increasing the signal strength or moving the beacon to a different location to avoid elements that may be blocking the bluetooth signal. If the signal coverage density is very high, you may want to consider spacing the devices further apart.

Figure 13 *Beacon Signal Strength*



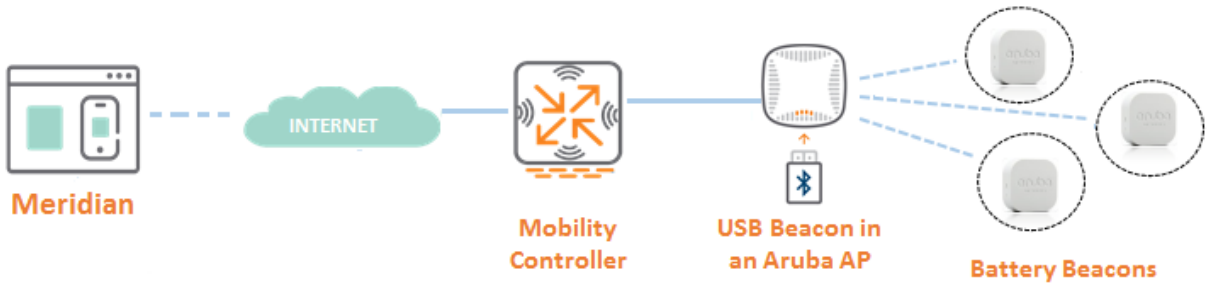
Use an Aruba USB beacon installed into the USB port of an Aruba AP or the beacon built in to AP-320 series AP to connect your battery-powered beacons to your Meridian account. Either of these types of beacons allow you to remotely monitor and manage battery-powered beacons withing the range of a beacon in an Aruba AP.

Beacon Management Workflow

Battery-powered beacons advertise their configuration to the beacon in an AP, and check for available config updates from a USB beacon every 500ms. The USB beacon uses information from battery powered beacons to update the BLE table on the AP. The controller then periodically sends the AP BLE table to Meridian via a secure (HTTPS) connection, and checks for config change requests from Meridian.

If any config changes are requested, the controller sends the config updates to the AP. The beacon in that AP pushes out the config changes to the battery beacon as a response to a battery beacon advertisement, the next time the battery beacon checks for an update. Messages passed between the USB beacon and the battery beacon are small (<50 byte) packets that follow the BLE protocol.

Figure 14 *Beacon Management Topology*



The first time the controller is configured to contact Meridian, the controller contacts Meridian every ten minutes. Once the controller sends an AP BLE table to Meridian, the controller sends updates more frequently; every five minutes.

When a configuration change is requested through your Meridian account, the beacon in the AP pushes updated config settings to the battery-powered beacons the next time the battery beacon checks for updates. The controller sends status updates to Meridian once a minute until the requested changes are made and confirmed on the network.

Beacon Management Considerations

Every ten minutes, a battery-powered beacon increases its transmission power level for five seconds, allowing it to send status messages and receive configuration updates from a USB beacon that might otherwise be out of range. Because there is a longer interval between HiPower beacon transmissions, battery-powered beacons sending status messages at low power levels and high-power proximity beacons located very far away from the AP may not be frequently heard by the USB beacons. This HiPower beacon interval, combined with the update intervals between the controller and Meridian account, means it may take up to an hour for a low-power or very distant proximity beacon to be recognized by Meridian.

If a USB beacon is installed in a ceiling-mounted AP, there may be some reduction in signal strength that impacts how well it sees other beacons. To improve the range at which the USB beacon can detect other

beacons, consider using a USB extension cable to move the USB beacon into better location not impacted by signal attenuation factors such as walls or wireless speakers.

Controllers running ArubaOS 6.4.3.3 or later can report to Meridian a maximum of 70 beacons per AP. This maximum capacity will be enhanced in later versions of ArubaOS.

Managing Campaigns

Campaigns are the mechanism by which a push notification such as a customized message or link is sent to mobile devices that are using a Meridian-powered app. When devices using the Meridian-powered app come within range of a proximity beacon, the app triggers push notifications for the campaign asigned to the proximity beacon. If your beacon deployment uses proximity beacons to trigger push notifications within your Meridian-powered app, you must create and manage your campaigns using the Meridian Editor.

Notifications can be scheduled to trigger when a mobile device first comes within range of the proximity beacon, or scheduled to coincide with a specific event or marketing campaign. For details on using the Meridian Editor to define campaigns for deployed proximity beacons, see Configuring and Testing Campaigns.

Before you Begin

Before you can use a USB beacon in an Aruba AP or an AP-320 series access point to manage the battery-powered beacons associated with your Meridian account, you must perform some additional network configuration tasks to configure your network and Aruba controller to securely access your Meridian account in the cloud.

Configure the Controller

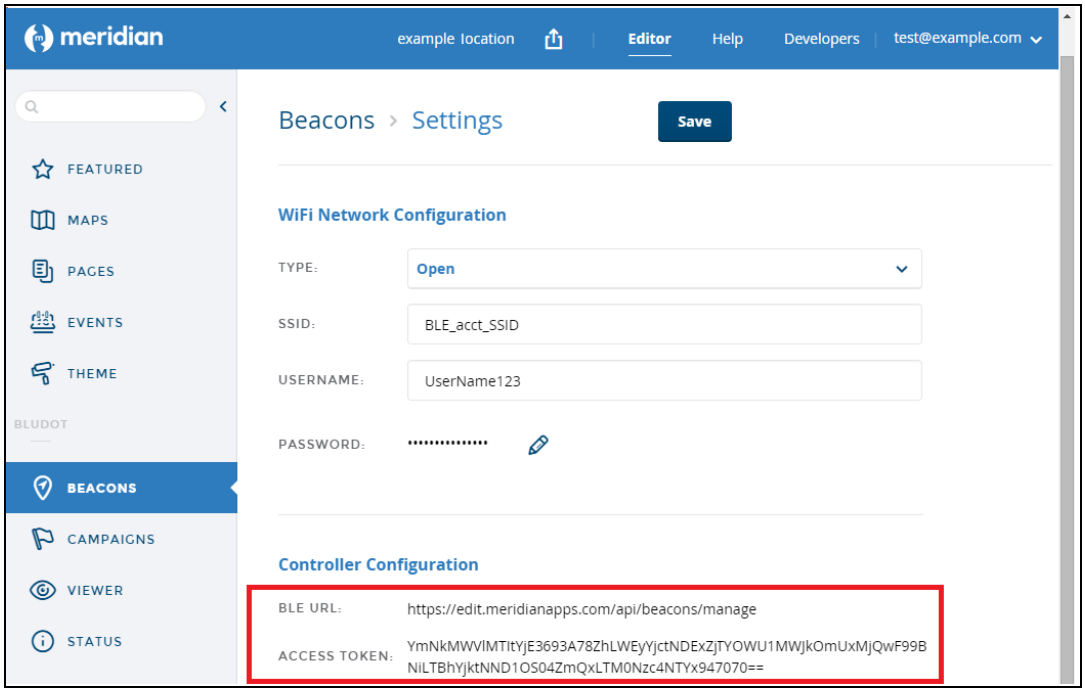
The following procedures describe the steps to configure the controller with the required data for your beacon deployment; the URL of the Meridian Editor (BLE URL) and the access token data from your Meridian account.

Using the WebUI

To configure the controller with the BLE URL and the authorization token for your Meridian account using the controller WebUI:

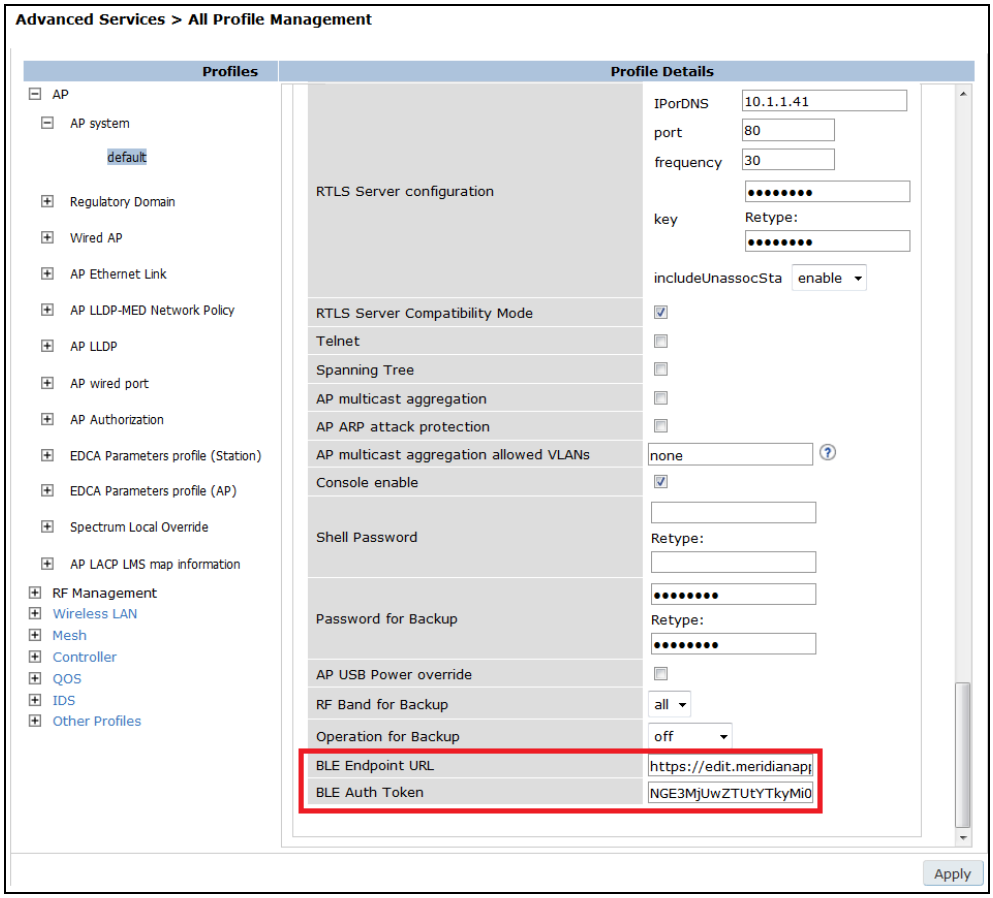
1. Log in to your Meridian account with a Meridian username and password that grants you organization-level privileges.
2. Click the **Beacons** link on the toolbar on the left side of the page.
3. Click the settings () icon on the upper right corner of the page. The **Beacons > Settings** page opens.
4. In the **Controller Configuration** section, copy the BLE URL and Access Token strings into your clipboard or a text file.

Figure 15 *Controller Config Settings in the Meridian Editor*



5. Next, log in to the Aruba controller managing your WLAN.
6. Navigate to **Configuration** > **Advanced Services** > **All Profiles**.
7. In the left window pane, Click **AP** to expand the **AP** menu.
8. Click **AP system** to expand the **AP system** menu.
9. Select the AP system profile for the access point that contains an Aruba beacon.
10. Click the **Advanced** tab.
11. Enter the BLE URL into the **BLE Endpoint URL** field.
12. Enter the access token into the **BLE Auth Token** field.
13. (Optional) If your network has APs that use a different AP system profile, repeat steps 9-12 to apply these changes to the AP system profiles for any other AP with a USB or built-in beacon.
14. Click **Apply**.
15. Click **Save Configuration**.

Figure 16 *BLE Settings in the Controller AP System Profile*



Using the CLI

To configure the controller with the Meridian Editor URL and Meridian authorization token using the controller command-line interface, access the controller command-line interface in config mode, and issue the following commands:

```
(host)(config)# ap-system profile <profile-name>
(host)(AP system profile <profile-name>)# ble-url <URL>
(host)(AP system profile <profile-name>)# ble-token <token>
```

For example:

```
(host)(config)# ap-system profile default
(host)(AP system profile "default")# ble-url https://edit.meridianapps.com/api/beacons/manage
(host)(AP system profile "default")# ble-token
NGE3MjUwZTUtYTkyMi00NmViLTg3MzEtN2NiODM4ZDQ4ZjkyOmU0ZGU3ZGE4LTExZmMtNDJjMS05OGY0LTkxZWFlMzdjMTU5Qg==
```

Firewall Security

The controller contacts Meridian using HTTPS on port 443. Ensure that this port is open in your firewall, or the communication between the controller and your Meridian account will be blocked.

Configure a DNS server

The controller must have access to a DNS server so it can resolve the Meridian URL and communicate with your Meridian account in the cloud.

1. From the controller command-line interface, issue the command **ip name-server <dns-server-ip>** to add a DNS server to your controller.

2. If prompted, save your configuration settings and reboot the controller. The controller may not recognize the DNS server until after it reboots.

Install the USB Beacon

AP-220 series, AP-210 series, and later model access points support USB-powered Aruba beacons. If you are using the beacon in an AP-320 series AP to manage the battery-powered beacons in your deployment, you can skip this task, and proceed to Verify the Controller Configuration.

To install the USB beacon , insert the beacon into an available USB port on a compatible AP that is powered on and active on the network. Figure 17 shows the USB beacon being installed into the USB port on an AP-210 Series access point.

Figure 17 *Inserting the Beacon into a USB port*

Once the beacon is installed, access the controller and reboot the AP. The AP will not recognize an installed USB beacon until it reboots.

To reboot the AP from the controller WebUI,

1. Navigate to **Configuration > AP installation**.
2. Click the checkbox by the AP you want to reboot then click **Provision**. The provisioning window opens.
3. Scroll down and click **Apply and Reboot.**

To reboot the AP from the controller command-line interface, access the command-line interface in config mode and issue the command **apboot ap-name <ap-name>** to reboot the AP.

Verify the Controller Configuration

After the AP reboots, you must verify that the USB beacon is powered up and active on the AP. To do this, access the controller command-line interface and issue the command **show ap debug ble-table ap-name <name>** to display the beacons table. Check to see if the MAC address for the recently installed USB beacon appears in the BLE table. If it appears in the table, that device powered up correctly. In this example, the entry for the USB beacon highlighted in yellow shows that it is powered on, active on the network, and has an uptime of five minutes and 40 seconds.

```
(host) # show ap debug ble-table ap-name AP1

BLE Device Table
```

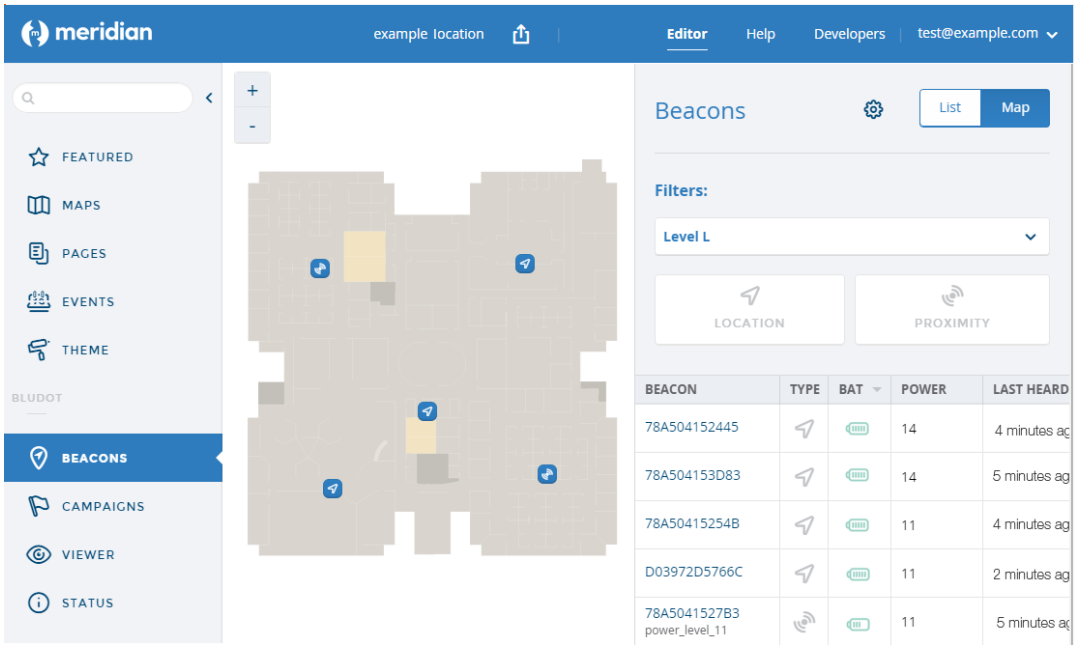
```
----------------
MAC                HW_Type    FW_Ver        Flags   Status  Batt(%)  RSSI  Major#  Minor#
UUID                                  Tx_Power  Last Update  Uptime
---                -------    ------        -----   ------  -------  ----  ------  ------  ---
-                                    --------  -----------  ------
7a:65:04:15:25:2e  LS-BT1     OAD A 1.0-28  0x0011  IA      100      -87   4932    252
4453384E-F99B-4A3B-86D0-9470S8FJ33A78  14        8s          260d:3h:46m:0s
7a:a5:04:15:2f:59  LS-BT1     OAD B 1.0-35  0x0003  IAH     100      -92   1000    1017
237338E1-A8CD-4733-9D4E-E7SDD4B4A5DA  14        172s         80d:23h:50m:0s
6c:e9:ef:1e:3a:58  LS-BT1     OAD B 1.1-4   0x0003  IAH     100      -87   0       0
2352554E-F99B-4SCT-86D0-947070693A78  14        117s         17d:17h:16m:30s
b4:99:4c:5a:ba:23  LS-BT1USB  OAD B 1.1-24  0x0083  LIA     USB      --    16005   16766
23338DEA-1SCT-404B-874D-29AC20909D58  15        10s          0d:0h:05m:40s
Total beacons:3
Note: Battery level for LS-BT1USB devices is indicated as USB.
Note: Uptime is shown as Days hour:minute:second.
Note: Last Update is time in seconds since last heard update.
Status Flags:L:AP's local beacon; I:iBeacon; A: Aruba Beacon; H: Aruba HiPower Beacon
:U:Image Upgrade Pending
```

Monitoring and Managing Beacons with Meridian

To view and change settings for a beacon on your network:

1. Log in to your Meridian account.
2. Click the **Beacons** tab.
3. Click the **Filters** drop-down and to select the map and floor with the beacon you want to manage. The beacons for that location appear in a table beside the location map.

Figure 18 *Beacons at the Selected Location*



4. Select any beacon in the table to view the following details for that device
   - Device Name
   - Type (proximity or location)
   - Power (for proximity beacons only)
   - MAC address

- Major/Minor values

5. To edit the device name, type, or (for proximity beacons only) the transmission power level, click **Edit**.
6. Make the required changes, then click **Save** to save your settings.

Requests for changes are sent to the controller the next time the controller contacts Meridian. Once the controller verifies the configuration is updated on the battery beacon, the controller communicates this to Meridian during the next update interval.

Troubleshooting

To verify that the AP and controller has received the configuration change request from Meridian, access the controller's command-line interface and issue the command **show ap debug ble-update-status ap-name <ap-name>**. The requested configuration change should appear in the **Desired/Pending** column. The example below shows a requested power change for a beacon with the MAC address.

```
(host) # show ap debug ble-update-status ap-name AP1
BLE Device Table
----------------
BLE Device MAC     Actual/Observed                    Desired/Pending
--------------     ---------------                    ---------------
5c:31:3e:fd:8e:4e  14                                 15
6c:ec:eb:1e:30:9d  14                                 14
6c:ec:eb:1e:30:9d  16005                              16005
6c:ec:eb:1e:30:9d  16773                              16773
5c:31:3e:fd:8e:4e  16005                              16005
5c:31:3e:fd:8e:4e  16804                              16804
Total beacons:6
Devices marked "Ineligible" are currently not capable of being upgraded.
```

Run the command again after some time to see if the change has taken effect.

```
(host) # show ap debug ble-update-status ap-name AP1
BLE Device Table
----------------
BLE Device MAC     Actual/Observed                    Desired/Pending
--------------     ---------------                    ---------------
5c:31:3e:fd:8e:4e  15                                 15
6c:ec:eb:1e:30:9d  14                                 14
6c:ec:eb:1e:30:9d  16005                              16005
6c:ec:eb:1e:30:9d  16773                              16773
5c:31:3e:fd:8e:4e  16005                              16005
5c:31:3e:fd:8e:4e  16804                              16804
Total beacons:6
Devices marked "Ineligible" are currently not capable of being upgraded.
```

Ineligible Devices

The output of the **show ap debug ble-update-status** command may include a note about ineligible devices. The **ineligible** flag was applied to some very early versions of Aruba beacon which were not capable of configuration upgrades. This issue was resolved in subsequent releases, and now all Aruba beacons currently being sold support configuration upgrades.

Hi-Power Beacons

For distant or lower-power beacons that the USB beacon cannot hear very well, use the **show ap debug ble-counters ap-name <name>** command to check when a battery beacon goes to HiPower mode. The **HiPwr** column of the BLE device table shows the number of times the AP detected the beacon transmitting in Hi Power mode.

```
(host) # show ap debug ble-counters ap-name AP1


BLE Device Table
----------------
MAC                Major#  Minor#  iBeacon     ScanRspV0   ScanRspV1   HiPwr   RSSI  LastUpdate  CfgRx                 CfgTx
---                ------  ------  -------     ---------   ---------   -----   ----  ----------  -----                 -----
78:1e:04:15:25:2e  4932    252            530         229           0       1  -88   3s          NoUpdate              NoUpdate
78:a5:04:15:2f:59  1000    1017           324         125           0       9  -90   15s         NoUpdate              NoUpdate
bc:6b:29:43:5d:d9  48850   13010         1521           0           0       0  -84   3s          NoUpdate              NoUpdate
78:a5:04:15:6b:6f  4932    56               1           0           0       7  -92   2321s       NoUpdate              NoUpdate
5c:43:3e:fd:8e:4e  16005   16772           21           0          15       2  -87   533s        07-07-2015 17:58:30   07-07-2015 17:49:39
bc:6b:29:33:5b:5d  294     23735         1040           0           0       4  -89   7s          NoUpdate              NoUpdate
6c:ec:6b:1e:30:9d  16005   16753           10           0           1       0  -90   1132s       07-07-2015 17:58:30   NoUpdate
5c:31:3e:43:d6:16  16005   16449            2           0           9      11  -83   11s         NoUpdate              NoUpdate
```

A *campaign* is the mechanism by which location and time-based push notifications are sent to visitors using a Meridian-powered app. Campaigns designed to push location-based notifications send a customized message or link to a mobile device running a Meridian-powered app when that device first comes within signal range of a proximity beacon associated with that campaign. Campaigns can also send time-based push notifications to mobile devices according to a defined schedule. Time-based campaigns can send a message or link to a device running a Meridian-powered app if that device comes in range of a proximity beacon during a selected time range, or send messages to users in signal range of a proximity beacon on a regular, reoccurring schedule, such as every Wednesday, or the first Saturday of every month.

Meridian campaigns can also notify your own custom endpoint when a device with a Meridian-powered app comes within range of a proximity beacon associated with that campaign, passing along login information for that user, as well as information about the venue location and campaign that was triggered.

Meridian campaigns automatically throttle the rate of notifications sent to a single user by observing a cooldown period between broadcasts, ensuring that no single user is subjected to excessive campaign notifications while they remain in your venue. Even if you have multiple campaigns defined within one area of your venue, Meridian will only send a notification to the same device once every 5 minutes, and a campaign can only be triggered by the same device once every 12 hours.

This chapter describes the basic steps to configure and test a push notification campaign. For complete information on creating a campaign using the Meridian Editor, refer to the Meridian online help at http://docs.meridianapps.com/help/beacons_app_deploy.

Creating a Campaign

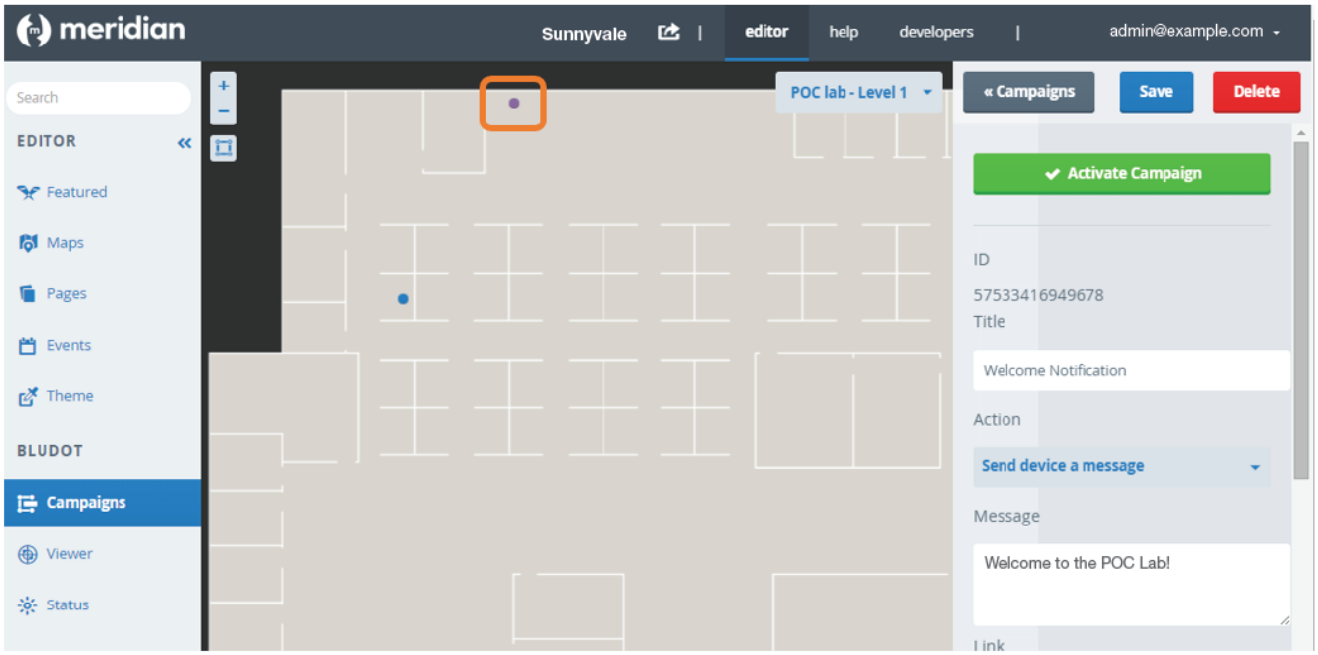
Use the following procedure to configure a campaign with the Meridian Editor that triggers an action on an iBeacon-compatible, Bluetooth-enabled device when that device comes in signal range of an Aruba proximity beacon.

When configuring and associating campaigns with proximity beacons, keep in mind that iOS devices can not process more than twenty push notifications, regardless of the number of proximity beacons around the device.

1. Log into your Meridian Editor account at https://edit.meridianapps.com, and select the venue location where you want customers to receive push notifications. Note that there is approximately a ten minute delay between the time a proximity beacon is first deployed and the time that beacon appears in the Meridian editor.
2. Select **Campaigns**.
3. Click the floor drop-down list at the top of the map, and select a floor.
4. Click the add (+) icon in the upper right corner of the window to associate a new campaign to a beacon on the selected floor.
5. Enter a title for the new campaign, then click **OK**.
6. Click on any beacon on the floor map to associate that beacon to the campaign. The Editor displays a popup window in which you can define the campaign settings.
7. Click the **Action** drop-down list and select one of the following options:
   - **Send device a message**: Send a message to the iBeacons-enabled device.
   - **Notify a custom end-point**: Send a query to a specified URL.

8. Configure the message text or endpoint URL.
9. Select one of the following broadcast types:
   - **Always**: Perform the specified action every time the action is triggered
   - **Scheduled**: Perform the specified action during the specified time frame. You can also define a repeating schedule, for actions that should repeat on a weekly or monthly schedule.
10. Click **Activate Campaign**.
11. Click **Save** to save your settings. Once the campaign is associated to a beacon, the campaign name will be highlighted in the Meridian Editor when you hover your mouse over that beacon.

Figure 19 *Creating a Campaign using the Meridian Editor*



Testing a Campaign

Once you have defined a campaign, you can use the Beacons app to test a campaign associated with your Meridian account. Note that the Beacons app is only used to test existing campaigns; new campaigns must be configured using the Meridian Editor.

NOTE

You and your mobile device must be physically present in the location where you are testing the campaign.

Use the following procedure to test an active campaign using the Beacons app.

1. To simplify the testing procedure, reduce the range of the proximity beacon by lowering its transmit power level. Start the test by standing farther away from the beacon (outside its range).
2. Tap the campaigns icon ( )to display the **Campaigns** tab, then tap and select an active campaign. Once you have selected a campaign, the Beacons app displays information about the selected campaign, including the action type, message or query URL, and broadcast schedule.
3. Tap the maps icon ( ) at the bottom of the screen to begin the test.

The mobile device running the Beacons app appears on the map as a small blue dot if beacons are deployed in the area. The beacon(s) associated with the campaign appear on the map as a blue or green pointer icon.

- **Blue pointer icon** (): The mobile device is outside the range of the proximity beacon.
- **Green pointer icon with a signal meter** (): The device has come within range of the beacon, and the push notification is triggered.
- **Green pointer icon with exclamation point** (): The device moved outside the range of the proximity beacon after the notification was triggered.
- **Green pointer icon with exclamation point and timer** (): The device moved outside of the range of the proximity beacon after the notification was triggered, and the campaign cooldown period has begun.

4. Move the mobile device closer to the proximity beacon, until the beacon appears as a green pointer icon with a signal meter, and the push notification is triggered on that device.
5. Move the mobile device further away from the beacon, until the device is outside the beacon's range. This is when the 30 second cool-down period starts, as indicated by the green beacon icon with the timer.

Once your mobile device is out of range of the beacon, that device will not receive a duplicate notification from that beacon until the campaign is reset. If you are outside the range of the beacon for the entire 30-second cooldown period, the beacon icon will appear as a blue pointer again, meaning you can manually reset the campaign associated with the beacon and run the test again.

Campaigns are automatically reset 12 hours after the device moves and remains out of range of the beacon.

To manually reset all campaigns for your device:

1. Tap the campaigns icon () to display the **Campaigns** tab.
2. Click **Reset**. A popup window appears, indicating that "Campaign cooldowns have been reset."

The beacon Received Signal Strength Indicator (RSSI) seen by a iBeacon-enabled client depends upon the beacon's power level, orientation, and the distance from the client. The signal strength is greatest for clients directly in front in the beacon. A client located to the side of the beacon or behind the beacon may detect a slightly lower signal strength than a client directly in front of the beacon, even if those clients are the same physical distance from the beacon.

Table 2 shows the results of informal RSSI testing for a sample beacon at the default power level 14, measured at varying distances from the beacon, and either directly in front of the beacon (0 degrees), behind the beacon (180 degrees), to the left side of the beacon (-90 degrees), and the right side of the beacon (90 degrees). Measurements were taken by the Texas Instruments Bluetooth low energy Multitool app on an iPhone 5C.

Table 2: *RSSI Testing at Power Level 14*

Distance (m)	RSSI, in -dBm			
	0 degrees	**180 degrees**	**-90 degrees**	**90 degrees**
1	68	70	-75	67
2	72	71	80	72
3	78	76	79	76
4	80	81	83	82
5	81	83	84	83
7	84	84	86	84
9	86	87	90	88
11	92	83	89	89
14	95	88	86	92
17	94	86	91	94
20	94	90	94	98
25	94	94	93	99

Table 3 below shows the results of informal RSSI testing for a beacon at power level 11.

Table 3: *RSSI Testing at Power Level 11*

Distance (m)	RSSI, in -dBm			
	0 degrees	**180 degrees**	**-90 degrees**	**90 degrees**
1	75	75	82	72
2	76	76	85	78
3	85	81	88	82
4	83	84	90	86
5	92	89	91	88
7	86	92	93	92
9	91	93	95	94
11	95	94	96	96
14	92	95	97	95
17	98	94	100	100
20	100	97	99	102
25	102	98	102	*

* RSSI value could not be measured.

Table 4 below shows the results of informal RSSI testing for a beacon at power level 3.

Table 4: *RSSI Testing at Power Level 3*

Distance (m)	RSSI, in -dBm			
	0 degrees	**180 degrees**	**-90 degrees**	**90 degrees**
1	91	93	101	90
2	97	91	100	95
3	98	95	*	97
4	100	99	*	102

Distance (m)	RSSI, in -dBm			
5	101	101	103	*
7	103	*	*	*
9 (and greater)	*	*	*	*

* RSSI value could not be measured.

Aruba Beacons version 1.0.8 and later versions of the Beacon app provide more granular transmission power settings for proximity beacons than earlier versions. The following table shows the correlation between the old transmission power settings in the earlier version of the app, and the power settings available in the current versions.

Table 5: *Transmission Power Settings*

Old Setting TX Power Level	New Setting TX Power Level	TX Power (in dBm)
-3	0	-29
-2	1	-27
-1	2	-25
0	3	-23
n/a	4	-21
	5	-18
	6	-16
	7	-14
	8	-12
	9	-10
	10	-8
1	11	-6
n/a	12	-4
	13	-2
2	14	0
3	15	4