Aruba Instant On 1.4.0 User Guide

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 Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This User Guide describes the features supported by Aruba Instant On 1.4.0 and provides detailed instructions for setting up and configuring the Instant On network.

Intended Audience

This guide is intended for administrators who configure and use Instant On APs.

Related Documents

In addition to this document, the Aruba Instant On 1.4.0 product documentation includes the following:

- Aruba Instant On Access Point Hardware Documentation
- Aruba Instant On 1.4.0 Release Notes

Contacting Support

Table 2: *Contact Information*

Main Site	arubainstanton.com
Support Site	support.arubainstanton.com
Instant On Social Forums and Knowledge Base	community.arubainstanton.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	community.arubainstanton.com/t5/Contact-Support/ct-p/contact-support
EULA	https://www.arubainstanton.com/eula/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

The Instant On Solution is a simple, fast, and secure solution designed for small business networks. It is an affordable to own and easy-to-use solution that is ideal for the businesses with simple technology requirements and setups that do not have IT staff. The product offers the very latest Wi-Fi technology so that your business can have fast experience even in a busy office or store.

Instant On mobile app and web application in the Instant On Solution suite enables provisioning, monitoring, and managing your networks. Instant On offers the following benefits:

- Mobile app and web application based quick setup and faster network bring-up
- Ease of use and right-sized feature set
- Simple statistics to view the network health and usage
- Remote monitoring capabilities
- Simple troubleshooting

Key Features

The key features introduced as part of the Aruba Instant On app are:

- Monitoring Site Health
- Configuring Networks
- Analyzing Application Usage
- Managing Clients
- Managing Sites Remotely

Supported Devices

Aruba Instant On currently supports the following APs:

Indoor Instant On APs

- AP11
- AP11D
- AP12
- AP15

Outdoor Instant On APs

- AP17

Whats New in this Release

This section lists the new features, enhancements, or hardware platforms introduced in Aruba Instant On 1.4.0.

New Features and Hardware Platforms

Table 3: *New Features in 1.4.0*

Feature	Description
Enhancements to the Clients Page	The Clients page now displays the list of connected and blocked clients in separate tabs.
Enhancements to the Applications Page	The following enhancements are introduced: ■ The Applications page now lists the Traffic usage per client. ■ A message is displayed on the UI when a client tries to access an application which is blocked, indicating that the administrator has restricted access to the category.
Enhancements to the Networks Page	The Networks page now allows you to block or unblock the application categories for specific networks.
Extend 2.4 GHz Range	A new option is added to disable or enable data transfer using 802.11b rates on the network.
Mesh Outdoor AP Deployment Scenarios	A new option is added to include or exclude the discovery of over-the-air outdoor access points when extending your network.
Open Security Option for Guest Networks	A new option is added to differentiate Open guest networks from portal and PSK-based guest networks.
PPPoE Configuration	You can choose to configure PPPoE for your Instant On device by using your ISP provided credentials.
Quiet Lights Mode	You can now turn on or off the device status light using the Quiet lights mode toggle switch.
RADIUS Proxy Configuration	You can now configure a RADIUS proxy and specify if the site should use a single IP address to communicate with the RADIUS server.
Replacing Router	You can now replace a router from the Inventory when it goes offline.
Radio Management	You can now configure a channel width and channel selection on which the APs at the site should operate.
Setting Radio Frequency	The Instant On mobile app and web application now allow you to set radio frequencies for your wireless network.
Visibility and Control	The Visibility and control option in the Applications page allows you to switch between detailed view of applications usage versus a condensed view.
Deploy Multicast Services	Instant On solution supports a variety of multicast services, which are typically performing streaming of content from a phone, tablet or laptop to a connected TV or speakers.

This chapter describes the following procedures:

Downloading the Mobile App

The Aruba Instant On mobile app enables you to provision, manage, and monitor your network on the go.

To start using the Instant On mobile app, perform the following actions:

1. Download the app on your smartphone
   - To install the app on iPhone, go to Apple App Store and search for Aruba Instant On.
   - To install the app on Android phones, go to Google Play Store and search for Aruba Instant On.
2. Launch the Instant On application and follow the on-screen instructions to complete the setup.

Alternatively, you may choose to complete the setup on a web browser using the Instant On web application. For more information, see Accessing Aruba Instant On Application.

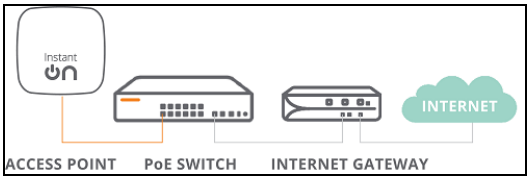
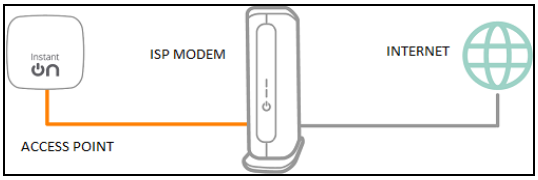
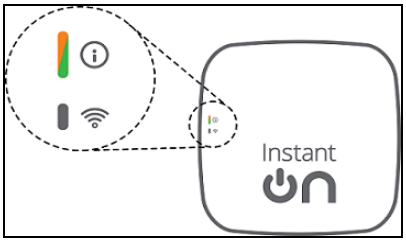
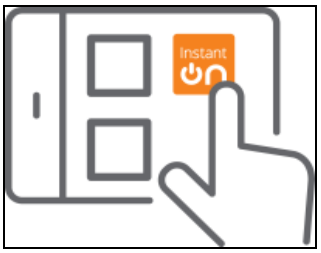
Setting Up Your Network

The Instant On Solution requires you to connect the Aruba Instant On APs to your wired network that provides internet connectivity.

Provisioning the Instant On Network

To provision your network, follow these steps:

Table 4: *Instant On Network Provisioning*

SL No	Steps	Illustration
1.	**Private Network Mode**—Power on the Aruba Instant On AP using the power adapter or using a Power over Ethernet (PoE) port on a PoE capable switch. Ensure that the AP is connected to your network using an Ethernet cable (included in the box).	
	Router Mode—Connect the E0/PT or ENET port of the Instant On device acting as a primary Wi-Fi router to the ISP provided modem using an Ethernet cable.	
2.	Verify the LED indicators, to check if the AP is successfully connected to your provisioning network and is ready for you to configure, the LED indicator starts blinking alternatively between green and amber.	
3.	Download the mobile app on your Android or iOS device. For more information, see Downloading the Mobile App. As an alternative, you may choose to configure the Instant On AP using the web application. For more information, see Accessing Aruba Instant On Application.	
4.	Launch the Instant On application and follow the on-screen instructions to complete the setup.	

AP Configuration Modes

Before you begin to add devices to a site during the initial setup, you must decide the mode in which the APs should be deployed in the network. Aruba Instant On currently supports the following modes in which your Instant On access points can be deployed:

Private Network Mode

The Instant On devices will be part of a private network behind a gateway or a firewall before reaching the internet. Use this mode if you already have a local network infrastructure in place that includes a DHCP server as well as a gateway or a firewall to the Internet.

Pre-Requisites

Before you begin to provision your Instant On AP, ensure that the following pre-requisites are adhered to:

- A working internet connection.
- A switch that is connected to the Internet gateway or modem.
- A DHCP server to provide IP addresses to the clients connecting to the Wi-Fi network. The DHCP server may be offered by the switch or the Internet gateway. This does not apply if you are configuring the network in NAT mode.
- TCP ports 80 and 443 and UDP port 123 should not be blocked by a firewall.
- The Instant On APs must be powered on and have access to the internet.

Configuring Your Instant On Devices in Private Network Mode

Follow these steps to add your Instant On devices to the network in private mode:

1. Connect the E0/PT or ENET port of the Instant On devices to your local network using an Ethernet cable.
2. Power on the Instant On devices. Alternatively, you can power on the devices using a Power over Ethernet (PoE) switch or a power adapter.
3. Observe the LED lights on the Instant On devices. It may take up to 10 minutes for new devices to upgrade their firmware and boot up. The devices will be ready to be discovered on the Instant On mobile app when the LED lights are alternating between green and amber.
4. Enable location and bluetooth services and set the Aruba Instant On app permissions to use location and bluetooth services in order to automatically discover nearby Instant On devices.
5. Review and add the devices to your network.

Router Mode

In the Router mode, an Instant On device will be connected directly to a modem supplied by your Internet Service Provider (ISP) and it will be your primary Wi-Fi router in the network. In this mode, the Instant On device will offer DHCP, gateway, and basic firewall services for your network. The Instant On AP also offers a provision configure and establish a PPPoE connection with the ISP.

Pre-Requisites

Before you begin to provision your Instant On AP as a primary Wi-Fi router, ensure that the following pre-requisites are adhered to:

- A working internet connection provided by your Internet Service Provider (ISP).
- TCP ports 80 and 443 and UDP port 123 should not be blocked by a firewall.

- The Instant On AP must be directly connected to the internet modem with no other device in between. It must therefore be the only AP connected to the internet. Other APs have to be powered down initially and added later through mesh using the extend network capability.

Configuring Your Instant On Device in Router Mode

Follow these steps to add your Instant On devices to the network in router mode:

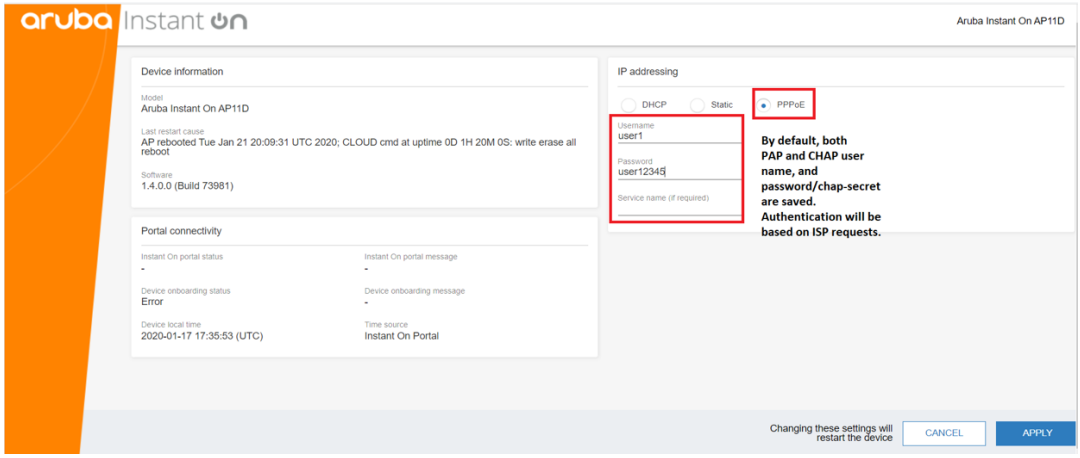
1. Connect the E0/PT or ENET port of the Instant On device acting as a primary Wi-Fi router to your modem using an Ethernet cable.
2. Power on the primary Wi-Fi router.
3. Observe the LED lights on the primary Wi-Fi router. It may take up to 10 minutes for new devices to upgrade their firmware and boot up. The router will be ready to be discovered on the Instant On mobile app when the LED lights are alternating between green and amber.
4. Enable location and bluetooth services on your mobile device and set the Aruba Instant On app permissions to use location and bluetooth services in order to automatically discover nearby Instant On devices.
5. Tap **Find my Device** on the Instant On mobile app to begin searching the network for nearby devices.

NOTE: After the end of the search, if the mobile app detects more than one primary Wi-Fi router in the area, tap the **Resolve** tab to choose the preferred device as the primary router.

In the Router mode, the network can only be extended over-the-air. For more information, see Extend over-the-air (Mesh).

Setting Up PPPoE for Your Network

PPPoE configuration is possible only when the Instant On AP is connected as a primary Wi-Fi Router and must be done before onboarding Instant On AP(s). The local web server on the device will offer to configure PPPoE only when the Instant On AP is in its factory default state and not if a DHCP address was obtained. Once the AP is connected to the cloud, the PPPoE configuration will not be available for modifications anymore. However, If the AP loses connectivity to the cloud and PPPoE failures are detected, you can access the local WebUI and update the settings again.



Follow the steps below to configure PPPoE on your network:

1. The Instant On AP should be connected to the ISP provided modem but does not have an IP address provided by the DHCP server.
2. The AP will broadcast an open SSID **InstantOn-AB:CD:EF**, where AD:CD:EF will correspond to the last three octets of the MAC address of the AP.
3. Connect your laptop or mobile device to the SSID and access the local web server through **https://connect.arubainstanton.com**. The local WebUI configuration page is displayed.
4. Under **IP addressing**, select the **PPPoE** radio button.
5. Enter the PPPoE **Username** and **Password** provided by your ISP, in the respective fields.
6. Click **Apply**. The AP will reboot once the PPPoE configuration is applied.
7. Wait for the LED lights to flash green and orange. This indicates that the PPPoE link is up and stable, you will see the device onboarding status now reads **"Waiting to be onboarded.."**. This step might take a few additional minutes, if the AP upgrades its firmware during the reboot process.
8. You can now proceed to creating a new site and adding devices. For more information, see Setup a New Site.

NOTE: If an AP with the PPPoE configuration is removed from the Inventory or the site is deleted, the AP will move to its factory default state and the PPPoE configuration will be erased from the AP.

Discovering Available Devices

There are multiple ways to add an Instant On AP to a site during the initial setup. You may choose any of the following methods to add devices for the first time and complete setting up your network:

- BLE Scanning—The Instant On mobile app or web application scans for nearby devices through BLE and displays the APs discovered, on the screen. Tap or click the **Add devices** button to add the devices discovered to the site. Alternatively, click **Search again** if there are more devices to be displayed. If the BLE

scanning fails to discover any devices in the vicinity, tap the **Add devices manually** tab and choose to add devices to your network by entering the serial number or by scanning the barcode of the AP.

- Serial Number— Enter the serial number located at the back of your Instant On AP and click **Add device**.
- Barcode Scanning—As an alternative to manually entering the serial number to add devices, tap the barcode scan icon on the mobile app and scan the barcode at the back of your Instant On AP.

BLE Troubleshooting

BLE troubleshooting happens automatically during the auto-detection of APs in the initial setup. If an error is detected you will see a message in the mobile App that helps you to troubleshoot any network or device related issues and complete the network setup successfully.

Multiple Sites

When you login to the Aruba Instant On mobile app using your administrator account credentials, the **My Sites** page is displayed if multiple Aruba Instant On sites are registered to your account. To view or manage the settings of a particular site, click on any of the registered sites listed on this page.

Account Management

To navigate to the **Account Management** page:

1. Click the **Account management** icon in the homepage of the Instant On mobile app or web application.

NOTE: The alphabet in the icon will appear based on the first letter of your registered email account.

2. Select **Account management** from the list to view the account settings. For more information, refer to Managing Your Account.

Setup a New Site

The Instant On application prompts you to set up a new site when you sign on to the app for the first time. The site must have at least one network which would be used as the main network. You can configure up to a maximum of 8 networks in a site.

1. To register a new Instant On site to your account:
   - In the mobile app—Tap the advanced menu (☰) icon and select **Setup a new site**. You will be redirected to the initial setup page.
   - In the web application—Click ⚙ **Setup a new site** from the drop-down list. You will be redirected to the initial setup page.
2. Follow the instructions given in Setting Up Your Network to add a new Instant On site.
3. If you already have more than one site configured, and would like to setup a new site under your registered account:
   - In the mobile app—Tap the advanced menu (⋮) icon in the **My Sites** screen.
   - In the web application—Click ⚙ **Setup a new site** and select **Continue**.

Sign Out

Click on this field to sign out from your Aruba Instant On account.

Help & Support

Takes you to the **Contact support** page. Following are the available technical support options:

- **Help center**—Opens the Aruba Instant On documentation portal. For more information, see https://www.ArubaInstantOn.com/docs.

- **Support center**—Opens the Aruba Instant On Support Portal, which provides information on warranty and support policy for the product you selected and also the on-call technical support. For more information, see https://community.arubainstanton.com/t5/Support/ct-p/Support.

Support resources—Allows you to generate a support ID by clicking on the **Generate Support ID** button. The ID is then shared with Aruba Support personnel to run a diagnosis on your device.

Deploying Multicast Services

The Instant On solution supports a variety of multicast services, which are typically performing streaming of content from a phone, tablet or laptop to a connected TV or speakers.

Some of the main services supported are:

- AirPlay™—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirDrop™—Apple® Airdrop allows you to share and receive photos, documents and more with other Apple devices that are nearby.
- Google Cast—This protocol is built-in to Chromecast devices or Android TV and allow playing audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.

The devices and multicast services can be discovered and accessed by wireless clients when they are located on the same network.

To configure multicast services with Instant On:

In Private network mode

- The Network must be configured as an Employee network. For more information on employee network, see Employee Network.
- The **IP and VLAN Assignment** settings must be set to **Same as local network (default)**. You may **Assign a VLAN to your network** if required by your local network. For information on IP and VLAN settings, see IP and VLAN Assignment
- Devices offering the service and clients using the service must be connected to the same Wi-Fi Network or local network and same VLAN if you choose to assign one.

NOTE: Multicast services on Guest networks or Employee networks configured with the option **Specific to this network** are not supported.

In Router mode

- The Network must be configured as an Employee network. For more information on employee network, see Employee Network.
- The **IP and VLAN Assignment** settings can be set to either **Same as local network (default)** or **Specific to this network**. For information on IP and VLAN settings, see IP and VLAN Assignment
- Devices offering the service and clients using the service must be connected to the same Wi-Fi Network.
- Alternatively, if an AP11D is used as the primary Wi-Fi router, the clients and services connected to ports E1, E2, E3 are also supported.

NOTE: Multicast services on Guest Networks or located on the WAN uplink are not supported.

Examples

Following are some of the examples for deploying multicast services:

- Private network mode with a combination of wired and wireless clients and services.
- Router mode with clients and services on same wireless network.
- Router mode with clients and services on same wired network.

Accessing Aruba Instant On Application

Ensure that your system meets the following device OS and browser requirements to access the Instant On mobile app or web application.

Mobile OS Requirements

The following mobile OS versions support the Aruba Instant On mobile app:

- Android 7 or later versions
- iOS 11 or later versions

Browser Requirements

The following versions of the web browsers support the Instant On web application:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

Create an Instant On Account

Follow these steps to create an Instant On account:

1. Launch the Instant On mobile app or web application.
2. Click **Create an account** to create a new Instant On account.
3. Enter an email ID in the **Email** field. The email ID should not be associated with another Instant On account.
4. Enter a password in the **Password** field.
5. Select the **End User License Agreement and Data Privacy Policy and Security Agreement** checkbox.
6. Click **Create Account**.
7. A verification email is sent to your email account. Follow the instructions in the email to activate your Instant On account.

NOTE: The email notification with the verification link might sometimes end up in the junk email folder instead of your inbox.

---

8. Once the above steps complete, click **Continue** on the mobile app or web application. You have now successfully registered an Instant On account.

You can use the same account credentials to sign in to the mobile app, web application, community site, or support site.

Logging in to Instant On

To log in to the Instant On application, launch the Aruba Instant On mobile app or web application.

In the Mobile App

If you are signing in for the first time, enter the registered email ID and password in the **Email** and **Password** boxes respectively, and then click **Log in**. For all future logins, the Instant On app stores the credentials and attempts to validate the same, every time the app is launched. Hence, for all future logins, the Instant On mobile app or web application displays the home page directly.

In the Web Application

1. Open a browser.
2. Type **https://portal.arubainstanton.com** in the address bar and press the **Enter** key.
3. If you are signing in for the first time, enter the registered email ID and password in the **Email** and **Password** boxes respectively, and then click **Log in**. For all future logins, the credentials are saved based on the web browser settings.

NOTE: The home page is displayed based on the number of sites associated with your account. For multiple sites associated with your account, you have the option to choose a site from the list before you are taken to the respective home page.

Follow the onscreen instructions to complete the access point setup, if the Instant On mobile app or web interface is launched for the first time.

Resetting Your Account Password

To reset your Instant On login password, follow these steps:

1. Click **Forgot your password?** on the login screen.
2. Enter the email address associated with your Aruba Instant On account in the space provided.
3. Click **Reset password**. The instructions to create a new password will be sent to your email address.
4. Open the link provided in the email. The change password page is displayed.
5. To change the password of your Instant On account, confirm your email address and enter a new password.
6. Click **Change Password**. An acknowledgment message that your password has been changed successfully is displayed on the screen.

NOTE: The email notification with the Reset password link may sometimes end up in the junk email folder instead of your inbox.

Managing Sites Remotely

Remote access allows you to configure, monitor, and troubleshoot Aruba Instant On deployments in remote sites.

- When an Instant On site is deployed and configured, it establishes a connection to the Instant On cloud, which allows you to access and manage sites remotely. The site information and account credentials associated with the site are registered and stored in the cloud. After the Instant On site is registered, it can be accessed and managed remotely through the Instant On application.

NOTE: The remote site must have access to the Internet in order to connect to the Instant On cloud. If the site loses Internet connectivity and fails to establish a connection to the cloud, you will not be able to access the site remotely.

- When you log in to the Instant On application, the entire list of sites associated with your account is displayed. Select a site from the list for which you want to initiate a remote access session. When the remote access session is established, you can begin managing the site remotely.

NOTE: The list of sites is only displayed if your account is associated with multiple sites. If your account is only associated with one site, the Instant On application connects directly to that site.

Username and Password Management

You can change your account username or password at any point in time remotely. The Instant On application automatically communicates with the Instant On cloud to update the credentials for all sites associated with the account.

Aruba Instant On User Interface

The Aruba Instant On user interface allows you to create, modify, and monitor network components from a central location. The user interface is designed to offer ease-of-use through an intuitive layout and simple navigation model.

The Instant On user interface comprises of a header, and the Instant On modules.

Figure 1 *Web Application User Interface Overview*

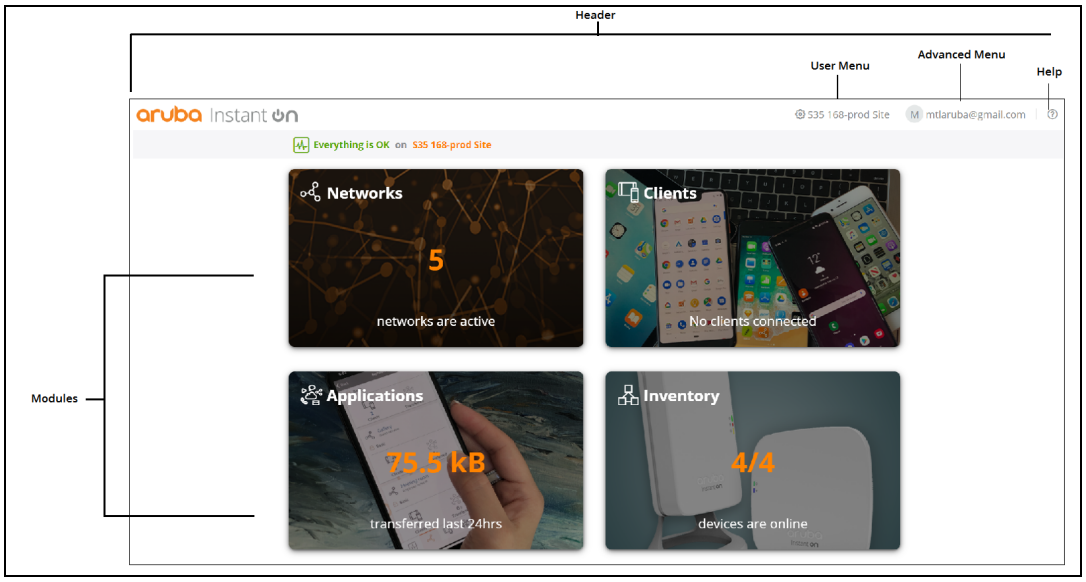
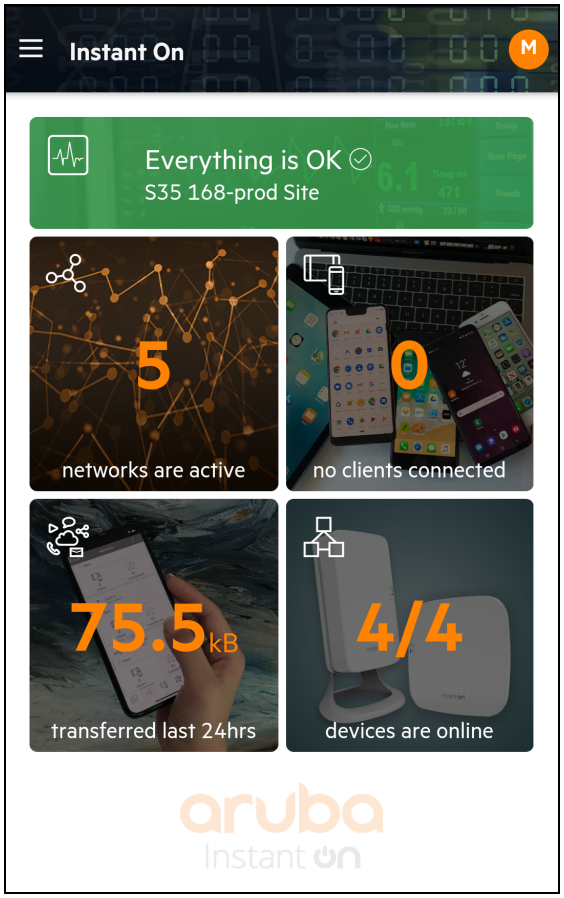


Figure 2 *Mobile App User Interface Overview*



Configuring Menu Items in the Header

The header includes the following menu items:

Table 5: *Menu Items in the Header*

Header Content	Description	Mobile App	Web Application
Alert Notification ( )	Displays the alerts that are triggered by the system when an unusual activity is observed on the network. See Alerts for more information.	Yes	Yes

Table 5: *Menu Items in the Header*

Header Content	Description	Mobile App	Web Application
Settings menu icon (for desktop ⚙) or advanced menu icon (for mobile ☰)	Displays the site name and provides menu options to administer your account and the sites associated with it.	Yes	Yes
	Help & Support (?)—Leads you to the **Contact support** page. Following are the available technical support options: ■ **Help center**—Opens the Aruba Instant On documentation portal. For more information, see https://www.ArubaInstantOn.com/docs. ■ **Support center**—Opens the Aruba Instant On Support Portal, which provides information on warranty and support policy for the product you selected and also the on-call technical support. For more information, see https://community.arubainstanton.com/t5/Support/ct-p/Support. **Support resources**—Allows you to generate a support ID by clicking on the **Generate Support ID** button. The ID is then shared with Aruba Support personnel to run a diagnosis on your device.	Yes	No
	Site management—Allows you to modify various account settings, including time zone and notifications. For more information, see Site Management.	Yes	Yes
	Add a new device—Opens the Extend my network page and allows you to add a new device. For more information, see Extending your Network.	Yes	Yes
	Connect to another site—Allows you to connect to another Instant On account. After clicking **Connect to another site**, you are logged out of your account and automatically redirected to the Aruba Instant On login page. Enter the registered email ID and password to access the respective Aruba Instant On. If you have multiples sites configured under the same administrator account, you will be redirected to the **My Sites** page from where you can select one of the listed sites.	Yes	Yes
	Setup a new site—Allows you to setup a new Aruba Instant On site. For more information, see Setting Up Your Network.	Yes	Yes
	About—Displays the software image version and the mobile app version that is currently installed on the Aruba Instant On site. See About Software for more details.	Yes	No

Table 5: *Menu Items in the Header*

Header Content	Description	Mobile App	Web Application
Registered email ID **NOTE:** The alphabet displayed is the first letter of your email ID.	Displays the account username registered email ID and provides options to administer account information and setup notifications or alerts. **Account management**—Allows you to modify your account information for all associated sites. For more information, see Managing Your Account. ■ **Change password**—Allows you to modify the password for the account. For more information, see Managing Your Account ■ **Notifications**—Allows you configure the notification settings for the alerts received from the site. For more information, see Notifications.	Yes	Yes
	Sign out—Allows you to log out of your Aruba Instant On account.	Yes	Yes
(?)	**Help**—Opens the Instant On online help documentation.	No	Yes
	Support—Leads you to the following support options: ■ **Contact Support**—Clicking the **Support Center** link opens the Aruba Instant On Support Portal, which provides information on warranty and support policy for the product you selected and also the on-call technical support. For more information, see https://community.arubainstanton.com/t5/Support/ct-p/Support. ■ **Support resources**—Allows you to generate a support ID by clicking on the **Generate Support ID** button. The ID is then shared with Aruba Support personnel to run a diagnosis on your device.	No	Yes
	About—Displays the software image version for the web application.	No	Yes

Configuring Settings in the Modules

Modules allow you to configure and monitor network components such as application usage and system alerts.

The Instant On user interface consists of the following modules:

■ **Site Health**: Provides the health status of devices connected to the network. See Monitoring Site Health for more information on the **Site Health** module.

■ **Networks**: Provides a summary of the networks that are available for primary and guest users. See Configuring Networks for more information on the **Networks** module.

■ **Clients**: Provides connection information for the clients in your network. See Managing Clients for more information on the **Clients** module.

■ **Applications**: Provides daily usage data for the different types of applications and websites accessed by clients in the network. See Analyzing Application Usage for more information on the **Applications** module.

■ **Inventory**: Specifies the number of devices on the site that are UP. This page also allows you to add a new device or remove an existing device. See Viewing and Updating Inventory for more information on the devices on the site.

Opening a Module

To open a module, click one of the following module tiles on the Instant On home page:

Table 6: *Module Tiles*

Module	Tile
Site Health	
Networks	
Clients	
Applications	
Inventory	

After opening a module, you can switch to another module by clicking one of the module tiles at the bottom of the page.

Closing a Module

In the Web Application—To close a module and return to the Instant On home page in the web application, do one of the following:

- Click **X** at the top-right corner of the module.
- Click the Aruba Instant On logo at the top-left corner of the page.

In the Mobile App—Click the back arrow (←) on the title bar of the mobile app to exit the module.

Site Management

The **Site Management** page displays the following user settings that can be modified in the Aruba Instant On application:

- Administration
- Time zone
- Guest portal
- Software update
- Device status lights

Viewing Site Management Settings

To view the **Site Management** page, follow these steps:

- In the web application—Click the settings menu () icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Site Management** page is displayed.
- In the mobile app—Tap the advanced menu () icon on the Aruba Instant On home screen. Select **Site management** from the menu.

Administration

The **Administration** page allows you to modify administrator information, including your Aruba Instant On site name and account credentials. You can also add a secondary administrator account to manage the site. See Administration Settings for more details on the **Administration** page.

Time Zone

The **Time Zone** page allows you to set the local time zone, date, and time for your Aruba Instant On site. See Time Zone Settings for more details on the **Time Zone** page.

Guest Portal

The Guest Portal page on the Instant On web application provides you with a Captive Portal Editor to design and customize a welcome page as you see fit. The page also provide you with the option to configure Facebook Wi-Fi service to connect to the Internet. This is used in Guest networks without the need for a secured password for authentication. See Enabling Guest Portal, for more information.

Software Update

You can now manage your software updates by creating schedules using the Instant On mobile app and web application. For more information, see Updating the Software Image on an Instant On Site.

Device Status Lights

The **Device status lights** page allows you to turn on or off the device status lights by using the **Quiet lights mode** toggle switch. The status lights are turned on by default to provide a clear visual indicator of the device's status at a glance. Slide the **Quiet lights mode** toggle switch to the right () to turn off the device status lights. Navigate to the **Inventory** page to check the status of devices when the status lights are turned off.

Administration Settings

The **Administration** page allows you to modify administrator information, including your Aruba Instant On site name and account credentials. You can also add a secondary administrator account to manage the site. Both accounts will have full privileges to the Instant On site configuration and status.

Modifying the Aruba Instant On Site Name

To modify the Aruba Instant On site name, follow these steps:

1. Go to the **Administration** page in the Aruba Instant On application.
   - In the web application—Click the settings menu () icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Administration** page is displayed by default.
   - In the mobile app—Tap the advanced menu () icon, and then select **Site management**. The **Site Management** screen displays the account administration settings.
2. Enter a new name for the Aruba Instant On site under **Site name**.

NOTE: The site name must be between 1 and 20 alphanumeric characters in length.

Adding a Secondary Account

Each Aruba Instant On site can be managed by two different administrator accounts. To add a secondary administrator account to your site, follow these steps:

1. Go to the **Administration** page in the Aruba Instant On application.
   - In the web application—Click the settings menu (⚙) icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Administration** page is displayed by default.
   - In the mobile app—Tap the advanced menu (☰) icon, and then select **Site management**. The **Site management** screen displays the account administration settings.
2. To add a secondary administrator account.

- In the mobile app—Click (+) next to **Assign another account**, to add a secondary account.
- In the web application—Click (+) next to **Account managing this site**, to add a secondary account.

3. Enter a valid email ID in the **Email** field and click **Assign account** to save the changes.

Transferring Account Ownership

Aruba Instant On allows you to transfer ownership from one administrator account to another. To transfer ownership of an Aruba Instant On site to another administrator account, follow these steps:

In the Web Application

1. Click the settings menu (⚙) icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Administration** page is displayed by default.
2. Under **Account(s) managing this site**, click **Transfer ownership**. The **Transfer Ownership** page opens.
3. Enter the new email ID under **Email**.
4. Click **Transfer ownership** to transfer ownership of the site to the new administrator account.

After your account is removed, you are logged out of the site. A confirmation message is displayed, stating that ownership has been transferred successfully.

In the Mobile App

1. Tap the advanced menu (☰) icon on the Aruba Instant On home screen.
2. Select **Site management** to view the administrator account settings.
3. Under **Account(s) managing this site**, tap the settings (⚙) icon and select **Transfer ownership**.
4. Enter the new email ID under **Email**.
5. Click **Transfer ownership** to transfer ownership of the site to the new administrator account.

After your account is removed, you are logged out of the site. A confirmation message is displayed, stating that ownership has been transferred successfully.

Time Zone Settings

The time zone is set automatically when the device is configured for the first time. However, if you wish to change the time zone settings, the **Time Zone** page allows you to set the local time zone, date, and time for your Aruba Instant On site. This information is used for the following Aruba Instant On features:

- Displaying daily statistics for your network.
- Enforcing network availability schedules.

- Performing daily image checks on the Aruba Instant On image server.

Setting a Local Time Zone

To set the local time zone for your Aruba Instant On site, follow these steps:

1. Go to the **Time Zone** page in the Aruba Instant On application.
   - In the web application—Click the advanced settings menu (⚙) icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Site management** page is displayed. From the **Site Management** page, click **Time zone** to open the **Time Zone** page.
   - In the mobile app—Tap the advanced menu (☰) icon on the Aruba Instant On home screen. Select **Site management** from the menu. From the **Site Management** screen, tap **Time zone** to open the **Time Zone** screen.
2. Select a time zone from the **Site local time zone** drop-down list.

After the local time zone is set, Aruba Instant On automatically updates the local date and time under **Site local date & time**.

About Software

The **About** page provides information about the software currently installed on the cluster and the mobile application. This page allows you to upgrade the software when new software versions are available.

To view the information in the **About** page, follow these steps:

- In the mobile app—Tap the advanced menu icon Click the advanced menu (☰) icon from the title bar and select **About** from the drop-down menu.
- In the web application—Click the help (?) icon from the page header and select **About** from the drop-down menu.

In the **About** page, you can view the version of the Aruba Instant On software currently running on the cluster and the mobile application.

This chapter describes the following features and tasks:

Monitoring Site Health

The **Site Health** page provides a summary of the health status of the Instant On devices connected to the network. It shows a consolidated list of alerts that are triggered from the devices provisioned at the site.

It also displays the inventory details of the connected devices and real-time data of active client connections on an hourly basis with the cumulative transfer speed of all the devices.

Viewing and Updating Inventory

The Inventory displays a list of devices in the network along with the devices' current operational status.

To view the **Inventory** page, follow these steps:

1. Click the **Inventory** ( ) tile on the Instant On mobile app or web application home page or click the **Site Health** banner and then click on **Show inventory**.
2. The **Inventory** page lists the APs added in the network and their operational status. Click an AP to view the details of the device.

The following table lists icons and their corresponding status:

Table 7: *Device Status*

Status	Icon	Condition
Up		Device is reachable.
Down		Device is not reachable.
Warning		Reachable device with a major alert reported by the device.
Minor warning		Reachable device with a minor alert reported by the device.

Adding a Device

To add a device to the inventory list, follow these steps:

1. Click the **Inventory** () tile on the Instant On mobile app or web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Navigate to the **Add a new device** page.
   - In the mobile app—Click add () at the bottom right corner of the page.
   - In the web application—Click **Add devices**.
3. Place your Instant On device in its destination area and make sure it is powered on. Now select **Search for my device**. It usually takes around 4-5 minutes for the Instant On devices to be detected. Alternatively, you can choose to extend your network by clicking on **How to extend my network**. For more information, see Extending your Network.
4. Review the device(s) discovered and add them to your site.
5. If you still cannot find your device, tap the **I don't see my device** button to view the troubleshooting options.

Extending your Network

The **How to Extend your Network** page provides instructions on two different ways by which you can add more devices to your network.

- Extend using a cable
- Extend over-the-air (Mesh)

Extend using a cable

This option is available to you on the UI only if you have chosen to configure the Instant On devices is private network mode. To extend your network using a cable, follow these steps in the mobile app or web application:

Table 8: *Steps to Extend Your Network Using a Cable*

Step No	Steps	Mobile App	Web Application
1.	In the **How to Extend your Network** page, choose **Extend using a cable**.	Yes	Yes
2.	To ensure optimal performance, connect your additional Instant On APs to the same switch as the first AP, using network cables. Power on the AP using Power over Ethernet (PoE) or DC power adapter (if you have ordered for it with the installation kit).	Yes	Yes
3.	Wait for the LED lights on the additional Instant On AP(s) to blink alternatively between green and amber.	Yes	Yes
4.	Select **Search for my device** to make the Aruba Instant On scan for both wired and wireless devices. The AP should show up in the list of devices detected in the network.	Yes	Yes
5.	Review the device(s) discovered and add them to your site.	Yes	Yes
6.	If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.	Yes	Yes

Extend over the air

To extend your network over the air, follow these steps in the mobile app or web application:

Table 9: *Steps to Extend Your Network Over-the-Air*

Step No	Steps	Mobile App	Web Applic-ation
1.	In the **How to Extend your Network** page, choose **Extend over-the-air**.	Yes	Yes
2.	Connect at least one Instant On AP to a local wired switch or a router and ensure that the initial setup is complete.	Yes	Yes
3.	Place a wireless Instant On AP in a location within the Wi-Fi range and power it on. For more information, see Instant On AP Wireless Access Point Placement Guidelines. **NOTE:** Ensure the wireless AP is in its factory default state and is not connected to a network using an Ethernet cable.	Yes	Yes
4.	Wait for the LED lights on the wireless Instant On AP(s) to blink alternatively between green and amber.	Yes	Yes
5.	Select **Search for my device** to make the Aruba Instant On scan for both wired and wireless devices. The AP should show up in the list of devices detected in the network.	Yes	Yes
6.	Review the device(s) discovered and add them to your site.	Yes	Yes
7.	If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.	Yes	Yes

Instant On AP Wireless Access Point Placement Guidelines

Consider the following guidelines when installing additional APs in the wireless network:

- **Interfering sources or obstacles**—Check for interfering sources or obstacles and install the APs on a ceiling or a wall.
- **Line of sight**—If you can clearly see the wired AP from where you stand, it is likely that the AP will offer a strong signal and good coverage.
- **No line of sight**—When line of sight is not possible, the APs should be placed in a close range to each other. The number of obstacles and type of materials heavily influence and attenuate the RF signal. In this scenario, a minimum distance of 16 feet (5 meters) and a maximum distance of 60 feet (18.25 meters) is recommended between the APs.
- **Wireless APs are placed on different floors**—If you place the APs on different floors, try to align them along a vertical line.

NOTE: These are general guidelines and you may need to experiment with the placement of your Instant On APs before settling down on a permanent location.

Deployment Scenarios for Outdoor Access Points

The versions prior to 1.4.0 of the Instant On product line includes both indoor and outdoor APs. However, the user interface did not allow specifying whether an AP is configured for servicing indoor or outdoor environments. In the case of an outdoor AP such as AP17 being setup as a mesh point, it may experience service disruptions if all the surrounding APs are indoor units since many regulatory domains reduce the available channels for outdoor use. The result is that the indoor AP may choose to use a channel that is

unavailable to the outdoor AP and hence, the AP17 mesh point will never be able to connect to the mesh portal. The following deployment scenarios for Outdoor APs help mitigate these problems:

Scenario 1: Provision a Site on the Outdoor AP Channel

In this solution, when the user attempts to extend the network, the UI prompts the user to confirm whether the new AP is an outdoor AP (example: AP17) being added as a mesh point. If so, the entire site is provisioned to operate on the outdoor AP channel as long as the outdoor AP is part of the Inventory. However, when an outdoor AP is removed from the Inventory, and there are no other outdoor APs present, then the site is switched back to operate on the AP installation default channel.

Scenario 2: New Site or Existing Site with no Outdoor Mesh Points

When extending the network, a choice is presented to the user to include the discovery of outdoor mesh APs in the search. One of the following two outcomes are possible in this scenario:

- If the user chooses to discover outdoor APs as part of the search by selecting the **Include over-the-air outdoor devices in search** checkbox. A warning message is displayed to indicate that the Wi-Fi network will be temporarily unavailable when search for over-the-air outdoor devices. All APs in the site are forced to the outdoor channel and power plan and all APs discovered in the search regardless of their type or connectivity status will be displayed and can be added to the inventory. If there are no outdoor APs discovered in this process, the site will revert to the default channel plan.
- If the user chooses not to include Outdoor APs as part of the discovery operation. The **Search for my device** operation will keep the default channel plan and search for both wired and wireless APs in the area. The over-the-air outdoor APs will be ignored in the search results. However, wired outdoor APs can still be found and added to the inventory, but they will operate separately on the outdoor channel plan.

Scenario 3: Existing sites with Mesh outdoor Access Points

- If a mesh outdoor AP cannot find a mesh portal on an outdoor channel, then it will be displayed as offline by the user interface.
- If a mesh outdoor AP is on a compatible channel, then the user interface displays it as up and running.

Scenario 4: Deleting Last Outdoor Mesh Point

When deleting the last outdoor mesh point, the site will revert to its default channel plan.

Radio Management

The **Radio Management** page allows you to configure the radio channel on which the AP needs to operate. This reduces interference and helps to optimize the AP radio performance as they will operate in optimal RF channels and bandwidth. The radio management configuration is global to a site and can be accessed from the advanced menu in the **Inventory** page. The APs in the site will use only the selected channels and allowed channels for the channel width.

Follow these steps to configure a radio channel on which the AP should operate:

1. Tap or click the **Inventory** tile on the Aruba Instant On Portal home page or click the **Site Health** banner and the click on **Show inventory**
2. Tap or click the advanced menu in the **Inventory** page.
   - In the mobile app—Tap the advanced menu (⋮) icon and select **Radio management**.
   - In the web application—Click the advanced settings (⚙) icon. The **Radio Management** page is displayed.

3. Choose an option for the **Channel width** and **Channel selection** for the 2.4 GHz and 5 GHz Radios. Based on your **Channel width** selection, the **Channel selection** options will be refreshed and the changes are saved automatically.

Access Point Details

The **Access Point Details** page provides details of the selected AP, which includes the AP name, IP address, MAC address, serial number, radio, ports, and model type of the AP. This page also provides a summary of the wireless radios including the number of clients that are currently connected. This page is displayed as **Router Details** in the mobile app, if your device is configured as a router.

Viewing AP/Router Details

To view the **Access Point Details** / **Router Details** page, follow these steps:

1. Tap or click the **Inventory**( ) tile on the Aruba Instant On home page or click the **Site Health**( ) banner and then click on **Show inventory**.
2. View the AP/Router details such as the AP name, IP address of the AP, MAC address, Serial number, AP type, radio, and the number of the clients connected on each radio channel.
   - In the mobile app—Tap any of the APs listed in the **Inventory** list. The **Access Point Details** page is displayed with details. The **Router Details** page is displayed if the device you selected is configured as a router.
   - In the web application—Click the ( ) arrow next to an AP in the **Inventory** list. The AP details is listed under the **Properties** tab.

Viewing Details of Ports

Every network requires the E0/PT or ENET port of the AP or Router to be connected to the gateway or switch using an Ethernet cable. Each Instant On AP has a single port, except for the AP11D devices which have an additional 3 LAN ports—E1, E2, and E3 respectively. These ports can be used to connect additional APs in the network. To view the details of the ports and the uplink status, follow these steps:

1. Navigate to the device details page.
   - In the mobile app—Tap any of the APs listed in the **Inventory** list. The **Access Point Details** page is displayed with details. The **Router Details** page is displayed if the device you selected is configured as a router.
   - In the web application—Click the ( ) arrow next to an AP in the **Inventory** list. The AP details is listed under the **Properties** tab.
2. Under the **Ports** section of the **Access Points Details** / **Router Details** page, view the details of the ports that are connected, the uplink status, and the upload and download throughput rates.

NOTE: The port details will not be displayed if the AP is connected as a mesh point in the network.

Restarting Your Device

To restart the device, follow these steps:

- In the mobile app—Click the advanced menu ( ) icon in the title bar of the **Access Points Details** / **Router Details** page and select **More actions** from the drop-down menu. The appropriate assistant page is displayed. Click **Restart device**.
- In the web application—Click the troubleshooting ( )icon, and click **Restart**.

Removing an AP from the Inventory

Follow these steps to remove an AP which is still online:

- In the mobile app—Click the advanced menu (⋮) icon in the title bar of the **Access Points Details** page and select **More actions** from the drop-down menu. The appropriate assistant page is displayed. Click **Remove from inventory**.
- In the web application—Navigate to **Inventory**. Select the AP you want to remove from the inventory by clicking the (›) arrow next to the AP name. In the **Properties** screen, click the troubleshooting ( ) icon, and click **Remove from inventory**.

Follow these steps to remove an AP which is offline:

On the **Access Point Details** page, a rectangular bar appears below the device name when an alert is triggered. The color of the rectangular alert bar will appear according to the alert type.

1. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity.

NOTE: The **Advanced** menu does not appear on the title bar when the status is down.

2. To remove the access point from the inventory, follow these steps:

   a. If the Instant On device is removed from the network, you can choose to remove the device from the inventory by clicking **Remove from inventory** in the **Access Point Details** page. A pop-up box appears on the screen requesting your confirmation.

   b. Click **Remove** to delete the device from the inventory.

Replacing a Router from the Inventory

Instant On allows you to replace a router from the inventory when it goes offline. A new AP or any existing AP from the site can be used to replace your old router. The old router needs to be manually reset to use as a normal AP.

To replace the router from the inventory, follow these steps:

In the Mobile app

1. Tap the **Inventory**( ) tile on the Aruba Instant On home page or tap the **Site Health**( ) banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Tap the offline router that you want to replace. The **Router Details** page is displayed. A rectangular bar appears below the device name when an alert is triggered.
3. Tap the **Alerts** link . You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the router.
4. In the **Alert Details** page, tap on the **replace** link. The **Replace router** page is displayed.
5. Unplug the router you want to replace and plug in your new Instant On device into your ISP modem.
6. When your device lights are alternating between green and amber, tap **Continue**. The mobile app begins BLE scanning to discover your new router. It usually takes around 4-5 minutes for the router to be detected.
7. Once your router is detected, tap **Replace** to configure the device as your primary Wi-Fi router.

NOTE: If the mobile app detects more than one primary Wi-Fi router in the area, you will see a message stating that more than one router is detected. In this scenario, keep the preferred router plugged and unplug the remaining routers from the network.

8. If the BLE scanning fails to discover your router in the vicinity, tap the **Add Wi-Fi router manually** button and choose to add your router to your network by entering the serial number or by scanning the barcode of the router.

NOTE: If you still cannot find your device, select I don't see my Wi-Fi router button to view the troubleshooting options.

9. Click **Finish** when your new router is added to your network.

In the Web Application

1. Click the **Inventory**( ) tile on the Aruba Instant On home page or click the **Site Health**( ) banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the ( ) arrow next to the router you want to replace from the **Inventory** list. The router details are listed under the **Properties** tab. A rectangular bar appears below the device name when an alert is triggered.
3. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the router.
4. In the **Alert Details** page, click on the **replace** link. The **Replace router** page is displayed.
5. Unplug the router that you want to replace and plug in your new Instant On device into your ISP modem. When your device's lights are alternating between green and amber, click **Continue**.
6. Enter the serial number located on your new Instant On primary Wi-Fi router and click **Search**.
7. Once your preferred router is detected, select **Replace** to configure the device as your primary Wi-Fi router.
8. Click **Finish** when your new router is added to your network.

Once the router is successfully added to your network, all other APs in the site will get synchronized automatically.

Configuring LAN Settings on an Instant On Device

You can either configure Instant On devices to automatically receive an IP address from an external DHCP server running on the LAN or manually configure a Static IP address.

1. Navigate to the **LAN Parameters** configuration page:
   - In the mobile app—In the mobile app—Under the **Connectivity** section of the **Access Point Details / Router Details** page, tap **Advanced LAN** parameters.
   - In the web application—Click the ( ) arrow next to an AP or router in the **Inventory** list and then click **Advanced**.
2. Choose one of the following:
   - **Automatic (default)**: This is the default setting for all APs . The Instant On device will request an IP address from a DHCP service running on the LAN. This option is visible only in the mobile app.
   - **Static**: To specify a fixed IP address on the LAN for your Instant On device, select the **Static** radio button in the mobile app or slide the toggle switch ( ) beside **Static IP address** in the **Advanced** tab of the web application and configure the following parameters:
     - **LAN IP**—Enter a Static IP address.
     - **Subnet mask**—Enter the subnet mask.
     - **Default gateway**—Enter the IP address of the Default Gateway.
     - **DNS server**—Enter the IP address of the DNS server.
3. Save the settings.
   - In the mobile app—Tap **DONE**.

- In the web application—Click **Save**.

Alerts

Alerts are triggered by the system when an unusual activity is observed with the network devices on the site.

To view the **Alerts** page, click the **Site Health** banner ( ) and tap **Show alert history**.

Types of alerts

The alerts are classified based on the severity. The Alerts page in the Instant On mobile app and web application prioritizes the alert that requires immediate attention by placing it at the top of the list. The alerts are classified as follows:

- Major active alert ( ) — The alerts classified as major are considered as the most severe by the system and prompt the user to take an immediate action. These alerts are triggered when there is a definite downtime of a device, synchronization failure, or when the Internet connectivity is down.
- Minor active alert ( ) — The alerts are classified as minor when a degradation in performance is observed, but without any downtime. These alerts are triggered when a system or device is overloaded, or a device MAC address is unauthorized.

Viewing Pending Alerts

The **Alert** ( ) icon appears on the title bar of the mobile app or web application when there is a pending alert. The number of alerts in the system is displayed as a colored badge on top of the **Alert** ( ) icon. The color of the badge determines the severity of the alert present in the system. When there are no alerts present in the system or all the alerts have been acknowledged, the **Alert ( )** icon will not appear in any of the title bars on the app or the application.

To view the Alert history, follow these steps:

1. Click the **Site Health** banner ( ) on the Instant On home page.
2. On the Site Health main page, you will see the details of the latest alert. Click **Show alert history**. The **Alerts** page displays a list of all the alerts received by the app, including the active alerts and the ones that have been cleared.
3. Choose the alert you want to acknowledge and view the **Probable causes** and **Recommended actions** you can take to clear the alert.
   - In the mobile app—Tap the alert you want to acknowledge. The **Alert Details** page is displayed with the details.
   - In the web application—Click the arrow ( ) next to the alert. The details of the alert is displayed.

NOTE: When there are multiple active alerts received by the application, the summary box in the **Site Health** page displays the active alerts with the highest severity in the system along with their color codes. For example: Major active alert takes the highest priority and is displayed in a red summary box. The **Alerts** page displays the list of active alerts in descending order of their severity and the order by which they should be acknowledged.

Configuring Networks

The Aruba Instant On mobile app or web application provides a summary of the networks that are available for employee and guest users.

Viewing the Network Summary

To view the **Networks** page, click **Networks** on the Aruba Instant On home page:

Table 10: *Network Information*

Parameter	Description	Mobile App	Web Application
Network Name	Identifies the Instant On network used to connect computers, tablets, or phones together. The network name is also used as the Wi-Fi identifier.	Yes	Yes
Network type	Indicates if the network is a employee or guest network.	Yes	Yes
Status	Shows the status of the network. Guest networks can be set to **Active** ( ) or **Inactive** ( ) by changing the status manually or by creating a network schedule to change the status at a specific day and time. See Guest Network for more details on setting network schedules.	Yes	Yes
Security	Shows the security option set for the network: **Network password (PSK)**—Secured using a shared password (PSK). Provides the following security options. ■ **WPA2 Personal**—This is the default setting. ■ **WPA2+WPA3 Personal** **NOTE: The Authentication server (RADIUS)** option is displayed only when you click on **Use authentication server (RADIUS) instead?**. **Authentication server (RADIUS)**—You must have a RADIUS server available to use this option. Secured using a higher encryption RADIUS authentication server. This option is available only for Employee networks. The following options are available. ■ **WPA2 Enterprise**—This is the default setting. ■ **WPA2+WPA3 Enterprise** ■ **Welcome page**—No security. Any user can connect to this network without entering a username or password. This option is available only for guest networks. This network requires Captive Portal to be configured.	Yes	Yes
Clients	Shows the number of clients currently connected to the network. Click the number listed under **Clients** to view the details of the client selected. See Managing Clients for more information about the **Clients** page.	Yes	Yes

Parameter	Description	Mobile App	Web Application
Transferred	Shows the volume of data, in bytes, transferred in the network throughout the day.	Yes	Yes

Viewing Network Configuration Details

For more details about a specific network, select a network from the **Networks** page. The **Employee Network Details** or **Guest Network Details** page opens. See Configuring an Employee Network for more information about the **Employee Network Details** page, or Guest Network for more information about the **Guest Network Details** page.

Employee Network

An Employee network is a classic Wi-Fi network. This network type is used by the employees in an organization and it supports passphrase-based (PSK) or 802.1X-based authentication methods. Employees may access the protected data of an enterprise through the employee network after successful authentication. The employee network is selected by default during a network profile configuration.

NOTE: The very first employee network you create for the site cannot be deleted unless you choose to delete the site entirely from your account.

Configuring an Employee Network

To configure an employee network:

1. Select **Employee** as the **Network type**.
2. Enter a **Network name** for the employee network. This will also be broadcast as the SSID for the WLAN network.
3. Choose a **Security** level for the network and update the required fields.
   - **Network password (PSK)**—Secures the network using a shared password (PSK). To set the Network password (PSK), tap or click the **Password** tab under **Security** and create a password of your choice in the **Network password** field. The following options can be configured.
     - **WPA2 Personal**
     - **WPA2+WPA3 Personal**

If you want to use a RADIUS authentication server, tap or click the **RADIUS** tab.

NOTE: You must configure the RADIUS server to allow APs individually or set a rule to allow the entire subnet.

   - **Authentication server (RADIUS)**—A RADIUS server must be available to use this option. Secures the network using a higher encryption RADIUS authentication server. Update the following fields:
     - **WPA2 Enterprise**
     - **WPA2 + WPA3 Enterprise**

Primary RADIUS Server—Configure the following parameters for the **Primary RADIUS Server**. If you are using the Instant On mobile app, tap **More RADIUS parameters** to view the below settings.

- **Server IP address**—Enter the IP address of the RADIUS server.
- **Shared secret**—Enter a shared key for communicating with the external RADIUS server.
- **Server timeout**—Specify a timeout value in seconds. The value determines the timeout for a RADIUS request. The Instant On AP attempts to send the request several times (as configured in the

Retry count) before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.

- **Retry count**—Specify a number between 1 and 5. Retry count indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
- **Authentication port**—Enter the authentication port number of the external RADIUS server within the range of 1–65535. The default port number is 1812.

Configure the following settings under **Network Access Attributes**, if you wish to proxy all RADIUS requests from the Instant On AP to the client.

- **NAS identifier**—Enter a string value for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.

NAS IP address—Select one of the following options if your Instant On devices are configured in a private network mode. The options below determine how the RADIUS authentication takes place across all networks.

NOTE: This option is grayed out if the Instant On AP is configured as a primary Wi-Fi router on the network. In which case each AP in the network will send RADIUS requests to the server with a matching Source IP address and NAS IP address.

- **Use device IP (default)**—This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients.
- **Use a single IP**—The RADIUS and NAS IP address will originate from a single IP address representing the site. Enter the **NAS IP address** for the site.

4. To configure a **Secondary RADIUS Server**, slide the toggle switch to the right ( ) and update the required fields.
5. To **Send RADIUS Accounting** requests, slide the toggle switch to the right ( ).
6. Click **Save**.

NOTE: After you configure an Employee network and save its settings for the first time, a toggle switch appears in the Employee Details page indicating the network is currently **Active** ( ). Use this switch to enable or disable the employee network.

Modifying Employee Network Details

In the Instant On mobile app or web application, the **Employee Details** page includes the following tabs to provide additional information about the network:

- **Identification**: Provides general identification and login information for the network. For more information, see Modifying the Employee Network Name and Password.
- **Options**: Allows you configure a bandwidth limit on the internet usage and IP and VLAN assignment for clients on employee networks. For more information, see Options.
- **Statistics**: Provides client and application usage statistics for the network. For more information, see Applications Statistics
- **Schedule**: Allows you to create a schedule during which the network is to be made available to users. For more information, see Schedule

Modifying the Employee Network Name and Password

To modify the network name or password of the employee network in the Aruba Instant On mobile app or web application, follow these steps:

Table 11: *Steps to Modify the Employee Network Name and Password*

No of Steps	Steps	Mobile app	Web application
1.	Click **Networks** on the Instant On home screen. The **Networks** screen is displayed.	Yes	Yes
2.	Select the employee network from the **Networks** list to view the **Employee Network Details** screen.	Yes	Yes
3.	Click **Identification** tab.	No	Yes
4.	Enter a new name under **Network name** to change the main network name or a new password under **Network password** to change the main network password. A warning message appears, indicating that changes to the network settings will disconnect all clients currently accessing the network.	Yes	Yes
5.	Save the settings. ■ In the mobile app—Tap **DONE**. ■ In the web application—Click **Save**.	Yes	Yes

Applications Statistics

The **Applications** tab in the Aruba Instant On mobile app or web application provides an overview of the client and application usage statistics for the employee or guest network. To view the statistics displaying the application usage data for the last 24 hours:

- In the mobile app—Tap the down arrow (﹀) next to the employee or guest network name and tap on the pie chart displaying the data transferred (in MB).
- In the web application—Select the employee or guest network and then click on the **Applications** tab.

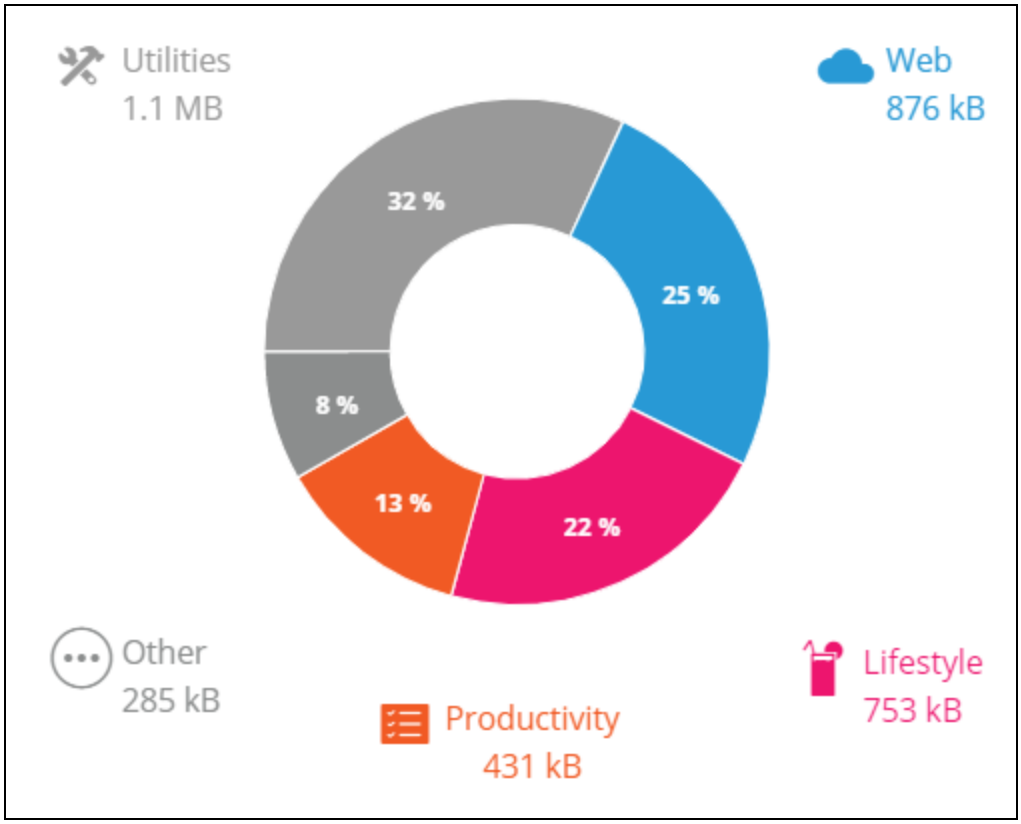
Viewing Client Count

The **Application** tab in the Aruba Instant On mobile app or web application displays the client count, which is the total number of clients currently connected to the network. Click on the number listed under **Clients** to view the total number of clients connected to the network. The **Connected clients** tab provides connection information for clients in the network. See Viewing Details of Active Clients for more information about the **Clients** page.

Viewing Applications Chart Data

The **Applications** chart in Aruba Instant On mobile app or web application provides data for the top five application categories, based on usage. Data is presented in both bytes and percentage.

Figure 3 *Applications Chart*



Viewing Total Data Transferred

The **Applications** tab in the Aruba Instant On mobile app or web application displays the total amount of data (in MB), transferred in the network throughout the day.

Viewing Blocked and Unblocked Application Categories

The **Applications** tab in the Aruba Instant On mobile app or web application displays the list of applications category that are blocked and unblocked in the network. For more information on blocking and unblocking the network categories, see Blocking Application Access.

Schedule

Aruba Instant On allows you to enable or disable a network for users at a particular time of the day. You can now create a time range schedule specific to the employee network, during which access to the Internet or network is restricted. This feature is particularly useful if you want the Wi-Fi network to be available to users only during a specific time, for example, only when your business is open.

Creating an Access Schedule on an Employee Network

To create a network access schedule for an employee network, follow these steps:

Table 12: *Steps to Configure an Employee Network Access Schedule*

Steps	Mobile App	Web Application
1. Select an employee network from the **Networks** list.	Tap **Networks** ( ) tile on the Instant On home page and select an employee network from the list. The **Employee Details** page is displayed.	Tap **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the employee network to view the configuration parameters.
2. Navigate to the **Network Schedule**. page.	Under **More options**, tap **Add a network access schedule**. The **Network Schedule** page is displayed.	Click the **Schedule** tab.
3. Enable the **Schedule**.	Slide the toggle switch beside **No schedule** ( ) to the right to enable the network schedule. The **Ruled by a schedule** setting is set to enabled ( ).	Slide the toggle switch beside **No schedule** ( ) to the right to enable the network schedule. The **Ruled by a schedule** setting is set to enabled ( ).
4. Configure a network schedule for the employee network.	Under **Days of the week**, select the day (s) during which the network will be active.	Under **Days of the week**, select the day (s) during which the network will be active.
5. Select the time period during which the network should stay active.	Select one of the following options under **Active hours during the day**: ■ **All day**: The network is active throughout the day. ■ **Active between**: The network is only active between the designated **Start Time** and **End Time**.	Select one of the following options under **Active hours during the day**: ■ **All day**: The network is active throughout the day. ■ **Active between**: The network is only active between the designated **Start Time** and **End Time**.
6. Save the configuration	Tap the back arrow ( ) to return to the **Employee Details** page. Tap **DONE**.	The changes are auto saved.

Options

The **More options** tab in the Aruba Instant On mobile app or the **Options** tab in the web application allows you to configure the bandwidth limit on the internet usage along with IP and VLAN assignment for clients on employee or guest networks. To configure these options:

- In the mobile app—Select the employee network or guest network and tap the **More options** drop-down.
- In the web application—Select the employee network or guest network and then click the **Options** tab.

IP and VLAN Assignment

The **IP and VLAN** setting in the Aruba Instant On mobile app and web application allows you to configure internal/external DHCP and NAT for clients on employee networks or guest networks. You can configure one of the following settings on your device:

- **Same as local network (default)**—This setting is referred to as **Bridged mode**. Clients will receive an IP address provided by a DHCP service on your local network. This option is enabled by default for employee networks. To configure a VLAN on the employee network, slide the toggle switch beside **Assign a VLAN to your network** to the right ( ) and enter a **VLAN ID**.
- **Specific to this network**—This setting is referred to as **NAT mode**. Clients will receive an IP address provided by your Instant On devices. Enter the **Base IP address** of the Instant On AP and select the client threshold from the **Subnet mask** drop-down list. This option is enabled by default for guest networks.

NOTE: The **Assign a VLAN to your network** toggle switch does not appear if the Instant On AP is configured as a Router in your network.

Restrict Network Bandwidth

The bandwidth consumption for an employee or guest network can be limited based on the client MAC address. The configured limit will be maintained even when the client roams from one AP to another within the network.

To configure a bandwidth limit, follow these steps:

Table 13: *Steps to Configure Bandwidth Usage*

Steps	Mobile App	Web Application
1. Select an employee network from the **Networks** list.	Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.	Click **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the employee or guest network or to view the configuration parameters.
2. Navigate to the **Options** page.	Select the employee or guest network and tap the **More options** drop-down.	Select the employee or guest network and then click on the **Options** tab.
3. Set the bandwidth usage limit.	Tap **Bandwidth Usage** and move the slider to set the speed limit for the employee or guest network. The limit is set to **Unlimited** by default. The available speed limits are: ■ **1 Mbps**—Good for emails, VoIP, web surfing, music, and social media. ■ **5 Mbps**—Good for online gaming, video conferences and streaming videos. ■ **10 Mbps**—Good for HD video streaming. ■ **25 Mbps**—Good for 4K video streaming. ■ **Unlimited**—There is no limit for internet usage per client.	Under **Bandwidth Usage** move the slider to set the speed limit for the employee or guest network. The limit is set to **Unlimited** by default. The available speed limits are: ■ **1 Mbps**—Good for emails, VoIP, web surfing, music, and social media. ■ **5 Mbps**—Good for online gaming, video conferences and streaming videos. ■ **10 Mbps**—Good for HD video streaming. ■ **25 Mbps**—Good for 4K video streaming. ■ **Unlimited**—There is no limit for internet usage per client.
4. Save the configuration	The changes are auto saved. Tap the back arrow ( ) to return to the employee or guest network details page.	Click **Save**.

Radio

Radio settings in the Aruba Instant On mobile app and web application allows you to configure radio frequencies for your wireless network.

To configure radio frequency, follow these steps:

Table 14: *Steps to Configure Radio Frequency*

Steps	Mobile App	Web Application
1. Select an employee network from the **Networks** list.	Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.	Click **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the employee or guest network or to view the configuration parameters.
1. Navigate to the **Options** page.	Select the employee or guest network and tap the **More options** drop-down.	Select the employee or guest network and then click on the **Options** tab.
2. Configure the radio settings.	Tap **Wireless options** and select the radio frequency available under **Radio** tab. The frequency is set to 2.4 GHz and 5 GHz by default. The available frequencies are: ■ **2.4 GHz and 5 GHz (default)**—The AP will broadcast the wireless network on either 2.4 GHz or 5 GHz radio frequencies. ■ **2.4 GHz only**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency. ■ **5 GHz only**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.	Under **Radio**, select the radio frequency. The frequency is set to 2.4 GHz and 5 GHz by default. The available frequencies are: ■ **2.4 GHz and 5 GHz (default)**—The AP will broadcast the wireless network on either 2.4 GHz or 5 GHz radio frequencies. ■ **2.4 GHz only**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency. ■ **5 GHz only**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.
3. Save the configuration.	The changes are auto saved. Tap the back arrow ( ) to return to the employee or guest network details page.	Click **Save**.

Extend 2.4 GHz range

Aruba Instant On allows you to enable or disable 802.11b rates from the network by using **Extend 2.4 GHz range** toggle switch. By default, 802.11b rates are disabled for all the networks. To enable this option, slide the toggle switch to the right ( ). This allows 2.4 GHz clients that are far away to connect to the network by enabling lower data rates.

NOTE: Enabling this option might slow down the network performance.

Show network

The **Show network** toggle switch is enabled by default ( ) to broadcast the employee network or guest in the list of available Wi-Fi networks. Slide the toggle switch to the left ( ) if you want to disable the selected network. In the mobile app, this option is available under **More options** >**Wireless options**.

Guest Network

A Guest Network is configured to provide access to non-enterprise users who require access to the Internet.

Creating a Guest Network

To create a Guest Network, follow these steps:

1. Tap or click the **Networks** tile on the Instant On mobile app or web application home page.
2. Add a new guest network.
   - In the mobile app—Click add ( ) and select the **Guest** tab.
   - In the web application—Click + Add and select the **Guest** tab.
3. Enter a **Network name.**
4. Select one of the following **Security** levels:

   a. **Open**—Any user can access this network without the requirement of entering a username or password.

   b. **Password**—Secures the network using a shared password (PSK) by using either WPA2 Personal or WPA2 + WPA3 Personal encryption. Enter a password of your choice in the **Network password** field.

   c. **Portal**—If you do not wish to secure the network with a password or if you want to redirect users to your Captive Portal page before being able to access the network. Tap or click the **Customize guest portal** link to enter the portal configuration page. For more information, see Enabling Guest Portal.
5. To configure additional settings for your guest network, see Options.

Changing the Guest Network Status Manually

To set the guest network status to **Inactive**, follow these steps:

Table 15: *Steps to Deactivate the Guest Network*

Steps	Mobile App	Web Application
1. Navigate to the **Guest Details** page.	Tap **Networks** ( ) tile on the Instant On home page. Tap on the guest network you want to deactivate. The **Guest Details** page is displayed.	Tap **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the guest network.
2. Deactivate the guest network.	Slide the **Active** toggle switch ( ) to the left to set the network to **Inactive** ( ).	Slide the **Active** toggle switch ( ) to the left to set the network to **Inactive** ( ).
3. Save the changes	Click **DONE**. The network is marked as **Inactive**, and all network settings are hidden.	Click **Save**. The network is marked as **Inactive**, and all network settings are hidden.

To set the guest network status to **Active**, follow these steps:

Table 16: *Steps to Activate the Guest Network*

Steps	Mobile App	Web Application
1. Navigate to the **Guest Details** page.	Tap **Networks** ( ) tile on the Instant On home page. Tap **ACTIVATE NETWORK** on the guest network you want to activate. The **Guest Details** page is displayed.	Tap **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the guest network.
2. Activate the guest network.	Slide the **Inactive** toggle switch ( ) to the right set the network to **Active** ( ).	Under the **Identification** tab, slide the **Inactive** toggle switch ( ) to the right set the network to **Active** ( ).
3. Save the changes	Click **DONE**. The network is marked as **Active**, and all network settings are made visible.	Click **Save**. The network is marked as **Active**, and all network settings are made visible.

Creating an Access Schedule on a Guest Network

To create a network access schedule for a guest network, follow these steps:

Table 17: *Steps to Configure a Guest Network Access Schedule*

Steps	Mobile App	Web Application
1. Select a guest network from the list of **Networks**.	Tap **Networks** ( ) tile on the Instant On home page and select a guest network from the list. The **Guest Details** page is displayed.	Click the **Networks** ( ) tile on the Instant On home page. The **Networks** page is displayed. Click the ( ) arrow next to the guest network to view the configuration parameters.
2. Navigate to the **Network Schedule**. page.	Under **More options**, tap **Add a network access schedule**. The **Network Schedule** page is displayed.	Click the **Schedule** tab.
3. Enable the **Schedule**.	Slide the toggle switch beside **No schedule** ( ) to the right to enable the network schedule. The **Ruled by a schedule** setting is set to enabled ( ).	Slide the toggle switch beside **No schedule** ( ) to the right to enable the network schedule. The **Ruled by a schedule** setting is set to enabled ( ).
4. Configure a network schedule for the guest network.	Under **Days of the week**, select the day(s) during which the network will be active.	Under **Days of the week**, select the day(s) during which the network will be active.
5. Select the time period during which the network should stay active.	Select one of the following options under **Active hours during the day**: ■ **All day**: The network is active throughout the day. ■ **Active between**: The network is only active between the designated **Start Time** and **End Time**.	Select one of the following options under **Active hours during the day**: ■ **All day**: The network is active throughout the day. ■ **Active between**: The network is only active between the designated **Start Time** and **End Time**.
6. Save the configuration	Tap the back arrow ( ) to return to the guest network details page. Tap **DONE**.	The changes are auto saved.

Enabling Guest Portal

Guest portal can be accessed using a web browser. It is available to newly connected users in a Wi-Fi network, before they are granted broader access to network resources. Guest portals are commonly used to present a landing or login page which may require the guest to accept your terms and policies before connecting to the Internet. You can also use the Guest portal to add details about your business and advertise special deals. Aruba Instant On offers you the ability to customize Guest Portal with your business logo, pictures, legal terms and other details. To configure Guest portal service on the Aruba Instant On mobile app or web application, follow these steps:

In the Mobile App

1. Click **Networks** from the Aruba Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, tap the **Portal** tab.
4. Tap the ( ) **Customize guest portal** link to modify the captive portal or splash page. The **Guest Portal** page is displayed.
5. Tap the drop-down arrow at the top-right hand corner of the screen and select either **Internal**, **External**, or **Facebook** settings.
6. Tap **Ok**.
7. Based on your selection, enter values in the required fields. For more information, see:
   - Configuring Internal Captive Portal
   - Configuring External Captive Portal
   - Facebook Wi-Fi
8. The changes are automatically saved.

In the Web Application

1. Click **Networks** from the Aruba Instant On home page.
2. Select one of the active Guest Network connections.
3. Under **Security** in the **Identification** tab, click the **Portal** tab.
4. Click the ( ) **customize guest portal** link to modify the captive portal or splash page. The Guest Portal page is displayed.
5. Select either **Internal**, **External**, or **Facebook** settings.
6. Based on your selection, enter values in the required fields. For more information, see:
   - Configuring Internal Captive Portal
   - Configuring External Captive Portal
   - Facebook Wi-Fi
7. Click **Apply changes**.

Configuring Internal Captive Portal

You can configure an internal captive portal splash page when adding or editing a guest network created for your Instant On site. Following are the internal captive portal configuration parameters:

Table 18: *Internal Captive Portal Configuration*

Parameter	Description	Mobile App	Web Application
Background	Tap the box to view the color palette and choose a color for the background of the internal captive portal page.	Yes	Yes
Welcome Message	Design the welcome message by updating the following fields: **Text**—Enter the text for the welcome message. Example: Welcome to Guest Network. **Font size**—Drag the slider to set the size of the font. **Font color**—Tap the box to view the color palette and choose a color for the font. **Font family**—Choose a font type from the drop-down list.	Yes	Yes
Logo / Image	Tap the image icon to browse and upload an image from your device.	Yes	Yes
Terms and Conditions	Design the **terms and conditions** section by updating the following fields: **Title text**—Enter the title text. Example: Please read the Terms and Conditions before using the Guest Network. **Font size**—Drag the slider to set the size of the font. **Font color**—Tap the box to view the color palette and choose a color for the font. **Font family**—Choose a font type from the drop-down list. **Terms content**—Enter or paste your terms and conditions in the text box. **Agree text**—Enter a comment in the text box. For example: **I agree to the terms and conditions**. ■ **Font color**—Tap the box to view the color palette and choose a color for the font. ■ **Font family**—Choose a font type from the drop-down list.	Yes	Yes
Accept Button	Design the **Accept Button** by updating the following fields: **Text**—Enter the text for the accept button. Example: I agree to the terms and conditions. **Border radius**—Drag the slider to set the border radius of the accept button. **Background color**—Tap the box to view the color palette and choose a color for the background. **Font color**—Tap the box to view the color palette and choose a color for the font. **Font family**—Choose a font type from the drop-down list.	Yes	Yes

Configuring External Captive Portal

You can design an external captive portal splash page for your guest network and also configure RADIUS authentication and accounting parameters. Following are the external captive portal configuration parameters:

Table 19: *External Captive Portal Configuration*

Parameter	Description	Mobile App	Web Application
Server URL	Enter the URL for the external captive portal server.	Yes	Yes
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.	Yes	Yes
Allowed domains	Specify the domain names of the sites that should be automatically whitelisted for unauthenticated users and click (+).	Yes	Yes
Send RADIUS Accounting	Slide the toggle switch to enabled ( ) to ensure the Instant On AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.	Yes	Yes

Table 19: *External Captive Portal Configuration*

Parameter	Description	Mobile App	Web Application
Primary RADIUS Server	Configure a primary RADIUS server for authentication by updating the following fields: ■ **Server IP address**—Enter the IP address of the external RADIUS server. ■ **Shared secret**—Enter a shared key for communicating with the external RADIUS server. Click the **More RADIUS parameters** link to configure the following parameters: ■ **Server timeout**—Specify a timeout value in seconds. The value determines the timeout for one RADIUS request. The Instant On AP retries to send the request several times (as configured in the **Retry count**) before the user gets disconnected. ■ **Retry count**—Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests. ■ **Authentication port**—Enter the authorization port number of the external RADIUS server within the range of 1–65,535. The default port number is 1812. ■ **Accounting port**—Enter the accounting port number within the range of 1–65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813. Configure the following settings under **Network Access Attributes**, if you wish to proxy all RADIUS requests from the Instant On AP to the client. ■ **NAS identifier**—Enter a string value for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server. ■ **NAS IP address**—Select one of the following options if your Instant On devices are configured in a private network mode. The options below determine how the RADIUS authentication takes place across all networks. • **Use device IP (default)**—This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients. • **Use a single IP**—The RADIUS and NAS IP address will originate from a single IP address representing the site. Enter the **NAS IP address** for the site. **NOTE:** This option is grayed out if the Instant On AP is configured as a primary Wi-Fi router on the network. In which case each AP in the network will send RADIUS requests to the server with a matching Source IP address and NAS IP address.	Yes	Yes

Table 19: *External Captive Portal Configuration*

Parameter	Description	Mobile App	Web Application
Secondary RADIUS Server	To configure a Secondary RADIUS Server, slide the toggle switch to the right ( ). **NOTE:** The configuration parameters for the **Secondary RADIUS Server** and the **Primary RADIUS Server** are the same.	Yes	Yes

Facebook Wi-Fi

Facebook Wi-Fi service is only relevant to the guest network. It offers the possibility to create a captive portal page that draws traffic to the business. The business information would appear in the person's feed when using the service and can be automatically seen by friends, thus attracting more people towards the business.

Configuring the Facebook Wi-Fi Service

To configure Facebook Wi-Fi service on the Aruba Instant On mobile app or web application, follow these steps:

In the Mobile App

1. Click **Networks** from the Aruba Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, tap the **Portal** tab.
4. Click the ( ) **Customize guest portal** link. The **Guest Portal** page is displayed.
5. Tap the drop-down arrow at the right hand corner of the screen and select **Facebook** from the menu.
6. Tap the ( ) **Configure Facebook Wi-Fi** link. You will be redirected to the Facebook page of the business.
7. Log in using your Facebook account and access the internet.

In the Web Application

1. Click **Networks** from the Aruba Instant On home page.
2. Select one of the active Guest Network connections.
3. Under the **Identification** page, click the **Portal** tab.
4. Click the ( ) **Customize guest portal** link. The **Guest Portal** page is displayed.
5. Select **Facebook** from the drop-down list.
6. Click **Apply changes**.
7. Click the ( ) **Configure Facebook Wi-Fi** You will be redirected to the Facebook page of the business.
8. Log in using your Facebook account and access the internet.

Analyzing Application Usage

Aruba Instant On provides daily usage data for the different types of applications and websites accessed by clients in the network.

Viewing Application Information

The **Applications** page provides the following information about types of applications accessed by clients in

your network:

Table 20: *Application Information*

Parameter	Description	Mobile App	Web Application
Name	Shows the name of the application category. See Analyzing Application Usage for the complete list of application categories.	Yes	Yes
Total Usage	Shows the total usage for a given application category, in bytes.	Yes	Yes
Total Usage %	Shows the total usage for a given application category, in percentage (%).	Yes	Yes

Applications Visibility and Control

The **Visibility and Control** page allows you to choose how the application usage information should be displayed in the following pages or tabs:

Applications page

Client Details page

Applications tab in the **Networks** page.

1. To navigate to the **Visibility and Control** page:
   - In the mobile app—Tap the **Applications** ( ) tile on the Instant On home screen. Tap the advanced menu (⋮) icon in the **Applications** page and select **Visibility and control**. The **Visibility and Control** page is displayed.
   - In the web application—Click the **Applications** ( ) tile on the Instant On home page .Click the settings ( ) icon on the **Overview** page header and select **Visibility and control**. The **Visibility and Control** page is displayed.
2. Select one of the available options:
   - **Application details (default)**—Provides a detailed view of date usage by different applications and websites accessed by clients in the network. Applications chart and Applications list are displayed only when this option is selected. This option is enabled by default and it may slow down the network performance.
   - **Application activity summary**—Provides an overview of uploaded and downloaded data of all the networks for the last 24 hours in the **Applications** page, **Client Details** page and **Applications** tab in the **Networks** page. Choose this option for better network performance. Selecting this option hides all other application data statistics .

NOTE: You cannot block or unblock the applications when this option is enabled.

Filtering Application Information in the Web Application

To filter the information that is displayed on the **Applications** page of the Instant On web application, follow these steps:

1. Click **Applications** on the Instant On home page. The **Applications** page opens.
2. Click the tool ( ) button at the top-right corner of the **Applications** list to open the parameter drop-down list.

3. Select the parameters that you want to display or hide from the **Applications** page.
   - Parameters with an orange check mark are displayed on the **Applications** page.
   - Parameters without an orange check mark are not displayed on the **Applications** page.

Analyzing Application Usage Data by Category

After you have filtered out the **Total Usage** data based on different application categories, you can view the data usage on each employee or guest network at the site.

To view the application data based on its category, follow these steps:

- In the mobile app—Tap the Applications ( ) tile on the Instant On home page. The **Total Usage** data is displayed in the **Applications** page. Tap on any of the web categories to view the usage data.
- In the web application—Click the Applications ( ) tile on the Instant On home page. The **Applications** tab displays the web categories and their **Total Usage** data on the network. Click the ( ) arrow beside the **Name** of any of the web categories to view the usage data.

The following data is displayed for each category:

- **Websites and applications most visited**—Displays the data for the top five application categories (by usage).
- **Activity for the last 24 hours**—Displays the data for the last 24 hours on the Instant On network.
  - **Network**—Displays the list of employee and guest networks active for the last 24 hours.
  - **Type**—Denotes if the network is an employee or a guest network
  - **Legend**—Includes the color codes to different each network. The color codes in the legend are used to display the donut chart.
  - **Allow use**—Allows you to block the traffic from the selected application category.
  - **Data Transferred**—Denotes the data transferred on the network specific to the selected web category, during the last 24 hours.
- **Traffic usage per client**—Displays the data usage of top five clients specific to the selected web category.

Sorting Application Information in the Web Application

Application data can be sorted in the Instant On web application to help you locate the information you need efficiently. For example, application data can be sorted in alphabetical order based on the application category name. Click one of the parameters at the top of the **Applications** list to sort the information based on your needs.

Applications Chart

Data for the top five application categories (by usage) is displayed in a donut chart. If more than five application categories have been accessed throughout the day, the fifth section of the **Applications** chart is represented as **Other**. Any applications that do not fall under the top four application categories are grouped into **Other**.

Applications List

Data for every application category is displayed in a list, which is organized in descending order by usage.

Table 21: *Application Categories and their Webroot Classification*

Application Category	Icon	Instant On Classification
Productivity—Sites and tools that help you stay productive and take control of your tasks like enterprise applications, antivirus, project management tools, collaborative software, reference and research, search engine, translation and web conferencing software.		■ Application Software
Utilities—Sites about tools and services that ease internet usage and navigation, such as search engines, cloud storage, and file transfer.		■ Computer and Internet Security ■ Computer and Internet Information ■ Translation ■ Reference and Research ■ Personal Storage ■ Search Engines ■ Pay-to-Surf ■ Internet Portals ■ Internet Communications ■ Web-based email ■ Shareware and Freeware ■ Dynamically Generated Content ■ Training and Tools ■ Web Hosting
Lifestyle—Sites that cover beauty and fashion trends, dining, entertainment and arts, maps and navigation, religion, society and travel.		■ Entertainment ■ Leisure ■ Travel ■ Location ■ Fashion
Web—Sites and tools containing computer and internet information and security, internet software, proxies and tunnels, routing protocols, web advertisements, etc.		■ Website Content ■ Internet Software ■ Online Advertisement
Streaming—Sites usually based on heavy video streaming or intensive network usage where a high throughput is needed, such as video, music, or movie streaming.		■ Streaming Media ■ Web Advertisements ■ Content Delivery Networks ■ Image and Video Search
Instant Messaging & Email—Websites and applications where users can send and receive messages and emails.		■ Email ■ Short Message Service ■ Messenger
Business & Economy—Sites about finance and economy news and information and professional services useful in a working environment, such as financial services and transactions, real estate, legal, stock market, stock advice and tools, etc.		■ Financial Services ■ Business and Economy ■ Job Search ■ Philosophy and Political Advocacy ■ Educational Institutions ■ Health and Medicine ■ Legal ■ Real Estate

Application Category	Icon	Instant On Classification
News & Media—Sites containing local and world news, breaking news, online newspapers, crowdsourced news, general information, and weather.		■ World News ■ Weather Report ■ Online News
Uncategorized—This category contains network protocols that could not be categorized but may be useful to run your network. Therefore, it cannot be blocked. It also includes sites that are uncategorized or no longer exist.		■ Dead Sites ■ Parked Domains **NOTE:** The data in these categories is negligible, they will be ignored in the data transferred calculation and nothing will be displayed about them in Aruba Instant On.
Social Network—Social applications include websites for social networking and media.		■ Social Networking ■ Dating ■ Personal sites and Blogs ■ News and Media
Adult Content—Adult content applications include websites with graphic adult content or illegal subjects.		■ Abused Drugs ■ Marijuana ■ Adult and Pornography ■ Nudity ■ Violence ■ Abortion ■ Hate and Racism ■ Gross ■ Illegal
Education—Sites about education information like schools, college, universities, and online training tools like Linda.com, LinkedIn learning, etc.		■ University ■ Education ■ Schools ■ Colleges ■ Online Learning
Explicit Content—Restricted content applications include websites with sensitive information or graphic content.		■ Cult and Occult ■ Sex Education ■ Gambling ■ Weapons ■ Swimsuits & Intimate Apparel ■ Alcohol and Tobacco ■ Cheating ■ Questionable
Gaming—Sites containing information about gaming, mostly referred as video games. Video games that are played partially or exclusively through the internet.		■ Online Gaming
Government & Politics—Military and government applications include websites on military and government information and services.		■ Military ■ Government

Application Category	Icon	Instant On Classification
Kids and Family—Sites aimed for kids and families with learning, educational and interactive content.		■ Educations ■ Kids ■ Learning
Malicious & Risk—High security risk applications include websites that contain known malicious Internet tools that can harm devices and damage the internal network.		■ Hacking ■ Keyloggers and Monitoring ■ Malware Sites ■ Phishing and Other Frauds ■ Proxy Avoidance and Anonymizers ■ Spyware and Adware ■ Bot Nets ■ Spam URLs
Shopping—Shopping applications include websites for online shopping.		■ Auctions ■ Shopping
Sports & Recreation—Recreational applications include websites on personal activities and interests.		■ Travel ■ Home and Garden ■ Entertainment and Arts ■ Local Information ■ Hunting and Fishing ■ Society ■ Sports ■ Music ■ Fashion and Beauty ■ Recreation and Hobbies ■ Motor Vehicles ■ Kids ■ Online Greeting cards ■ Religion

Viewing and Blocking Application Access

The **Applications** page in the mobile app and web application provides a brief description of the various application categories and allows you to restrict or grant access to those applications on your employee or guest network. This page also provides details of the total data usage (in bytes), total usage percentage, and the networks for which the application category is blocked.

Viewing Applications

To view the **Applications Details** for a specific application category, follow these steps:

1. Click **Applications** on the Aruba Instant On home page. The **Applications** page opens.
2. Select an application category from the Applications list to view the details of the application.

Blocking Application Access

The Aruba Instant On mobile app and web application allows you to set restrictions to access certain applications on basis of their category:

Blocking Application Access Per-Category

1. Tap **Applications** on the Instant On home screen. The various application categories are displayed.
2. Select an application category from the **Applications** list. The selected application category opens.
3. Enable restrictions for the selected networks:

a. In the mobile app—Under **Allow network access to this category**, slide the toggle switch(es) against each employee or guest network to enable restrictions for the selected network(s) ( ).

b. In the web application—Under **Activity for the last 24 hours**, uncheck the **Allow use** checkboxes for the selected employee or guest networks.

NOTE: If the client tries to access a website which is blocked, a notification is displayed on the screen indicating that access to the website is blocked by web policies set by the administrator.

Managing Clients

Aruba Instant On provides details of the clients in your network.

Viewing AP Clients

The **Client Details** page provides additional information about the clients in your network.

To view the **Client Details** page for a specific client, follow these steps:

1. Click the **Clients** ( ) tile on the Instant On home page. The **Clients** page is displayed.
2. Click the ( ) icon beside the client name from the **Connected clients** list. The **Client Details** page for the selected client is displayed.

For more information, refer to Client Details Information

Viewing Details of Active Clients

The following information is available on the **Client Details** page. For details on the client information preceding the **Client Details** page in the Aruba Instant On web application, see Client Details Information.

Table 22: *Client Details Information*

Parameter	Description	Mobile App	Web Application
Name	Denotes the name of the client.	Yes	Yes
IP Address	Denotes the IP address of the client. **NOTE:** Not displayed by default. See Filtering Client Information in the Web Application for details on displaying this parameter on the **Clients** page.	Yes	Yes
OS	Operating system (OS) of the client device. **NOTE:** Not displayed by default. See Filtering Client Information in the Web Application for details on displaying this parameter on the **Clients** page.	Yes	Yes
Network	Shows the network to which the client is connected. Click the network name to view the **Network Details** page. See Configuring an Employee Network for more details on the **Main Network Details** page, or Guest Network for more details on the **Guest Network Details** page.	Yes	Yes

Parameter	Description	Mobile App	Web Application
Device	Shows the access point to which the client is connected. Click the device name to view the **Access Point Details** page. See Access Point Details for more details on the **Access Point Details** page.	Yes	Yes
Duration	Denotes the amount of time that the client has been connected to the network.	Yes	Yes
Signal	Indicates the client signal quality, based on the client's Signal-to-Noise Ratio (SNR). See Table 2 for details on the different signal qualities.	Yes	Yes
MAC Address	Denotes the MAC address of the client.	Yes	Yes
Downloading	Shows the download throughput within the last 30 seconds, in bytes per second.	Yes	Yes
Uploading	Shows the upload throughput within the last 30 seconds, in bytes per second.	Yes	Yes
Top Application Category	Shows the most frequently used application type.	No	Yes
Applications Chart	Shows the application usage data for the selected client, in bytes. In the Aruba Instant On mobile app, tap the donut chart preceding **Transferred** to open the **Applications** chart for the client.	Yes	Yes
Transferred	Shows the total amount of data transferred during the client session, in bytes.	Yes	Yes

Table 23: *Signal Quality*

Signal Quality	Icon	Signal Strength
Good		30 dB or higher
Fair		16 dB—29 dB
Poor		15 dB or lower

Viewing Application Information for a Specific Client

You can view the application usage information for a specific client in your network by selecting a client from the **Clients** list. See Viewing Application Information for details on the type of application usage information that is displayed.

In the Web Application

To view application information for a specific client in the Instant On web application, follow these steps:

1. Click **Clients** on the Instant On home page. The **Clients** page opens.

2. Click the ( ) icon beside the client name from the **Connected clients** list to view the details of the client. The **Applications** chart for the selected client is displayed directly on this page.

In the Mobile App

To view application information for a specific client in the Instant On mobile app, follow these steps:

1. Tap **Clients** on the Instant On home screen. The **Clients** screen opens.
2. Select a client from the **Connected** clients list to open the **Client Details** screen.
3. Tap the donut chart preceding **Transferred** to open the **Applications** chart for the selected client.

Blocking and Unblocking Clients

The Instant On mobile app and web application allows you to block clients from associating with any of the APs on site. Each client can only be blocked manually using the Instant On mobile app or web application. Client blocking is possible only for clients who are already connected to the network. At any point in time, you may choose to unblock a blocked client by visiting the Blocked Clients list.

Follow these steps to block a client from accessing the network:

1. Tap or click on the **Clients** ( ) tile in the Instant On homepage of the Instant On mobile app or web application. The list of connected clients is displayed.
2. From the list of **Connected clients**, block the client which should not be allowed to access the network.
   - In the mobile app—Swipe from right to left on the client from the connected client list and tap on the block icon. The client is immediately blocked and moved to the **Blocked** clients list. Alternatively, you can also block clients from the **Client Details** screen by clicking the advanced menu icon ( ) and selecting **Block client**.
   - In the web application—The block button is displayed when hovering the cursor at the end of the client row. Click the block button and the client is immediately blocked and moved to the **Blocked clients** list.

Follow these steps to unblock a blocked client:

1. Tap or click on the **Clients** ( ) tile in the Instant On homepage of the Instant On mobile app or web application. The list of connected clients is displayed. Tap the **Blocked clients** tab in the **Clients** page. The blocked clients appear grayed out.
2. From the list of **Blocked clients**, unblock the clients you wish to provide access to the network again. The clients should be able to immediately access the network once they are unblocked.
   - In the mobile app—Tap the client you want to unblock. A pop-up box appears on the screen with client's name for confirmation. Tap **Unblock**. The client is immediately unblocked and moved to the **Connected** clients list. Alternatively, you can also unblock the client by swiping from right to left on the client and tapping the unblock icon.
   - In the web application—The allow button is displayed when hovering the cursor at the end of the client row. Click the allow button and the client is immediately unblocked and moved to the **Connected clients** list.

Filtering Client Information in the Web Application

To filter the information that is displayed on the **Clients** page of the Instant On web application, follow these steps:

1. Click **Clients** on the Instant On home page. The **Clients** page opens.

2. Click the tool ( ) button at the top-right corner of the **Clients** list to open the parameter drop-down list.
3. Select the parameters that you want to display or hide from the **Clients** page.
   - Parameters with a green check mark are displayed on the **Clients** page.
   - Parameters without a green check mark are not displayed on the **Clients** page.

To restore the default settings, follow these steps:

1. Click **Clients** on the Instant On home page. The **Clients** page opens.
2. Click the tool ( ) button at the top-right corner of the **Clients** list to open the parameter drop-down list.
3. Select **Restore Defaults** to restore the Instant On to the default settings.

Sorting Client Information in the Web Application

Client data can be sorted in the Instant On web application to help you locate the information you need efficiently. For example, client data can be sorted in alphabetical order based on the client name. Click one of the parameters at the top of the **Clients** list to sort the information based on your needs.

Managing Your Account

The **Account Management** page allows you to modify your administrator account information for all associated sites.

NOTE: The **Account Management** page is only available from the **My Sites** page when your account is registered to multiple Aruba Instant On sites.

Modifying Administrator Account Information

To modify your administrator account information for all associated Aruba Instant On sites, follow these steps:

In the Web Application

1. From the page header, click the icon next to your account name and select **Account Management** from the advanced drop-down menu on the Aruba Instant On header. The **Account Management** page is displayed.

NOTE: The alphabet in the icon will appear based on the first letter of your registered email account.

2. Modify the password for your registered account.
   - Select the **Change password** tab.
   - To modify your account password, enter your current password, followed by a new password.
3. Click **Change password** to save your changes.

In the Mobile App

1. In case of multiple sites, select the advanced menu (⋮) icon on the **My Sites** screen. Else, tap the icon with an alphabet, on the mobile app header. The **Account Management** page is displayed.

NOTE: The alphabet in the icon will appear based on the first letter of your registered email account.

2. Tap **Password**.
3. Under Change Password, enter your current password, followed by a new password.
4. Click **Change password** to save your changes.

The Account management screen also allows you to enable or disable alert notifications for the site. For more information, see Notifications.

Notifications

Notifications are standard messages that are sent to mobile devices connected to the Aruba Instant On when an alert is triggered by the system. The notification mechanism updates administrators about any alerts that are triggered on site.

When you click a notification, your registered device automatically opens the Instant On app and takes you to the corresponding management interface for the Instant On site. The stored user credentials are validated against the management interface. Upon successful login, you are directed to the **Alerts** page corresponding to the selected notification. If no action is taken on the alert, the notification remains in the notification bar and can still be viewed at anytime until it is cleared.

Enabling or Disabling Alert Notifications

To enable notifications for alerts, follow these steps:

1. Go to the **Notifications** page in the Aruba Instant On application.
   - In the web application—From the page header, click the icon next to your account name and select **Account Management** from the advanced drop-down menu on the Aruba Instant On header. The **Account Management** page is displayed. From the **Account management** page, click **Notifications** to open the **Notifications** page.
   - In the mobile app— Tap the icon with an alphabet, on the mobile app header. The **Account Management** page is displayed. From the **Account management** screen, tap **Notifications** to open the **Notifications** screen.

NOTE: The alphabet in the icon will appear based on the first letter of your registered email account.

2. Click the notification toggle switch(es) to enable ( ) or disable ( ) the alerts you want to be notified about. For more information on viewing and managing alerts, see Alerts.

NOTE: By default, the notifications are enabled for all three alert types.

Notification Messages

The Operating System (OS) of each registered device determines how the notification messages are displayed. The following table lists the notification messages and their corresponding alert types:

Table 24: *Notification Messages and Alert Types*

Notification Message	Corresponding Alert
Connection problem	Cannot access Internet
Device problem	<device> has problem <device> unauthorized <device> is down

Simple Notification

By default, a simple notification is displayed on 2 distinct lines:

- The first line displays the name of the alert.
- The second line displays the site name.

Collapsed Notification

When the system triggers multiple alerts from the same site, the notification mechanism collapses all the

notifications generated from the alerts. The notification mechanism displays it as a single notification on the registered device.

Firmware is the software programmed on Instant On APs to make sure the devices run and provide functionality to users. The firmware installed on the Instant On APs is the Instant On software image. When the firmware is upgraded, device performance and functionality is improved through feature enhancements and bug fixes.

Upgrading the AP Firmware

When an AP is deployed into the network, it joins an Instant On site, which is a group of APs that are configured and managed from a single location. Upon joining the site, the AP automatically syncs its Instant On software image with the software image version configured on the site. Each time the software image is updated on the site, all APs in the site are upgraded to the new software image version.

Instant On Image Server

Every version of the Instant On software image is uploaded and stored in a public cloud-based image server that is hosted by Aruba. The image server always contains the latest version of the Instant On software so that you can keep your system up-to-date. See Updating the Software Image on an Instant On Site for more details on updating your APs to the latest version of the Instant On software image.

Updating the Software Image on an Instant On Site

Instant On allows you to control when a software update on the site needs to take place. This is done by configuring a day of the week and time of your preference for the site on the Instant On mobile app or web application.

To create a schedule for the software update to be installed automatically on the site, follow these steps:

1. Navigate to the Site management page.
   - In the web application—Click the settings menu () icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Site management** page is displayed.
   - In the mobile app—Tap the advanced menu () icon on the Aruba Instant On home screen. Select **Site management** from the menu.
2. Click the **Software update** tab to view the scheduling options.
3. Select the **Preferred day of the week *** for the software update to be installed automatically.
4. Select a suitable **Time *** from the drop-down menu.

Each AP installs the new software image and reboots. After every AP in the site has rebooted with the new version of the Instant On software image, the upgrade process is complete.

NOTE: Critical software updates may override the settings configured by you and will be installed within 24 hours.

Verifying Client Connectivity During Upgrade

APs are automatically rebooted with the new version of the Instant On software image during a software upgrade. When an AP goes down during the reboot, the wireless clients connected to that AP are either moved to another AP in the Instant On site or completely dropped from the network. Though this scenario is expected, keep in mind that a firmware upgrade can cause major disruptions for the clients in your network.

This is limited to the time-period that the APs take to reboot, which is 3-5 minutes. We recommend that you schedule this activity for when you don't expect users connected to the network actively.

Upgrade Failure

If a software upgrade fails, the Instant On continues to run the software image version currently installed on the APs. You can continue running the current software image version or the upgrade will be retried at the next time set by the schedule.

Instant On Mobile App Compatibility

Though the Instant On mobile app is backward-compatible with older versions of the Instant On software image, the Instant On software image is NOT backward-compatible with older versions of the mobile app. If the mobile app installed on your device is older than the Instant On software image running on your Instant On site, a warning message appears when you attempt to launch the app.

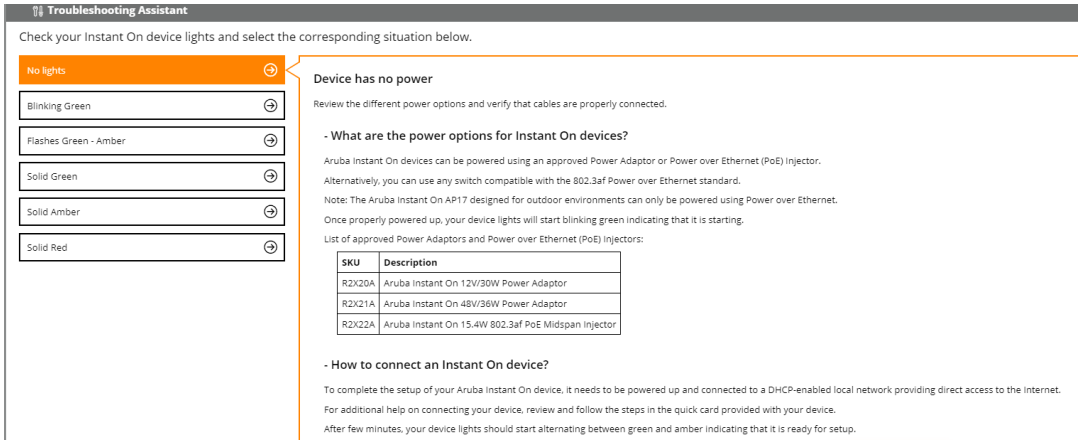
The mobile app can only be launched if it is updated to the latest version. To update the mobile app, click the app store icon that is available below the warning message.

To help the administrator troubleshoot problematic situations, a troubleshooting assistant is used for managing the Aruba Instant On. It helps the user identify an issue and provide guidance on how to resolve it. The troubleshooting assistant is designed to cover most typical situations and heavily relies on LED patterns to identify problems.

The troubleshooting assistant can be invoked from the **Alert Details** page:

1. Navigate to **Site Health** and click **Show alert history**.
2. In the **Alert Details** page, review the **Recommended actions** to clear the alert.
3. For additional troubleshooting options, click **Need more help?**. The **Troubleshooting Assistant** page is displayed with the following information:
   a. Most typical situations based on the LED patterns.
   b. Recommended actions.

Figure 4 *Troubleshooting Assistant Page*



4. Check the status of the LED lights on the Instant On and click the corresponding solution in the troubleshooting assistant.
5. If you are unable to find a solution to the problem, navigate to Help & Support to view additional support options.