

Aruba Instant On 2.6.0 User Guide

Mobile App Version

aruba Instant On

Copyright Information

© Copyright 2022 Hewlett Packard Enterprise Development LP.

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

Contents

Contents 3

Revision History 5

About this Guide 6
- Intended Audience 6
- Related Documents 6
- Contacting Support 6

Aruba Instant On Solution 7
- Key Features 7
- Supported Devices 7

Whats New in this Release 9
- New Features and Hardware Platforms 9

Aruba Instant On Deployment Concepts 10
- Wireless Deployment—Access Point Only 10
- Wired Deployment—Switch Only 10
- Wired and Wireless Deployment—Access Point and Switch 11

Provisioning your Aruba Instant On Devices 12
- Downloading the Mobile App 12
- Official Cloud URLs for Instant On 12
- Setting Up Your Wireless Network 13
- Setting Up Your Wired Network 14
- AP Configuration Modes 15
- Local Management for Switches 17
- IP Assignment for Access Points 18
- Discovering Available Devices 20
- Deploying Multicast Shared Services 21
- Managing Sites Remotely 23
- Application Error Messages 24

Aruba Instant On User Interface 25
- Configuring Menu Items in the Header 26
- Configuring Settings in the Modules 27
- Site Management 28
- About Software 31

Monitoring Site Health 32
- Alerts 33
- Network Tests 33

Viewing and Updating Inventory 35
- Adding a Device 35

Types of Devices 36
Extending your Network 36
Radio Management 39
Loop Protection 40
Power Schedule 41
DNS 42
Access Point Details 42
Router Details 48
Switch Details 55
Cloud-Managed Stacking 65
Topology 78
Auto-Detection and Auto-Configuring of Switch Ports 82

Configuring Networks 83
Employee Network 84
Guest Network 92
Wired Network 97

Analyzing Application Usage 103
Viewing Application Information 106
Viewing and Blocking Application Access 107

Managing Clients 109
Viewing AP Clients 109
Wired Clients 113

Managing Your Account 116
Changing Account Password 116
Security 116
Notifications 117
Communication Preferences 119
Delete Account 119

Managing AP Firmware Upgrades 120
Upgrading the Firmware for an Instant On AP or Switch 120
Instant On Image Server 120
Updating the Software Image on an Instant On Site 120
Verifying Client Connectivity During Upgrade 121

Troubleshooting 122

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
About this Guide

This User Guide describes the features supported by Aruba Instant On 2.6.0 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 2.6.0 product documentation includes the following:

- Aruba Instant On Access Point Hardware Documentation
- Aruba Instant On Release Notes
- Aruba Instant On 1830 Switch Series Management and Configuration Guide
- Aruba Instant On 1830 Installation and Getting Started Guide
- Aruba Instant On 1930 Switch Series Management and Configuration Guide
- Aruba Instant On 1930 Installation and Getting Started Guide
- Aruba Instant On 1960 Switch Series Management and Configuration Guide
- Aruba Instant On 1960 Installation and Getting Started Guide

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

Chapter 2
Aruba Instant On Solution

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 and switching technologies 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 devices:

Indoor Instant On Access Points

- Aruba Instant On AP11 Access Points
- Aruba Instant On AP11D Access Points
- Aruba Instant On AP12 Access Points
- Aruba Instant On AP15 Access Points
- Aruba Instant On AP22 Access Points
- Aruba Instant On AP25 Access Points

Outdoor Instant On Access Points

- Aruba Instant On AP17 Access Points

For more information on the currently supported Aruba Instant On hardware and how to purchase an Instant On Solution, see:

- Aruba Instant On Hardware Documentation
- Buy Now from a Local Reseller

Instant On Switches

- Aruba Instant On 1930 8G 2SFP Switch
- Aruba Instant On 1930 8G Class4 PoE 2SFP 124W Switch
- Aruba Instant On 1930 24G 4SFP/SFP+ Switch
- Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch
- Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 370W Switch
- Aruba Instant On 1930 48G 4SFP/SFP+ Switch
- Aruba Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch
- Aruba Instant On 1960 24G 2XGT 2SFP+ Switch
- Aruba Instant On 1960 24G 20p Class4 4p Class6 PoE 2XGT 2SFP+ 370W Switch
- Aruba Instant On 1960 48G 2XGT 2SFP+ Switch
- Aruba Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 2SFP+ 600W Switch
- Aruba Instant On 1960 12XGT 4SFP+ Switch
- Aruba Instant On 1830 8G Switch
- Aruba Instant On 1830 8G 4p Class4 PoE 65W Switch
- Aruba Instant On 1830 24G 2SFP Switch
- Aruba Instant On 1830 24G 12p Class4 PoE 2SFP 195W Switch
- Aruba Instant On 1830 48G 4SFP Switch
- Aruba Instant On 1830 48G 24p Class4 PoE 4SFP 370W Switch

Chapter 3
Whats New in this Release

This section lists the new features, enhancements, and hardware platforms introduced in Aruba Instant On 2.6.0.

New Features and Hardware Platforms

Table 3: *New Features Introduced in Instant On 2.6.0*

Feature	Description
Delete Account	The **Delete Account** screen allows you to delete an Instant On administrator account and revoke access to any associated products and services.
Enhancements to Client Details	The client details of wireless and wired clients will now include the connection health status of the client, and other minor enhancements.
FQDN Support for RADIUS Server Address	When configuring the Primary RADIUS Server or Secondary RADIUS Server settings, you can specify either an IP address or a fully qualified domain name of the RADIUS server.
Network Assignment for Wireless Networks Network Assignment for Instant On APs	A wireless network can now be assigned to a specific AP on site. Alternatively, the wireless networks can also be assigned to an Instant On AP in the device details page.
New Options Added in Restricted Access Settings for Router Mode	The **Restricted access** settings in Router mode now provide users with three options to modify access permissions for Instant On clients.
Per-AP Quiet Light Mode	The **Quiet Light Mode** configuration is now available at the device level instead of the site level.
Support for 160 MHz Channel Width on AP25 Mesh Points	The 160 MHz channel width configuration is supported only on AP25 access points. This includes the AP25 access points which are deployed as mesh points.
Support for Captive Portal with PSK	If the guest network is secured using a shared password (PSK), users can now choose to first authenticate to the guest network using the PSK, then they will be redirected to the captive portal page.
Unsupported Devices Cannot be Added to an Instant On Site	Enhancements have been made to ensure that unsupported devices cannot be added to an Instant On site.

Chapter 4
Aruba Instant On Deployment Concepts

The Instant On Solution currently supports three types of deployments, namely:

- Wireless Deployment—Access Point Only
- Wired Deployment—Switch Only
- Wired and Wireless Deployment—Access Point and Switch

During the initial setup, you need to select one of the above deployment modes based on the type of network you want to create.

Wireless Deployment—Access Point Only

The wireless deployment mode is suitable for users whose network infrastructure would mainly consist of the Instant On access points. You begin to create your site by powering on your Instant On APs and ensuring they are connected to the internet. A choice is presented to configure the APs in a private network or a router based setup. The network you create when you go through the initial setup will be the default network in your site and cannot be deleted. The SSID of this default network will be in the read-write mode and can be modified as deemed necessary. However, the management VLAN assigned to this default network will be read-only and cannot be modified. Once you have completed the initial setup, you can choose to extend your network using additional APs or switches. In this deployment, you are allowed to create a maximum of 8 wireless networks on a site. For more information, see Setting Up Your Wireless Network.

Wired Deployment—Switch Only

The wired deployment mode is suitable for users whose network infrastructure is focused mainly on the onboarding of Instant On switches. The initial setup using the Instant On mobile app or web application takes you through a step-by-step process of onboarding your switch. The switch must be powered on and connected to the internet to complete the onboarding process. A wired network is created on completing the initial setup and will serve as the default network for the site and cannot be deleted. Unlike the wireless networks, the wired network will not require you to create an SSID and password for the network. The site name is retained as the wired network name and a default management VLAN ID is set during this process. At a later point in time, you can choose to add Instant On APs to the site by extending your network and following the process of creating a wireless SSID. In this deployment, you are allowed to create a maximum of 22 wired networks on a site. For more information, see Setting Up Your Wired Network.



If there are any Instant On APs powered on and ready in the network, they will be discovered during the initial setup and added to the network along with the switch.

Wired and Wireless Deployment—Access Point and Switch

The wired and wireless deployment is suitable for users whose network infrastructure includes a combination of wired Instant On switches and wireless Instant On APs. The initial setup is similar to that of the wireless network, where you are presented with two choices, to either connect your APs in a private network or a router based setup. In this deployment, you are allowed to create a maximum of 30 networks (22 wired and 8 wireless) on a site. There are 2 types of scenarios involved when deploying AP and switch together in a site:

- Deploying an AP and a Switch in Private Network Mode
- Deploying an AP and a Switch in Router Mode

When you begin creating a new site, select the **Access point and switch** radio button from the **Getting started** screen and click **Continue**. Now follow the instructions provided in the AP Configuration Modes section to onboard your devices based on the preferred mode.

Chapter 5
Provisioning your Aruba Instant On Devices

This chapter describes the following procedures:

- Downloading the Mobile App
- Setting Up Your Wireless Network
- Setting Up Your Wired Network
- AP Configuration Modes
- Discovering Available Devices
- Managing Sites Remotely

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.

Mobile OS Requirements

The following mobile OS versions support the Aruba Instant On 2.6.0 mobile app:

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

Official Cloud URLs for Instant On

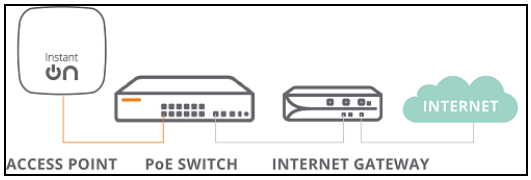
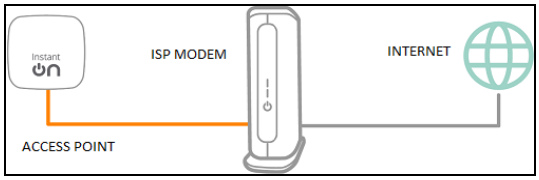
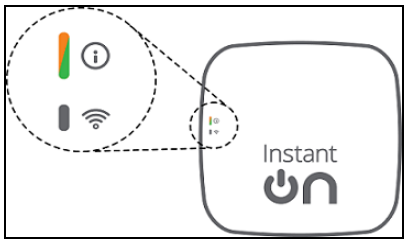
The following cloud URLs are officially used in Aruba Instant On to add in the allowed domains list:

- Onboarding URL used by non-configured Instant On device to reach the cloud: **https://onboarding.portal.arubainstanton.com/**
- Cloud Connect URL used by configured Instant On devices to send data to the cloud: **https://iot.portal.arubainstanton.com**
- Software Upgrade URL is used by Instant On devices to get their firmware: **https://downloads.portal.arubainstanton.com**

Setting Up Your Wireless Network

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

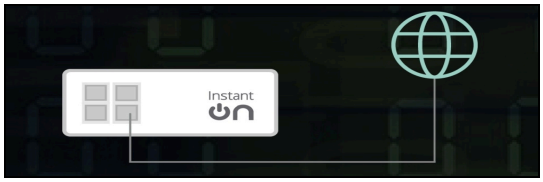
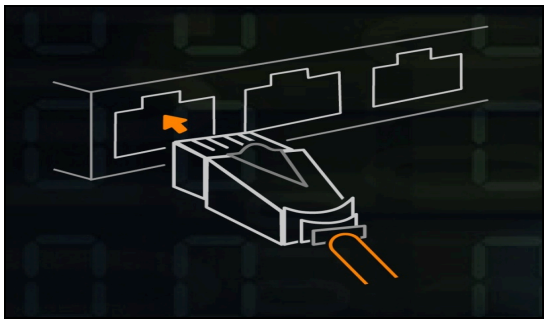
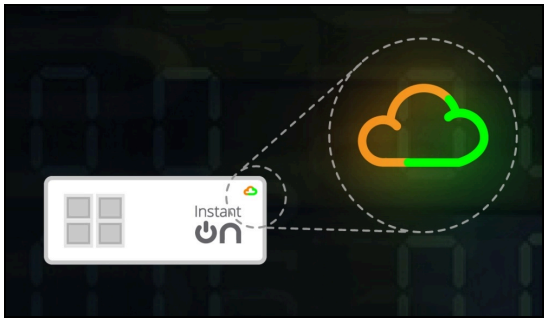
Table 4: *Instant On Wireless Network Provisioning*

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.	Configure the Instant On AP using the web application. For more information, see Accessing Aruba Instant On Application. As an alternative, you may choose to download the mobile app on your Android or iOS device. For more information, see Downloading the Mobile App.	
4.	Launch the Instant On web or mobile application and follow the on-screen instructions to complete the setup.	

Setting Up Your Wired Network

The following procedure is a step-by-step process of the initial setup to onboard Aruba Instant On switches to a site:

Table 5: *Instant On Wired Network Provisioning*

SL No	Steps	Illustration
1.	Ensure that the Instant On switch is connected to the internet to be discovered.	
2.	Connect the port you want to use as your switch uplink to your local network using an Ethernet cable, then power it on. **NOTE:** If you have more than one Instant On switch, you will be able to add them later on.	
3.	Power on the switch. The switch will be ready to be discovered when the cloud LED light alternates between green and amber. For more information, see Cloud LED and AP LED Light Status	
4.	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 switch using the web application. For more information, see Accessing Aruba Instant On Application.	
5.	Launch the Instant On web or mobile application and follow the on-screen instructions to complete the setup.	

The following table displays the various LED status you might see when onboarding Instant On APs or switches to a site:

Table 6: *Cloud LED and AP LED Light Status*

Switch Cloud LED or AP LED	Status
No Lights	Indicates that the device has no power. Review the different power options and verify that the cables are properly connected.
Blinking Green	Indicates that the device is booting or upgrading. It can take up to 8 minutes for the device to be ready.
Solid Amber	Indicates that the device has detected a problem. Click or Tap the **Troubleshoot** link to learn more.
Alternate Green and Amber	Indicates that the device is ready to onboard.
Solid Green	Indicates that the device is connected and configured.
Rapidly Blinking Amber	Indicates that insufficient power is supplied to the device.
Slowly Blinking Amber	Indicates that the identification of the device has been turned ON. **NOTE:** This applies only to Instant On access points and not the switches.
Solid Red	Indicates that the device has an issue. Unplug and replug the device to restore connectivity. Contact support if the issue persists. **NOTE:** This applies only to Instant On access points and not the switches.

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
- Router Mode

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.

Prerequisites

Before you begin to provision your Instant On AP, ensure that the following prerequisites 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 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. In the mobile app—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.

   In the web application—Enter the Serial Number of the device.

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 to configure and establish a PPPoE connection with the ISP.

Prerequisites

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

- A working internet connection provided by your Internet Service Provider (ISP).
- TCP ports 80 and 443 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:

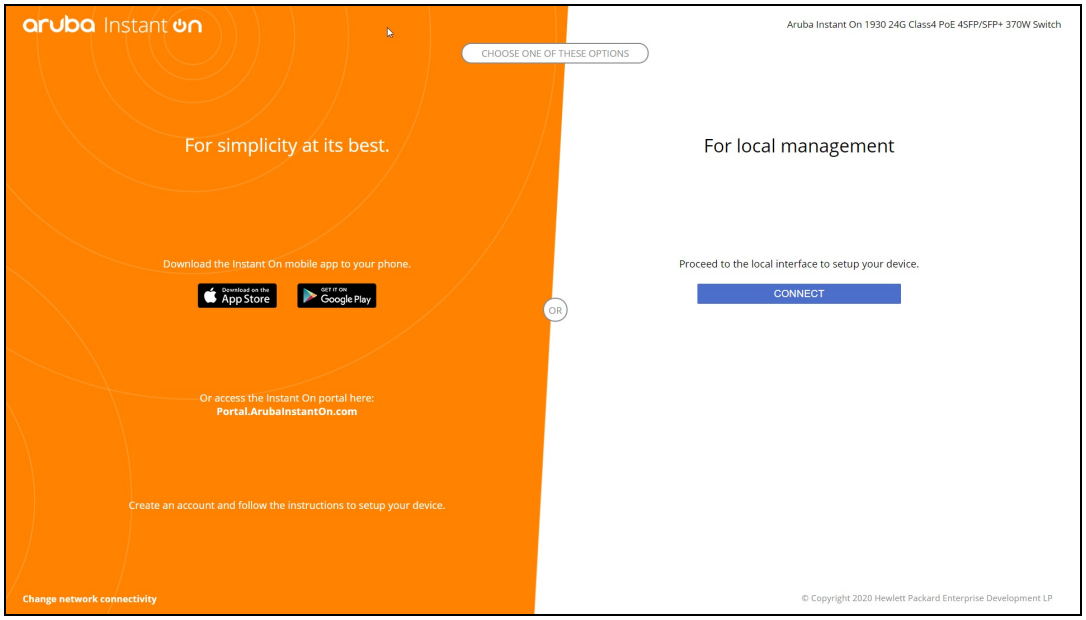
1. Connect the E0/PT or ENET port of the Instant On device acting as a primary Wi-Fi router to your modem using an Ethernet cable.
2. Power on the primary Wi-Fi router.

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. In the mobile app—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.

In the web application—Enter the Serial Number of the device.

Local Management for Switches

The Aruba Instant On switches can also be managed using the local WebUI of the switch. This can be done when the switch is in its factory default state and connected to the internet.



The following procedure describes how to access the local WebUI of the switch:

1. Type the IP address of the switch in your web browser and press enter. The landing page of the local WebUI is displayed.
2. Click the **CONNECT** tab in the **For Local Management side** of the landing page.

NOTE

The switch cannot be onboarded or managed from the Instant On mobile app once the local management for the switch is selected. The switch needs to be reset to factory default from the local WebUI to switch to the cloud management mode.

If you had opted to manage the switches using the cloud mode earlier (Instant On mobile app), and want to switch to the local WebUI:

1. Click the **Inventory**( ) tile on the Aruba Instant On home page or click the **Site Health**( ) banner and then click on **Show inventory**.
2. Click the ( ) arrow next to a switch in the **Inventory** list and then click **Actions** tab.
3. Select **Switch to local management**. Selecting this option will remove the switch and its configuration from the inventory.

Switch Provisioning Using the Local WebUI

The local WebUI provides an option to configure a static IP on the Instant On switch. The switch receives its default IP address from the DHCP server. The following procedure configures a static IP address and other IP addressing information on the switch using the local WebUI:

1. In the local WebUI, click the **Change network connectivity** link at the bottom of the page.
2. Under IP addressing, select the **Static** radio button.
3. Enter the **IP address**, **Netmask**, **Gateway IP,** and **DNS** information.
4. Click **Apply**.

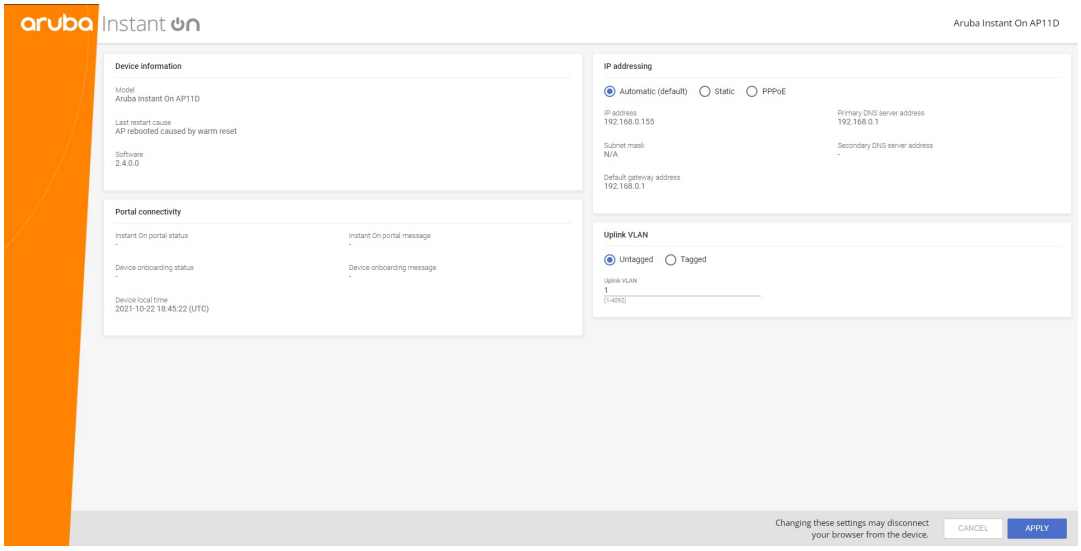
The following procedure configures a management VLAN for the switch using the local WebUI:

1. Under **Management VLAN**, select the **Tagged on uplink port** radio button.
2. Enter the **Management VLAN** ID and the **Uplink port** ID.
3. Click **Apply**.

IP Assignment for Access Points

The IP address for the access point can be assigned using the local WebUI during onboarding. The local WebUI allows you to configure the following IP addressing types:

- Automatic (default)
- Static
- PPPoE



Starting with Instant On 2.4.0, support is added for tagging the Access Point uplink VLAN. By default, the uplink VLAN is untagged with VLAN ID 1. This can now be modified to a tagged VLAN and different VLAN ID between 1 and 4092.

DHCP or Static IP Addressing

The following procedure describes how to assign IP address for the access point using the local WebUI:

1. Connect the AP to the network.
2. Once the LED on the AP becomes solid orange, the AP will broadcast an open SSID **InstantOn-AB:CD:EF** approximately after one minute, where AB:CD:EF corresponds 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. In the **IP addressing** section, configure either of the following options to assign an IP address for the access point:
   a. **Automatic (default)**: The DHCP server assigns an IP address for the access point. This option is selected by default.
   b. **Static**: To define a static IP address for the access point, specify the following parameters:
      i. **IP address**—IP address for the access point.
      ii. **Subnet mask**—Subnet mask.
      iii. **Default gateway**—IP address of the default gateway.
      iv. **DNS server**—IP address of the DNS server.
   c. **PPPoE**: The ISP assigns an IP address for the access point. This option is configurable only on AP11D access points when it is functioning as the primary router for the network. For more information on configuring PPPoE, see Setting Up WAN Connectivity for Your Network.
5. a. Under **Uplink VLAN**, select the **Tagged** radio button.
   b. Specify a VLAN ID between 1 and 4092 for the **Uplink VLAN**.
   c. Save the configuration.

   After the uplink VLAN is set, the AP will reboot to apply the new configuration, and the AP will receive an IP address.
6. Once the AP is added to a site, the management VLAN can be modified from Tagged to Untagged and vice versa in the **Ports** tab of the Instant On AP.
7. Click **Apply**. The AP will restart after the configurations are applied.

The IP assignment settings can be seen in the **Connectivity** tab of **AP Details** and **Router Details** page for APs and routers respectively.

Setting Up WAN Connectivity for Your Network

The 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 should use the local WebUI and update the settings.



Sometimes the ISP provider might lock the MAC address of the first connected device on the PPPoE server. Subsequently, when the user tries to replace their PPPoE device by the Instant On device, they may encounter authentication problems. In such cases, the user needs to contact their ISP provider to release the MAC address of the first device to allow the connection of the Instant On device.

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. Once the LED on the AP becomes solid orange, the AP will broadcast an open SSID **InstantOn-AB:CD:EF** approximately after one minute, where AB:CD:EF corresponds 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**, click the **PPPoE** radio button.
5. Enter the PPPoE **Username**, **Password**, and **MTU** provided by your ISP in the respective fields.
6. Under **Uplink VLAN**, select the **Tagged** radio button.
7. Specify a VLAN ID between 1 and 4092 for the **Uplink VLAN**.
8. Click **Apply**. The AP will reboot once the PPPoE configuration is applied.
9. 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 an additional five minutes, if the AP upgrades its firmware during the reboot process.
10. You can now proceed to creating a new site and adding devices. For more information, see:
    - Setup a New Site using the Mobile App.



If an AP with the PPPoE configuration is removed from the Inventory or the site is deleted, the AP will move to its factogry 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 and switches 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 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 or switch 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 or switch.
- QR Code—The Instant On 1960 Switch Series have their serial number in a QR code instead of a barcode. The Instant On 1960 switch hardware includes an orange pullout tag which displays the QR code when pulled out. This option is available only in the Instant On mobile app, and is available when adding new devices during the intial setup and also in the **Extend network** configuration.

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

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. For more information, refer to Managing Your Account.



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

Setup a New Site

1. To register a new Instant On site to your account, tap the advanced menu (☰) icon and select **Setup a new site**. You will be redirected to the initial setup page.
2. Follow the instructions given in Setting Up Your Wireless 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, tap the advanced menu (⋮) icon in the **My Sites** screen.

Sign Out

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

Help & Support

Tap the advanced menu (☰) icon and select (?) help to launch **Help & 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.
- **Community** - Provide a place for members or participants to search for information, read and post about topics of interest, and learn from each other. For more information, see https://community.arubainstanton.com/.
- **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 Shared Services

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

The devices and multicast services can be discovered and accessed by both wired and wireless clients based on the network VLAN ID. For more information, see Shared Services.

Multicast services can be configured in one of the following modes:

Private Network Mode

To detect services available on the same network (Same VLAN):

- The networks can be configured either as employee network or guest network.
- Devices offering the service and clients using the service must be connected to the same Wi-Fi Network or different networks with same VLAN ID.
- The **IP and network Assignment** settings must be set to **Same as local network (default)**. You can assign a different network if required by your local network. For information on IP and network settings, see IP and Network Assignment.
- The **Network Access** setting must be set to **Unrestricted access**.For more information, see Network Access .



You can also configure **Network Access** setting to **Restricted access** to use the service offered by devices but need to specify the IP address.

To detect services available on the different networks (Cross VLAN):

- The networks must be configured as an Employee network.
- Devices offering the service and clients using the service can be connected to other employee networks with the different VLAN ID.
- The **IP and network assignment** settings must be set to **Same as local network (default)** or **Specific to this network**. For information, see IP and Network Assignment.
- The **Network Access** setting of employee network must be set to **Unrestricted access**. The clients connected to guest network can use shared services from employee network when its network access is set to **Unrestricted access** , **IP and network assignment** settings is set to **Same as local network** and service is allowed to access. In the case of guest network, services available on other networks will not be detected. For more information, see Network Access .



Multicast services on Guest networks or Employee networks configured with the option **Specific to this network** are not supported if devices offering the service and clients using the service are located on different VLAN.

You can also configure **Network Access** setting to **Restricted access** to use the service offered by devices but need to specify the IP address.

Router Mode

To detect services available on the same network (Same VLAN):

- The networks can be configured either as employee network or guest network.
- Devices offering the service and clients using the service must be connected to the same Wi-Fi Network or different networks with same VLAN ID.
- The **IP and network Assignment** settings must be set to **Same as local network (default)**. You can assign a different network if required by your local network. For information on IP and network settings, see IP and Network Assignment.
- The **Network Access** setting must be set to **Unrestricted access**.
- 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. In the case of wired network, , the cross-vlan services will always be able to access.

To detect services available on the different networks (Cross VLAN):

- The network must be configured as employee network.
- Devices offering the service and clients using the service can be connected to other employee networks with the different VLAN ID.
- The **IP and network assignment** settings can be set to **Same as local network (default)** or **Specific to this network**. For more information, see IP and Network Assignment.
- The **Network Access** setting of employee networks must be set to **Unrestricted access (default)** . The clients connected to guest network can access shared services from employee network when its network access is set to **Unrestricted access** and **IP and network assignment** settings is set to **Same as local network**. For more information, see Network Access .



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.

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.



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.



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.

Cloud Service Unavailability Indicator

When there is an AWS outage in your region, the Aruba Instant On 2.6.0 portal cannot be remotely accessed until it is back to functioning to its normal state. The Instant On web application and mobile app cannot be accessed, but its sites, networks and devices should be working as usual and are not be affected by the outage.

As a result, during the downtime a message is displayed on the login page indicating the temporary unavailability of the application.

Application Error Messages

Starting from Instant On 2.4.0, the mobile app and web application displays error messages if an unexpected event occurs when performing certain operations. The error message also includes a recommended action, if applicable, to troubleshoot the issue. The message is displayed on the screen for a fixed duration based on the error type. Below are some of the error messages displayed by the application when an unexpected event occurs:

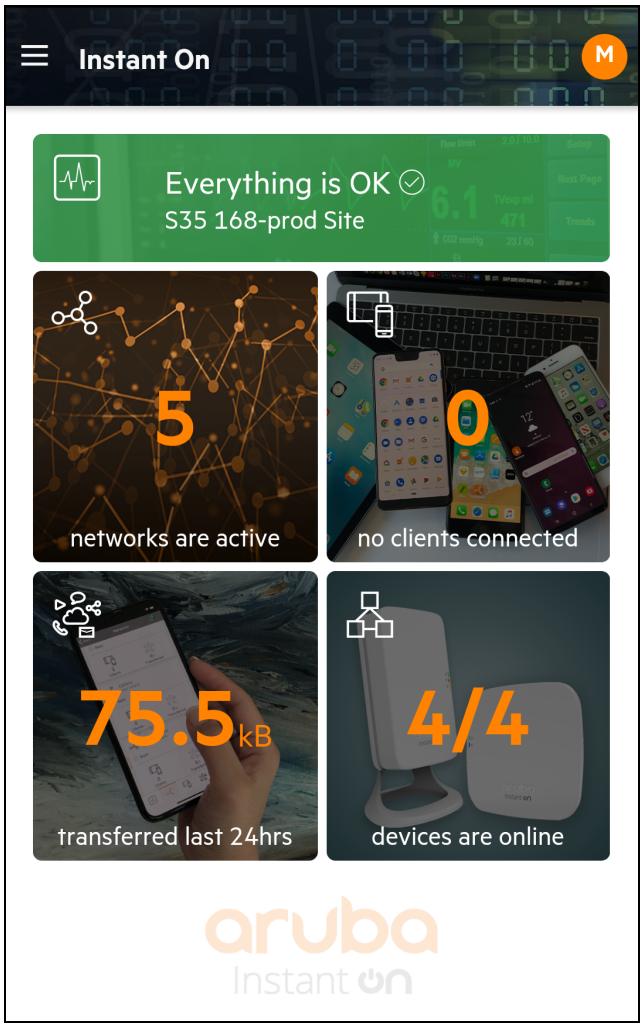
Table 7: *Application Error Messages*

Error Type	Error Message	Message Lifespan
Operation Failed	Operation failed to be executed. The data will be reloaded.	Message is displayed on the screen for a short duration and then removed.
Connectivity Lost	Your internet connection appears to be offline.	Messaged is displayed on the screen until connectivity with the cloud is recovered.
Application Error	Instant On has encountered a system error. Please try again and contact support if the problem persists.	Message is displayed on the screen until the user takes action or logs out.

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 *Mobile App User Interface Overview*



Configuring Menu Items in the Header

The header includes the following menu items:

Table 8: *Menu Items in the Header*

Header Content	Description
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.
Advanced menu icon ( )	Displays the site name and provides menu options to administer your account and the sites associated with it.
	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.
	Site management—Allows you to modify various account settings, including time zone and notifications. For more information, see Site Management.
	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.
	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.
	Setup a new site—Allows you to setup a new Aruba Instant On site. For more information, see Setting Up Your Network.
	Technology partners & promotions—Provides details on the product, how it works, link to the support, and community page. For more information see https://www.arubainstanton.com/.
	About—Provides information about the software currently installed on the mobile app, and also the following information: ▪ End User License Agreement ▪ Data Privacy Policy and Security Agreement
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. ▪ **Password**—Allows you to modify the password for the account. For more information, see Managing Your Account

Table 8: *Menu Items in the Header*

Header Content	Description
	▪ **Security**—Allows you to configure two-factor authentication for the site. For more information, see Security. ▪ **Notifications**—Allows you configure the notification settings for the alerts received from the site. For more information, see Notifications.
	Sign out—Allows you to log out of your Aruba Instant On account.

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 9: *Module Tiles*

Module	Tile
Site Health	
Networks	
Clients	

Module	Tile
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

Tap the back arrow ( ) on the title bar of the mobile app to exit the module.

Site Management

To view the **Site Management** page, tap the advanced menu ( ) icon on the Aruba Instant On home screen. The **Site Management** page displays the following user settings that can be modified in the Aruba Instant On application:

- Administration
- Time zone
- Software update

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.

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.

Administration Settings

The **Site Management** page allows you to modify administrator information, including your Aruba Instant On site name and account credentials. You can also add two other administrator accounts to manage the site. All three 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. 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 32 alphanumeric characters in length.

Adding Secondary Accounts

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

1. Tap the advanced menu ( ) icon, and then select **Site management**. The **Site management** screen displays the account administration settings.
2. Tap **Add account**, to add a secondary account.
3. Enter a valid email ID in the **Email** field and click **Add account** to save the changes.

Locking the Administrator Account

The **Lock account** option prevents other users accessing the site through a secondary account from revoking or transferring account ownership. This setting is available only for the primary administrator account which was used to create the site. Follow these steps to lock the primary or secondary administrator accounts:

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 managing this site**, tap the settings ( ) icon beside the administrator account and tap **Lock account**.
4. Tap **Lock**. A lock indicator ( ) is added to the account.
5. To unlock the account, repeat steps 1 to 3, and tap **Unlock**.

NOTE

The **Lock account** operation is a per-site configuration. For example, if account A is locked on site 1, it will not be locked on site 2 until user sets account A on the site 2 as locked.

Revoking Account Ownership

Aruba Instant On allows you to revoke the ownership of an existing administrator account managing the site. To revoke account ownership of an Aruba Instant On site, follow these steps:

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 managing this site**, tap the settings ( ) icon beside the administrator account and tap **Revoke ownership**.

4. Tap **Revoke ownership** again in the subsequent screen.

The account is signed out immediately and can no longer be used to access the site.

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:

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 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.

Deleting a Site

To delete an Instant On site, follow these steps:

1. Tap the advanced menu ( ) icon on the Aruba Instant On home screen.
2. Select **Site management** to view the administrator account settings.
3. Tap the ( ) icon in the title bar of the **Site Management** screen.
4. Tap **Delete this site**.
5. Tap **Delete** in the **Confirmation** window.

NOTE

Deleting the site will permanently erase all information related to its associated devices and will prevent anyone from remotely accessing it.

All devices within the site will be reset to factory default and you will need to reconfigure them in order to regain full access.

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. Tap the advanced menu ( ) icon on the Aruba Instant On home screen. 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 web application. To view the following information in the **About** page, tap the advanced menu ( ) icon from the title bar and select **About** from the drop-down menu:

- End User License Agreement
- Data Privacy Policy and Security Agreement

Chapter 7
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.

One of the following messages is displayed at the bottom of the Site Health icon:

Table 10: *Site Health Messages*

Message	Description
 Everything is OK	This information alert indicates that there are no issues with the Site Health. The color code is green.
 Potential Issue	This minor alert indicates one or several potential issues detected in the system. The color code is yellow.
 Attention Required	This major alert indicates one or several issues detected in the system that require immediate attention. These alerts have the highest severity level. The color code is red.

The alerts are classified based on the severity. The Alerts page in the Instant On mobile app or web application prioritizes the alert that requires immediate attention by placing it at the top of the list. The Instant On triggers an alert when an unusual activity occurs on the site and requires timely action to be taken by the administrator. 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.

Registered devices send or receive notifications when an alert is triggered by the Instant On due to an unusual activity on the site. For information on how to enable or disable notifications for alerts, refer to Notifications.

The Site Health page also displays the Current transfer speed in bytes per second.

Tap Show all alerts to view the list of alerts received on the site.

Click Show inventory to view a list of all the devices in the network, along with their operational status.

Alerts

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

The **Alert** ( ) icon appears on the title bar of the mobile app 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 mobile app.

To view the Alert history, follow these steps:

1. Tap 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. Tap the alert you want to acknowledge and view the **Probable causes** and **Recommended actions** you can take to clear the alert.

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.

Alert Triggered When Instant On AP25 Access Point is Underpowered

The Instant On AP25 access points require a minimum power 802.3at (Class 4) to function properly. In an event where the device is underpowered, an alert is displayed on the **Access Point Details** page. The **Radios** section of the page also displays a warning after disabling the radio settings of the AP. The LED on the device continues to flash rapid amber until sufficient power supply is provided and turns to solid green.

NOTE

When the underpowered AP25 access points is a mesh point, no alert or warning will be displayed on the Instant On application.

Network Tests

The **Network tests** option is used to test the reachability of an Instant On device. To perform a network test, you need to select a **Source** device on which the commands will be executed, and a **Destination** to be reached.

To run a network test on an Instant On device, follow these steps:

1. Tap the **Site Health** banner ( ) on the Instant On home page.
2. Under **Network tests**, tap **Run a connectivity test**. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On device from the drop-down list.

Only active devices of a site can be selected in this field. It could be a Switch or an AP.

4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

The table below shows the possible test results from the network tests:

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Fast connectivity to <host / IP address> **Expandable row**: More details
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Intermittent connectivity to IP address **Line 2**: <IP address> **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Unable to reach IP address **Line 2**: <IP address> **Line 3**: Very slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details

Chapter 8
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. Tap the **Inventory** ( ) tile on the Instant On mobile app home page or click the **Site Health** banner and then click on **Show inventory**.
2. The **Inventory** page lists the APs and switches added in the network and their operational status. Tap on an AP or switch to view the details of the device.



If a stack is present in the inventory, the actual number of online devices / total number of devices in the stack is displayed beside the stack name. For example, the **State** column would show **Active (2/2)**.

The following table lists icons and their corresponding status:

Table 11: *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 home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Tap add ( ) at the bottom right corner of the page.
3. Place your Instant On device in its destination area and make sure it is powered on and connected to the Internet. 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.



Any unsupported device found during device discovery cannot be added to the inventory. An error message stating **This device model is not supported** will be displayed.

5. If you still cannot find your device, tap the **I don't see my device** button to view the troubleshooting options.

Types of Devices

Instant On supports three types of devices:

- Access Points
- Routers
- Switches

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:

1. In the **How to Extend your Network** page, choose **Extend using a cable**.

To include devices which are connected over-the-air, click the **Include over-the-air outdoor devices in search** checkbox.

2. To ensure optimal performance, connect your additional Instant On devices 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).
3. Wait for the LED lights on the additional Instant On devices to blink alternatively between green and amber.
4. Select **Search for my device** to make the Aruba Instant On scan for both wired and wireless devices. The Instant On device(s) should show up in the list of devices detected in the network.
5. Review the device(s) discovered and add them to your site.



Any unsupported device found during device discovery cannot be added to the inventory. An error message stating **This device model is not supported** will be displayed.

6. If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.

Extend over the air

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

1. In the **How to Extend your Network** page, choose **Extend over-the-air**.
2. Connect at least one Instant On AP to a local wired switch or a router and ensure that the initial setup is complete.
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.

4. Wait for the LED lights on the wireless Instant On AP(s) to blink alternatively between green and amber.
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.
6. Review the device(s) discovered and add them to your site.

NOTE

Any unsupported device found during device discovery cannot be added to the inventory. An error message stating **This device model is not supported** will be displayed.

7. If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.

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 Instant On 1.4.0, 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.

Scenarios That Trigger Error Messages When Adding Devices in the Inventory

Following are some of the scenarios that trigger an error message when adding an Instant On device during the Initial setup or through Extend my network:

Scenario	Error Message
Entering a serial number of a device that is already onboarded on another site	Already assigned to another site.
Adding a device that is connected between the ISP modem and the Instant On router	Upon clicking Search for devices, the system will recognize and display the devices along with the following error message:

Scenario	Error Message
	▪ A new Instant On device that is connected between the ISP modem and the Instant On router shall not be allowed to be added to the network.
Entering the serial number of a device that is connected to another site, but not yet assigned	Device is on the same network as another site

Some of the error messages include a **View details** link. Click on **View details**, for a popup window with the explanation.

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 by operating in an optimal RF channel 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 use only the selected channels and allowed channels for the channel width.



Changing these settings may disconnect clients from the network.

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

1. Tap the **Inventory** tile on the Instant On home page or tap the **Site Health** banner and select **Show inventory**
2. Tap the advanced menu (⋮) icon and select **Radio management**.
3. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio—**20MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio—**20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.



The channel width of 160 MHz is available as a global setting only after an AP25 access point is added to the inventory for the first time. However, the **20/40/80/160 MHz** setting will still be available after all the AP25 access points are removed from the inventory.

4. Based on your selection for each radio, the **Channel selection** options are refreshed. All channels are enabled by default and are displayed in orange. The disabled channels are displayed in gray.
5. Configure the Transmit power range for the 2.4 GHz and 5 GHz radios by adjusting the slider between a minimum and maximum value. For example, if the slider is set between **Very high** and

Max, the radio transmits between 30 dBm and maximum power. The available values are:

Transmit Power Level	Threshold for 2.4 GHz Radio (in dBm)	Threshold for 5 GHz Radio (in dBm)
Low	6 dBm	15 dBm
	9 dBm	18 dBm
	12 dBM	
Medium	15 dBm	21 dBm
	18 dBm	
High	21 dBm	24 dBm
	24 dBm	27 dBm
	27 dBm	
Very high	30 dBm	30 dBm
Max	This is the default setting.	This is the default setting.

6. The changes made in the above procedure are saved automatically.

Loop Protection

The **Loop Protection** page is available only when there are one or more switches in the inventory. Instant On devices use two mechanisms for loop protection:

- Aruba Proprietary Mechanism
- Rapid Spanning Tree Protocol (RSTP)

Aruba Proprietary Mechanism

This mechanism is in-built on AP11D access points to protect them against loops or storms. This mechanism cannot be disabled on the device using the Instant On mobile app. The device sends out a proprietary packet and blocks any port that receives the same packet. The device will recover in 60 seconds once the fault is removed.

Rapid Spanning Tree Protocol (RSTP)

This mechanism is available only on the Instant On switches and is compliant with the 802.1w standard. RSTP provides loop protection in an interoperable environment with third-party networking equipment.

The RSTP mechanism can be enabled or disabled on the network using the Instant On mobile app. When this mechanism is enabled, probe packets are sent out every 2 seconds from the root bridge device. If the same packet is seen in more than one port of a downstream device, it indicates that a loop in the network exists, and RSTP will block ports to create a loop-free topology.

Follow these steps to enable RSTP on the network:

1. Tap the **Inventory** tile on the Aruba Instant On home page or tap the **Site Health** banner and select **Show inventory**.
2. Tap the advanced menu (⋮) icon in the **Inventory** page and select **Loop protection**.
3. Slide the **Rapid spanning tree (RSTP)** toggle switch to enabled ( ), to configure loop protection on the network. The page lists the spanning tree diagnostics such as the **Root switch device** connected to the network and its **priority** value. It also indicates the duration and number of times the **Topology changed** for the root switch device on the network.



When there is a stack present in the inventory, RSTP is enabled by default and does not have toggle switch to disable this setting. If the stack is removed, RSTP will still be enabled on the Instant On 1960 switch, but would now have a toggle switch to disable the setting.

Starting from Instant On 2.4.0, RSTP is enabled by default when creating a new site.

Bridge Priority Assignments

The **Bridge Priority** page displays the participating spanning tree devices and their bridge priority. The priority will be automatically determined using the topology and the position of the devices related to each other. The root bridge is assigned to the Instant On switch or router that is closest to the internet router or entry point to a private network. The root bridge priority is assigned the default value of 32768. All subsequent Instant On switches and routers are assigned priority values based on their distance from the root bridge.

For example, a network with three Instant On devices can have the following priority assignments:

- Instant On 1 would be assigned priority 32768 (root)
- Instant On 2 would be assigned priority 36864
- Instant On 3 would be assigned priority 40960

To view the bridge priority details and modify the base priority, follow these steps:

1. Tap the **Inventory** tile on the Aruba Instant On home page or tap the **Site Health** banner and select **Show inventory**.
2. Tap the advanced menu (⋮) icon in the **Inventory** page and select **Loop protection**.
3. Slide the **Rapid spanning tree (RSTP)** toggle switch to enabled ( ).
4. Tap the **Bridge priority assignments** link. The details of the **Base priority** and **Root bridge** are displayed.
5. To modify the **Base priority**, tap the drop-down arrow and select a priority from the list.
6. If you choose to recalculate the bridge priority, tap the advanced menu on the header and then tap **Recalculate bridge priority**.

The changes are auto saved.

Power Schedule

The **Power Schedule** page allows you to configure a schedule for Instant On switches and PoE capable devices to supply power to devices connected to them. This setting is global and applies to switches and PoE capable access points.

Follow these steps to configure a power schedule for PoE powered devices on the network:

1. Tap the **Inventory** tile on the Aruba Instant On home page or tap the **Site Health** banner and select **Show inventory**.
2. Tap the advanced menu (⋮) icon in the **Inventory** page and select **Power Schedule**.
3. Select the days on which you want the switch should supply power to devices under **Days of the week**.
4. Configure the time period for when the devices should be powered through PoE under **Active hours during the day**.
   a. **All Day** - The switch provides power to the connected PoE devices throughout the day.
   b. **Active Between** - The switch provides power to the connected PoE devices for the specified time period. Configure the **Start Time** and **End Time** for PoE supply as required.



When the **End Time** is configured earlier than the starting time, a **Next day** label is displayed, indicating that the switch will turn off PoE supply for the device at the configured time on the next day.

Though the Power Schedule option is global, the schedule can be turned off for individual ports. The option to turn off power schedule for individual ports is available under **More Options** in the **Port Details** page of respective port. For more information, see More Options.

DNS

The **DNS** page allows you to configure the DNS server used by the Instant On network. This is a global setting for the Instant On network.

Follow these steps to configure a DNS server for the network:

1. Tap the **Inventory** tile on the Aruba Instant On home page or tap the **Site Health** banner and select **Show inventory**.
2. Tap the advanced menu (⋮) icon in the **Inventory** page and select **DNS.**
3. Select one of the following options:
   - **Automatic(Default)** — Configure Cloudflare DNS (1.1.1.1) as the DNS server.
   - **Network assigned** — Configure DNS assigned by the network as the DNS server, for networks without a router.
   - **ISP assigned** — Configure DNS assigned by ISP as the DNS server, for networks with a router.
   - **Custom** — Specify a custom DNS server. You can create up to 3 DNS servers for the network. To create a custom DNS server,
     a. Select the **Custom** radio button.
     b. Enter the IP address of the **DNS server** and click **+**. To remove a DNS server click on the **delete** icon next to the DNS entry.

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.

Viewing Access Point Details

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

1. Tap the **Inventory**() tile on the Aruba Instant On home page or tap the **Site Health**() banner and then tap **Show inventory**.
2. Tap any of the APs listed in the **Inventory** list. The **Access Point Details** page is displayed with details. View the AP 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.

Connectivity

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. Under the **Connectivity** section of the **Access Point Details** page, tap **Advanced LAN parameters**.
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. Tap **DONE** to save the settings.

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 E0/ENET port. To view the details of the port and the uplink status, follow these steps:

1. Tap any of the APs listed in the **Inventory** list. The **Access Point Details** page is displayed with details.
2. Under the **Ports** section of the **Access Points Details** page, view the details of the ENET port, the name of the switch port, the uplink status, and the upload and download throughput rates.

Port Details

Access points operate only on the E0/ENET port. The **Port details** link for APs displays the name of the ENET port in read and write mode.



The **Port details** link is not displayed if the AP is connected as a mesh point in the network.

Connected Clients and Devices

The following procedure describes how to view the clients and devices connected to the ENET port on the AP:

1. Under **Ports**, tap the ENET port on the AP.
2. Tap the **Clients and devices on this port** link. You are redirected to the **Clients and Devices** page which displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address.
3. To filter the clients and devices connected to a specific network, tap the drop-down arrow (▼) and select a network from the list.

Radios

This section provides details on the clients operating on the 2.4 GHz and 5 GHz radios of the device:

- Number of clients connected—Denotes the number of clients connected to the radio.
- Operation channel—Denotes the radio channel on which the connected clients are operating.
- Radio transmit power—Denotes the radio transmit power rate (in dBm) for the connected clients.
- Airtime utilization—Denotes the airtime utilization (in %) detected by the radio.

Radio Details

The **Radio Details** page overrides the radio settings configured at the site level and allows you to configure 2.4 GHz and 5 GHz radio settings which are specific to the selected Instant On device.

Follow these steps to override the site level radio settings and configure 2.4 GHz and 5 GHz radio settings specific to the device:



Instant On APs connected over-the-air do not have the option to override the 5 GHz radio configuration made at the site level. These devices are allowed to configure only the 2.4 GHz radio settings at the device level.

1. Under **Radios**, tap on (⚙) **Radio details**.
2. Slide the toggle switch (🔘) beside **Specific radio management** for **2.4GHz Radio** and **5 GHz Radio** respectively to view the device specific radio settings.
3. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio—**20MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio—**20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.



- The channel width of 160 MHz is supported only on AP25 access points. This includes AP25 access points which are deployed as mesh points.
- When the channel width is set to **20/40/80/160 MHz**, the only corresponding channels available for selection are **36** and **100**.

4. Based on your selection for each radio, the **Channel selection** options are refreshed. All channels are enabled by default and are displayed in orange. The disabled channels are displayed in gray.
5. Configure the Transmit power range for the 2.4 GHz and 5 GHz radios by adjusting the slider between a minimum and maximum value. For example, if the slider is set between **Very high** and **Max**, the radio transmits between 30 dBm and maximum power. The available values are:

Transmit Power Level	Threshold for 2.4 GHz Radio (in dBm)	Threshold for 5 GHz Radio (in dBm)
Low	6 dBm	15 dBm
	9 dBm	18 dBm
	12 dBM	
Medium	15 dBm	21 dBm
	18 dBm	
High	21 dBm	24 dBm
	24 dBm	27 dBm
	27 dBm	
Very high	30 dBm	30 dBm
Max	This is the default setting.	This is the default setting.

The changes made in the above procedure are saved automatically.

Network Assignment

The **Network Assignment screen** allows you to assign an Instant On AP to the wireless networks configured on site.

The following procedure describes how to assign an Instant On AP to a wireless network:

1. Under **Radios**, tap on (⚙) **Network assignment**.

The **Network Assignment** screen is displayed.

2. Under **Allow access to the following networks**, slide the toggle switch beside the listed wireless networks, to the right (🔘) to assign the AP to a network.



When a new AP is added to the site, by default all the available wireless network will be assigned to the AP.

Access Point Lights

The **Access Point Lights** section allows you to turn on or off the AP status and radio lights. The device lights are turned on by default to provide a clear visual indicator of the device's status at a glance.

Follow these steps to modify the status of the access point lights:

1. Tap the **Inventory** tile on the Aruba Instant On Portal home page or tap the **Site Health** banner and select **Show inventory**
2. Select an AP from the inventory.
3. In the **Access Point Details** screen, scroll down to the **Access Point Lights** section and choose one of the following options:
   - **Normal mode (default)**— Use this option to turn on the status and radio lights. This option is selected by default.

- **Quiet light mode**—Use this option to turn off the status and radio lights. When this option is selected, the device lights are turned off during normal operation.

Advanced Menu

Locating Your Instant On AP

The **Locate** option helps you to locate your device when there are many devices in the site. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

To locate your Instant On AP, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Access Point Details** screen.
2. Tap **Locate**. The locator light is activated on the device.

Running a Connectivity Test

The **Network tests** option is used to test the reachability of an Instant On device. To perform a network test, you need to select a **Source** device on which the commands will be executed, and a **Destination** to be reached.

To run a network test on an Instant On access point, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Access Point Details** screen.
2. Tap on **Connectivity test** from the drop-down menu. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On device from the drop-down list.

Only active devices of a site can be selected in this field. It could be a Switch or an AP.

4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

The table below shows the possible test results from the network tests:

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Fast connectivity to <host / IP address> **Expandable row**: More details
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Intermittent connectivity to IP address **Line 2**: <IP address> **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Unable to reach IP address **Line 2**: <IP address> **Line 3**: Very slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details

Restarting Your Instant On AP

To restart your AP, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Access Points Details** screen.
2. Select **Restart** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Restart**.

Removing an AP from the Inventory

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

1. Tap the advanced menu (⋮) icon in the title bar of the **Access Points Details** screen.
2. Select **Remove from inventory** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Remove**.

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.
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 tapping **Remove from inventory** in the **Access Point Details** page. A pop-up box appears on the screen requesting your confirmation.
   b. Tap **Remove** to delete the device from the inventory.

Replacing a Failed AP from the Inventory

Instant On allows you to replace an AP from the inventory in the unlikely event of a failure. A new AP or any existing AP from the site can be used to replace the failed device. During this operation, the current configuration of the failed AP is also transferred to the replaced device.



It is recommended to replace the failed AP with a working AP of the exact same model to successfully restore all configurations. Replacing the failed device with a different AP model may not restore the same configurations as the old AP. For example: Replacing a Wi-Fi 6 AP with a Wi-Fi 5 AP will result in the Wi-Fi 6 specific configurations not being transferred to the Wi-Fi 5 AP.

To replace a failed AP from the inventory, follow these steps:

1. Tap the **Inventory** tile ( ) on the Instant On home page or tap the **Site Health** ( ) banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Tap the failed AP that you want to replace. The **AP 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 AP.

4. On the **Alert Details** page, tap on the replace link. The **Replace Access Point** page is displayed. Alternatively, you can also perform this action by tapping the advanced menu (⋮) icon in the title bar of the **Access Point Details** screen and selecting **Replace device** from the menu.
5. Unplug the AP you want to replace and plug in your new AP to the network.
6. When your device lights are alternating between green and amber, tap **Continue**. The mobile app begins BLE scanning to discover your new AP. It usually takes around 4-5 minutes for the AP to be detected.
7. Once your AP is detected, tap **Replace**.
8. If you still cannot find your device, select **I don't see my device** button to view the troubleshooting options.

Router Details

The **Router Details** page provides details of the selected Wi-Fi router, which includes the Router name, IP address, MAC address, serial number, radio, ports, and model type. This page also provides a summary of the wireless radios including the number of clients that are currently connected. Instant On currently supports AP11D devices to operate as a primary Wi-Fi router in the network.

Viewing Router Details

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

1. Tap the **Inventory**( ) tile on the Aruba Instant On home page or tap the **Site Health**( ) banner and then tap **Show inventory**.
2. Tap the router listed in the **Inventory** list. The **Router Details** page is displayed with details. View the Router details such as the Router name, IP address, MAC address, Serial number, Router type, radio, and the number of the clients connected on each radio channel.

Connectivity

The Instant On AP11D device is connected as a primary Wi-Fi router to the ISP provided modem, using an Ethernet cable. The **Connectivity** section lists the gateway IP address of the uplink and the **Internet IP** forwarded by the ISP provided modem to the router. The Instant On router acts as a DHCP service on the local network and provides IP addresses to requesting devices.

The following procedure configures the local network settings on an Instant On router:

1. Under the **Connectivity** section of the **Router Details** page, tap **Advanced LAN parameters**.
2. In the **IP Assignment** page, enter the **Base IP address**.
3. Under **Subnet mask**, tap the drop-down arrow (▼) and select the IP address range for the network.
4. Tap **Ok**.

DHCP IP Address Reservation

In router mode deployments, the Instant On AP is used as a primary Wi-Fi router and also provides DHCP IP addresses to the Instant On APs connected to it. The router is capable of reserving DHCP IP addresses for clients and devices such that the same DHCP IP address is issued to the client or device when they connect to same the network in the future. This feature is supported when the devices are managed by a wired network. The devices of the site will always have an IP address on the default wired device. The clients can have their IP address reserved on any of the wired networks, and all the wired

networks are managed by the router. In addition, this feature is supported for bridged wireless clients on site with a gateway.



The DHCP IP reservation feature will not work for clients using MAC randomization since it uses the MAC address to reserve an IP address for the client or device.

The following Router mode deployments support DHCP IP address reservation:

- Router Mode - Wireless Only
- Router Mode - Wired and Wireless

Configuring DHCP IP Address Reservation in Router Mode - Wireless Only

On a wireless-only site, where an Instant On device is functioning as a primary Wi-Fi router, an IP address can be reserved through the client or device details page that you want to reserve the IP or by the **Router Details** page.

To reserve DHCP IP addresses from the **Router Details** page, follow these steps:

1. Under the **Connectivity** section of the **Router Details** page, tap **Advanced LAN parameters**.
2. Under **IP address reservations for Router**, tap **Reserve an IP address**. The list of clients connected to the site are displayed along with their IP addresses.
3. Tap on the client or device to reserve its DHCP IP address. The device and its IP address will be added to the **IP address reservations for Router** list.



If you choose to modify the reserved IP address of the client or device, tap the edit icon next to the device or client name and enter the new IP address. The changes are auto saved when you tap the back arrow (←) icon.

4. Tap the back arrow (←) icon. The changes are auto saved.

To reserve an IP address from the **Client Details** page, follow these steps:

1. Select a wireless client connected to the primary Wi-Fi router.
2. In the **Client Details** page, tap the advanced menu (⋮) icon and tap **IP reservation** from the drop-down list.
3. Under IP address, modify the IP address of the client, if required and then tap **Reserve**. The device and its IP address will be added to the **IP address reservations for Router** list in the **IP assignment** page of the router.

Configuring DHCP IP Address Reservation in Router Mode - Wired and Wireless

In this mode, the DHCP IP address reservation can either be done in the **Router Details** or **Client details** page, as shown above for the wireless network, and from the **Network Details** page for the wired network.

To reserve DHCP IP addresses from the **Network Details** page, follow these steps:

1. Select a wired network to which a primary Wi-Fi router is connected.
2. In the **Network Details** page, tap **More options** and then tap **IP assignment** from the drop-down list.

3. Under **IP address reservations for Router**, tap **Reserve an IP address**. The list of clients associate to the wired network is displayed along with their IP addresses.
4. Tap on the client or device to reserve its DHCP IP address. The device and its IP address will be added to the **IP address reservations for Router** list.



If you choose to modify the reserved IP address of the client or device, tap the edit icon next to the device or client name and enter the new IP address. The changes are auto saved when you tap the back arrow (←) icon.

5. Tap the back arrow (←) icon. The changes are auto saved.

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. Tap any of the AP11D routers listed in the **Inventory** list. The **Router Details** page is displayed.
2. Under the **Ports** section of the **Router Details** page, view the details of the ports that are connected, the uplink status, and the upload and download throughput rates.

Status

The **Status** tab view under **Ports** is selected by default when you arrive on the **Router Details** page. The ports are visually represented on the page in the same manner as the actual physical ports on the device. The E0/PT or ENET port is always selected by default and acts as the default uplink port for the router. Tap on any of the ports to view the following details:

- Port number—The physical port number of the router.
- Port status—The speed of the trunk is displayed if the port is the member of a trunk.
- Upstream and Downstream throughput—The upstream and downstream throughput of the trunk is displayed when the port is the member of a trunk.

Port Details

Instant On currently supports an AP11D device to operate as a router in the network. The **Port Details** page for Routers consists of the following settings:

- Name of the port in read and write mode.
- A toggle switch that allows you to set the port status to **Active** ( ) or **Inactive** ( ) . This field is set to **Active** by default.
- **Port access control (802.1X)**—Configures port-based network access control designed to enhance 802.11 WLAN security. This field consists of a toggle switch which can be active ( ) or inactive ( ).
  - Inactive ( )—The toggle switch is set to inactive by default. This indicates that any client can connect to this port without requiring authentication.
  - Active ( )—Indicates that the first device connected to the port must be authenticated prior to using the port. Configure the following RADIUS settings when this option is enabled:

- **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.
- **RADIUS Server IP address or domain name**—Enter the IP address or fully qualified domain name 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 device 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.

- To configure a **Secondary RADIUS Server**, slide the toggle switch to the right ( ) and update the required fields.
- To **Send RADIUS Accounting** requests, slide the toggle switch to the right ( ).
- Tap **Done**.

Included networks

- **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.

Networks

After creating your network, you have the option to map the network to a VLAN port which, either allows traffic from all networks or only for a specific network. Each port in the Instant On AP11D device can be assigned a separate VLAN ID and configured to manage the network traffic. The following procedure describes how to map a network to a VLAN port:

1. Tap any of the AP11D routers listed in the **Inventory**. The **Router Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the router.
3. From the **Selected network** drop-down list, choose the network you want to map a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.

- **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.

7. Tap **Done** to finish mapping the network to the port.

Connected Clients and Devices

The following procedure describes how to view the clients and devices connected to a specific port on the AP11D router:

1. Select a port on the router.
2. Tap the **Clients and devices connected on this port** link. You are redirected to the **Clients and Devices** page which displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address.
3. To filter the clients and devices connected to a specific network, tap the drop-down arrow (▼) and select one of the networks.

This section provides details on the clients operating on the 2.4 GHz and 5 GHz radios of the device:

- Number of clients connected—Denotes the number of clients connected to the radio.
- Operation channel—Denotes the radio channel on which the connected clients are operating.
- Radio transmit power—Denotes the radio transmit power rate (in dBm) for the connected clients.
- Airtime utilization—Denotes the airtime utilization (in %) detected by the radio.

Radio Details

The **Radio Details** page overrides the radio settings configured at the site level and allows you to configure 2.4 GHz and 5 GHz radio settings which are specific to the selected Instant On device.

Follow these steps to override the site level radio settings and configure 2.4 GHz and 5 GHz radio settings specific to the device:



Instant On APs connected over-the-air do not have the option to override the 5 GHz radio configuration made at the site level. These devices are allowed to configure only the 2.4 GHz radio settings at the device level.

1. Under **Radios**, tap on (⚙) **Radio details**.
2. Slide the toggle switch () beside **Specific radio management** for **2.4GHz Radio** and **5 GHz Radio** respectively to view the device specific radio settings.
3. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio—**20MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio—**20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.

- The channel width of 160 MHz is supported only on AP25 access points. This includes AP25 access points which are deployed as mesh points.
- When the channel width is set to **20/40/80/160 MHz**, the only corresponding channels available for selection are **36** and **100**.

4. Based on your selection for each radio, the **Channel selection** options are refreshed. All channels are enabled by default and are displayed in orange. The disabled channels are displayed in gray.
5. Configure the Transmit power range for the 2.4 GHz and 5 GHz radios by adjusting the slider between a minimum and maximum value. For example, if the slider is set between **Very high** and **Max**, the radio transmits between 30 dBm and maximum power. The available values are:

Transmit Power Level	Threshold for 2.4 GHz Radio (in dBm)	Threshold for 5 GHz Radio (in dBm)
Low	6 dBm	15 dBm
	9 dBm	18 dBm
	12 dBM	
Medium	15 dBm	21 dBm
	18 dBm	
High	21 dBm	24 dBm
	24 dBm	27 dBm
	27 dBm	
Very high	30 dBm	30 dBm
Max	This is the default setting.	This is the default setting.

The changes made in the above procedure are saved automatically.

Network Assignment

The **Network Assignment screen** allows you to assign an Instant On AP to the wireless networks configured on site.

The following procedure describes how to assign an Instant On AP to a wireless network:

1. Under **Radios**, tap on ( ) **Network assignment**.

The **Network Assignment** screen is displayed.

2. Under **Allow access to the following networks**, slide the toggle switch beside the listed wireless networks, to the right ( ) to assign the AP to a network.

When a new AP is added to the site, by default all the available wireless network will be assigned to the AP.

Advanced Menu

Locating Your Instant On Router

The **Locate** option helps you to locate your device when there are many devices in the site. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

To locate your Instant On device, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Router Details** page.
2. Tap **Locate**.
3. Slide the **Activate lights** toggle switch to the right ( ). The locator light is activated on the switch.

Running a Connectivity Test

The **Network tests** option is used to test the reachability of an Instant On device. To perform a network test, you need to select a **Source** device on which the commands will be executed, and a **Destination** to be reached.

To run a network test on an Instant On router, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Router Details** screen.
2. Tap on **Connectivity test** from the drop-down menu. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On device from the drop-down list.

Only active devices of a site can be selected in this field. It could be a Switch or an AP.

4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

The table below shows the possible test results from the network tests:

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Fast connectivity to <host / IP address> **Expandable row**: More details
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Intermittent connectivity to IP address **Line 2**: <IP address> **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Unable to reach IP address **Line 2**: <IP address> **Line 3**: Very slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details

Restarting Your Instant On Router

To restart your router, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Router Details** screen.
2. Select **Restart** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Restart**.

Replacing a Router from the Inventory

Instant On allows you to replace a router from the inventory when it goes offline. A new AP11D router or any existing router 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:

1. Tap the **Inventory** ( ) tile on the Instant On Solution 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. Alternatively, you can also perform this action by tapping the advanced menu (⋮) icon in the title bar of the **Router Details** screen and selecting **Replace device** from the menu.
5. Unplug the router you want to replace and plug in your new Instant On AP11D 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.
9. If you still cannot find your device, select **I don't see my Wi-Fi router** button to view the troubleshooting options.

Switch Details

The **Switch Details** page provides details of the selected switch. To view the **Switch Details** page, follow these steps:

1. Tap the **Inventory**( ) tile on the Aruba Instant On home page or click the **Site Health**( ) banner and then click on **Show inventory**.
2. Tap any of the switches listed in the **Inventory** list. The **Switch Details** page is displayed with details. View the switch details such as the switch name, IP address of the switch, MAC address, Serial number, switch model, and ports.

The **Switch Details** page has the following sections:

- Connectivity
- Power over Ethernet (PoE)
- Ports

Connectivity

This section displays details of the uplink connection and LAN IP information of the switch. You can either configure Instant Onswitches to automatically receive an IP address from an external DHCP server running on the LAN or manually configure a Static IP address.

1. Under the **Connectivity** section of the **Switch Details** screen, tap **Advanced LAN parameters**.
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 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. Tap **DONE** to save the settings.

Power over Ethernet (PoE)

The **Power over Ethernet** section in the switch details page provides the following information:

- **Total budget**—The total power in watts that can be provided by the switch.
- **Power consumption**—The amount of power in watts currently being consumed by the connected PoE devices.

Ports

The **Ports** section in the **Switch Details** page visually displays the physical ports for the switch and provides additional statistics and configuration specific to a port. The Instant On mobile app provides a segmented view of the following options, selecting each of which will change the view of the ports accordingly:

To view the **Ports** section of the **Switch Details** page, follow these steps:

1. Tap the **Inventory**( ) tile on the Aruba Instant On home page or tap the **Site Health**( ) banner and then tap on **Show inventory**.
2. Tap any of the switches listed in the **Inventory**. The **Switch Details** screen is displayed with details.

The **Ports** section of the **Switch Details** page provides the following options:

- Status
- Networks
- Link Aggregation

- Port Details
- Connected Clients and Devices

Status

The **Status** tab view under **Ports** is selected by default when you arrive on the **Switch Details** page. The ports are visually represented on the page in the same manner as the actual physical ports on the device. Each port is numbered according to the port number on the switch and displays its current status. Port 1 is always selected by default and acts as the default uplink port for the switch. Tap on any of the switch ports to view the following details:

- Port number—The physical port number of the switch.
- Port name—The port name is displayed when a custom name is provided.
- Port status—The speed of the trunk is displayed if the port is the member of a trunk.
- Upstream and Downstream throughput—The upstream and downstream throughput of the trunk is displayed when the port is the member of a trunk.
- Member of <port membership name>—The name of the trunk is displayed, if the port is the member of a trunk.
- Port details—A hyperlink that redirects you to the **Port Details** page for configuration options.

Networks

After creating your network, you have the option to map the network to a VLAN port which, either allows traffic from all networks or only for a specific network. Each port in the Instant On switch can be assigned a separate VLAN ID and configured to manage the network traffic. The following procedure describes how to map a network to a VLAN port:

1. Tap any of the switches listed in the **Inventory**. The **Switch Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the switch.
3. From the **Selected network** drop-down list, choose the network you want to map to a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Included networks**—This section includes the following configuration settings:
     - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
     - **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.
   - **Specific network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.
7. Tap **Done** to finish mapping the network to the port.

Link Aggregation

Link aggregation configuration depends on the number of ports available on the switch. Instant On currently supports switches with the following number of ports:

Table 12: *Switch Ports Aggregation*

Number of Ports per Switch	Number of LAG Supported	Number of LAG members supported
8 ports	4 trunks	4 trunk members
24 ports	8 trunks	4 trunk members
48 ports	16 trunks	8 trunk members

The following procedure describes how to add a link aggregation group on the switch:

1. Tap any of the switches listed in the **Inventory**. The **Switch Details** page is displayed.
2. Under the **Ports** section, select the **Link Aggregation** tab.
3. Tap the **Add link aggregation** link.
4. The **Link Aggregation Details page** provides the following configuration options:
   - Provide a custom name for the Link aggregation in the text box.
   - **Active** ( )—This option is enabled by default. It indicates that the port members of the link aggregation are available for devices to connect. Slide the toggle switch to Inactive ( ) if you choose to disable this setting.
   - **Port membership**—Tap on the respective ports you want to add as members for the link aggregation. The selected port members are displayed below separated by commas.
   - **Aggregation mode**—Select one of the following aggregation modes:
     - **Static (default)**—This option is selected by default. It indicates simple aggregation of ports with no active link detection or failover.
     - **LACP**—Selecting this option indicates dynamic detection and automatic failover when connected to other LACP (802.3ad) capable switches. This mode will allow only one user defined network through the aggregated link. This option will pass the management VLAN network as untagged and all other networks as tagged.
   - **Included networks**—This section includes the following configuration settings:
     - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
     - **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.
   - **Specific network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Similar to the **All networks (default)** setting, selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.
5. Click **Done**.

A **Link aggregation details** link is displayed in the **Switch Details** page which allows you to modify the settings for the recently added link aggregation.

To delete a link aggregation, tap the advanced menu (⋮) icon in the **Link Aggregation Details** page and tap **Delete this link aggregation**.

Port Details

The **Port Details** page consists of the following settings:

- Name of the port in read and write mode.
- A toggle switch that allows you to set the port status to **Active** ( ) or **Inactive** ( ) . This field is set to **Active** by default.

Authentication and Security

The **Authentication and Security** section consists of the following options:

- **No authentication (default)**—Instant On devices and clients can connect to the port without authenticating. This is the default setting.
- **Port-based**—All Instant On devices and clients connected to the port are authorized after the initial 802.1x RADIUS authentication is successful.
- **Client-based**—Requires each Instant On device or client connecting to the port to separately authenticate to the 802.1x RADIUS server to gain access. You can also enable the 802.1X+MAC authentication toggle-switch ( ) to consider MAC authentication as the secondary option in case the RADIUS authentication is unsuccessful.

The **Port-based** and **Client-based** authentication methods, require configuration of RADIUS settings to determine how authentication behaves across all access controlled ports. The 802.1x RADIUS authentication parameters are listed in the table below with their descriptions:

Parameters	Description
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 or domain name**—Enter the IP address or fully qualified domain name 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 device 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.

Parameters	Description
Secondary RADIUS Server	Serves as a backup server to the primary RADIUS server. To configure a **Secondary RADIUS Server**, slide the toggle switch to the right ( ) and update the RADIUS server details. The available parameters are the same as that of the RADIUS server.
Send RADIUS Accounting	To **Send RADIUS Accounting** requests, slide the toggle switch to the right ( ).

- **Security protections**—Enable this setting when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. For more information, see Network Security.

Included networks

- **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.

More Options

Tap **More Options** to view additional configuration options in the Port Details screen. This section currently consists of the power management configuration settings.

Power Management — Under **More options**, tap **Power management** to view the power management configuration settings for the switch. These options are unavailable for ports that are part of LACP. The following options allow you to configure POE power supply for the device connected to the port:

- **Usage (default)** — The power allocated to the port is based on usage and is unrestricted.
- **Class** — The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts
Class 2	7 Watts
Class 3	15.4 Watts
Class 4	30 Watts
Class 5	45 Watts
Class 6	60 Watts

- **Port priority** — Assigns a priority level to the ports. When there is a budget constraint for delivering PoE power at the switch, power is delivered to the connected devices based on the port priority. The power is delivered in the following order: **Critical > High > Low**. Under **Port priority**, assign any one of the following priority level to the port:
  - **Low (default) —** Configures the port as a low priority port.
  - **High —** Configures the port as a high priority port.
  - **Critical —** Configures the port as a critical priority port.



When two ports belonging to the same priority are demanding power, the port with the least port number is given priority. Example: When port 2 and 5 are assigned **Critical** class and the switch has a power budget constraint, device on port 2 will receive full power and the remaining power budget will be allocated to the device on port 5.

PoE priority cannot be configured for Instant On devices. By default, Instant On devices are configured with **Usage** mode and **Critical** for **Port Priority.**

Use site power schedule — Toggle this switch to either enable ( ) or disable ( ) power schedule on the port. If enabled, the PoE supply to the port will be determined by the power schedule defined. To change the power schedule, tap on **Edit site power schedule**. For more information on configuring **Power Schedule**, see Power Schedule.

Connected Clients and Devices

The **Clients and devices connected on this port** link displays the list of clients and infrastructure devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. To filter the clients and devices connected to a specific network, tap the drop-down arrow (▼) and select one of the networks.

Clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. For indirectly connected clients, only their MAC address is displayed.

Locking Clients and Devices Connected to a Port

The lock button on the top-right of the **Clients and Devices** page allows you to lock the port and stop new clients from joining the port. When a port is locked, all clients connected to the port are allow-listed and granted access to the port while new devices are blocked. To connect new devices, the port must be unlocked. This option is unavailable on ports in which Instant On devices are connected.

To lock or unlock a port on an Instant On switch, tap on the lock button on the top right of the screen. The icon indicates that the port is locked and the icon indicates that the port is unlocked.



The maximum number of ports that can be locked in an Instant On switch is 10.

The maximum number of client that can be locked per port is 10.

Advanced Menu

The advanced menu (⋮) in the **Switch Details** screen provides the following configuration options:

- Locate
- Connectivity Test
- Restart

- Routing
- Port Mirroring
- Switching to Local Management
- Replace Device
- Remove from Inventory

Locate

The **Locate** option helps you to locate your device when there are many devices in the site. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

To locate your Instant On switch, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Tap **Locate**.
3. Slide the **Activate lights** toggle switch to the right ( ). The locator light is activated on the switch.

Connectivity Test

The **Network tests** option is used to test the reachability of an Instant On device. To perform a network test, you need to select a **Source** device on which the commands will be executed, and a **Destination** to be reached.

To run a network test on an Instant On switch, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Tap on **Connectivity test** from the drop-down menu. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On device from the drop-down list.

Only active devices of a site can be selected in this field. It could be a Switch or an AP.

4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

The table below shows the possible test results from the network tests:

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Fast connectivity to <host / IP address> **Expandable row**: More details
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Intermittent connectivity to IP address **Line 2**: <IP address> **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Unable to reach IP address **Line 2**: <IP address>

Connectivity Rating	Roundtrip Time	Test Results Format
		Line 3: Very slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details

Restart

To restart the device:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Select **Restart** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Restart**.

Routing

Configure routing on the Instant On switch. Routing is disabled by default. To configure routing for the switch perform the following steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Select **Routing** from the drop-down list. The Routing page is displayed.
3. To enable routing on a switch, toggle the **Allow routing between networks** switch to enable.
4. When **Allow routing between networks** is selected, icon is displayed next to networks that can be routed. If the icon is not visible, it implies that routing is turned off for the network.
5. To configure routing for a network, select the network to view the routing options:
   a. Toggle the **Allow routing** switch to enable.
   b. Configure either of the following options to assign an IP for the network:
      - **Automatic (default)** — The network will receive IP address from a DHCP server.
      - **Static** — Define the IP address assignment for the network by entering the following network parameters:
        - **Network IP address** — Enter the IP address for the network.
        - **Subnet mask** — Enter the subnet mask for the network.
6. Tap on **Done** to apply configuration changes. The routing configuration is applied after the Instant On switch reboots.



A minimum of two wired networks must be configured in the site to perform routing.

The Instant On switch must be online to configure routing.

Routing can be performed by only one Instant On switch in a site.

Port Mirroring

The Instant On switches have the ability to trace the packets sent and received from a port, by mirroring the data and sending it to a destination port. This feature is useful to troubleshoot network issues. Only one port mirroring session can be configured for each Instant On switch. If a site has multiple switches, there can be multiple port mirroring sessions active at the same time on different devices. When a port

mirroring session is active, a destination port cannot be selected as a member of a Link aggregation group.



When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.

To configure a port mirroring session on a port, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Select **Port mirroring** from the drop-down list.
3. In the **Port Mirroring** screen, select a switch port from the drop-down list, to which the traffic should be mirrored. This setting is configured as the destination port. The destination can be any port on the switch, except for the following:
   - The uplink port
   - A port where the Instant On device is connected.
   - A port that is configured as part of a trunk.
   - A port that uses 802.1x
4. Under **Source**, select one of the following options:
   a. **Network**—Select one of the available networks from the drop-down list.
   b. **Ports**—Select the port(s) to be used as the source port(s).



You can select up to eight ports as a source port.

5. Select one of the following as the **Traffic direction**:
   a. Transmit and receive
   b. Transmit
   c. Receive
6. Tap **Start mirroring** to initiate the mirroring of the packets sent from the source to the destination.

To stop the mirroring, tap **Stop mirroring** at anytime.

Switching to Local Management

The **Switch to local management** option allows you to change the switch management from cloud to local mode. When this option is selected, the switch will be removed from the site and the existing configuration will be stored on the switch. For more information, see Local Management for Switches.

To change switch management to local mode, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** page.
2. Tap **Switch to local management**. The appropriate assistant page is displayed to change the switch management to local mode.

Replace Device

Follow these steps to replace a failed Instant On switch with another Instant On switch, while maintaining the specific device configurations:



This option is visible only when the Instant On switch is offline.

It is recommended to replace the failed switch with a working switch of the exact same model to ensure all device configurations are successfully transferred to the replaced switch.

1. In the inventory, tap the failed Instant On switch. The **Switch Details** screen is displayed.
2. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
3. Tap **Replace device**.
4. In the **Replace Device** screen, tap **Search**.

The standalone Instant On switches connected to the network are displayed.

5. Tap the Instant On switch to replace with the failed switch in the inventory.
6. Tap **Replace**.
7. Tap **Finish**.

Remove from Inventory

To remove the switch when it is still online:

1. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
2. Select **Remove from inventory** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Remove**.

The Instant On switch can be removed from the inventory when it goes offline. On the **Switch 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.
2. To remove the switch from the inventory, follow these steps:
   a. If the Instant On switch is removed from the network, you can choose to remove the switch from the inventory by clicking **Remove from inventory** by tapping the advanced menu (⋮) icon in the **Switch Details** page.
   b. Click **Remove** to delete the switch from the inventory.

Cloud-Managed Stacking

Aruba Instant On supports cloud-managed stacking, which is a method of binding multiple Instant On switches so that they can act as a single switch. The switches must be directly connected to each other to form a chain or ring topology. This feature is supported only on the Instant On 1960 Series switches. A maximum of four switches can be deployed in a stack. Each Instant On site can accommodate multiple stacks. The switches in the stack comprise of the following roles:

- Conductor—Primary switch to which the uplink cable is connected.
- Backup—Secondary switch which takes over the responsibilities of the Conductor in case of a failover.
- Member—Constitutes the remaining two switches in the stack.

The Conductor is responsible for providing Layer 3 services. In an event where the Conductor goes offline, the Backup switch takes over the responsibilities of the Conductor until the Conductor is back online.

A stack must contain at least two Aruba Instant On 1960 Series switches. A stack can be created by one of the following methods:

- Creating a new site during the initial setup.
- Creating a new stack after the initial setup

Creating a New Stack— During Initial Setup

During the initial setup, a new stack can be created when creating a new site, or when extending the network. To discover Instant On 1960 Series switches during the initial setup, the switches must be connected in a ring or chain topology. A minimum of two switches and maximum of four switches need to be connected on the same layer 2 network. The layer 2 network should be the management network.

Figure 2 *Ring Topology*



Figure 3 *Chain Topology*



The following procedure allows you to create a new stack during the initial setup of an Instant On site:

1. Connect the Instant On 1960 Series in a ring or chain topology and follow the instructions provided in Setup a New Site. The discovery protocol should be able to detect the Instant On 1960 switch stack.
2. In the **Add new devices** page, select the stack from the list of discovered devices in the network.
3. Click **Finish**.

The newly created stack is now displayed in the site inventory.

To create a new stack using the extend my network setting, follow the instructions provided in Extend using a cable. This method allows you to deploy a stack only when it is connected in a ring topology.

Creating a New Stack— After Initial Setup

After completing the initial setup, you are allowed to deploy a stack using either the ring or chain topology. The following procedure describes how to create a new stack after completing the initial setup for the site:

1. Tap the **Inventory**( ) tile on the Aruba Instant On home screen or click the **Site Health**( ) banner and then click on **Show inventory**.
2. Tap the standalone Instant On 1960 Series switch on which the stack is to be created. The **Switch Details** screen is displayed.
3. Tap the advanced menu (⋮) icon in the title bar of the **Switch Details** screen.
4. Tap **Create stack**. The screen displays the standalone Instant On 1960 Series switches that are part of the site inventory.
5. Tap the Instant On 1960 Series switch you wish to add to the stack and then tap **Add device**.
6. In the **Roles** screen, set the Backup role for the newly added Instant On 1960 switch. The switch that was used to initiate creating the stack automatically assumes the roles of the Conductor.
7. Tap **Continue**.

The newly created stack is now displayed in the site inventory.



Out of the four Aruba Instant On 1960 switches in a stack, one switch should be assigned the role of the **Conductor** and another switch as the **Backup**. The remaining two switches in the stack will assume the role of **Member** switches. If a stack comprises of only two switches, then it would have a **Conductor** switch and a **Backup** switch, but no **Member** switch.

Adding an Instant On 1960 Series Switch to an Existing Stack

The following procedure allows you to add an Instant On 1960 Series switch to an existing stack in the inventory, which comprises of less than three Instant On 1960 Series switches:

1. Tap the **Inventory**( ) tile on the Aruba Instant On home screen or click the **Site Health**( ) banner and then click on **Show inventory**.
2. Ensure that the Instant On 1960 switch to be added in the stack is listed in the inventory.
3. Tap on the stack listed in the **Inventory** list. The **Stack Details** screen is displayed.
4. Tap the **Stack management** link in the **Stack Details** screen. The Instant On 1960 switches are listed in order of their assigned roles.
5. Tap the advanced menu (⋮) icon in the title bar of the **Stack Management** screen and then tap **Add device to stack**. The screen displays the standalone Instant On 1960 Series switches that are part of the site inventory, but not part of the stack.
6. Tap the Instant On 1960 Series switch you wish to add to the stack and then tap **Add device**.

The selected Instant On 1960 Series switch is now added to the stack in the inventory.

Stack Details

The **Stack Details** page provides details of the selected stack comprising of Aruba Instant On 1960 switches. To view the **Stack Details** page, follow these steps:

1. Tap the **Inventory**( ) tile on the Aruba Instant On home screen or click the **Site Health**( ) banner and then click on **Show inventory**.
2. Tap on the stack listed in the **Inventory** list. The **Stack Details** screen is displayed with details. The summary details include the **Stack name** and **Device name** of all the devices in the stack. It is followed by the details of each of the devices.

The **Stack Details** page has the following sections:

- Stack Management
- Connectivity
- Power over Ethernet (PoE)
- Ports

Stack Management

Stack management is used to add or remove an Instant On 1960 Series switch from the stack, and also to re-assign the role assigned to each switch in the stack. The **Stack Management** screen displays every device in the stack sorted by their role, namely, Conductor, Backup, and Member. Each Instant On 1960 switch is recognized by its current acting role, followed by the custom name set by the user. If a switch in the stack has not been assigned a custom name, then it's serial number will be used instead. The roles will appear in the screen based on the number of Instant On 1960 switches in the stack.

Assigning a Role for a Switch in the Stack

The following procedure is used to manage the roles assigned to each Instant On 1960 switch in the stack:

1. Tap the **Stack management** link in the **Stack Details** screen. The Instant On 1960 switches are listed in order of their assigned roles.
2. Tap the drop-down under any of the roles listed in the **Stack Management** screen to assign a different switch to the role. The Instant On 1960 switches present in the stack are displayed either by their custom name or their serial number.
3. Tap the Instant On 1960 switch from the list, to which the role needs to be assigned.
4. Tap **Ok**.
5. Tap **Done**.

Removing a Switch from the Stack

The following procedure is used to remove a member switch from the stack:

1. Tap the **Stack management** link in the **Stack Details** screen. The Instant On 1960 switches are listed in order of their assigned roles.
2. Tap the advanced menu (⋮) icon in the title bar of the **Stack Management** screen.
3. Tap **Remove device from stack**. The **Remove from Stack** page is displayed with the member switches.



This option is available only if there are member switches in the stack. You can only remove member switches from the stack. The switches assigned to the conductor and backup roles cannot be removed.

4. Tap the member switch to be removed from the stack.
5. Tap **Remove**.

Removing a switch from the stack does not remove the device from the site, the switch will be listed on the site as a standalone switch.



An Instant On 1960 series switch cannot be removed from the stack as long as it is assigned the role of a conductor or backup. To remove the switch, you must first swap the role of the conductor with a member and then remove the switch from the stack.

Connectivity

This section displays details of the uplink connection and LAN IP information of the switch. You can either configure Instant On switches to automatically receive an IP address from an external DHCP server running on the LAN or manually configure a Static IP address.

1. Under the **Connectivity** section of the **Stack Details** screen, tap **Advanced LAN parameters**.
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 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.
     - **Secondary DNS server**—Enter the IP address of the secondary DNS server.
3. Tap **DONE** to save the settings.

Power over Ethernet (PoE)

The **Power over Ethernet** section provides the following information:

- **Total budget**—The total power in watts that can be provided by the Instant On 1960 Series switch. This information is displayed individually for each PoE switch in the stack.
- **Power consumption**—The amount of power in watts currently being consumed by the connected PoE switches.



The **Power over Ethernet** section will not be displayed for non-PoE switches.

Ports

The **Ports** section in the **Stack Details** page visually displays the physical ports for the switch and provides additional statistics and configuration specific to a port. The Instant On mobile app provides a segmented view of the following options, selecting each of which will change the view of the ports accordingly:

To view the **Ports** section of the **Stack Details** page, follow these steps:

1. Tap the **Inventory**() tile on the Aruba Instant On home page or tap the **Site Health**() banner and then tap on **Show inventory**.
2. Tap on the stack listed in the **Inventory** list. The **Stack Details** screen is displayed with details.

The **Ports** section of the **Stack Details** page provides the following options:

- Status
- Networks
- Aggregation
- Port Details
- Connected Clients and Devices

Status

The **Status** tab view under **Ports** is selected by default when you arrive on the **Stack Details** page. The ports are visually represented on the page in the same manner as the actual physical ports on the device. Each port is numbered according to the port number on the switch and displays its current status. Tap on any of the switch ports to view the following details:

- Port number—The physical port number of the switch.
- Port name—The port name is displayed when a custom name is provided.
- Port status—The speed of the trunk is displayed if the port is the member of a trunk.
- Upstream and Downstream throughput—The upstream and downstream throughput of the trunk is displayed when the port is the member of a trunk.
- Member of <port membership name>—The name of the trunk is displayed, if the port is the member of a trunk.
- Port details—A hyperlink that redirects you to the **Port Details** page for configuration options.

Networks

After creating your network, you have the option to map the network to a VLAN port which, either allows traffic from all networks or only for a specific network. Each port in the Instant On switch can be assigned a separate VLAN ID and configured to manage the network traffic. The following procedure describes how to map a network to a VLAN port:

1. Tap on the stack listed in the **Inventory** list. The **Stack Details** screen is displayed
2. Select the **Networks** tab, under **Ports** to view the ports on the switch.
3. From the **Selected network** drop-down list, choose the network you want to map to a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Included networks**—This section includes the following configuration settings:
     - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
     - **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes

against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.

- **Specific network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.

7. Tap **Done** to finish mapping the network to the port.

Aggregation

Link aggregation configuration depends on the number of ports available on the switch. Instant On currently supports switches with the following number of ports:

Table 13: *Switch Ports Aggregation*

Number of Ports per Switch	Number of LAG Supported	Number of LAG members supported
12 ports	16 trunks	8 trunk members
24 ports		
48 ports		

The following procedure describes how to add a link aggregation group on the switch:

1. Tap on the stack listed in the **Inventory** list. The **Stack Details** screen is displayed
2. Under the **Ports** section, select the **Link Aggregation** tab.
3. Tap the **Add link aggregation** link.



You can configure a maximum of 16 Link Aggregation Groups on a stack. The 16 LAGs can either be configured all on a single device in the stack, or distributed between all the devices in the stack. The **Add link aggregation** link will no longer be available once the maximum number of link aggregation groups are configured on the stack.

4. The **Link Aggregation Details page** provides the following configuration options:
   - Provide a custom name for the Link aggregation in the text box.
   - **Active** ( )—This option is enabled by default. It indicates that the port members of the link aggregation are available for devices to connect. Slide the toggle switch to Inactive ( ) if you choose to disable this setting.
   - **Port membership**—Tap on the respective ports you want to add as members for the link aggregation. The selected port members are displayed below separated by commas.
   - **Aggregation mode**—Select one of the following aggregation modes:
     - **Static (default)**—This option is selected by default. It indicates simple aggregation of ports with no active link detection or failover.
     - **LACP**—Selecting this option indicates dynamic detection and automatic failover when connected to other LACP (802.3ad) capable switches. This mode will allow only one user defined network through the aggregated link. This option will pass the management VLAN network as untagged and all other networks as tagged.

- **Included networks**—This section includes the following configuration settings:
  - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
  - **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.
- **Specific network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Similar to the **All networks (default)** setting, selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.

5. Click **Done**.

A **Link aggregation details** link is displayed in the **Switch Details** page which allows you to modify the settings for the recently added link aggregation.

To delete a link aggregation, tap the advanced menu (⋮) icon in the **Link Aggregation Details** page and tap **Delete this link aggregation**.



Link aggregation to an uplink switch from two members in a stack is supported only in an active or passive mode and not a load balancing mode.

Port Details

The **Port Details** page consists of the following settings:

- Name of the port in read and write mode.
- A toggle switch that allows you to set the port status to **Active** ( ) or **Inactive** ( ) . This field is set to **Active** by default.

Authentication and Security

The **Authentication and Security** section consists of the following options:

- **No authentication (default)**—Instant On devices and clients can connect to the port without authenticating. This is the default setting.
- **Port-based**—All Instant On devices and clients connected to the port are authorized after the initial 802.1x RADIUS authentication is successful.
- **Client-based**—Requires each Instant On device or client connecting to the port to separately authenticate to the 802.1x RADIUS server to gain access. You can also enable the 802.1X+MAC authentication toggle-switch ( ) to consider MAC authentication as the secondary option in case the RADIUS authentication is unsuccessful.

The **Port-based** and **Client-based** authentication methods, require configuration of RADIUS settings to determine how authentication behaves across all access controlled ports. The 802.1x RADIUS authentication parameters are listed in the table below with their descriptions:

Parameters	Description
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 or domain name**—Enter the IP address or fully qualified domain name 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 device 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.
Secondary RADIUS Server	Serves as a backup server to the primary RADIUS server. To configure a **Secondary RADIUS Server**, slide the toggle switch to the right ( ) and update the RADIUS server details. The available parameters are the same as that of the RADIUS server.
Send RADIUS Accounting	To **Send RADIUS Accounting** requests, slide the toggle switch to the right ( ).

- **Security protections**—Enable this setting when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. For more information, see Network Security.

Included networks

- **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged**—The port will receive and send traffic from the default network using the management VLAN tag. To custom map the port to a tagged VLAN, tap the checkboxes against the networks listed under **Tagged networks**. A maximum of 22 tagged networks can be mapped to a port at a given time.

More Options

Tap **More Options** to view additional configuration options in the Port Details screen. This section currently consists of the power management configuration settings.

Power Management — Under **More options**, tap **Power management** to view the power management configuration settings for the switch. These options are unavailable for ports that are part of LACP. The following options allow you to configure POE power supply for the device connected to the port:

- **Usage (default)** — The power allocated to the port is based on usage and is unrestricted.
- **Class** — The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts
Class 2	7 Watts
Class 3	15.4 Watts
Class 4	30 Watts
Class 5	45 Watts
Class 6	60 Watts

- **Port priority** — Assigns a priority level to the ports. When there is a budget constraint for delivering PoE power at the switch, power is delivered to the connected devices based on the port priority. The power is delivered in the following order: **Critical > High > Low**. Under **Port priority**, assign any one of the following priority level to the port:
  - **Low (default) —** Configures the port as a low priority port.
  - **High —** Configures the port as a high priority port.
  - **Critical —** Configures the port as a critical priority port.



When two ports belonging to the same priority are demanding power, the port with the least port number is given priority. Example: When port 2 and 5 are assigned **Critical** class and the switch has a power budget constraint, device on port 2 will receive full power and the remaining power budget will be allocated to the device on port 5.

PoE priority cannot be configured for Instant On devices. By default, Instant On devices are configured with **Usage** mode and **Critical** for **Port Priority.**

Use site power schedule — Toggle this switch to either enable ( ) or disable ( ) power schedule on the port. If enabled, the PoE supply to the port will be determined by the power schedule defined. To change the power schedule, tap on **Edit site power schedule**. For more information on configuring **Power Schedule**, see Power Schedule.

Connected Clients and Devices

The **Clients and devices connected on this port** link displays the list of clients and infrastructure devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. To filter the clients and devices connected to a specific network, tap the drop-down arrow (▼) and select one of the networks.

Clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. For indirectly connected clients, only their MAC address is displayed.

Locking Clients and Devices Connected to a Port

The lock button on the top-right of the **Clients and Devices** page allows you to lock the port and stop new clients from joining the port. When a port is locked, all clients connected to the port are allow-listed and granted access to the port while new devices are blocked. To connect new devices, the port must be unlocked. This option is unavailable on ports in which Instant On devices are connected.

To lock or unlock a port on an Instant On switch, tap on the lock button on the top right of the screen. The icon indicates that the port is locked and the icon indicates that the port is unlocked.



The maximum number of ports that can be locked in an Instant On switch is 10.

The maximum number of client that can be locked per port is 10.

Advanced Menu

The advanced menu (⋮) in the **Stack Details** screen provides the following configuration options:

- Locate
- Connectivity Test
- Restart
- Routing
- Port Mirroring
- Unstack
- Replace Device

Locate

The **Locate** option helps you to locate your device when there are many devices in the site. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default and can be turned on for a particular stack member or for the entire stack.

To locate your Instant On switch, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Tap **Locate**.
3. Slide the **Activate lights** toggle switch to the right ( ). The locator light is activated on the switch.

Connectivity Test

The **Connectivity tests** option is used to test the reachability of an Instant On device. The connectivity test for a stack is not different from the one performed on a standalone switch. When a hostname or IP address is provided, the test is executed on each of the devices in the stack and the results are displayed accordingly. To perform this test, you need to select a **Source** device on which the commands will be executed, and a **Destination** to be reached.

To run a connectivity test on an Instant On stack, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Tap on **Connectivity test** from the drop-down menu. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On stack from the drop-down list.

4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

The Connectivity tests will be executed and displayed for every device in the stack.

The table below shows the possible test results from the network tests:

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Fast connectivity to <host / IP address> **Expandable row**: More details
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Intermittent connectivity to IP address **Line 2**: <IP address> **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Unable to reach IP address **Line 2**: <IP address> **Line 3**: Very slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Expandable row**: More details

Restart

To restart the device:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Select **Restart** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Restart**.

Routing

An Instant On 1960 Series switch stack allows routing for all the devices in the stack. The routing on a stack is defined at the stack level. If the conductor switch goes offline, then the backup switch takes over the routing service for the stack. Routing is disabled by default. To configure routing for the switches in the stack, perform the following steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Select **Routing** from the drop-down list. The Routing page is displayed.
3. To enable routing on a switch, toggle the **Allow routing between networks** switch to enable.
4. When **Allow routing between networks** is selected, icon is displayed next to networks that can be routed. If the icon is not visible, it implies that routing is turned off for the network.

5. To configure routing for a network, select the network to view the routing options:
   a. Toggle the **Allow routing** switch to enable.
   b. Configure either of the following options to assign an IP for the network:
      - **Automatic (default)** — The network will receive IP address from a DHCP server.
      - **Static** — Define the IP address assignment for the network by entering the following network parameters:
        - **Network IP address** — Enter the IP address for the network.
        - **Subnet mask** — Enter the subnet mask for the network.
6. Tap **Done** to apply configuration changes.

NOTE

A minimum of two wired networks must be configured in the site to perform routing.

The Instant On switch must be online to configure routing.

Port Mirroring

The Instant On switches have the ability to trace the packets sent and received from a port, by mirroring the data and sending it to a destination port. This feature is useful to troubleshoot network issues. Only one port mirroring session per stack is supported. When a port mirroring session is active, a destination port cannot be selected as a member of a Link aggregation group.

NOTE

When configuring port mirroring, avoid oversubscribing the destination port to prevent the loss of mirrored data.

To configure a port mirroring session on a port, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Select **Port mirroring** from the drop-down list.
3. In the **Port Mirroring** screen, select a switch port from the drop-down list, to which the traffic should be mirrored. This setting is configured as the destination port. The destination can be any port on the switch, except for the following:
   - The uplink port
   - A port where the Instant On device is connected.
   - A port that is configured as part of a trunk.
   - A port that uses 802.1x
4. Under **Source**, select one of the following options:
   a. **Network**—Select one of the available networks from the drop-down list.
   b. **Ports**—Select the port(s) to be used as the source port(s).

NOTE

You can select up to eight ports as a source port.

5. Select one of the following as the **Traffic direction**:
   a. Transmit and receive
   b. Transmit
   c. Receive

6. Tap **Start mirroring** to initiate the mirroring of the packets sent from the source to the destination.

To stop the mirroring, tap **Stop mirroring** at anytime.

Unstack

Follow these steps to unstack the Instant On 1960 Series switches:

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Tap **Unstack**. The **Unstack** screen is displayed, requiring your confirmation.
3. Tap **Unstack**.

The stack is removed and the switches will now appear as standalone devices in the inventory.

Replace Device

Follow these steps to replace an Instant On 1960 Series switch from the stack with another Instant On 1960 switch, while maintaining the specific device configurations:



This option is visible when at least one of the Instant On 1960 switch in the stack is offline.

1. Tap the advanced menu (⋮) icon in the title bar of the **Stack Details** screen.
2. Tap **Replace device**. The offline Instant On switch is displayed.
3. Tap the offline Instant On switch.
4. In the **Replace Device** screen, tap **Search**.

The standalone Instant On 1960 switches connected to the network are displayed.

5. Tap the Instant On 1960 switch to replace with the offline switch in the stack.
6. Tap **Replace**.
7. Tap **Finish**.

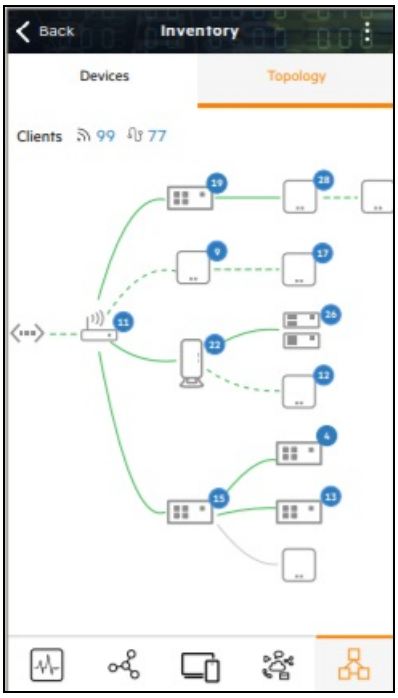


Replacing an Instant On 1960 switch for a model with lesser ports, or replacing a PoE device for a non-PoE switch is allowed. However, the new switch would not be capable of adopting the same configurations that only applied to the replaced switch.

Topology

The **Topology** tab in the Inventory page displays an overview of the Instant On network. Information such as the network topology, state of network devices, number of connected clients, and status of links between network devices are displayed in this page. Detailed information of a device can be viewed by tapping on it.

An example of the topology page is displayed below:

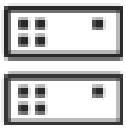


NOTE

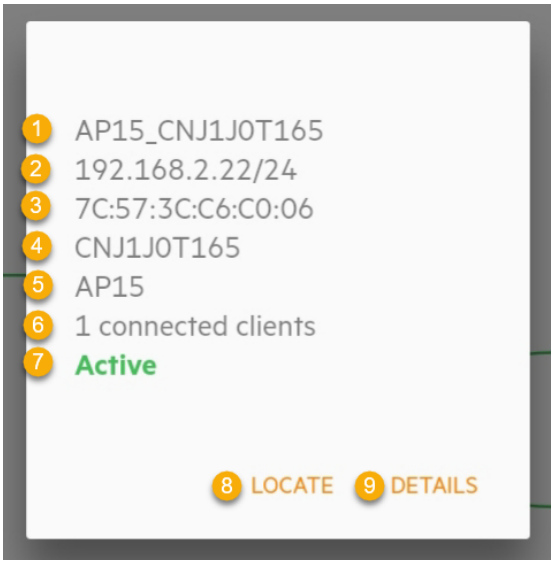
Pinch to zoom in or zoom out.

Description of Topology Icons

Icon	Description
Links	
	Indicates an active wired connection.
	Indicates an active wireless connection.
	Indicates an inactive wired connection.
	Indicates an inactive wireless connection.
	Indicates the devices constituting a wired connection are being restarted.
	Indicates the device connected over-the-air being restarted.
	Indicates the device constituting a wired connection is being deleted.
	Indicates the device connected over-the-air is being deleted.
Devices	
	Indicates an AP11, AP12, AP15, or AP22 access point.
	Indicates an AP17 access point.

Icon	Description
	Indicates an AP11D access point.
	Indicates an Instant On router.
	Indicates an Instant On switch.
	Indicates third party switches. This icon is displayed in the topology only if Instant On devices are connected to the third party switch.
	Indicates the Aruba Instant On 1960 Series switches connected in a stack.
Connection Type	
	Indicates that the network is connected to a router.
	Indicates that the network is connected to a private network.
Connected Clients	
	Indicates the number of wired and wireless clients connected to the device.

Description of Device Information Card



1. Device name
2. IP address
3. MAC address
4. Serial Number
5. Device Model (for Instant On devices only)
6. Number of connected clients
7. Status of device connectivity
8. Locate button that allows you to locate the AP. When used, the LED light on the device will blink amber for 30 minutes. This feature is supported only on Instant On devices.
9. Device Details link that takes you to the device details page.

NOTE: If the serial number of the device is the same as the device name, the serial number is not displayed in the device information card. The serial number of the AP is used as the device name by default.

NOTE: If the MAC address of the device is the same as the device name, the MAC address is not displayed in the device information card.

Stack Topology

A stack comprises of its own topology within the device inventory. To view the topology of the stack, follow these steps:

1. Tap the **Inventory** ( ) tile on the Instant On mobile app home page or click the **Site Health** banner and then click on **Show inventory**.
2. Tap **Topology** .
3. Slide the **View stack topology** toggle switch to the right ( ).

The topology formed by the devices in the stack is displayed.

The stack topology displays the following details:

- Interconnections between the devices in the stack.
- Devices in the stack which are connected to another Instant On device that is not part of the stack.
- Connectivity status between devices.
- Third party devices that are connected to the stack, resulting in an invalid topology.
- Displays the devices in the stack that are experiencing problems. The warning icon ( ) is displayed on the bottom-left corner of the device.
- Displays the connections between a device of the stack and another Instant On device in the inventory.
- Displays the summary details for each device of the stack and stand-alone devices.

Auto-Detection and Auto-Configuring of Switch Ports

In a scenario where one Instant On device is connected to another, the Instant On system configures the ports with automatic settings to avoid the complexity of manually reconfiguring the port. The auto-detection and auto-configuration feature provides the following capabilities:

- When a second Instant On device is requesting power on a port, this port is set to Critical PoE priority to maintain the service as much as possible.
- All networks are made available on that port, in order to ensure that services from another Instant On device can operate freely.
- If the auto-configured port is connected to another Instant On device, the status of the port is set to Trusted.
- Users are not permitted to change the **Ports** settings that interfere with the auto-configuration service.

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

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

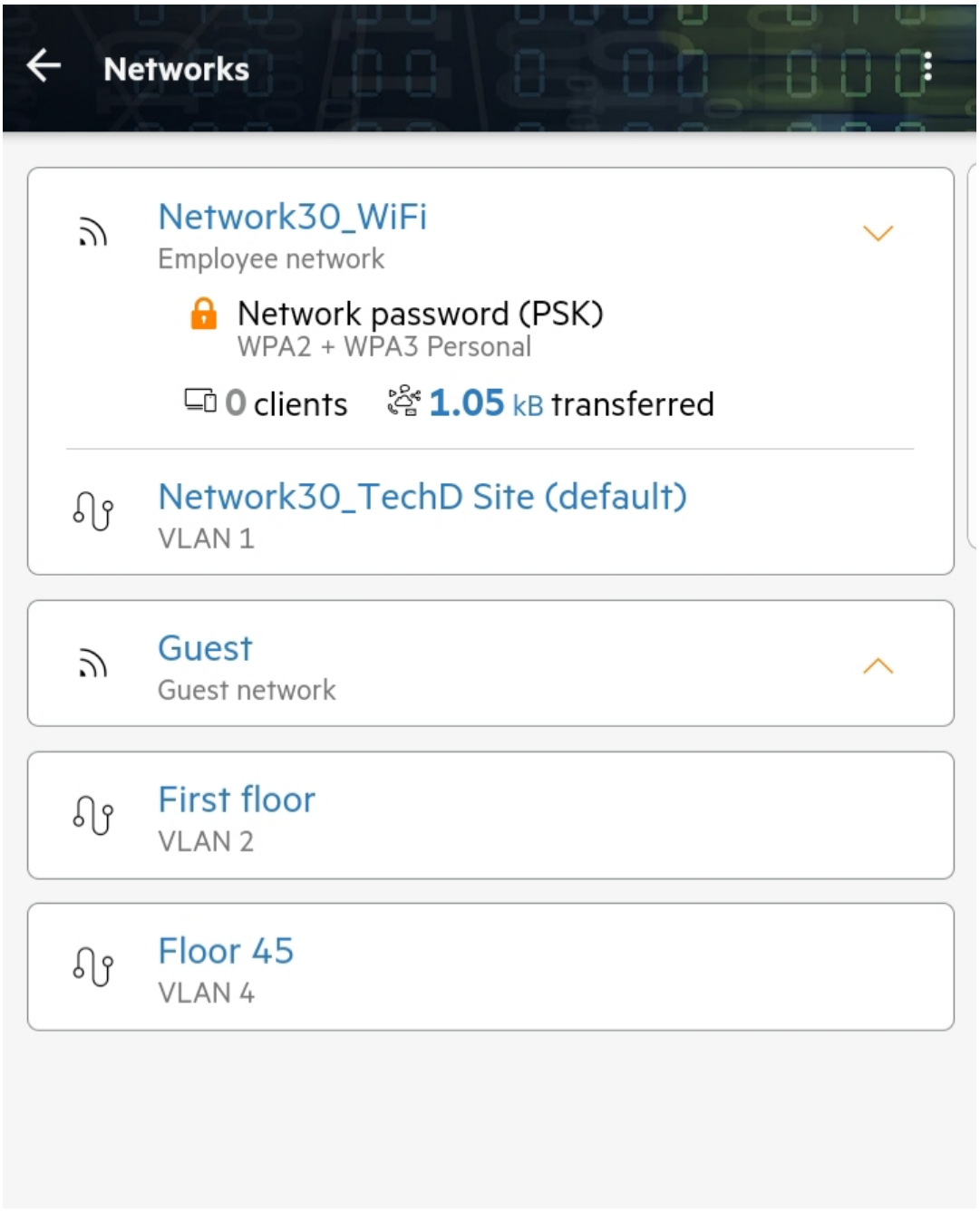


Figure 4 *Screenshot of Networks Page in the Instant On Mobile Application*

The Networks page of the Instant On Mobile Application displays the lists of networks configured in the site. Clicking on the arrow icon beside the network name displays brief information about the network such as the network security type, number of clients connected, and volume of data transferred in the network. Click on the network name will take you to the **Network Details** page.

For more details about a specific network, select one of the following links:

- Employee Network
- Guest Network
- Wired Network

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 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.

To configure an employee network:

1. Tap **Networks** tile on the Instant On mobile app home page.
2. Tap Add (+) and select the **Wireless** tab as the **Network type**. This tab appears only when your site has both wired and wireless networks.
3. Select **Employee**, under Usage to indicate that the network is for an enterprise.
4. Enter a **Network name** for the employee network. This will also be broadcasted as the SSID for the WLAN network.
5. Configure any one of the following security options:
   - **Password**—Selecting this option displays the **Network password (PSK)** options. This enables you to secure the network using a shared password (PSK). Create a password of your choice in the **Network password** field. WPA2 Personal is enabled by default. To enable WPA2 + WPA3 Personal, select the checkbox.
   - **RADIUS**—Selecting this option displays the **Authentication server (RADIUS)**options. This enables you to secure the network using a higher encryption RADIUS authentication server. To configure a RADIUS server, update the following parameters:

NOTE

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

     - **WPA2 + WPA3 Enterprise**—WPA2 Enterprise is enabled by default. To enable WPA2 + WPA3 Enterprise, select the checkbox. To configure the other radius parameters, tap **More Radius parameters**. The **Authentication Servers** screen is displayed. Configure the following parameters:
       - **Send RADIUS Accounting**—Toggle the switch to enable RADIUS accounting messages.
       - **Primary RADIUS Server**—Configure the following parameters for the **Primary RADIUS Server**.

- **RADIUS Server IP address or domain name**—Enter the IP address or fully qualified domain name 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.
- **Secondary RADIUS Server**— Toggle the switch to enable to configure a secondary RADIUS server. When selected, configure the following parameters:
  - **Server IP address**—Enter the IP address of the secondary RADIUS server.
  - **Shared secret**—Enter a shared key for communicating with the secondary RADIUS server.

    Authentication port—Enter the authentication port number of the secondary RADIUS server within the range of 1–65535. The default port number is 1812.

- **Network Access Attributes** - 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. 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.

6. Tap the back arrow (←) to return to the employee details page.



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 the Employee Network Name and Password

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

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Select the employee network from the **Networks** list to view the **Employee Details** screen.
3. Under **Identification**, 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.
4. Tap **DONE** to save the settings.

More Options

The **More options** drop-down in the Aruba Instant On mobile app allows you to configure following settings for clients on employee networks:

- IP and Network Assignment
- Network Access Schedule
- Bandwidth Usage
- Network Access
- Wireless Options
- Shared Services
- Applications Statistics

IP and Network Assignment

The **IP and network assignment** setting in the Aruba Instant On mobile app 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. By default, the default network created during setup is assigned as your local network. To assign other networks, select the network from the **Assigned network** drop-down. The VLAN ID will be assigned to your network based on your network assignment. This option is enabled by default for employee networks.
- **Specific to this wireless 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.

Network 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.

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

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee network from the list. The **Employee Details** page is displayed.
2. Under **More options**, tap **Add a network access schedule**. The **Network Access Schedule** page is displayed.

3. 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. Under **Days of the week**, select the day(s) during which the network will be active.
5. 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**. Network access can be configured to end on the same day or the next day. When a time prior to the **Start Time** is selected as the **End Time**, a **Next Day** alert is displayed indicating that the end time is configured on the next day. This enables you to configure scheduled networks for your business when the active hours extend to the early hours of the next day.
6. Tap the back arrow ( ) to return to the **Employee Details** page. Tap **DONE**.

Bandwidth Usage

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. As an alternative, you can choose to set the bandwidth on an entire network, instead of restricting the usage per client.

To configure a bandwidth limit for each client connected to the network, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.
2. Tap the **More options** drop-down.
3. Tap **Bandwidth Usage**.
4. Set the **Limit bandwidth usage** toggle switch to enabled ( ).
5. Tap the **Client** radio button and move the slider to set the speed limit for the employee or guest network. The limit is set to **25 Mbps** by default. The available speed limits are:
   - **5 Mbps**—Good for online gaming, video conferences and streaming videos.
   - **1 Mbps**—Good for emails, VoIP, web surfing, music, and social media.
   - **10 Mbps**—Good for HD video streaming.
   - **25 Mbps**—Good for 4K video streaming.
6. The changes are auto saved. Tap the back arrow ( ) to return to the employee or guest network details page.

To configure a bandwidth limit on the per-AP SSID network, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.
2. Select the employee or guest network and tap the **More options** drop-down.
3. Tap **Bandwidth Usage**.
4. Set the **Limit bandwidth usage** toggle switch to enabled ( ).
5. Tap the **Network** radio button and enter the **Downstream (Mbps)** and **Upstream (Mbps)** limit between 1—64 Mbps.

Network Access

The **Network Access** option in the Instant On mobile app, allows you to configure network access restrictions for wireless clients based on IP destination addresses.

The following procedure configures network access restrictions on a wireless network:

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee or guest network from the list. The network details page is displayed.
2. Under **More options**, tap **Network access**. The **Network Access** screen is displayed.
3. Configure one of the of the following settings on your network:
   - **Unrestricted access (default)**—This is the default setting for Employee networks. This option allows users to access any destination available to the network.
   - **Restricted access**—This is the default setting for Guest networks. This option restricts users to access only the internet and prevents them from accessing internal network resources. To allow the users to access specific network resources, enter the **IP address** in the list of IP addresses and tap + .

   If the Instant On AP is deployed in the Router mode, configure one of the following **Restricted access** settings:
   - **Allow internet access**—Allows the client to access the Internet.
   - **Allow network access**—Allows traffic between clients of the same subnet and blocks the traffic to other subnets.
   - **Allow specific IP address**—Allows the client to access specific resources using an IP address. Enter the **IP address** in the list of IP addresses and tap + .

Wireless Options

The **Wireless options** in the Aruba Instant On mobile app allows you to configure radio frequencies for your wireless network.

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**.

Wi-Fi 6

The **Wi-Fi 6** switch toggles the Wi-Fi 6 (802.11ax) capabilities of the network. When enabled, 802.11ax capable clients can make use of enhanced throughput and transmission capabilities of the 802.11ax standard.

This setting is enabled ( ) in the mobile app by default. Slide the toggle switch to the left if you want to disable ( ) the Wi-Fi 6 setting.

NOTE

- The Wi-Fi 6 option is only available when the device inventory has at least one Aruba Instant On AP22 or AP25 access point.
- Disable this feature if the client experiences problem connecting to the network.

Multiple Clients Optimizations

This setting is available only when the Wi-Fi 6 toggle switch is enabled. This feature improves the channel efficiency when multiple Wi-Fi 6 clients are connected by enabling OFDMA. This setting is disabled by default on the network, slide the toggle switch ( ) to the right to enable this feature.

Optimize for Video Streaming

This option enhances the quality and reliability of streaming videos by converting multicast streams into unicast streams over the wireless network, while also preserving the bandwidth available to the non-video clients.



This option is disabled by default, as some wireless clients may not be compatible with this optimization.

To configure optimization for video streaming, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.
2. Select the employee or guest network and tap the **More options** drop-down.
3. Tap **Wireless options**.
4. Set the Optimize for video streaming toggle switch to enabled ( ).
5. The changes are auto saved. Tap the back arrow ( ) to return to the employee or guest network details page.

Radio

Radio settings in the Aruba Instant On 2.6.0 mobile app allows you to configure radio frequencies for your wireless network.

To configure radio frequency, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and select an employee network or guest network from the list.
2. Select the employee or guest network and tap the **More options** drop-down.
3. 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.
4. The changes are auto saved. Tap the back arrow ( ) to return to the employee or guest network details page.

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.



Enabling this option might slow down the network performance.

Shared Services

Aruba Instant On mobile app allows clients to discover devices and access shared services available on the same or different networks in your site. To use the Shared services feature, you must first enable the Shared services setting in the Instant On mobile app. For information on deploying shared services, see Deploying Multicast Shared Services.

NOTE

The Shared services enable ( ) or disable ( ) option appears in the Instant On mobile app, only when the site is configured with two or more networks/VLANs.

To configure shared services on an employee network or guest network, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and tap the advanced menu ( ) icon in the header.
2. Select **Shared services** from the menu and slide the toggle switch next to Shared services, to the right ( ) to enable the Shared services feature on the network.
3. Once you have enabled the Shared services setting, navigate back to the **Networks** page and select an employee, guest, or wired network from the list. The **Employee Details**/ **Guest Details** / **Networks Details** page is displayed.
4. Under **More options**, tap **Shared services** to view the following information:
   - **Services detected on this network**—Lists all the services available on the current network. The services detected on the same network are always available for the clients to access without restriction.
   - **Services detected on other networks**—Lists all the services available on other employee networks of your site. By default, the services connected to other networks are disabled. Slide the toggle switch to enabled( ), to allow clients to access the shared services available on other networks.

NOTE

For Shared services to be available on Guest networks, the Network assignment must be bridged (Same as local network) and the network access must be set to Unrestricted.

List of Supported Services

The list of supported services is displayed per device on the Instant On mobile app. A multiple services icon is displayed next to the device if it provides more than one service. New services discovered on a known shared device are automatically shared. However, for new devices, the new services discovered will not be shared until the user allows access to share. 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.
- AirPrint™—Apple® AirPrint allows you to print from an iPad, iPhone or iPod Touch directly to any AirPrint compatible printers.

- Sharing—Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple® devices.
- RemoteMgmt—Use this service for remote login, remote management, and FTP utilities on Apple® devices.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

Applications Statistics

The **Applications** tab in the Aruba Instant On mobile app 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:

1. Tap the down arrow (﹀) next to the employee or guest network name.
2. Tap on the pie chart displaying the data transferred (in MB).

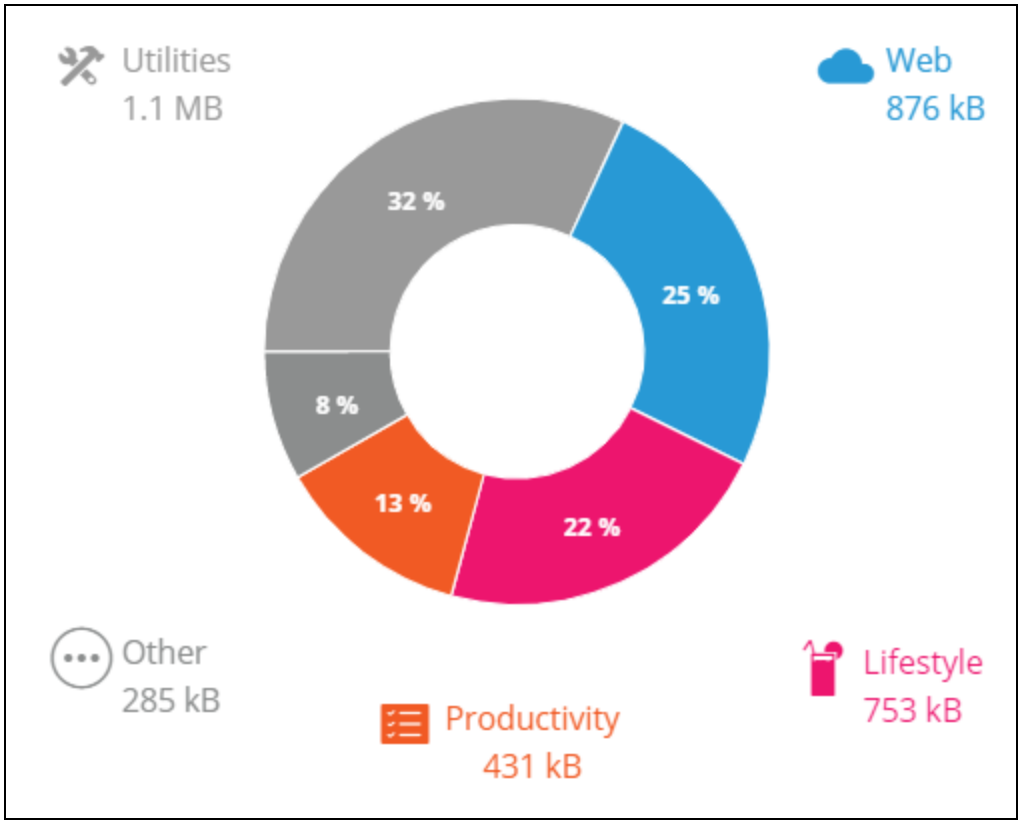
Viewing Client Count

The **Application** tab in the Aruba Instant On mobile app displays the client count, which is the total number of clients currently connected to the network. For more information, 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 provides data for the top five application categories, based on usage. Data is presented in both bytes and percentage.

Figure 5 *Applications Chart*



Viewing Total Data Transferred

The **Applications** tab in the Aruba Instant On mobile app 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 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.

Guest Network

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

- To create a Guest Network, follow these steps:

  1. Tap **Networks** tile on the Instant On mobile app home screen.
  2. Tap Add ( ) and select the **Wireless** tab. This tab appears only when your site has both wired and wireless networks.
  3. Select **Guest**, under **Usage** to indicate that the network is for guest users.
  4. Enter a name for the guest network.
  5. Select one of the following **Security** levels:
     a. Tap **Open**, if you want the user to access this network without the requirement of entering a username or password. You are also provided the option to enable **Guest Portal** and **Wi-Fi Enhanced Open** on the network. For more information, see Enabling Guest Portal and Wi-Fi Enhanced Open (OWE)
     b. Tap **Password**, if you want to 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. Selecting this option will require you to first authenticate to the guest network using the PSK, then you will be redirected to the captive portal page.
  6. To configure a guest portal in addition to the security levels, enable the **Guest portal** toggle switch ( ) and follow the instructions provided in Enabling Guest Portal.

- To change the guest network status manually, follow these steps:

  1. Tap **Networks** ( ) tile on the Instant On home page and select a guest network from the list. The **Guest Details** page is displayed.
  2. Slide the **Inactive** toggle switch ( ) to the right set the network to **Active** ( ).
  3. Tap **DONE**. The network is marked as **Active**, and all network settings are made visible.

Wi-Fi Enhanced Open (OWE)

Wifi-Enhanced Open (OWE) is the open security type derived from WPA3. It runs concurrently with an equivalent legacy Open SSID. Essentially, 2 similar SSIDs are broadcast and OWE capable clients will connect to the OWE version of the SSID, while non-OWE clients will connect to the legacy version of the SSID. Enhanced open provides improved data encryption in open Wi-Fi networks and protects data from sniffing.

The option to configure OWE is available only when **Open** is chosen as a security choice for a Wireless Network.

To configure OWE on the Guest network, follow these steps:

1. Ensure that the **Security** type for the Guest network is set to **Open**.
2. Move the Wi-Fi Enhanced Open toggle switch to enabled ( )
3. Tap **Done**.

More Options

The **More options** drop-down in the Aruba Instant On mobile app allows you to configure following settings for clients on guest networks:

- IP and Network Assignment
- Network Access Schedule
- Bandwidth Usage
- Network Access
- Wireless Options
- Shared Services

Enabling Guest Portal

Guest portal can be accessed using the Instant On mobile app. 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, follow these steps:

1. Click **Networks** from the Aruba Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, enable the **Guest portal** toggle switch ( ).
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.

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 14: *Internal Captive Portal Configuration*

Parameter	Description
Background	Tap the box to view the color palette and choose a color for the background of the internal captive portal page.
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.
Logo / Image	Tap the image icon to browse and upload an image from your device. **NOTE:** Ensure that you upload the image only in the png, jpg, gif, or bmp formats.
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.
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. ■ **Redirect URL**—Specify the custom URL to which users should be redirected after clicking the accept button. ■ **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.

Configuring External Captive Portal

You can configure an external captive portal for your guest network in one of the following ways:

- Use third-party captive portals
- Customize the captive portal by configuring RADIUS authentication and accounting parameters

Using Third-Party Captive Portal

Instant On supports the following third-party external captive portal providers:

- Aislelabs
- Purple Wi-Fi
- Skyfii.io
- Wavespot
- Zoox

1. Select the preferred captive portal provider tile. You must have an account with the selected provider.
2. Configure the following parameters:

- **Social WiFi identifier**—Enter the social Wi-Fi identifier provided by the provider. This field is applicable only for Aislelabs.
- **Preferred servers**—Select the preferred server from the drop-down list. This field is applicable only for Aislelabs.
- **Select your region**—Select the region from the drop-down. This field is not applicable for Aislelabs.
- **Allowed domains**— Slide the toggle switches to enabled ( ) to allow access to social network domains. Enter a domain name in the **New domain name** and tap + to add additional domains. This allows unrestricted access to additional domains.

Customizing Captive Portal

You can customize an external captive portal splash page if you do not wish to use above mentioned third-party providers.

To customize the external captive portal, follow these steps:

1. Tap the **Custom** tile on the **Guest Portal** page.
2. Configure the following external captive portal configuration parameters:

Table 15: *External Captive Portal Configuration*

Parameter	Description
Server URL	Enter the URL for the external captive portal server.
Redirect URL	Specify a redirect URL if you want to redirect the users to another URL.
Allowed domains	Slide the toggle switches to enabled ( ) to allow access to social network domains. Enter a domain name in the **New domain name** and click + to add additional domains. This allows unrestricted access to additional domains.
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.
Primary RADIUS Server	Configure a primary RADIUS server for authentication by updating the following fields: ▪ **Server IP address or domain name**—Enter the IP address or fully qualified domain name of the external RADIUS server. ▪ **Shared secret**—Enter a shared key for communicating with the external RADIUS server. Tap the **More RADIUS parameters** link to configure the following parameters:

Table 15: *External Captive Portal Configuration*

Parameter	Description
	▪ **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.
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.

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, follow these steps:

1. Tap **Networks** from the Aruba Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, enable the **Guest portal** toggle switch ( ).

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.

Wired Network

The wired network is suitable for users whose network infrastructure is focused mainly on the onboarding of Instant On switches. Choosing the wired-only option during the initial setup automatically creates a default wired network. The default network has a management VLAN whose value is read-only. The default wired network that was created during initial setup cannot be deleted unless you choose to delete the site entirely from your account. Once the initial setup is complete, you can use the following procedure to create up to a maximum of 22 wired networks for a site.

The following procedure creates a wired network:

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Tap + to create a new network. The **Create Network** screen is displayed.
3. Select **Wired** as **Network type**. This tab appears only when your site has both wired and wireless networks.
4. Enter a **Network name** for the network.
5. Enter a **VLAN** for your network.
6. Tap **Done**.

Modifying the Network Name or VLAN ID

The following procedure is used to modify an existing wired network:

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Select the wired network from the **Networks** list to view the **Network Details** screen.
3. Under **Identification**, enter a new name under **Network name** to change the network name or enter a new **VLAN** to change the VLAN ID.
4. Tap **Done**.



If the selected wired network is a default network, then you cannot modify your **Management VLAN**.

Enabling or Disabling a Wired Network

The following procedure enables or disables a wired network:

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Select the wired network from the **Networks** list to view the **Network Details** screen.
3. Under **Identification**, slide the toggle switch to the right to set the network to **Active** ( ), or to the left to set the network to **Inactive** ( ).

NOTE

The default wired network is used to manage the Instant On device does not have the option to be enabled or disabled.

Important Points to Note:

- Deactivating the wired network means that no wired network station will be able to connect. The network will be shut down at the port level and would not be able to pass traffic anymore. The network is removed from all the wired ports.
- Deactivating a wired network that has one or more associated wireless-network(s) displays a dialog box indicating that all the wireless networks and associated clients will be disconnected from the network. Tap **Deactivate** to continue this operation.
- Re-activating a wireless-network on a wired-network that was previously deactivated displays a dialog box indicating that the associated wired-network will also be activated. Tap **Activate** to continue this operation.
- Re-activating a wired-network that has one or more associated wireless-networks, activates the associated-wireless networks as well. Tap **Activate** to continue this operation.

Configuring a Voice Network

Instant On allows you to configure a VLAN on the switch to prioritize voice traffic over all other traffic. The voice traffic is tagged to have higher priority over other data by using Class of Service (CoS) values.

To configure a wired network VLAN as a Voice VLAN, follow these steps:

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Select the wired network from the **Networks** list to view the **Network Details** screen.
3. Under **Identification**, slide the **Voice network** toggle switch to the right ( ) to allow clients with voice capabilities to be automatically redirected to this network.
4. Tap **Done**.

Important Points to Note:

- Only one Voice network can be configured per site.
- The Voice network cannot be assigned to the management VLAN.
- The Voice network feature is available only for IP phones that are directly connected to the switch.
- If you connect a phone on a dedicated port with restricted access, the restricted access configuration will also be applied to the Voice VLAN.

Energy Efficient Ethernet

Energy Efficient Ethernet (EEE) or Green Port Management reduces power consumption on switch ports when data activity is low or idle. Regular heartbeats are sent to gauge port activity. Ports are fully enabled when data activity resumes. This function operates in the background and does not display a configurable option or activity status in the Instant On mobile app.

NOTE

Instant On currently supports only a subset of the EEE feature (802.3az). The ability to detect copper and optical link length and reduce power accordingly is not supported.

More Options

The **More options** drop-down in the Aruba Instant On mobile app allows you to configure following settings for clients on wired networks:

- Network Access
- Network Security
- Shared Services
- Network Assignment

Network Access

The **Network Access** option in the Instant On mobile app, allows you to configure network access restrictions for wired clients based on IP destination addresses.

The following procedure configures network access restrictions on a wired network:

1. Tap **Networks** ( ) tile on the Instant On home page and select a wired network from the list. The network details page is displayed.
2. Under **More options**, tap **Network access**. The **Network Access** screen is displayed.
3. Configure one of the of the following settings on your network:
   - **Unrestricted access (default)**—This is the default setting for wired networks. This option allows users to access any destination available to the network.
   - **Restricted access**—This option restricts users to access only the internet and prevents them from accessing internal network resources. To allow the users to access specific network resources, enter the **Resource IP address** in the list of IP addresses and click + .

Network Security

The **Network Security** option in the Instant On mobile app, allows you to configure security protection against DHCP and ARP attacks.

DHCP Snooping

DHCP snooping provides network security by filtering DHCP messages from untrusted sources in the network. It differentiates between ports connected to untrusted end user devices and ports connected to trusted DHCP servers or other Instant On devices. To take effect, security protections must be enabled both at the network and at the port level. Uplink ports as well as ports interconnecting Instant On devices together are automatically configured to trust the devices connected.

ARP Attack Protection

ARP attack protection is a security feature that validates ARP packets in a network and discards ARP packets with invalid IP-to-MAC address bindings. The system automatically learns the IP to MAC bindings from the DHCP exchanges in the network and it protects the network from certain man-in-the-middle and impersonation attacks.

The option to enable DHCP Snooping and ARP Attack security protection only apply to Instant On switch ports and is displayed when the site has at least one Instant On switch in the device inventory. The following procedure enables Network Security on the Instant On network:

1. Tap **Networks** ( ) tile on the Instant On home page and select a wired network from the list. The network details page is displayed.

2. Under **More options**, tap **Network Security**. The **Network Security** screen is displayed.
3. Slide the toggle switch ( ) to enable the **Network security protections** setting. This setting is disabled by default.
4. Click **Enable** in the pop up window to confirm.
5. Ensure that the **Security protections** setting is also enabled in the **Port Details** page for the port on which the network is configured. For more information on **Security protections**, see Switch Details.
6. Tap **Done**, to save the configuration.

Shared Services

Aruba Instant On mobile app allows clients to discover devices and access shared services available on the same or different networks in your site. To use the Shared services feature, you must first enable the Shared services setting in the Instant On mobile app. For information on deploying shared services, see Deploying Multicast Shared Services.

NOTE

The Shared services enable ( ) or disable ( ) option appears in the Instant On mobile app, only when the site is configured with two or more networks/VLANs.

To configure shared services on an employee network or guest network, follow these steps:

1. Tap **Networks** ( ) tile on the Instant On home page and tap the advanced menu ( ) icon in the header.
2. Select **Shared services** from the menu and slide the toggle switch next to Shared services, to the right ( ) to enable the Shared services feature on the network.
3. Once you have enabled the Shared services setting, navigate back to the **Networks** page and select an employee, guest, or wired network from the list. The **Employee Details**/ **Guest Details** / **Networks Details** page is displayed.
4. Under **More options**, tap **Shared services** to view the following information:
   - **Services detected on this network**—Lists all the services available on the current network. The services detected on the same network are always available for the clients to access without restriction.
   - **Services detected on other networks**—Lists all the services available on other employee networks of your site. By default, the services connected to other networks are disabled. Slide the toggle switch to enabled( ), to allow clients to access the shared services available on other networks.

NOTE

For Shared services to be available on Guest networks, the Network assignment must be bridged (Same as local network) and the network access must be set to Unrestricted.

List of Supported Services

The list of supported services is displayed per device on the Instant On mobile app. A multiple services icon is displayed next to the device if it provides more than one service. New services discovered on a known shared device are automatically shared. However, for new devices, the new services discovered will not be shared until the user allows access to share. 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.
- AirPrint™—Apple® AirPrint allows you to print from an iPad, iPhone or iPod Touch directly to any AirPrint compatible printers.
- Sharing—Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple® devices.
- RemoteMgmt—Use this service for remote login, remote management, and FTP utilities on Apple® devices.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

Network Assignment

Network Assignment for Wired Networks

The **Network Assignment** page facilitates the assignment of wired networks to Instant On devices at the site. All the ports on an Instant On AP11D router or switch can now be configured at the same time and assigned to a particular VLAN network. The **Network Assignment** page provides a global view of the wired network and displays all the devices deployed at the site. Every port on the Instant On devices at the site can be assigned in bulk to a particular VLAN, expect for the following:

- The uplink port
- A port where an Instant On device is connected.
- A port that is configured as part of a trunk.
- A port that uses 802.1x

The following procedure configures the network assignment on Instant On devices:

1. Tap **Networks** ( ) tile on the Instant On home page and select a wired network from the list. The network details page is displayed.
2. Under **More options**, tap **Network assignment**. The **Network Assignment** screen is displayed with the list of all the wired Instant On devices at the site.
3. Select a wired device and tap on one of the following options, to assign the network VLAN in bulk to all the ports:
   - **Clear**—Removes the VLAN from all the ports.
   - **All tagged**—Assigns and tags the VLAN of a particular wired network to all the ports of the selected Instant On device.
   - **All untagged**—Assigns and untags the VLAN of a particular network to all the ports of the selected Instant On device.



Besides assigning the VLAN in bulk to all the ports, you can also modify the status of each port by tapping on it. The status of the port is changed to **C** (clear), **T** (tagged), or **U** (untagged) subsequently every time you tap on a particular port.

4. Tap the back arrow (←). The changes are saved automatically.

Network Assignment for Wireless Networks

Instant On provides the option to assign employee and guest wireless networks to the APs on site. By default, all APs are selected for a newly created wireless network. You can also choose not to assign any APs to a particular wireless network.

The following procedure describes how to assign Instant On APs to a wireless network:

1. Tap **Networks** () tile on the Instant On home page and select a wireless network from the list. The network details page is displayed.
2. Under **More options**, tap **Network assignment**. The **Network Assignment** screen is displayed with the list of all the Instant On APs at the site.
3. Slide the toggle switch to the right (), next to the listed APs to assign them to the wireless network.
4. Tap the back arrow (←) to return to the network details page.
5. Tap **Done**.

Alternatively, the wireless networks can also be assigned to an Instant On AP in the device details page. For more information, see Network Assignment for Instant On APs.

Chapter 10
Analyzing Application Usage

An application is a program or group of programs that allows end users to perform specific tasks or activities on devices such as computers and smartphones. Aruba Instant On provides daily usage data for the different types of applications and websites accessed by clients in the network.

The Aruba Instant On solution classifies the traffic into a large number of categories, to reduce the complexity of the feature in the Aruba Instant On solution. These large number of categories are grouped into one main category based on their classification.

Below are the different application categories and the respective web content classification:

Table 16: *Application Categories and their Classification*

Application Category	Icon	Instant On Classification
Wired—This category is essential for basic network and Internet connectivity. It is always allowed for all networks and cannot be blocked.		▪ Wired networks
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

Application Category	Icon	Instant On Classification
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
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

Application Category	Icon	Instant On Classification
		▪ 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
Kids and Family—Sites aimed for kids and families with learning, educational and interactive content.		▪ Educations ▪ Kids ▪ Learning
Malicious and 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 and recreation—Recreational applications include websites on personal activities and interests.		▪ Travel ▪ Home and Garden ▪ Entertainment and Arts ▪ Local Information ▪ Hunting and Fishing

Application Category	Icon	Instant On Classification
		■ Society ■ Sports ■ Music ■ Fashion and Beauty ■ Recreation and Hobbies ■ Motor Vehicles ■ Kids ■ Online Greeting cards ■ Religion

Viewing Application Information

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

Table 17: *Application Information*

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

Applications Visibility and Control

This page allows you to configure application visibility and control settings for the network. To configure application visibility and control settings on the network, follow these steps:

1. To navigate to the **Visibility and Control** page, 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.
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 only an overview of uploaded and downloaded data of all the networks for the last 24 hours in the Applications page. Choose this option for better network performance. Selecting this option hides the Applications tab in the mobile app.

Application visibility and control setting configured in this page affects how the application wise data usage information of the client is displayed in the following pages:

- **Applications** page.
- **Client Details** page.
- **Applications** tab in the **Networks** 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 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.

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

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.

Viewing and Blocking Application Access

The **Applications** page in the mobile app 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 allows you to set restrictions to access certain applications on basis of their 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. 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) ( ).



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.

Chapter 11
Managing Clients

Aruba Instant On provides details of the clients in your network. A client is a hardware, such as a computer, server, tablet, or phone, that is connected to your Wi-Fi or wired network. The **Clients** page on the Instant On mobile app or web application displays a list of connected clients and blocked clients in separate pages. To view the **Clients** page, click the **Clients** tile on the Instant On home page.

The **Connected clients** page displays the list of active clients in the site and the **Blocked clients** tab displays the list of clients blocked in the site. The **Connected clients** page and **Blocked clients** page can be accessed by clicking on the **Connected clients** and **Blocked clients** tab in the Clients page.

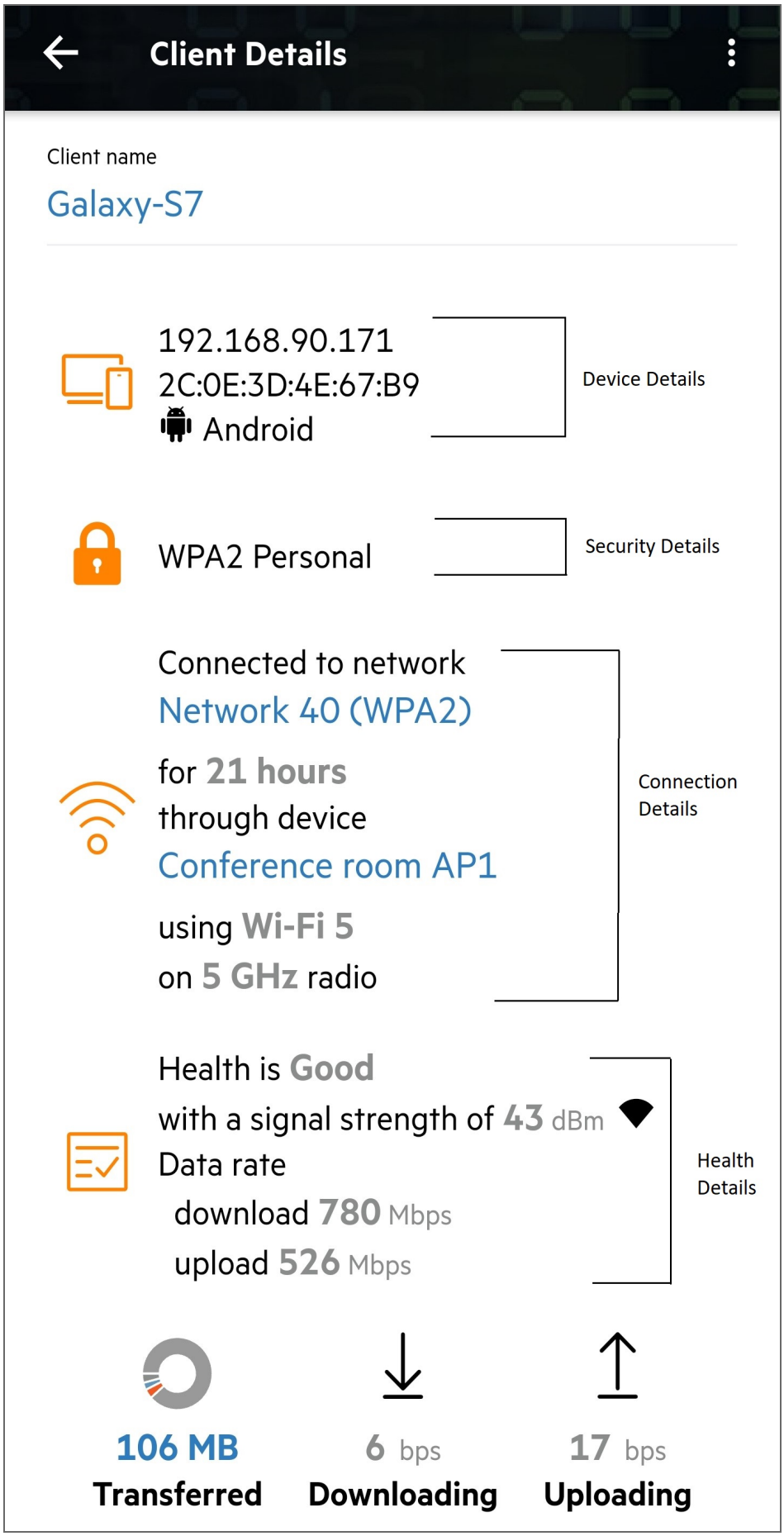
Viewing AP Clients

The **Client Details** page provides detailed information about clients in your network. The **Client Details** page is accessed from the list of **Connected clients**. Instant On clients are of two types — wired and wireless. Wireless clients include laptops, personal computers, tablet, mobile phones, etc. that connect to the Instant On network through wireless. Wired clients on the other hand are printers, server, switches, and infrastructure devices connected to the wired 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 on the client name from the **Connected clients** list. The **Client Details** page for the selected client is displayed.

The following is an example of the Client Details page:


Client Details
Client name
Galaxy-S7
192.168.90.171
2C:0E:3D:4E:67:B9
Android
Device Details
WPA2 Personal
Security Details
Connected to network
Network 40 (WPA2)
for 21 hours
through device
Conference room AP1
using Wi-Fi 5
on 5 GHz radio
Connection Details
Health is Good
with a signal strength of 43 dBm
Data rate
download 780 Mbps
upload 526 Mbps
Health Details
106 MB
Transferred
6 bps
Downloading
17 bps
Uploading

Viewing Details of Active Clients

The **Client Details** page lists the following information:

- Client Name
- Device Details
- Security Details
- Connection Details
- Connection Health
- Data Usage and Transfer Rates

Column Label	Description
Client Name	
Client name	Denotes the name of the wireless client. The client name can be edited and updated to a custom name of your choice. The length of the client name can be between 1 to 32 characters. Blank spaces and special characters are accepted as a valid characters in the client name.
Device Details	
IP Address	IP address of the client.
MAC Address	MAC address of the client.
OS	Operating system (OS) of the client device.
Security Details	
Security Details	This section displays the security standard used by the wireless client to connect to the network.
Connection Details	
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
Duration	Displays the duration for which the client is connected to the network.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Device Connected On	Displays the details of the Instant On 1960 Series switch in a stack to which the client is connected to. **NOTE:** This information is displayed only for clients connected to a stack.
Wi-Fi Standard	The Wi-Fi standard of the client connection. The Wi-Fi standard mapping is displayed as follows: ■ **Wi-Fi 6**— 802.11ax client ■ **Wi-Fi 5**— 802.11ac client ■ **Wi-Fi 4**— 802.11n client **NOTE:** The Wi-Fi standard will not be displayed for legacy Wi-Fi clients using 802.11b or

Column Label	Description
	802.11g standards.
Interface	The radio of the AP to which the client is connected.
Connection Health	
Status	The general health status of the client.
Signal / Speed	Indicates the client signal quality. Based on the client's Signal-to-Noise Ratio (SNR), the signal quality is denoted as follows: ■ **Good** — Signal Strength of 25 dB or higher. ■ **Fair** — Signal strength between 16 dB and 25 dB. ■ **Poor** — Signal strength of 15 dB or lower
Transfer Rates	The download and upload rates of the client in Mbps.
Data Usage and Transfer Rates	
Downloading	The download throughput of the device in the last 30 seconds, in bytes per second.
Uploading	The upload throughput of the device in the last 30 seconds, in bytes per second.
Transferred	Shows the total amount of data transferred during the session, in bytes. Clicking on the donut chart will take you to the Applications page of the client, where detailed application usage information of the client is displayed.

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.

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 on the donut chart preceding **Transferred** to open the **Applications** chart for the selected client.

Blocking and Unblocking Clients

The Instant On mobile app 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. 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. 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.
3. 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**.

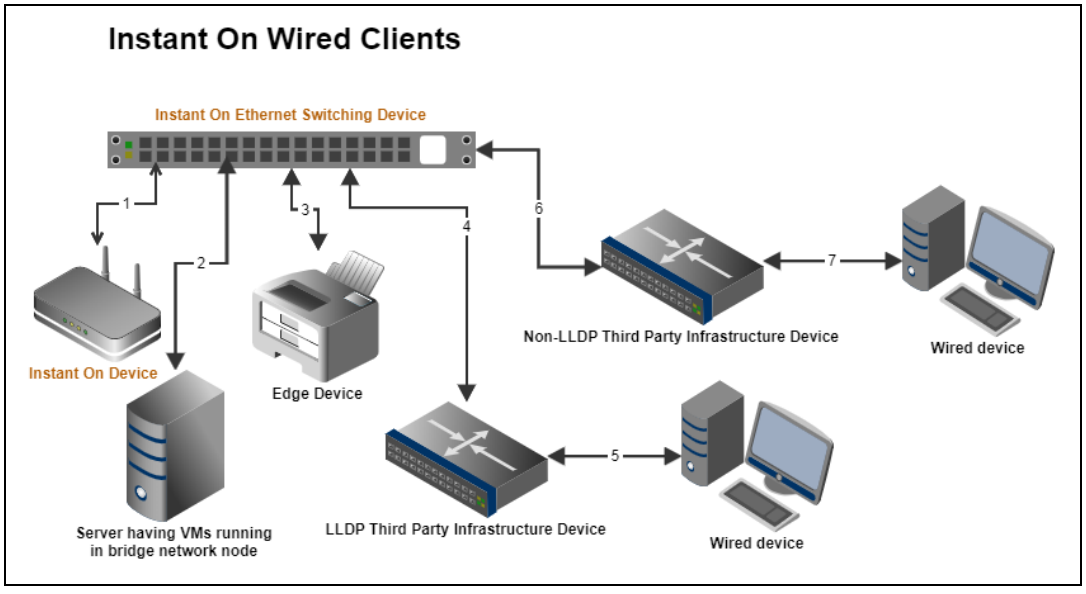
Follow these steps to unblock a blocked client:

1. Tap or click on the **Clients** ( ) tile in the Instant On homepage of the Instant On mobile app. 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.
3. 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.

Wired Clients

A wired client is defined as a client connected to an Instant On device that supports Ethernet switching. Wired clients are categorized based on the following scenarios:

Figure 6 *Wired Client Scenarios*



- **Scenario 1:** The Instant On device connected to the Instant On switching device will not be shown as a wired client.
- **Scenario 2:** The server will be shown as an edge wired client.

VMs running on the server might report additional MAC addresses to the same Ethernet port. In such cases, each of the MAC addresses will be displayed as a wired client.

- **Scenario 3:** The edge device will be shown as an edge wired client.
- **Scenario 4:** The third-party infrastructure device will be shown as an infrastructure wired client.
- **Scenario 5:** The wired device connected to the third-party infrastructure device will not be shown as a wired client.
- **Scenario 6:** The infrastructure device will be shown as an edge wired client.
- **Scenario 7:** The wired device will be shown as a wired client.

Wired Client Details

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

1. Tap the **Clients** () tile on the Instant On home page. The **Clients** page is displayed.
2. Select a wired client from the list of Connected clients. The **Clients Details** page for the wired client is displayed.

The Client Details page for the wired client displays the following information:

Table 18: *Wired Client Details Information*

Parameter	Description
Client name	Denotes the name of the wired client. The client name can be edited and updated to a custom name of your choice. The length of the client name can be between 1 to 32 characters. Blank spaces and special characters are accepted as a valid characters in the client name.
Type	Denotes the type of the wired client. The client can either be an infrastructure client or a voice client.
IP Address	IP address of the client.
MAC Address	Denotes the MAC address of the wired client.
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
Interface	Denotes the device interface to which the client is connected. The Wired client will display the port ID or the custom port name to which it is connected.
Duration	Displays the duration for which the client is connected to the network.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Port	Denotes the switch port through which the wired client is connected to the network.
Client Health	Denotes the health status of the wired client.
Status	Represents the ratio of the number or error packets on all the packets. ▪ **Good**—In full duplex mode, the error rate is less than 0.1%. In half duplex mode, the error rate is less than 2%.

Parameter	Description
	▪ **Fair**—In full duplex mode, the error rate is above 0.1%. In half duplex mode, the error rate is above 2%.
Duplex Mode	Denotes if the wired client is connected in a full duplex or half duplex mode.
Downloading	Shows the download throughput within the last 30 seconds, in bytes per second.
Uploading	Shows the upload throughput within the last 30 seconds, in bytes per second.
Transferred	Shows the total amount of data transferred during the client session, in bytes.

PoE Power Cycle

Instant On provides the ability to remotely power cycle wired clients. This option is available only for clients that are either connected to a PoE port on an Instant On router or a switch. The following procedure is used to power cycle the port of the wired client:

1. Tap the **Clients** ( ) tile on the Instant On home page. The **Clients** page is displayed.
2. Under the **Connected** clients list, swipe from right to left on a wired client. A power cycle ( ) button is displayed at the end of the row.
3. Tap the power cycle ( ) button to power cycle the client. The row displays a message that the client is being power cycled. As an alternate option, you can also tap on the wired client and select the **Power cycle** setting from the advanced menu (⋮) of the **Clients Details** screen for the wired client.

NOTE

The PoE supplier should be an Instant On device.

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

Changing Account Password

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

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.



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. Tap **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.

Security

The **Security** page allows administrators to add Two-Factor Authentication (TFA) on their own account. TFA provides an extra security layer for the account on which it is activated. This feature is disabled by default and is available only for verified administrator accounts.



An authenticator app is required to set up Two-factor Authentication. If you do not have an authenticator app installed on your device, download one for your corresponding operating system.

Activating Two-Factor Authentication

To set up Two-Factor Authentication for your administrator account, follow these steps:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Security**.
3. Tap **Set up two-factor authentication**.
4. Under **Validate Password**, enter your current Instant On account password.
5. Tap **Validate password**.
6. Under **Authenticator**, copy the key provided below and enter it in the authenticator app.

7. The authenticator app will validate the key and generate a one-time password, which should be entered in the **Authenticator** screen of the Instant On mobile app.
8. Tap **Validate one-time password**.
9. If the one-time password is successfully validated, a **Recovery code** screen is displayed.
10. Copy and save the 12-character recovery code in a private location as a backup, in case you have trouble logging in to your administrator account.



This recovery code is the only method you can use to login to your device, in case you have trouble logging in to your account. It is advised that you keep the recovery code saved and stored safely in a private location, from which you can retrieve the code easily.

11. Tap the **I have saved my recovery code checkbox** to confirm that you have privately stored the recovery code.
12. Tap **Complete setup** to activate Two-Factor Authentication on your account.



Once the two-factor authentication is activated on the administrator account, you will be required to enter the one-time password generated by the authenticator app, each time you login to the Instant On mobile app.

Deactivating Two-Factor Authentication

To deactivate Two-Factor Authentication for your administrator account, follow these steps:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Security**.
3. The **Security** screen displays that **Two-Factor Authentication** is currently enabled on your account.
4. Tap the advanced menu (⋮) icon in the header and tap **Disable two-factor authentication**.
5. Under **Validate password**, enter the current Instant On administrator account password.
6. Tap **Validate password**.
7. Under **Authenticator**, enter the one-time password generated by the authenticator app.
8. Tap **Validate one-time password**. The two-factor authentication is deactivated on the administrator account.

Notifications

Notifications are standard messages that are sent to the mobile managing an Aruba Instant On site, when an alert is triggered by the system. The notification mechanism updates administrators about any alert that is triggered on the site. The notification is displayed in 2 distinct lines, the first line displays the name of the alert and the second line displays the site name. However, when the system triggers multiple alerts from the same site, the notification mechanism collapses all the notifications generated from the alerts and displays it as a single notification on the registered device.

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. 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. All alerts triggered on the site can be viewed by clicking on **Show all alerts** in the **Site Health** tile.

Enabling or Disabling Alert Notifications

To enable notifications for alerts, follow these steps:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Notifications**.
3. Under **Alert Categories**, you have the option to enable either **Mobile** or **Email** notifications, or both. Slide the toggle switch(es) to enable ( ) or disable ( ) the alerts you want to be notified about as mobile or email notifications. The alerts you have enabled will be displayed in the **Site Health** tile in the home page. For more information on viewing and managing alerts, see:

- Viewing and Managing Alerts using the Mobile App



By default, the **Mobile** notifications are enabled for all four alert types.

Alert Categories

Alert categories offer a selection of device related events for which you may receive a notification alert. You can choose to either enable or disable notifications for a specific alert category. The alert category types available are:

- Connection Problem
- Device Problem
- Device Capacity Exceeded
- New Software Available

Connection Problem

Enabling this option will trigger notification alert when there are connectivity issues in the site. This alert indicates that clients are experiencing issues with internet connectivity. The following are possible scenarios when the alert is triggered:

- Internet gateway loses connectivity with your Internet Service Provider.
- Internal network issues.

Device Problem

Enabling this option will trigger notification alerts when an Instant On device malfunctions or is disconnected from the network. The following are possible scenarios when an alert will be triggered:

- Instant On Device loses power.
- Instant On Device is disconnected from the network.
- Local network or Internet connectivity issue.
- Instant On Device is restarting due to an unexpected condition.

Device Capacity Exceeded

Enabling this option will trigger a notification when the power budget of the Switch reaches the maximum limit and the Switch can no longer power new devices through PoE. This alert is triggered when the Switch denies a device's request for PoE supply. The total power budget of the switch and the power consumption information is displayed in the **Switch Details** page in the **Inventory** module.

New Software Available

Enabling this option will trigger a notification when a new software version is available to be installed on the Instant On network. An informational alert is generated on the Instant On mobile app and web application indicating a new software is available for installation. Tapping on the informational alert will redirect you to the software update screen. For more information on installing software updates, see Updating the Software Image on an Instant On Site.

Communication Preferences

The Communication Preferences screen allows you to subscribe to the latest offers and promotions provided by HPE or Aruba. Follow these steps to subscribe to these updates:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Communication Preferences**.
3. Under **Offers and promotions**, perform the following actions:
   a. Select the **May HPE/Aruba provide you with personalized email communications about HPE/Aruba and select HPE/Aruba-partner products, services, offers, and events?** checkbox.

      The details of the latest offers and promotions by HPE/Aruba will be sent to your registered email account.



This check box is also displayed in the **Create an account** page.

   b. Under **Validate your country**, tap the drop-down icon and select the country you reside in, from the list.

To view more information on how HPE/Aruba manages, uses, and protects user data, tap the **HPE Privacy Statement** link.

Delete Account

The **Delete Account** screen allows you to delete an Instant On administrator account and revoke access to any associated products and services. The administrator account will be deleted with all its associated data.If the deleted account was being used as the primary administrator account, all sites that belonged to the account will be deleted, and all devices will be factory reset.Sites with multiple administrator accounts will not be deleted if one of the accounts is deleted.The following procedure allows you to delete an Instant On administrator account:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Delete account**.
3. In the **Delete Account** screen, tap **Delete account**.
4. A pop-up is displayed on the screen. Tap **Delete**, to permanently delete the Instant On administrator account.

Chapter 13
Managing AP Firmware Upgrades

Firmware is the software programmed on Instant On APs and switches 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 Firmware for an Instant On AP or Switch

When an AP or switch is deployed into the network, it joins an Instant On site, which is a group of APs and switches that are configured and managed from a single location. Upon joining the site, the AP or switch 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 and switches 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 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. When a new software update is available, an information alert is displayed with sufficient information of when the update will occur. The **Software update** page displays the new version number and the **What's new:** information in the release. The page also includes the scheduled time for the update and the options—**Install now** or **Postpone by a week**.



The **Postpone by a week** option can only be used once to extend the duration of the software update by a week.

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

1. 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.

The real-time status of the upgrade is displayed in the **Software update** page, indicating the software update is in progress. The upgrade is displayed as a progress bar in three stages, **Downloading and installing software**, **Restarting devices**, and **Update is complete**.

The status of the upgrade is simultaneously displayed for each device in the **Inventory** page and in the following order:

- Downloading software
- Installing software
- Restarting device
- Synchronizing
- Active

When the software is up-to-date, the page will show the current Instant On software version and the date of the last update.

Verifying Client Connectivity During Upgrade

Instant On APs and switches 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.

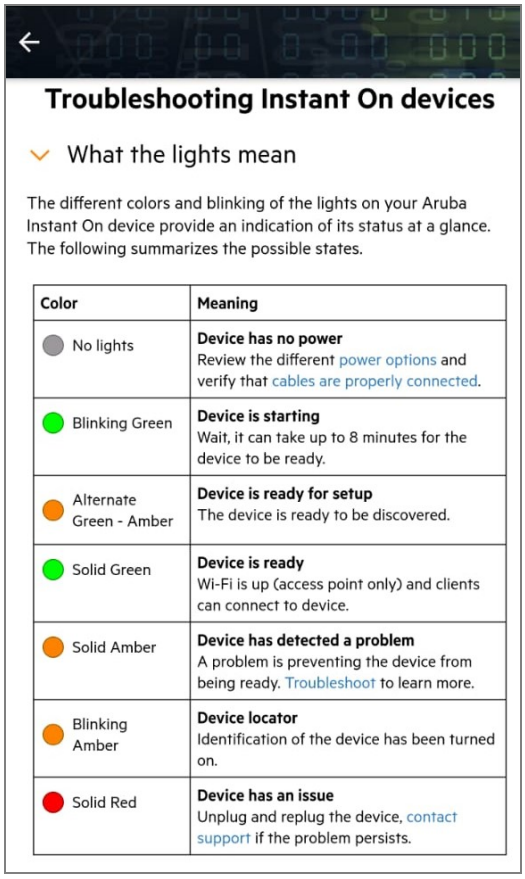
The mobile app can only be launched if it is updated to the latest version. To update the mobile app, click the app store icon that is available below the warning message.

Chapter 14
Troubleshooting

To help the administrator troubleshoot problematic situations, a troubleshooting assistant is embedded within the Aruba Instant On application. It helps the user identify an issue and provides guidance on how to resolve it. The troubleshooting assistant is designed to cover most typical situations and relies on LED patterns to identify problems. The troubleshooting assistant can be invoked from the **Alert Details** page.

To open troubleshooting assistant, follow these steps:

1. Select the **Site Health** module and click on **alert history** in the alerts section or click on ( ) button in the page header. The **Alerts** page is displayed.
2. Click on › icon beside the alert to view the **Alert Details** page.
3. In the **Alert Details** page, review the **Recommended actions** to clear the alert.
4. For additional troubleshooting information, click **Troubleshooting Instant On devices**. The **Troubleshooting Assistant** page is displayed with the following information:
   a. Most typical situations based on the LED patterns.
   b. Recommended actions.



5. If you are unable to find a solution to the problem, navigate to the following link to view additional support options.
   - Help & Support in the Mobile App