



Aruba Instant On 2.9.0

User Guide

Web Application Version



Copyright Information

© Copyright 2023 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	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	11
Wireless Deployment—Access Point Only	11
Wired Deployment—Switch Only	11
Wired and Wireless Deployment—Access Point and Switch	11
Provisioning your Aruba Instant On Devices	13
Setting Up Your Wireless Network	14
Setting Up Your Wired Network	15
Accessing Aruba Instant On Application	16
AP Configuration Modes	18
Local Management for Switches	19
IP Assignment for Access Points	21
Discovering Available Devices	23
Deploying Multicast Shared Services	24
Managing Sites Remotely	26
Application Error Messages	27
Aruba Instant On User Interface	28
Using the Instant On User Interface	30
Site Management	30
About Software	35
Monitoring Site Health	36
Alerts	37
Network Tests	37
Viewing and Updating Inventory	39
Adding a Device	39
Types of Devices	40
Extending your Network	40
Radio Management	43
Loop Protection	44

Power Schedule	45
DNS	46
Access Point Details	47
Router Details	53
Switch Details	60
Cloud-Managed Stacking	72
Topology	85
Auto-Detection and Auto-Configuring of Switch Ports	88
Configuring Networks	90
Employee Network	90
Guest Network	98
Wired Network	110
Analyzing Application Usage	117
Viewing Application Information	120
Viewing and Blocking Application Access	122
Managing Clients	123
Viewing Wireless Clients in the Site	123
Viewing Client Details	125
Wired Clients	127
Managing Your Account	131
Changing Account Password	131
Security	131
Notifications	132
Communication Preferences	134
Delete Account	134
Troubleshooting	136

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

This user guide describes the features supported by Aruba Instant On 2.9.0 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 2.9.0 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/ctp/contact-support
EULA	https://www.arubainstanton.com/eula/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

The Instant On Solution is a simple, fast, and secure solution designed for small business networks. It is an affordable to own and easy-to-use solution that is ideal for the businesses with simple technology requirements and setups that do not have IT staff. The product offers the very latest Wi-Fi 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 web application 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
- HPE Networking Instant On AP22D Access Points

Outdoor Instant On Access Points

- Aruba Instant On AP17 Access Points

Instant On Switches

- 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/SFP+ Switch
- Aruba Instant On 1960 8p 1G Class 4 4p SR1G/2.5G Class 6 PoE 2p 10GBASE-T 2p SFP+ 480W 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

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](#)

This section lists the new features, enhancements, and hardware platforms introduced in Aruba Instant On 2.9.0.

New Features and Hardware Platforms

Table 3: *New Features Introduced in Instant On 2.9.0*

Feature	Description
Additional Information on SFP Transceivers	The SFP transceiver information displayed for switch ports now includes the following categories: Supported transceivers Unsupported transceivers Incompatible or faulty
Allowed Clients and Devices List for Switch Ports	This new feature allows users to select clients from the Connected clients list and add them to the Allowed clients list. Once added to a list, only clients in the Allowed clients list will be able to access a network when connected to a specific port.
Configuring Multicast Optimizations for Wired Networks	The Multicast Optimizations setting is no longer enabled by default for wired networks and can now be configured to reduce traffic to registered multicast groups in the network.
Dynamic Channel Display	Starting with Instant On 2.9.0, the list of available Wi-Fi channels is displayed according to the site's country DRT regulations and also depending on AP types included in the Instant On site.
Email Localizations	Language specific email notifications for site related events will now be sent based on the language preference set by the administrator when creating a new Instant On account. The supported languages are: <ul style="list-style-type: none">▪ English▪ German▪ French▪ Spanish▪ Korean▪ Japanese▪ Portuguese▪ Italian▪ Simplified Chinese▪ Traditional Chinese
Enhancements to the PoE Power Schedule	A new option called Select ports that will follow this schedule is introduced in the PoE power schedule configuration. This allows users to configure the power schedule on multiple ports of each Instant On AP or switch which has downlink PoE support.

Table 3: *New Features Introduced in Instant On 2.9.0*

Feature	Description
Enhancements to Port Details and Graphics	Additional information regarding switch ports in the form of new texts and icons, as well as changing the color of the ports shown to represent the port health is introduced. The PoE specification details are also displayed when the port is powered by PoE.
Extended Deadline for Software Updates	The software updates can now be postponed to a maximum of 30 days from the time the alert is generated.
Optional BLE Search to Add New Devices	Starting from this release the Search for devices process using the mobile app has been modified to now have BLE as an option instead of by default.
Support for New Aruba Instant On Access Points	The following new indoor Aruba Instant On access points are introduced in this release: <ul style="list-style-type: none">■ AP22D
20 MHz Bandwidth Support on 5 GHz Radio - Local AP Radio Settings 20 MHz Bandwidth Support on 5 GHz Radio - Global Radio Settings	Starting from this release, it is now possible to configure 20 MHz channel bandwidth and select specific 20 MHz channels for the 5 GHz radio. This option can be configured in the global radio management settings or from the local AP radio settings.

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

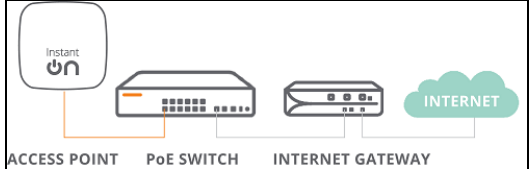
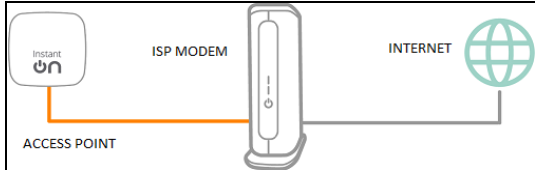
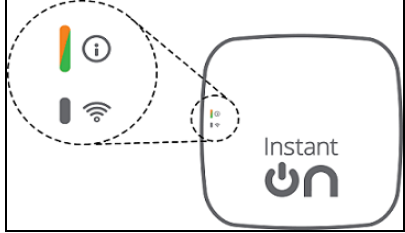


This chapter describes the following procedures:

- [Setting Up Your Wireless Network](#)
- [Setting Up Your Wired Network](#)
- [AP Configuration Modes](#)
- [Discovering Available Devices](#)
- [Accessing Aruba Instant On Application](#)
- [Managing Sites Remotely](#)

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.

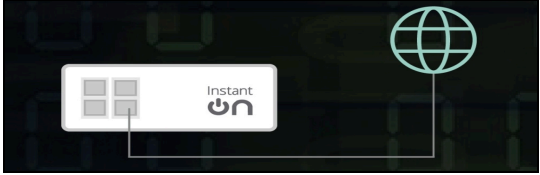
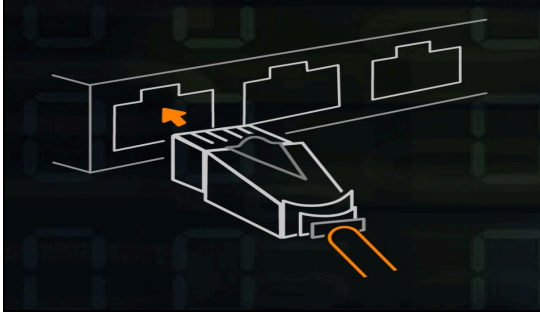
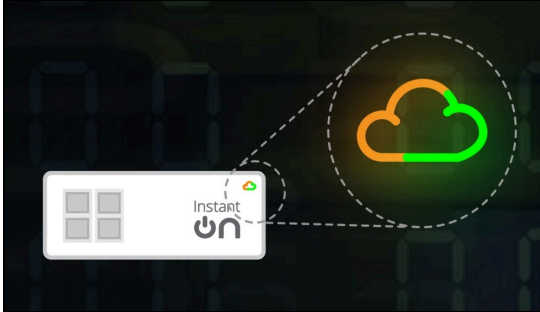


Table 4: *Instant On Wireless Network Provisioning*

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.
Slowly Blinking Green	Indicates that the device is booting or upgrading. It can take up to 8 minutes for the device to be ready.
Rapidly Blinking Green	Indicates that the Instant On device has been powered on.
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	<p>Indicates that the Instant On device is connecting. The connection to the Instant On portal is taking longer than expected. This should be temporary and the device will connect as soon as possible.</p> <p>NOTE: This applies only to Instant On access points and not the switches.</p>
Solid Red	<p>Indicates that the device has an issue. Unplug and replug the device to restore connectivity. Contact support if the issue persists.</p> <p>NOTE: This applies only to Instant On access points and not the switches.</p>

Accessing Aruba Instant On Application

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

Browser Requirements

The following web browsers support the Instant On web application:

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

Create an Instant On Account

Follow these steps to create an Instant On account:

1. Open a browser.
2. Type **https://portal.arubainstanton.com** in the address bar and press the **Enter** key.
3. Click **Sign up** to create a new Instant On account.
4. Enter an email ID in the **Email** field. The email ID should not be associated with another Instant On account.
5. Enter a password in the **Password** field.
6. Select the **End User License Agreement and Data Privacy Policy and Security Agreement** checkbox.
7. Click **Create account**.
8. A verification email is sent to your email account. Follow the instructions in the email to activate your Instant On account.



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

9. Once the above steps are complete, click **Continue** on the web application. You have now successfully registered an Instant On account.

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

Logging in to Instant On

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

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



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

4. Follow the onscreen instructions to complete the access point setup, if the web interface is launched for the first time.

Resetting Your Account Password

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

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

6. Click **Reset password**. An acknowledgment message that your password has been changed successfully is displayed on the screen.



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

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>

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. test

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

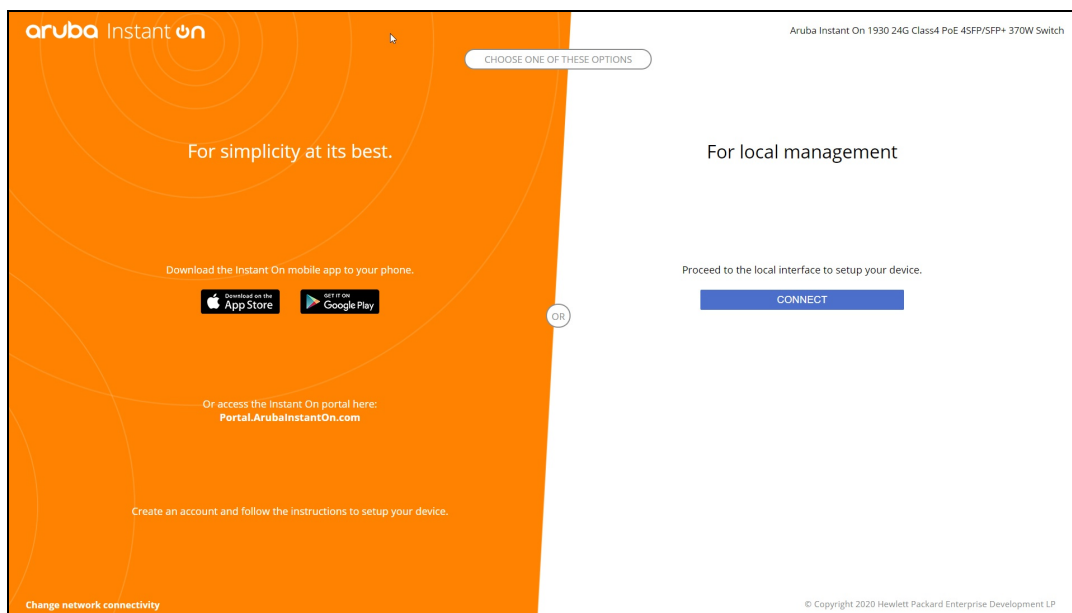
Follow these steps to add your Instant On devices to the network in router mode:

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.



The switch cannot be onboarded or managed from the Instant On web interface 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 web application), 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

The screenshot displays the Aruba Instant On AP110 WebUI configuration page. The page is divided into several sections: 'Device information', 'Portal connectivity', 'IP addressing', and 'Uplink VLAN'. The 'IP addressing' section is currently active, showing three radio button options: 'Automatic (default)' (selected), 'Static', and 'PPPoE'. Below these options, fields for 'IP address' (192.168.0.155), 'Subnet mask' (N/A), 'Default gateway address' (192.168.0.1), 'Primary DNS server address' (192.168.0.1), and 'Secondary DNS server address' are visible. The 'Uplink VLAN' section shows two radio button options: 'Untagged' (selected) and 'Tagged'. Below these, the 'Uplink VLAN' field is set to '1' with a range of '(1-4092)' in parentheses. The 'Device information' section on the left shows the model as 'Aruba Instant On AP110' and the software version as '2.4.0.0'. The 'Portal connectivity' section shows the 'Instant On portal status' and 'Device onboarding status'. At the bottom of the page, there is a warning message: 'Changing these settings may disconnect your browser from the device.' and two buttons: 'CANCEL' and 'APPLY'.

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 AP111D 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 Web Application](#)



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

Discovering Available Devices

There are multiple ways to add an Instant On AP 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 initial 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 application using your administrator account credentials, the **My Sites** page is displayed if multiple Aruba Instant On sites are registered to your account. To view or manage the settings of a particular site, click on any of the registered sites listed on this page.

Account Management

To navigate to the **Account Management** page, click the icon next to your account name in the page header and select **Account management** from the drop-down menu. The alphabet in the icon will change based on the first letter of your registered email account. For more information, refer to [Managing Your Account](#).

Setup a New Site


To register a new Instant On site to your account:

1. Click on the site name and select  **Setup a new site** from the drop-down list. You will be redirected to the initial setup page.
2. Follow the instructions given in [Setting Up Your Wireless Network](#) to add a new Instant On site.

Sign Out

Click on **Sign out** to sign out from your Aruba Instant On account.

Help

Click the  button in the page header to view help options. The following options to access technical support are available:

- **Help**—Opens the Aruba Instant On documentation portal. For more information, see <https://www.arubainstanton.com/techdocs/en/content/home.htm>.
- **Support**—The following options are available to reach Aruba Instant On support:
 - **Contact support** - 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://www.arubainstanton.com/contact-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.
- **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/>.
- **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 web application, and also the following information:
 - [End User License Agreement](#)
 - [Data Privacy Policy and Security Agreement](#)

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 can 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 other 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)**. 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**. For more information, see [Network 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 must be set to **Same as local network (default)**. 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 2.9.0 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*

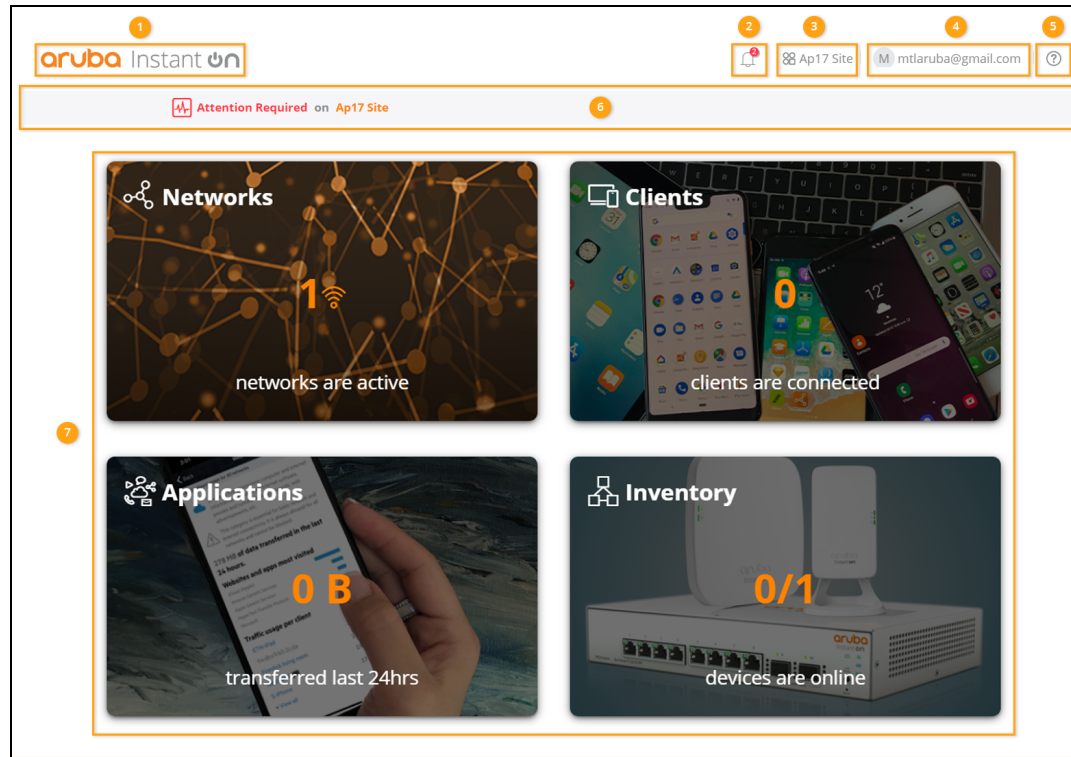
Error Type	Error Message	Message Lifespan
Operation Failed	Operation failed to be executed. The data will be reloaded.	Message is displayed on the screen for a short duration and then removed.
Connectivity Lost	Your internet connection appears to be offline.	Message is displayed on the screen until connectivity 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.

Chapter 6

Aruba Instant On User Interface

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

Figure 1 Web Application User Interface Overview



The Instant On user interface comprises of the following components:

Table 8: Aruba Instant On User Interface Components

Legend	Header Content	Description
1	Aruba Instant On logo	Displays the Aruba Instant On logo and functions as a button to return to the Instant On home page.
2	Alerts (🔔)	Displays the alerts that are triggered by the system when an unusual activity is observed on the network. See Alerts for more information.
3	Site options (📍📍📍)	Displays the site name and provides the following options to manage sites under your administration: <ul style="list-style-type: none"> ▪ Site management—Allows you to modify various account settings, including time zone and notifications for the selected site. For more

Table 8: Aruba Instant On User Interface Components







Legend	Header Content	Description
		<p>information, see Site Management.</p> <ul style="list-style-type: none"> ▪ Add new devices—Opens the Extend 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 site. After clicking Connect to another site, you are logged out of your current site and 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 multiple 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.
4	Account options ()	<p>Displays the registered email ID and provides options to administer account information and setup notifications. The first letter of your e-mail id will be displayed in the circle. Account options allows you to perform the following actions:</p> <ul style="list-style-type: none"> ▪ Account management—Allows you to modify your account information for all associated sites. For more information, see Managing Your Account. ▪ Sign out—Allows you to log out of your Aruba Instant On account.
5	Help ()	<p>Provides the following options to reach Aruba Instant On support and additional details of the product:</p> <ul style="list-style-type: none"> ▪ Help—Opens the Aruba Instant On documentation portal. For more information, see https://www.arubainstanton.com/techdocs/en/content/home.htm. ▪ Support—Listed below are the options available: <ul style="list-style-type: none"> ◦ Contact support - 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://www.arubainstanton.com/contact-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. ▪ 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/. ▪ 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 web application, and also the following information: <ul style="list-style-type: none"> ◦ End User License Agreement ◦ Data Privacy Policy and Security Agreement

Table 8: Aruba Instant On User Interface Components

Legend	Header Content	Description
6	Site health monitor	Provides the health status of devices connected to the network. Clicking on the site health monitor will take you to the Site Health page. See Monitoring Site Health for more information on the Site Health module.
7	Modules	<p>Modules allow you to configure and monitor network components such as application usage and system alerts. Clicking on a module tile allows you to configure settings relevant to the module. The Instant On user interface consists of the following modules:</p> <ul style="list-style-type: none">▪  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.

Using the Instant On User Interface

Network operations of the Instant On network is managed through the site health monitor and modules present in the homepage.

Opening a Module

To open a module click on the module tile in the home page. The settings relevant to the particular module will be displayed. When a particular module is open, the module tiles are arranged at the bottom of the home page. You can switch between modules by clicking on the tiles below.

Closing a Module

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

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

Site Management

Click on the site name and select **Site management** from the drop-down menu. The **Site Management** page displays the following user settings that can be modified in the Aruba Instant On application:

- Administration
- Time zone
- Guest portal
- Software update

Administration

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

Time Zone

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

Guest Portal

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

Software Update

You can now manage your software updates by creating schedules using the Instant On web application. For more information, see [Updating the Software Image on an Instant On Site](#).

Administration Settings

The **Administration** page allows you to modify administrator information, including your Aruba Instant On site name and account credentials. You can also add 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. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. Enter a new name for the Aruba Instant On site under **Site name**.



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 secondary administrator accounts to your site, follow these steps:

1. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. To add a secondary administrator account, click (+) next to **Account managing this site**.
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. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. Under **Accounts managing this site**, click **Lock account**.
3. Click **Lock** in the window that appears on the screen. The account is locked for ownership modifications.
4. To unlock the account, repeat steps 1 and 2, and click **Unlock**.



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. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. Under **Accounts managing this site**, click **Revoke ownership**.
3. Click **Revoke ownership** again in the window that appears on the 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. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. Under **Accounts managing this site**, click **Transfer ownership**. The **Transfer Ownership** page is displayed.
3. Enter the new email ID under **Email**.
4. Click **Transfer ownership** to transfer ownership of the site to the new administrator account.

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

Deleting a Site

To delete an Instant On site, follow these steps:

1. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed.
2. Under **Site Operations**, click **Delete this site**.
3. Click **Delete this site** again in the subsequent window that appears on the screen.



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. Click on the site name and select **Site management** from the drop-down menu. The **Administration** page is displayed by default.
2. Click **Time zone** to open the **Time Zone** page.
3. 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**.

Managing AP Firmware Upgrades

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

Upgrading the 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 using the Instant On web application. 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 **Schedule update**. Clicking on the **Schedule update** link opens a calendar from which the administrator can pick a specific date on which the update is preferred. The software update can be extended up to a maximum of 30 days from when the alert is generated. If a date is not set in the calendar, the software update will take place based on the **preferred day of the week** setting.

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

1. Click the settings menu () icon on the Aruba Instant On header and select **Site management** from the drop-down menu. The **Site management** page is displayed.
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 status of the upgrade is displayed in the **Software update** page by means of a progress bar. The progress bar will be green if the firmware update was successful or yellow if some device(s) failed to install the firmware.

At the end of the software update, a list is displayed that lets the user know how many devices successfully installed the firmware successfully and how many did not complete the installation.

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 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, an alert is generated to advise the user about a possible issue on the network. The Instant On APs or switches will continue to operate on the existing software version and the new software upgrade will be retried again during the next maintenance window.

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.

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, click the help (🔍) icon from the page header and select **About** from the drop-down menu:

- [End User License Agreement](#)
- [Data Privacy Policy and Security Agreement](#)




Click **OK** to exit from the **About** page.

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 9: *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 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 [Enabling or Disabling Alert Notifications](#).

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

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

Viewing Alert History

To view the Alert history, follow these steps:

1. Click the **Site Health** banner () on the Instant On home page.
2. On the Site Health main page, you will see the details of the latest alert. Click **Show all alerts**. 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. Click the arrow () next to the alert. The details of the alert is displayed.



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.




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. Click the **Site Health** banner () on the Instant On home page.
2. Under **Network tests**, click **Run a connectivity test**. The **Connectivity test** 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. Click **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 9

Viewing and Updating Inventory

The Inventory displays a list of devices in the network along with the devices' current operational status. To view the **Inventory** page, follow these steps:

1. Click the **Inventory** (🏠) tile on the Instant On web application 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. Click 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 10: *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 web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click + **Add devices**.
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, click 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](#)



You can add a maximum of up to 50 Instant On devices per site.

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 in private network mode. To extend your network using a cable, follow these steps in the web application:

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click **+ Add devices**.
3. 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.

4. 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).
5. Wait for the LED lights on the additional Instant On AP(s) to blink alternatively between green and amber.
6. 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.

7. 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.

8. 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 web application:

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](#).
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.



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.

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: <ul style="list-style-type: none">▪ 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.

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.



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

Deployment Scenarios for Outdoor Access Points

The versions prior to 1.4.0 of the Instant On product line includes both indoor and outdoor APs. However, the user interface did not allow specifying whether an AP is configured for servicing indoor or outdoor environments. In the case of an outdoor AP such as AP17 being setup as a mesh point, it may experience service disruptions when all the surrounding APs are indoor units. This is because 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. All APs discovered in the search regardless of their type or connectivity status will be displayed and can be added to the inventory. If there are no outdoor APs discovered in this process, the site will revert to the default channel plan.

If the user chooses not to include Outdoor APs as part of the discovery operation:

- The **Search for my device** operation will keep the default channel plan and search for both wired and wireless APs in the area. The over-the-air outdoor APs will be ignored in the search results. However, wired outdoor APs can still be found and added to the inventory, but they will operate separately on the outdoor channel plan.

Scenario 3: Existing sites with Mesh outdoor Access Points

If a mesh outdoor AP cannot find a mesh portal on an outdoor channel, then it will be displayed as offline by the user interface.

If a mesh outdoor AP is on a compatible channel, then the user interface displays it as up and running.

Scenario 4: Deleting Last Outdoor Mesh Point

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

Radio Management

The **Radio Management** page allows you to configure the radio channel on which the AP needs to operate. This reduces interference and helps to optimize the AP radio performance 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 might disconnect clients from the network.

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

1. Click the **Inventory** tile on the Aruba Instant On Portal home page or click the **Site Health** banner and then click on **Show inventory**.
2. Click the advanced settings (⚙️) icon and select **Radio management**.
3. Choose a **Channel width** for each of the following:
 - a. 2.4 GHz Radio—**20 MHz (default)** or **20/40 MHz**.
 - b. 5 GHz Radio—**20 MHz, 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. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.
 - 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.
-

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 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 above values are governed by the DRT regulations for each country. If a country does not support transmit power level above 23 dBm under 5 GHz, the user will be limited by this value coming from the DRT regulatory when using the max TX Power setting.

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 web application. 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 web application. 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. 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 advanced settings (⚙️) icon 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.



RSTP is enabled by default when a stack is present in the inventory and does not have the toggle switch to disable the setting. However, if the stack is removed from the inventory, RSTP will still be enabled, but the toggle switch becomes available to enable or disable the setting.

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. 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 advanced settings (⚙️) icon and select **Loop protection**.
3. Slide the **Rapid spanning tree (RSTP)** toggle switch to enabled (🟡). The details of the **Base priority** and **Root bridge** are displayed.
4. Under **Bridge priority assignments**, click the drop-down arrow and select a priority from the **Base Priority** list.
5. If you choose to recalculate the bridge priority, click the advanced settings (⚙️) icon next to **Bridge priority assignments** and then click **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 access points to supply power to devices connected to them. This setting is global and applies to all switches and PoE capable access points. Starting with Instant On 2.8.0, the power schedule configuration is applied to every PoE port with or without connected site devices.

The Power Schedule feature does not take effect on:

- Uplink port
- Link aggregation ports

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

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 advanced settings (⚙️) icon and select **Power Schedule**.
3. Under **Ruled by a schedule**, click one of the following options:
 - a. **Fixed**—Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) during which the switch enables the power supply for the PoE ports.
 - Select the days on which the switch should supply power to the PoE ports.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The switch provides power to the PoE ports throughout the day.
 - **Active between**: The switch provides power to the PoE ports for the specified time period. Configure the **Start Time** and **End Time** for PoE supply as required.
 - b. **Variable**—Indicates the schedule configuration that allows users to set up a different time range on a daily basis.
 - Follow these steps to enable the power schedule for specific days of the week:
 - After selecting **Variable**, click on the day of the week for which you need to configure a schedule.
 - Select the **Active** checkbox.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The switch provides power to the PoE ports throughout the day.
 - **Active between**: The switch provides power to the PoE ports for the specified time period. Configure the **Start Time** and **End Time** for PoE supply as required.



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

You can also configure the PoE power schedule on multiple ports for devices in the inventory.

- a. Under **Select ports that will follow this schedule**, click on an Instant On router or switch from the list of devices displayed.
- b. Click on the ports for which the power schedule should be enabled. Alternatively, you can also click on **All follow**, to enable the power schedule for all the available PoE ports on that device.


Click **X** to exit. The configuration is automatically saved.

Although the Power Schedule option is globally applicable, the usage of the schedule can be turned off for individual ports. The option to turn off power schedule for individual ports is available in the **Port** section of the **Switch Details** page. For more information, see [Power Management](#).

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. 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 advanced settings () icon and select **DNS**.
3. Select either of the three options:
 - **Automatic(default)** — Configure Cloudflare DNS (1.1.1.1) as the DNS server. This option is selected by default.
 - **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, follow these steps:
 - 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 following options are available in the expanded view of an access point in the inventory:

- [Identification](#)
- [Connectivity](#)
- [Ports](#)
- [Network Assignment](#)
- [Radios](#)
- [Actions](#)

Identification

The **Identification** 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. To view the details of the AP, follow these steps:

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 an AP in the **Inventory** list. The AP details such as the AP name, IP address of the AP, MAC address, Serial number, SKU, AP type, radio, and the number of the clients connected on each radio channel are displayed.

Access Point Lights

The **Access Point Lights** section allows you to turn on or off the device status and radio lights. The lights are turned on by default to provide a clear visual indicator of the device's status at a glance. This setting is available only for Instant On access points.

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

1. Click the **Inventory** tile on the Aruba Instant On Portal home page or click the **Site Health** banner and then click on **Show inventory**.

2. Click the (>) arrow next to an AP in the **Inventory** list.
3. Under **Access Point Lights**, select one of the following options:
 - a. **Normal mode (default)**— Use this option to turn on the status and radio lights. This option is selected by default.
 - b. **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.
4. Click **Save**.



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.

Connectivity

You can either configure Instant On devices to automatically receive an IP address from an DHCP server running on the LAN or manually configure a Static IP address. To configure IP assignment for the access point, follow these steps:

1. Click the **Inventory**() tile on the Aruba Instant On home page or click the **Site Health**() banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP in the **Inventory** list and then click **Connectivity** tab.
3. Select any one of the following options to assign an IP address for the AP:
 - **Automatic(default)** — The IP address for the AP is assigned by the DHCP server.
 - **Static** — Assign a static IP address for the AP and configure the following parameters:
 - a. **LAN IP** —Enter a Static IP address.
 - b. **Subnet mask**—Enter the subnet mask.
 - c. **Default gateway**—Enter the IP address of the Default Gateway.
 - d. **DNS server**—Enter the IP address of the DNS server.
4. Click **Save**.

Ports

Every network requires the E0/PT or ENET port of the AP to be connected to the gateway or switch using an Ethernet cable. The Port Details page displays the ENET port, the uplink status, and the upload and download throughput rates. The name of the Ethernet port can be changed by entering a new name in the **Port ENET** text field.



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

Connected Clients and Devices

On selecting the ENET port, the **Clients and devices connected to this port** section 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. To filter the clients and devices connected to a specific network, select a network from the **Show** drop-down list.

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. Click the **Inventory** (🏠) tile on the Aruba Instant On home page or click the **Site Health** (📶) banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP in the **Inventory** list and then click **Network Assignment** tab.
3. Under **Allow access to the following networks**, click the checkbox next to a network name to assign the AP to that network.



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

Radios

The **Radios** tab provides an option to override the radio settings configured at the site level and allows you to configure radio settings which are specific to the selected Instant On device.

Follow these steps to override the site level radio settings and configure 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**, click the **Use specific configurations for this radio** checkbox for **2.4 GHz Radio**, **5 GHz Radio** respectively to view the device specific radio settings.
2. Under **Radio Details**, select the **Use specific channels and power configuration** checkbox for each of the radios, to modify their channel and power values.
3. Choose a **Channel width** for each of the following:
 - a. 2.4 GHz Radio—**20 MHz (default)** or **20/40 MHz**.
 - b. 5 GHz Radio—**20 MHz**, **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. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.
-

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 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 above values are governed by the DRT regulations for each country. If a country does not support transmit power level above 23 dBm under 5 GHz, the user will be limited by this value coming from the DRT regulatory when using the max TX Power setting.

The changes made in the above procedure are saved automatically.

Dynamic Channel Display

Starting with Instant On 2.9.0, the list of available Wi-Fi channels is displayed according to the site's country DRT regulations and also depending on AP types included in the Instant On site. Some key functions of dynamic channel display feature are described as follows:

- The DRT regulations are per AP type and per country.
- The global radio management section includes a union of all available channels regarding the AP types included in the site.
- Available channels and bandwidths might differ depending on whether the site mode is indoor (default) or outdoor (extend network with outdoor devices like AP17).
- The channels and bandwidths displayed under the global radio management section are updated accordingly if a device is added or removed from the site.
- When a new DRT file is available in future Instant On versions, the changes will reflect automatically in the radio sections if needed.

Actions

The **Actions** tab provides the following configuration options.

Locate

Instant On allows you to locate your device when there are many devices in the site.

To locate your device, follow these steps:

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP in the **Inventory** list and then click on **Actions** tab.
3. Slide the **Activate lights** toggle switch to right (🔴) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

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 access point, follow these steps:

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP in the **Inventory** list and then click on **Actions** tab.
3. Click the **Connectivity tests** tab beside **Network tests**. The **Connectivity test** screen is displayed.
4. 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.

5. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
6. Click **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

Restart



Aruba allows you to restart the device if you suspect any problem with it.

To restart your device, follow these steps:

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 an AP in the **Inventory** list and then click **Actions** tab.
3. Click **Restart**.

Remove from Inventory

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

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. Select the AP you want to remove from the inventory by clicking the (>) arrow next to the device name.
3. In the **Actions** tab, click **Remove** next to **Remove from inventory**.
4. Click **Remove** in the popup window that appears on the screen.

Follow these steps to remove an AP which is offline:

1. Navigate to **Inventory**. Select the AP you want to remove from the inventory by clicking the (>) arrow next to the AP name. In the **Actions** tab, 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.
2. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity. The **Advanced** menu does not appear on the title bar when the status is down.
3. If the Instant On device is removed from the network, you can choose to remove the device from the inventory by clicking **Remove from inventory** in the **Actions** tab. A pop-up box appears on the screen requesting your confirmation.
4. Click **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 device 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. Click the **Inventory** tile  on the Aruba Instant On home page or click the **Site Health**  banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the arrow (>) next to the failed AP you want to replace from the **Inventory** list. A rectangular bar appears below the device name when an alert is triggered.
3. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the AP.

4. On the **Alert Details** page, click on the **replace** link. The **Replace Access Point** page is displayed. Alternatively, you can perform this action by clicking the **Replace** button next to **Replace device** in the **Actions** tab.
5. Unplug the AP you want to replace and plug in your new AP to the network. When your device's lights are alternating between green and amber, click **Continue**.
6. Enter the serial number located on your new Instant On AP and click **Search**.
7. Once your AP is detected, select **Replace**.
8. Click **Finish** when your new AP is added to your network.

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 or AP22D devices to operate as a primary Wi-Fi router in the network.

To view the Router Details page, follow these steps:

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 the router in the **Inventory** list.

Identification

The Identification section displays details such as the Router name, IP address, MAC address, Serial number, SKU, Router type, radio, and the number of the clients connected on each radio channel.

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.

Connectivity

The Instant On AP11D or AP22D 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. To configure LAN IP assignment for the AP11D or AP22D router, use the following procedure:

1. **Base IP address** — Configure the LAN IP address for the router interface.
2. **Subnet mask** — Configure the subnet mask for the network.
3. Click **Save**.

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.



On a Wireless-Only site, any Instant On AP can be used as the primary Wi-Fi router.

To reserve DHCP IP addresses from the router details page, follow these steps:

1. In the **Devices** page, click the **Connectivity** tab.
2. Under **IP address reservations**, click **+ Reserve an IP address**. The list of clients connected to the site are displayed along with their IP addresses.
3. Click 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** list.



If you choose to modify the reserved IP address of the client or device, click the edit icon next to the device or client name and enter the new IP address.

4. Click **Save**.

To reserve DHCP IP addresses from the client details page, follow these steps:

1. Click on the **Clients** (📁) tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Connected clients** tab to view the list of connected clients.
3. Click the (>) icon next to the client name of a wireless client connected to the primary Wi-Fi router. The client's details are displayed.
4. Click the **IP reservation** link positioned beside the IP address of the client. You are re-directed to the network details page of the wired network.
5. Under **IP address reservations**, click **+ Reserve an IP address**. The list of clients connected to the site are displayed along with their IP addresses.
6. Click 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** list.
7. Click **Save**.

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 networks.

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

1. In the **Networks** page, click the (>) icon next to the name of a wired network connected to the primary Wi-Fi router. The network details are displayed.
2. Click **Options**.
3. Under **IP address reservations**, click **+ Reserve an IP address**. The list of clients connected to the site are displayed along with their IP addresses.
4. Click 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** list.
5. Click **Save**.

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 or AP22D 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. 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. To view the details of the ports and the uplink status, follow these steps:

1. Click the (>) arrow next to an AP11D or AP22D router in the **Inventory** list.
2. Under the **Ports** tab, select 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.

Instant On currently supports an AP11D or AP22D device to operate as a router in the network. The **Ports** section for unconnected ports consists of the following settings:

- **Active** — Select the checkbox to enable the port. To disable the port, unselect the checkbox.
- Name of the port in read and write mode.

Authentication and Security

- **Port access control (802.1X)** —Select the checkbox to enable port-based network access control designed to enhance 802.11 WLAN security. 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.
- **Send RADIUS Accounting** — Select the checkbox to send RADIUS accounting messages.
 - **Secondary RADIUS Server** — Select the checkbox to configure a secondary RADIUS server and configure the following parameters:
 - **Server IP address or domain name**—Enter the IP address or the fully qualified domain name of the secondary RADIUS server.
 - **Shared secret**—Enter a shared key for communicating with the external RADIUS server.
 - **Authentication port**—Enter the authentication port number of the external RADIUS server within the range of 1–65535. The default port number is 1812.

Included networks

Select one of the following options:


- **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, click 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**—To custom map the port to a tagged VLAN, select 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.

Clients and devices connected to this port

On selecting a specific port of an AP11D or AP22D router, the **Clients and devices connected to this port** section 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. To filter the clients and devices connected to a specific network, select a network from the **Show** drop-down list.

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 or AP22D 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. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP11D or AP22D router in the **Inventory** list and then click on **Networks** tab
3. From the **Selected network** drop-down list, choose the network you want to map a specific port.

- Click the port to which you want to assign the selected network.
- Click the **Ports** tab to view the configuration details of the port mapped to the selected network.
- Click **Save** to finish mapping the network to the port.

Radios

The **Radios** tab provides an option to override the radio settings configured at the site level and allows you to configure radio settings which are specific to the selected Instant On device.

Follow these steps to override the site level radio settings and configure 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.

- Under **Radios**, click the **Use specific configurations for this radio** checkbox for **2.4 GHz Radio**, **5 GHz Radio** respectively to view the device specific radio settings.
- Under **Radio Details**, select the **Use specific channels and power configuration** checkbox for each of the radios, to modify their channel and power values.
- Choose a **Channel width** for each of the following:
 - 2.4 GHz Radio—**20 MHz (default)** or **20/40 MHz**.
 - 5 GHz Radio—**20 MHz**, **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. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.

- 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.
- Configure the **Transmit power** range for the 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	

Transmit Power Level	Threshold for 2.4 GHz Radio (in dBm)	Threshold for 5 GHz Radio (in 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 above values are governed by the DRT regulations for each country. If a country does not support transmit power level above 23 dBm under 5 GHz, the user will be limited by this value coming from the DRT regulatory when using the max TX Power setting.

The changes made in the above procedure are saved automatically.

Dynamic Channel Display

Starting with Instant On 2.9.0, the list of available Wi-Fi channels is displayed according to the site's country DRT regulations and also depending on AP types included in the Instant On site. Some key functions of dynamic channel display feature are described as follows:

- The DRT regulations are per AP type and per country.
- The global radio management section includes a union of all available channels regarding the AP types included in the site.
- Available channels and bandwidths might differ depending on whether the site mode is indoor (default) or outdoor (extend network with outdoor devices like AP17).
- The channels and bandwidths displayed under the global radio management section are updated accordingly if a device is added or removed from the site.
- When a new DRT file is available in future Instant On versions, the changes will reflect automatically in the radio sections if needed.

Actions

The **Actions** tab provides the following configuration options.

Locate

Instant On allows you to locate your device when there are many devices in the site.


To locate your device, follow these steps:

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP11D or AP22D router in the **Inventory** list and then click on **Actions** tab.
3. Slide the **Activate lights** toggle switch to right (🔴) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

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 router, follow these steps:

1. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to an AP in the **Inventory** list and then click on **Actions** tab.
3. Click the **Connectivity tests** tab beside **Network tests**. The **Connectivity test** screen is displayed.
4. 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.

5. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
6. Click **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

Restart

Aruba allows you to restart the device if you suspect any problem with it.



To restart your device, follow these steps:

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 an AP11D or AP22D router in the **Inventory** list and then click **Actions** tab.
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 or 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 router. This option is available only if the device selected from the inventory list is a router.

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

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

Switch Details

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

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. The **Device details** page of the switch is displayed.

The **Device details** page of the switch contains the following sections:

- [Identification](#)
- [Connectivity](#)
- [Ports](#)
- [Networks](#)
- [Link Aggregation](#)
- [Actions](#)
- [Tools](#)

Identification

Displays the device information such as device name, SKU, PoE power usage, uplink connectivity, and the IP address.

Device name

The device name is displayed in read/write mode. You can change the name of the device, if required. The maximum number of characters supported is 32.

Connectivity

Displays the details of uplink connection. When the switch is connected to a network device on the uplink port, a link to the device details page of the device is displayed.

Local network IP

Displays the local network IP of the switch.

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 switch.
- **Power consumption**—The amount of power in watts currently being consumed by the connected PoE devices.

Connectivity

LAN IP

Configure the IP assignment for the Instant On switch. You can configure either one of the following options:





The Instant On switch will reboot to apply the configuration changes.

- **Automatic (Default)** — The Instant On switch will inherit the IP address assigned by the DHCP in the network.
- **Static** — Specify a static IP address for the Instant On switch by entering the following network parameters:
 - **LAN IP** — Enter the IP address for the switch.
 - **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.

Routing

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

1. To enable routing on a switch, select the **Allow routing between networks** checkbox. To disable routing, deselect the checkbox.
2. 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.
3. To configure routing for a network, select the network to view the routing options:
 - a. Select the **Allow routing** checkbox to turn on routing. To turn off routing, deselect the checkbox.

- 
- NOTE**

- Viewing and Updating Inventory | 62

Color of the Ports












The color of the port is based on the number of error packets seen on the port over the total number of packets that pass on the port

The color of the port will be:

- Green, if the error rate is less than 0.1% and the port is in full-duplex mode
- Yellow, if the error rate is greater than 0.1% and the port is in full-duplex mode
- Green, if the error rate is less than 2% and the port is in half-duplex mode
- Yellow, if the error rate is greater than 2% and the port is in half-duplex mode

Port Icons

The following table lists some of the key icons that are displayed on the switch ports.

Symbol	Definition
	Uplink
	PoE
	Auto configured port
	Auto configured PoE port.
	Device connected, but port or link is down.
	Powered by PoE.
	PoE denied, indicating that the port is disconnected.
	PoE fault
	Transceiver issue.
	Link flapping
	Loop detected

PoE Specification

The port details also displays the PoE specification, when the port is powered by PoE. The information is displayed as power supplied, power allocated, PoE class as highlighted in the screen capture below.

The screenshot shows a network switch interface with 16 ports. Port 1 is highlighted with an orange box. Below the port grid, there is a section for Port 1. It shows a green lightning bolt icon and the text "Active". Below this, it says "This port is available for clients and devices to draw power and connect." Underneath, it says "Port 1". At the bottom, there are two rows of status information. The first row shows "2.5 Gbps / Full" and "6.31 W / 51 W (Class 6)". The second row shows "15.8 kbps" and "75 bps". The "6.31 W / 51 W (Class 6)" text is highlighted with a red box.

1 3 5 7 9 11 13 15
2 4 6 8 10 12 14 16

Active
This port is available for clients and devices to draw power and connect.

Port 1


2.5 Gbps / Full 6.31 W / 51 W (Class 6)
15.8 kbps 75 bps

Authentication and Security

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



These settings are available only for PoE or non-PoE ports that do not have any clients or devices connected to it.

- **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: <ul style="list-style-type: none">■ Server IP address or domain name—Enter the IP address or fully qualified domain name of the RADIUS server.

Parameters	Description
	<ul style="list-style-type: none"> ▪ 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 , select the checkbox) 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, select the checkbox.

- **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


Select one of the following options:

- **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, click 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**—To custom map the port to a tagged VLAN, select 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.

Allowed Clients and Devices

This setting allows users to select clients from the connected clients list and add them to the **Allowed clients and devices list**. Only the clients that appear in the list will be able to access the network when connected through that port. Disabling this feature will allow any wired client to connect to the port.

The following procedure describes how to add clients and devices to the allowed list, for a specific port on an Instant On switch:

1. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to a switch in the **Inventory** list and then click on the **Ports** tab.

3. Under **Allowed Clients and Devices**, select the **Allow selected clients and devices** checkbox.
4. Click the + icon next to **Add new clients and devices**.
5. Click the **Search for new clients and devices** button and connect the clients and devices to the port to be discovered.
6. Once the search is complete, select the checkbox next to the clients and devices you want to add to the Allowed list and click the **Add clients and devices** button.
7. Click **Save**.



- The **Allowed selected clients and devices** setting can be enabled on a maximum of 10 ports on the switch, and you can add only up to 10 allowed clients to one port.
- This setting is not supported for Instant On 1830 switches and cannot be enabled for Uplink ports or ports to which Instant On devices are connected.

Clients and devices connected to this port

Show— Allows you to view devices connected to port sorted by network. By default, **All Networks** is selected. To filter the clients and devices connected to a specific network, select a network from the Show drop-down list. The clients and infrastructure devices directly connected to the port are displayed as a link that takes you to the client details page. The indirectly connected clients are displayed by their MAC address.

link aggregation.

Transceiver Details

Instant On switches are capable of detecting an SFP transceiver. When a transceiver is connected to a switch, the details of the transceiver are displayed under the **Ports** tab of the switch details page. It is possible that the transceiver details are displayed even if the port state is up, down, loop detected, or link flapping.

The following transceiver details are displayed under the Ports tab:

Line No	Transceiver Details
Line 1	Denotes the transceiver compatibility in the following categories: <ul style="list-style-type: none">▪ Supported transceiver—Official transceiver models recommended by Aruba and appearing on the switch datasheet.▪ Unsupported transceiver—Third party transceiver models that are compatible with the switch.▪ Incompatible or faulty—Third party transceiver models that are unsupported and incompatible with the switch. The transceiver information is unavailable in this case.
Line 2	Name of the Vendor
Line 3	Type of transceiver
Line 4	Serial number of the transceiver.
Line 5	Model number of the transceiver.



- If the switch port to which the transceiver is connected is offline, an informative message is displayed stating **The link is down, or the transceiver is not functioning.**
- Instant On supported transceivers are recommended for optimal performance. Please refer to the Instant On product datasheets for supported transceiver list and Aruba Instant On 2.9.0 Transceiver Guide for additional detail. Unsupported transceivers are not guaranteed for proper operation and may experience function limitation. Information displayed for unsupported transceivers may be limited and inaccurate.

Power Management

Power management options allow you to configure PoE supply to devices connected to the switch. These options are unavailable for ports that are part of LACP.

- **Power supply policy** — Select either one of the following options to configure a power supply policy for 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** — Select this checkbox to either enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **Edit site power schedule**. For more information on configuring **Power Schedule**, see [Power Schedule](#).

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.

To assign network to a port, click on **Selected network** drop-down list and choose the network you want to map 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 11: *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. Click the (>) arrow next to a switch in the **Inventory** list and select the **Link Aggregation** tab.
 2. Click the + **Add link aggregation** link. The following configuration options are displayed:
- **Active**—Select this option to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. Unselect the checkbox to disable the LACP ports.
 - **Name**—Provide a custom name for the Link aggregation in the text field.
 - **Port members**—Click on the respective ports you want to add as members for the link aggregation. The selected port members are displayed below separated by commas.
 - **Delete**—Click on delete to delete the **Link Aggregation**.

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.

Select one of the following options:

- **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, click 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**—To custom map the port to a tagged VLAN, select 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.

Clients and devices connected on this link aggregation

- **Show**— Allows you to view devices connected to port sorted by network. By default, **All Networks** is selected. To filter the clients and devices connected to a specific network, select a network from the Show drop-down list. The clients and infrastructure devices directly connected to the port are displayed as a link that takes you to the client details page. The indirectly connected clients are displayed by their MAC address.

Actions



The Actions tab displays the following options:

- [Locate](#)
- [Network Tests](#)
- [Restart](#)
- [Switch to Local Management](#)
- [Replace Device](#)
- [Remove from Inventory](#)

Locate

Instant On allows you to locate your device when there are many devices in the site.

To locate your device, follow these steps:


1. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to a switch in the **Inventory** list and then click on **Actions** tab.
3. Slide the **Activate lights** toggle switch to right () to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.

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 switch, follow these steps:

1. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to a switch in the **Inventory** list and then click on **Actions** tab.
3. Click the **Connectivity tests** tab beside **Network tests**. The **Connectivity test** screen is displayed.
4. 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.



5. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
6. Click **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

Restart

To restart the device, follow these steps:

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 an AP in the **Inventory** list and then click **Actions** tab.
3. Click **Restart**.

Switch 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](#).



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. Click the **Inventory** tile () on the Aruba Instant On home page or click the **Site Health** banner () and then click on **Show inventory**.
2. Select the failed switch you want to replace from the inventory by clicking the arrow (>) next to the switch name.
3. Click the **Actions** tab.
4. Click the **Search** tab next to **Replace device**.

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



5. Select a switch from the list and click **Replace**.
6. Click **Finish**.

Remove from Inventory

Follow these steps to remove a switch which is still online:

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. Select the switch you want to remove from the inventory by clicking the (>) arrow next to the device name.
3. In the **Actions** tab, click **Remove** next to **Remove from inventory**.
4. Click **Remove** from the popup window to remove the switch from the inventory.

Follow these steps to remove a Switch which is offline:

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. Select the switch you want to remove from the inventory by clicking the (>) arrow next to the switch name.
3. In the **Actions** tab, 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.
4. Click the **Alerts** link. You will be directed to the Alert Details page which provides more information about the unusual activity. The **Advanced** menu does not appear on the title bar when the status is down.
5. If the Instant On device is removed from the network, you can choose to remove the device from the inventory by clicking **Remove** next to **Remove from inventory** in the **Actions** tab. A pop-up box appears on the screen requesting your confirmation.
6. Click **Remove** to delete the device from the inventory.

Tools

The **Tools** tab currently provides an option to configure port mirroring on the Instant On switch.



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. Click the **Inventory**  tile on the Aruba Instant On home page or click the **Site Health**  banner and then click on **Show inventory**.
2. Select the switch from the inventory by clicking the (>) arrow next to the switch name.
3. Click **Tools**.
4. Under **Port mirroring**, 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
5. 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.

6. Select one of the following as the **Traffic direction**:
 - a. Transmit and receive
 - b. Transmit
 - c. Receive
7. 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.

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



-
- There are a total of six SKUs for the Instant On 1960 switches and a stack can be formed by picking any variant of the 1960 switches. For example, an Instant On 1960 24 port PoE switch can be stacked with a 1960 8p 1G 4p 2.5G hybrid access switch.
 - Instant On 1960 switches support Hybrid Stacking. For example, an Instant On stack can contain a mix of 1960 access or aggregator switches to form a stack.
 - Instant On 1960 stack can be connected with either 1G / 2.5G or 10G ports however it is recommend to connect both ends of the stacking ports to the same speed.
-

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.



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 are connected in a ring 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.

Create a New Stack—After Initial Setup

The following procedure allows you to create a new stack in an inventory comprising of more than one Aruba Instant On 1960 Series switches in the site inventory:

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 (>) arrow next to the standalone Instant On 1960 Series switch on which the stack is to be created.
3. Under the **Actions** tab, click on **Create stack**. The screen displays the standalone Instant On 1960 Series switches that are part of the site inventory.
4. Click the Instant On 1960 Series switch you wish to add to the stack and then click **Add device**.
5. 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.
6. Click **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 Aruba Instant On 1960 Series switch to an existing stack in the inventory, which comprises of less than three Instant On 1960 Series switches:

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. Ensure that the Instant On 1960 switch to be added in the stack is listed in the inventory.
3. Click the (>) arrow next to the stack in the **Inventory** list. The device details of the stack is displayed.
4. Under the **Stack** tab, click **Add device**. The screen displays the standalone Instant On 1960 Series switches that are part of the site inventory, but not part of the stack.
5. Select the Instant On 1960 Series switch you wish to add to the stack and then click **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 at least two Aruba Instant On 1960 Series switches. To view the **Stack Details** page, follow these steps:

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 stack in the **Inventory** list. The **Device details** page of the stack is displayed.

The **Device details** page of the stack contains the following sections:

- [Identification](#)
- [Connectivity](#)
- [Ports](#)
- [Networks](#)
- [Link Aggregation](#)
- [Stack](#)
- [Actions](#)
- [Tools](#)

Identification

Displays the device information such as device name, PoE power usage, uplink connectivity, and the IP address.

Stack name

Denotes the name of the stack. By default, the serial number of the Conductor switch is used as the stack name. The user may also edit and specify a custom name for the stack.

Device name

The device name is displayed in read/write mode. You can change the name of the device, if required. The maximum number of characters supported is 32.

Conductor

The Conductor is the Aruba Instant On 1960 Series switch on which the stack is created.

Backup

Denotes the secondary Aruba Instant On 1960 Series switch which is configured in the stack. The Backup switch takes over the operations when the Conductor switch is offline.

Member

Denotes the third or fourth Aruba Instant On 1960 Series switch which is part of the stack.

Connectivity

Displays the details of uplink connection. When the stack is connected to a network device on the uplink port, a link to the device details page of the device is displayed.

Local network IP

Displays the local network IP of the Instant On 1960 Series switches in the stack.

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.

Connectivity

The **Connectivity** tab allows you to configure **LAN IP** settings separately for each device and **Routing** for the stack. To configure the **LAN IP** and **Routing** settings for the Instant On 1960 Series switches in the stack, click the drop-down above the **LAN IP** heading and select a device from the list.



LAN IP

Configures the IP assignment for an Instant On 1960 Series switch. You can configure either one of the following options:

- **Automatic (Default)** — The Instant On switch will inherit the IP address assigned by the DHCP in the network.
- **Static** — Specify a static IP address for the Instant On switch by entering the following network parameters:
 - **LAN IP** — Enter the IP address for the switch.
 - **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.

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. Click the (>) arrow next to a stack in the **Inventory** list. The stack details are displayed.
2. Select the **Allow routing between networks** checkbox. To disable routing, deselect the checkbox.
3. 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.
4. To configure routing for a network, select the network to view the routing options:
 - a. Select the **Allow routing** checkbox to turn on routing. To turn off routing, deselect the checkbox.
 - 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.
5. Click **Save** to apply configuration changes.



-
- 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.
-

Jumbo Frames

Jumbo frames improve data transmission efficiency by reducing the number of frames and overheads for switches to process. Jumbo frames can be configured on a cloud-managed stack. Once the setting is enabled on the stack, the configuration is applied to every Instant On switch in the stack. A new switch added to the stack will automatically adopt the jumbo frames configuration from the stack.

The following procedure describes how to enable jumbo frames on a stack:

1. Under **Jumbo frames**, select the **Jumbo frames** checkbox.
2. Click **Save**.

The Instant On switches in the stack automatically reboot to apply the changes.

Ports

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. Select a port to open the port configuration. When a port is selected the following options are displayed:

- Name of the port in read and write mode. The default name of the port is port <selected port ID number>.
- **Active** — Select the checkbox to enable the port. To disable the port, unselect the checkbox.




In a stack, the settings in the **Ports** tab can be configured separately for each Instant On 1960 Series switch in the stack.

Authentication and Security

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



These settings are available only for PoE or non-PoE ports that do not have any clients or devices connected to it.

- **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: <ul style="list-style-type: none">▪ Server IP address or domain name—Enter the IP address or fully

Parameters	Description
	<p>qualified domain name of the RADIUS server.</p> <ul style="list-style-type: none"> ▪ 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 , select the checkbox) 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, select the checkbox.

- **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

Select one of the following options:

- **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, click 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**—To custom map the port to a tagged VLAN, select 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.

Clients and devices connected to this port

- **Lock**— Allows you to lock the port and stop new devices 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 clients are blocked. The port must be unlocked for allowing new devices to connect. This option is unavailable on ports in which Instant On devices are connected. This option is displayed when clients and devices are connected to the port.

To lock a port on an Instant On switch, select the **Lock** checkbox. Deselect the **Lock** checkbox to unlock the port.



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.

- **Show**— Allows you to view devices connected to port sorted by network. By default, **All Networks** is selected. To filter the clients and devices connected to a specific network, select a network from the Show drop-down list. The clients and infrastructure devices directly connected to the port are displayed as a link that takes you to the client details page. The indirectly connected clients are displayed by their MAC address.

Power Management

Power management options allow you to configure PoE supply to devices connected to the switch. These options are unavailable for ports that are part of LACP.

- Power supply policy — Select either one of the following options to configure a power supply policy for 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.

- **Use site power schedule** — Select this checkbox to either enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **Edit site power schedule**. For more information on configuring **Power Schedule**, see [Power Schedule](#).

Networks

The **Networks** tab displays the current mapping of the switch ports to a specific VLAN ID. To view the port mapping information on a specific network, click the drop-down under **Selected network** and select one of the available networks from the list.

Link Aggregation

The **Link Aggregation** tab for a stack provides options to configure link aggregation groups for each device in the stack. 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
12 ports	16 trunks	8 trunk members
24 ports		
48 ports		

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

1. Click the (>) arrow next to the stack in the **Inventory** list and select the **Link Aggregation** tab.
2. Under the **Device** section, click on any of the Instant On 1960 Series switches listed in order of their assigned roles.
3. Click the **+ Add link aggregation** link. The following configuration options are displayed:
 - **Active**—Select this option to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. Unselect the checkbox to disable the LACP ports.
 - **Name**—Provide a custom name for the Link aggregation in the text field.
 - **Port members**—Click on the respective ports you want to add as members for the link aggregation. The selected port members are displayed below separated by commas.
 - **Delete**—Click on delete to delete the **Link Aggregation**.

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.



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.

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.

Select one of the following options:

- **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, click 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**—To custom map the port to a tagged VLAN, select 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.

Clients and devices connected on this link aggregation


- **Show**— Allows you to view devices connected to port sorted by network. By default, **All Networks** is selected. To filter the clients and devices connected to a specific network, select a network from the Show drop-down list. The clients and infrastructure devices directly connected to the port are displayed as a link that takes you to the client details page. The indirectly connected clients are displayed by their MAC address.

Stack

The **Stack** tab provides options 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** page 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 its 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. Click the **Inventory**  tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to the stack in the **Inventory** list and then click on **Stack** tab.
3. Under **Roles**, click the drop-down under any of the roles listed in the **Stack** 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.
4. Select the Instant On 1960 switch from the list, to which the role needs to be assigned.
5. Click **Done**.

Removing a Switch from the Stack

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

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to the stack in the **Inventory** list and then click on **Stack** tab.
3. Click the **Remove** tab beside **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. Select the member switch to be removed from the stack.
5. Click **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.

Actions

The **Actions** tab displays the following options:

- [Locate](#)
- [Network Tests](#)
- [Restart](#)
- [Unstack](#)
- [Replace Device](#)

Locate

Instant On allows you to locate your device when there are many devices in the site.


To locate your device, follow these steps:

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to the stack in the **Inventory** list and then click on **Actions** tab.
3. The toggle switches for the devices in the stack are displayed next to the **Locate** field. Slide the toggle switch to right (🔴) to turn on the locator light in the device. 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.

Network Tests

The **Network tests** option is used to test the reachability of an Instant On device. The network 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 network test on an Instant On stack, follow these steps:

1. Click the **Inventory** () tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**. The **Inventory** page is displayed.
2. Click the (>) arrow next to a stack in the **Inventory** list and then click on **Actions** tab.
3. Click the **Connectivity tests** tab beside **Network tests**. The **Connectivity test** screen is displayed.
4. Under **Source**, select an Instant On device from the drop-down list.

Only active devices of a site can be selected in this field.

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



The Network 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 stack, follow these steps:

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 the stack in the **Inventory** list and then click **Actions** tab.
3. In the **Restart <Device name>** window, select All devices, if you want to restart all the devices in the stack, or select an individual device in the stack.
4. Click **Restart**.

Unstack

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

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. Select the stack you want to unstack into separate devices in the inventory by clicking the (>) arrow next to the device name.
3. In the **Actions** tab, click **Unstack**. A popup appears on the screen requiring confirmation.
4. Click **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. Click the **Inventory**  tile on the Aruba Instant On home page or click the **Site Health**  banner and then click on **Show inventory**.
2. Select the offline switch you want to replace from the inventory by clicking the (>) arrow next to the switch name.
3. Click the **Actions** tab.
4. Click the **Search** tab next to **Replace device**.

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

5. Select a switch from the list and click **Replace**.
6. Click **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.

Tools

The **Tools** tab currently provides an option to configure port mirroring on the Instant On stack.



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.



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. Click the **Inventory**  tile on the Aruba Instant On home page or click the **Site Health**  banner and then click on **Show inventory**.
2. Select the stack from the inventory by clicking the (>) arrow next to the stack name.
3. Click **Tools**.
4. Under **Port mirroring**, select a switch from the stack as the **Mirroring device**.

5. 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
6. 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.

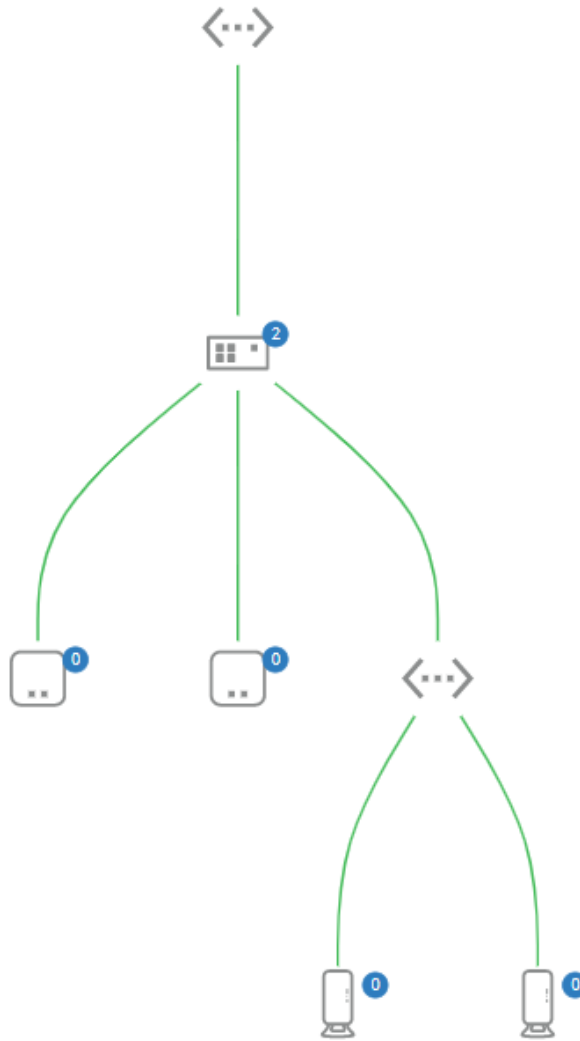
7. Select one of the following as the **Traffic direction**:
 - a. Transmit and receive
 - b. Transmit
 - c. Receive
8. Tap **Start mirroring** to initiate the mirroring of the packets sent from the source to the destination.

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

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. Place the cursor over a device to view the [device information card](#). Click on a device to go the device settings page.









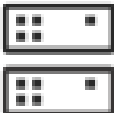



An example of the topology page is displayed below:



Use the mouse scroll to zoom in and zoom out of the network topology.

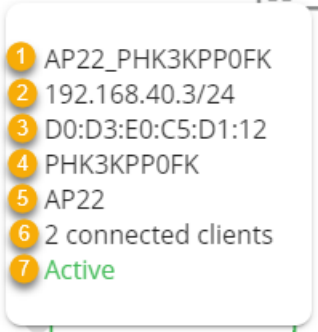
Description of Topology Icons

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.

Icon	Description
	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.
	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.

The following details are displayed when you hover the cursor over a device in the topology:

Description of Device Information Card

	<ol style="list-style-type: none"> 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
	<p>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.</p> <p>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.</p>

Stack Topology

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

1. Click the **Inventory** (🏠) tile on the Instant On web application home page or click the **Site Health** banner and then click on **Show inventory**.
2. Click the **Topology** tab.
3. Slide the **View stack topology** toggle switch to 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.

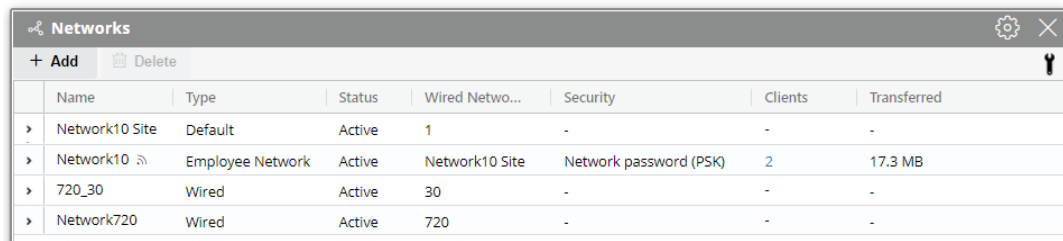
Auto-Detection and Auto-Configuring of Switch Ports

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 web application provides a summary of the networks that are available for employee and guest users.

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



Name	Type	Status	Wired Network	Security	Clients	Transferred
Network10 Site	Default	Active	1	-	-	-
Network10	Employee Network	Active	Network10 Site	Network password (PSK)	2	17.3 MB
720_30	Wired	Active	30	-	-	-
Network720	Wired	Active	720	-	-	-

Figure 2 Screenshot of Network Dashboard

Table 13: Network Information

Parameter	Description
Name	Identifies the Instant On network used to connect computers, tablets, or phones together. The network name is also used as the Wi-Fi identifier.
Type	Indicates if the network is a employee guest network.
Status	Shows the status of the network.
Wired Network / VLAN	Wired Networks: Shows the VLAN ID that was assigned for the network. Wireless Network: Shows the network name of the network.
Security	Shows the security option set for the network.
Clients	Shows the number of clients currently connected to the network. Click the number listed under Clients to view the details of the client selected. See Managing Clients for more information about the Clients page.
Transferred	Shows the volume of data, in bytes, transferred in the network throughout the day.

For more details about a specific network, select one of the following networks from the **Networks** page:

- [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.



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. Click the **Networks** tile on the Instant On web application home page.
2. Click Add (+) and select **Identification** tab.
3. Select the **Wireless** option in the **Network Type** selection. The wireless option appears only when your site has both wired and wireless networks.
4. Select **Employee**, under Usage to indicate that the network is for an enterprise.
5. Enter a **Network name** for the employee network. This will also be broadcasted as the SSID for the WLAN network.
6. Configure any one of the following security options:
 - a. **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.



The **Network password** settings will be grayed out when only the 6 GHz radio spectrum is selected for the wireless network. For more information, see [Radio](#).

- b. **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:



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.
- **Send RADIUS Accounting**—Select this checkbox to send RADIUS accounting messages.
- **Primary RADIUS Server**—Configure the following parameters for the **Primary RADIUS Server**.
 - **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**— Select this checkbox to configure a secondary RADIUS server. When selected, configure the following parameters:
 - **Server IP address or domain name**—Enter the IP address or fully qualified domain name 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.
7. Click **Save**.



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

Identification

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

1. Click **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 Network Details** screen.
3. Click **Identification** tab.
4. Enter a new name under **Network name** to change the main network name or a new password under **Network password** to change the main network password. A warning message appears, indicating that changes to the network settings will disconnect all clients currently accessing the network.
5. Click **Save**.

Options

The **Options** tab in the web application allows you to configure the bandwidth limit on the internet usage along with IP and VLAN assignment for clients on employee or guest networks. To configure these options, select the employee network or guest network and then click the **Options** tab.

Show Network

The **Show network** checkbox is selected by default to broadcast the employee or guest network in the list of available Wi-Fi networks. Deselect the checkbox if you want to disable the selected network.

Wi-Fi 6

The **Wi-Fi 6** checkbox configures Wi-Fi 6 (802.11ax) capabilities of the network. When selected, 802.11ax capable clients can make use of enhanced throughput and transmission capabilities of the 802.11ax standard. This setting is enabled by default.

To disable this option, deselect the **Wi-Fi 6** checkbox.



- The Wi-Fi 6 option is only available when the device inventory has at least one Aruba Instant On AP22 access points.
- 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, select the **Multiple clients optimization** checkbox 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Optimize for video streaming** checkbox.
4. Click **Save**.

Limit 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Limit bandwidth usage** checkbox.

4. Under **Restrict bandwidth usage by**, select the **Client** radio button.
5. Move the slider to set the bandwidth limit for the employee or guest network. The limit is set to **1 Gbps** by default.
6. Click **Save**.

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (➤) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Limit bandwidth usage** checkbox.
4. Select the **Network** radio button and move the slider to set the bandwidth limit between 1 Mbps to 1 Gbps for the employee or guest network.
5. Click **Save**.

IP and Network Assignment

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

- **Same as local network (default)**—This setting is referred to as **Bridged mode**. Clients will receive an IP address provided by a DHCP service on your local network. 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.

Radio

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

To configure radio frequency, follow these steps:

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed. Click the (➤) arrow next to the employee or guest network or to view the configuration parameters.
2. Select the employee or guest network and then click on the **Options** tab.
3. Under **Radio**, select the radio frequency. The available frequencies are:
 - **2.4 GHz**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
 - **5 GHz**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.
 - **6 GHz**—The AP will broadcast the wireless network only on the 6 GHz radio frequency.

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** checkbox. By default, 802.11b rates are disabled for all the networks. To enable this option, select the checkbox. 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.

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 or guest 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 operational.

Creating an Access Schedule for an Employee Network

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed. Click the (>) arrow next to the employee network or guest to view the configuration parameters.
2. Click the **Schedule** tab.
3. Select **Ruled by a schedule** checkbox, to enable the network schedule.
4. Select one of the following options:
 - a. **Fixed**—Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) equally to those of the employee or guest network schedule.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The network is active throughout the day for the selected days.
 - **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.
 - b. **Variable**—Indicates the schedule configuration that allows users to set up a different time range on a daily basis.
 - Follow these steps to enable the network schedule for specific days of the week:
 - After selecting **Variable**, click on the day of the week for which you need to configure a schedule.
 - Select the **Active** checkbox.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The network is active throughout the day for the selected days.
 - **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.
5. Click **Save**.

Network Access

The **Network Access** tab in the Instant On web application 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network and click on **Network Access** tab.
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 **Resource IP address** in the list of IP addresses and click + .

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 click + .

Allowed Clients

The **Allowed Clients** feature is used to provide network access only to the clients that are added to the list. This feature is available only on employee networks that are configured with a network password (PSK) authentication. The **Allowed Clients** setting is disabled by default. This setting can be enabled per-network and not globally. Each applicable network can have its own list of allowed clients. You can add a maximum of 128 wireless clients to the **Allowed Clients** list.

The following procedure describes how to enable and edit the allowed clients list:

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network and click on **Network Access** tab.
3. Select the **Use allowed clients list** checkbox.
4. Click + **Add clients**.
5. Click Search for new clients. The Instant On devices begins scanning for nearby clients that are available to connect to the network.
6. Choose the clients that should be added to the **Allowed Clients** list.



After selecting the clients from the **Add Clients** wizard, the allowed clients can connect to a specific network with the correct PSK key, and only then will the clients appear in the "Allowed Clients" list.



7. Click **Save**.

Once the changes are saved, the connected wireless clients that are not in the **Allowed Clients** list will be disconnected immediately.





Shared Services

Aruba Instant On web application 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 web application. For information on deploying shared services, see [Deploying Multicast Shared Services](#).



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

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

1. Click **Networks** () tile on the Instant On home page. The **Networks** page is displayed.
2. Click the settings () icon in the header and select **Shared services** from the drop-down.
3. Slide the toggle switch next to **Shared services**, to the right () to enable the Shared services feature on the network.
4. Once you have enabled the Shared services setting, navigate back to the main networks page and click the () arrow next to the employee network or guest network to view the configuration parameters.
5. Click **Shared services** tab to view the following information:
 - a. **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.
 - b. **Services detected on other networks**—Lists all the services available on other employee networks in your site. By default, the services connected to other networks are disabled. Click on the checkbox under **Allow access** to allow access to shared services available on other networks.



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 web application. 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.

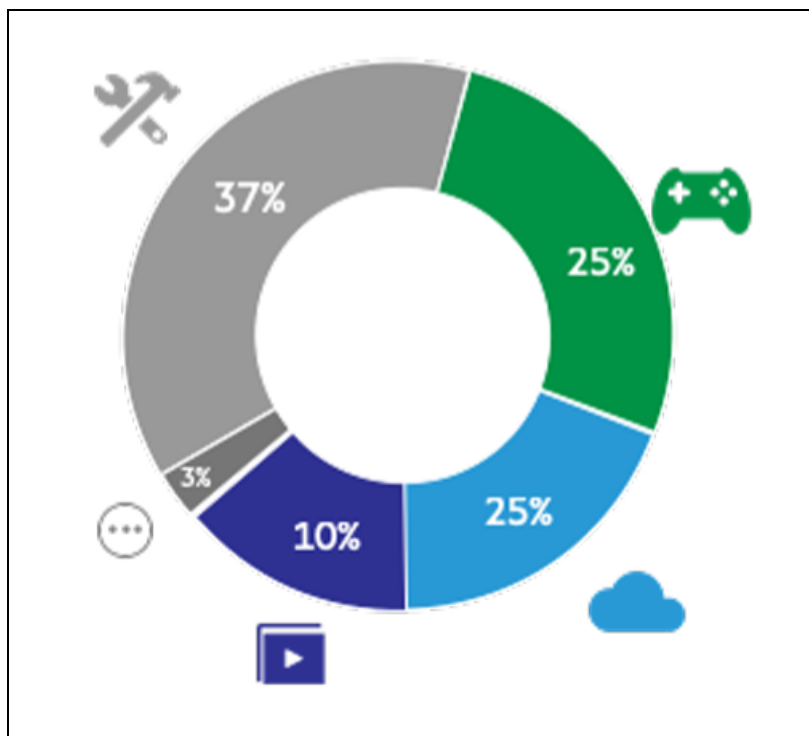
- DLNA Print—This service is used by printers that support DLNA.
- Smart Speakers—Includes multimedia services like Alexa.
- Multiple Services—A device offering more than one service will be bundled together in this category.

Applications

The **Applications** tab in the Aruba Instant On web application provides the following information:

- An overview of the client and application usage statistics for the employee or guest network.
- Displays the client count, which is the total number of clients currently connected to the network. Click on the number listed under **Clients** to view the total number of clients connected to the network. The **Connected clients** tab provides connection information for clients in the network. See [Viewing Client Details](#) for more information about the **Clients** page.
- Provides data for the top five application categories, based on usage. Data is presented in both bytes and percentage.

Figure 3 *Applications Chart*



- Displays the total amount of data (in MB), transferred in the network throughout the day.
- 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. Click the **Networks** tile on the Instant On web application home page.
2. Click 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 **Network name**.
5. Select one of the following **Security** levels:
 - a. Click **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 [Configuring Guest Portal](#) and [Wi-Fi Enhanced Open \(OWE\)](#).
 - b. Click **Password**, if you want to secure 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.



The Network password settings will be grayed out when only the 6 GHz radio spectrum is selected for the wireless network. For more information, see [Radio](#).

6. To configure a guest portal in addition to the security levels, click the **Guest portal** checkbox and follow the instructions provided in [Configuring Guest Portal](#).
- To change the guest network status manually, follow these steps:
 1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed. Click the (>) arrow next to the guest network.
 2. Under the **Identification** tab, select the **Active** checkbox to enable the network. To disable the network, deselect the checkbox.
 3. Click **Save**. The network is marked as **Active**, and all network settings are made visible.

Wi-Fi Enhanced Open (OWE)

Wi-Fi 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.


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. Select the **Wi-Fi Enhanced Open** checkbox to enable the feature.
3. Click **Save**.

Configuring Guest Portal

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

business logo, pictures, legal terms and other details. To configure Guest portal service on the Aruba Instant On web application, follow these steps:

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

Configuring Captive Portal

Use the following links to learn how to configure captive portal for the guest network:

- [Configuring Internal Captive Portal](#)
- [Configuring External Captive Portal](#)

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	Click 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: <ul style="list-style-type: none">▪ 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—Click 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	Click 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: <ul style="list-style-type: none">▪ 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—Click the box to view the color palette and choose a color for the font.

Table 14: Internal Captive Portal Configuration

Parameter	Description
	<ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ◦ Font color—Click 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	<p>Design the Accept Button by updating the following fields:</p> <ul style="list-style-type: none"> ▪ 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—Click 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 portal
- Customize an external captive portal by configuring RADIUS authentication and accounting parameters.



Using Third-Party Captive Portal Providers

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

- Aislelabs
- Purple WiFi
- Skyfii.io
- Wavespot
- Zoxx

To use third-party providers for external captive portal, follow these steps:

1. Under **Select preferred provider**, select the preferred 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 click  to add additional domains. This allows unrestricted access to additional domains.

3. Click **Apply changes**.

Customizing the Captive Portal Page

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. Under **Other**, select the **Custom** tile on the **Guest Portal** page.

The **Custom** external captive portal offers two types of user accessibility to the Internet through the guest portal under Guest user access. Choose one of the following options.

User authentication (default)—Users are required to enter their credentials in the guest portal page to access the Internet. The credentials entered by the user are sent to the RADIUS server for validation. This is the default setting for the custom external captive portal.

Guest portal acknowledgement—The guest portal must return a predefined string **Aruba.InstantOn.Acknowledge** to grant user access to the Internet. When selected, a predefined authentication text is returned by the external server after successful user authentication.

3. 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	<p>Configure a primary RADIUS server for authentication by updating the following fields:</p> <ul style="list-style-type: none"> ▪ 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. <p>Click the More RADIUS parameters link to configure the following parameters:</p> <ul style="list-style-type: none"> ▪ Server timeout—Specify a timeout value in seconds. The value

Table 15: *External Captive Portal Configuration*


Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> ▪ 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. <p>Configure the following settings under Network Access Attributes, if you wish to proxy all RADIUS requests from the Instant On AP to the client.</p> <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ◦ 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. <p>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.</p>
Secondary RADIUS Server	<p>To configure a Secondary RADIUS Server, slide the toggle switch to the right ().</p> <p>NOTE: The configuration parameters for the Secondary RADIUS Server and the Primary RADIUS Server are the same.</p>
Network Access Attributes	<p>This option is available only if User authentication (default) is selected under Guest user access. Configure the following parameters under network access attributes:</p> <ul style="list-style-type: none"> ▪ NAS Identifier—Enter a string value for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.

Table 15: External Captive Portal Configuration

Parameter	Description
	<p>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.</p> <p>Use device IP (default)—This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients.</p> <p>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.</p>

4. Click **Apply changes**.

Options

The **Options** tab in the web application allows you to configure the bandwidth limit on the internet usage along with IP and VLAN assignment for clients on employee or guest networks. To configure these options, select the employee network or guest network and then click the **Options** tab.

Show Network

The **Show network** checkbox is selected by default to broadcast the employee or guest network in the list of available Wi-Fi networks. Deselect the checkbox if you want to disable the selected network.

Wi-Fi 6

The **Wi-Fi 6** checkbox configures Wi-Fi 6 (802.11ax) capabilities of the network. When selected, 802.11ax capable clients can make use of enhanced throughput and transmission capabilities of the 802.11ax standard. This setting is enabled by default.

To disable this option, deselect the **Wi-Fi 6** checkbox.



- The Wi-Fi 6 option is only available when the device inventory has at least one Aruba Instant On AP22 access points.
- 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, select the **Multiple clients optimization** checkbox 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Optimize for video streaming** checkbox.
4. Click **Save**.

Limit 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Limit bandwidth usage** checkbox.
4. Under **Restrict bandwidth usage by**, select the **Client** radio button.
5. Move the slider to set the bandwidth limit for the employee or guest network. The limit is set to **1 Gbps** by default.
6. Click **Save**.

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network to view the configuration parameters and then click **Options**.
3. Select the **Limit bandwidth usage** checkbox.
4. Select the **Network** radio button and move the slider to set the bandwidth limit between 1 Mbps to 1 Gbps for the employee or guest network.
5. Click **Save**.

IP and Network Assignment

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

- **Same as local network (default)**—This setting is referred to as **Bridged mode**. Clients will receive an IP address provided by a DHCP service on your local network. 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.

Radio

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

To configure radio frequency, follow these steps:

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed. Click the (>) arrow next to the employee or guest network or to view the configuration parameters.
2. Select the employee or guest network and then click on the **Options** tab.
3. Under **Radio**, select the radio frequency. The available frequencies are:
 - **2.4 GHz**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
 - **5 GHz**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.
 - **6 GHz**—The AP will broadcast the wireless network only on the 6 GHz radio frequency.

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** checkbox. By default, 802.11b rates are disabled for all the networks. To enable this option, select the checkbox. 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.

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 or guest 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 operational.

Creating an Access Schedule for an Employee Network

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed. Click the (>) arrow next to the employee network or guest to view the configuration parameters.
2. Click the **Schedule** tab.
3. Select **Ruled by a schedule** checkbox, to enable the network schedule.
4. Select one of the following options:
 - a. **Fixed**—Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) equally to those of the employee or guest network schedule.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The network is active throughout the day for the selected days.
 - **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.

- b. **Variable**—Indicates the schedule configuration that allows users to set up a different time range on a daily basis.
 - Follow these steps to enable the network schedule for specific days of the week:
 - After selecting **Variable**, click on the day of the week for which you need to configure a schedule.
 - Select the **Active** checkbox.
 - Select one of the following options under **Active hours during the day**:
 - **All day**: The network is active throughout the day for the selected days.
 - **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.

5. Click **Save**.

Network Access

The **Network Access** tab in the Instant On web application 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network and click on **Network Access** tab.
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 **Resource IP address** in the list of IP addresses and click +.

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 click +.

Allowed Clients

The **Allowed Clients** feature is used to provide network access only to the clients that are added to the list. This feature is available only on employee networks that are configured with a network password (PSK) authentication. The **Allowed Clients** setting is disabled by default. This setting can be enabled

per-network and not globally. Each applicable network can have its own list of allowed clients. You can add a maximum of 128 wireless clients to the **Allowed Clients** list.

The following procedure describes how to enable and edit the allowed clients list:

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the employee or guest network and click on **Network Access** tab.
3. Select the **Use allowed clients list** checkbox.
4. Click **+ Add clients**.
5. Click Search for new clients. The Instant On devices begins scanning for nearby clients that are available to connect to the network.
6. Choose the clients that should be added to the **Allowed Clients** list.



After selecting the clients from the **Add Clients** wizard, the allowed clients can connect to a specific network with the correct PSK key, and only then will the clients appear in the "Allowed Clients" list.

7. Click **Save**.

Once the changes are saved, the connected wireless clients that are not in the **Allowed Clients** list will be disconnected immediately.

Shared Services

Aruba Instant On web application 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 web application. For information on deploying shared services, see [Deploying Multicast Shared Services](#).



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

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the settings (⚙️) icon in the header and select **Shared services** from the drop-down.
3. Slide the toggle switch next to **Shared services**, to the right (🔴) to enable the Shared services feature on the network.
4. Once you have enabled the Shared services setting, navigate back to the main networks page and click the (>) arrow next to the employee network or guest network to view the configuration parameters.
5. Click **Shared services** tab to view the following information:
 - a. **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.
 - b. **Services detected on other networks**—Lists all the services available on other employee networks in your site. By default, the services connected to other networks are disabled. Click on the checkbox under **Allow access** to allow access to shared services available on other networks.



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 web application. 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:

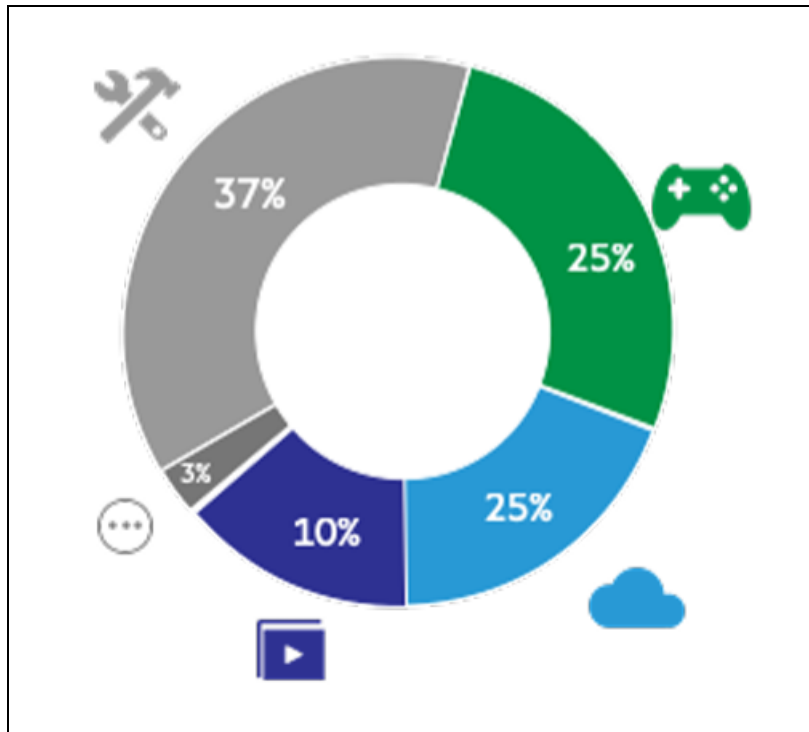
- AirPlay™—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- AirDrop™—Apple® Airdrop allows you to share and receive photos, documents and more with other Apple devices that are nearby.
- Google 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.
- Smart Speakers—Includes multimedia services like Alexa.
- Multiple Services—A device offering more than one service will be bundled together in this category.

Applications

The **Applications** tab in the Aruba Instant On web application provides the following information:

- An overview of the client and application usage statistics for the employee or guest network.
- Displays the client count, which is the total number of clients currently connected to the network. Click on the number listed under **Clients** to view the total number of clients connected to the network. The **Connected clients** tab provides connection information for clients in the network. See [Viewing Client Details](#) for more information about the **Clients** page.
- Provides data for the top five application categories, based on usage. Data is presented in both bytes and percentage.

Figure 4 *Applications Chart*



- Displays the total amount of data (in MB), transferred in the network throughout the day.
- 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](#).

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. Click the **Networks** tile on the Instant On web application home page. The **Networks** page is displayed.
2. Click **+ Add** and select **Wired** as **Network type** under the **Identification** tab.
3. Under **Identification** tab, Enter a **Network name** for the network.
4. Enter a **VLAN** for your network.
5. Click **Save**.

Modifying the Network Name or VLAN ID

To modify the wired network:

1. Click **Networks** tile on the Instant On home screen. The **Networks** page is displayed.
2. Select the wired network from the list of **Networks**.

3. Under **Identification** tab, enter a new name under **Network name** to change the main network name or enter a new **VLAN** to change the VLAN ID.
4. Click **Save**.



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. Click **Networks** tile on the Instant On home screen. The **Networks** page is displayed.
2. Select the wired network from the list of **Networks**.
3. Under **Identification** tab, select the **Active** checkbox to enable the network. To disable the network, deselect the checkbox.



The default wired network is used to manage the Instant On device and 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. Click **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. Click **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. Click **Activate** to continue this operation.


Configuring a Voice Network

Instant On allows you 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. Click **Networks** tile on the Instant On home screen. The **Networks** page is displayed.
2. Select a wired network from the list of **Networks**.
3. Under **Identification** tab, select the **Voice network** checkbox to allow clients with voice capabilities to be automatically redirected to this network.
4. Click **Save**.

Important Points to Note:

- Only one Voice network can be configured per site. The Voice network toggle switch will remain visible on other wired networks, but will be grayed out, preventing the user from enabling it. A .

icon is displayed next to Voice network. Clicking on the icon displays a popup indicating that the Voice network is already enabled on a different network.

- 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 web application.



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.

Network Access

The **Network Access** tab in the Instant On web application 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the wired network and click on **Network Access** tab.
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 + .

Important Points to Note

- The locked port and restricted network features are independent. A single wired port cannot be locked and be dedicated to a restricted network at the same time.
- If a scenario occurs where a wired port is used both as a locked port and in a restricted network, the locked port feature will take precedence.
- A maximum of eight wired networks can be restricted at the same time. Once the maximum limit is reached, a message is displayed on the page indicating the same.

Options

The **Options** tab for wired networks in the web application allows you to configure the multicast optimization setting.

Multicast Optimizations

The multicast optimization or IGMP Snooping feature helps reduce traffic to registered multicast groups in the network. This setting can be configured per wired network and currently applies only to the Aruba Instant On switches. Disable this setting when experiencing problems with multicast applications.

To configure multicast optimizations on a wired network, follow these steps:

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to a wired network to view the configuration parameters and then click **Options**.
3. Select the Multicast Optimizations checkbox.
4. Click **Save**.



This feature is currently not configurable on AP11D and AP22D devices.

Shared Services

Aruba Instant On web application 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 web application. For information on deploying shared services, see [Deploying Multicast Shared Services](#).



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

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

1. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the settings (⚙️) icon in the header and select **Shared services** from the drop-down.
3. Slide the toggle switch next to **Shared services**, to the right (🔴) to enable the Shared services feature on the network.
4. Once you have enabled the Shared services setting, navigate back to the main networks page and click the (>) arrow next to the employee network or guest network to view the configuration parameters.
5. Click **Shared services** tab to view the following information:
 - a. **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.
 - b. **Services detected on other networks**—Lists all the services available on other employee networks in your site. By default, the services connected to other networks are disabled. Click on the checkbox under **Allow access** to allow access to shared services available on other networks.



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 web application. 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.
- **Smart Speakers**—Includes multimedia services like Alexa.
- **Multiple Services**—A device offering more than one service will be bundled together in this category.

Network Security

The **Network Security** option in the Instant On web application, 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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the wired network and click on **Network Security** tab.
3. Select the **Network security protections** checkbox to enable network protections. This setting is disabled by default.
4. Click **Enable** in the popup window.
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. Click **Save** to save the configurations.

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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the wired network and click on **Network assignment** tab.
3. Under **Devices**, 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. Click **Save**.

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. Click **Networks** (🔗) tile on the Instant On home page. The **Networks** page is displayed.
2. Click the (>) arrow next to the wireless network and click on **Network assignment** tab.
3. Under **Select devices that will accept connections to this network**, click the checkboxes next to the APs listed to assign them to the wireless network.
4. Click **Save**.

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 11





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.		<ul style="list-style-type: none">▪ 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.		<ul style="list-style-type: none">▪ Application Software
Utilities —Sites about tools and services that ease internet usage and navigation, such as search engines, cloud storage, and file transfer.		<ul style="list-style-type: none">▪ 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.		<ul style="list-style-type: none">▪ 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.		<ul style="list-style-type: none"> 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.		<ul style="list-style-type: none"> Streaming Media Web Advertisements Content Delivery Networks Image and Video Search
Instant messaging and email —Websites and applications where users can send and receive messages and emails.		<ul style="list-style-type: none"> Email Short Message Service Messenger
Business and 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.		<ul style="list-style-type: none"> Financial Services Business and Economy Job Search Philosophy and Political Advocacy Educational Institutions Health and Medicine Legal Real Estate
News and media —Sites containing local and world news, breaking news, online newspapers, crowdsourced news, general information, and weather.		<ul style="list-style-type: none"> World News Weather Report Online News
Uncategorized —Do not consider these web categories. These include websites that cannot be grouped under any of the categories described in this list		<ul style="list-style-type: none"> Dead Sites Parked Domains <p>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.</p>
Social network —Social applications include websites for social networking and media.		<ul style="list-style-type: none"> Social Networking Dating Personal sites and Blogs News and Media
Adult content —Adult content applications include websites with graphic adult content or illegal subjects.		<ul style="list-style-type: none"> Abused Drugs Marijuana Adult and Pornography Nudity Violence Abortion Hate and Racism Gross Illegal

Application Category	Icon	Instant On Classification
Education —Sites about education information like schools, college, universities, and online training tools like Linda.com, LinkedIn learning, etc.		<ul style="list-style-type: none"> University Education Schools Colleges Online Learning
Explicit content —Restricted content applications include websites with sensitive information or graphic content.		<ul style="list-style-type: none"> 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.		<ul style="list-style-type: none"> Online Gaming
Government and politics —Military and government applications include websites on military and government information and services.		<ul style="list-style-type: none"> Military Government
Kids and family —Sites aimed for kids and families with learning, educational and interactive content.		<ul style="list-style-type: none"> 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.		<ul style="list-style-type: none"> 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.		<ul style="list-style-type: none"> Auctions Shopping
Sports and recreation —Recreational applications include websites on personal activities and interests.		<ul style="list-style-type: none"> Travel Home and Garden Entertainment and Arts Local Information Hunting and Fishing Society Sports

Application Category	Icon	Instant On Classification
		<ul style="list-style-type: none"> ■ Music ■ Fashion and Beauty ■ Recreation and Hobbies ■ Motor Vehicles ■ Kids ■ Online Greeting cards ■ Religion

Viewing Application Information



The **Applications** page provides the application wise data usage:

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. Click **Applications**  tile on the Instant On home page .Click the settings  icon on the **Overview** page header and select **Visibility and control**. The **Visibility and Control** page is displayed.
2. Select one of the available options:
 - **Application details (default)**—Provides a detailed view of date usage by different applications and websites accessed by clients in the network. Applications chart and Applications list are displayed only when this option is selected. This option is enabled by default.
 - **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 web application.

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.

Filtering Application Information in the Web Application

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

1. Click **Applications** on the Instant On home page. The **Applications** page opens.
2. Click the tool (⚙️) button at the top-right corner of the **Applications** list to open the parameter drop-down list.
3. Select the parameters that you want to display or hide from the **Applications** page.
 - Parameters with an orange check mark are displayed on the **Applications** page.
 - Parameters without a check mark are not displayed on the **Applications** page.

To restore the default settings, follow these steps:

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

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, click the Applications (📱) tile on the Instant On home page. The **Applications** tab displays the web categories and their **Total Usage** data on the network. Click the (>) arrow beside the **Name** of any of the web categories to view the usage data.

The following data is displayed for each category:

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

Sorting Application Information in the Web Application

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

Applications Chart

Data for the top five application categories (by usage) is displayed in a donut chart. If more than five application categories have been accessed throughout the day, the fifth section of the **Applications**

chart is represented as **Other**. Any applications that do not fall under the top four application categories are grouped into **Other**.

Applications List

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

Viewing and Blocking Application Access

The **Applications** page 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 web application allows you to set restrictions to access certain applications on basis of their category:

1. Click **Applications** on the Instant On home screen. The various application categories are displayed.
2. Navigate to **Applications** tab and select an application category from the **Applications** list. The selected application category opens.
3. Under **Activity for the last 24 hours**, uncheck the **Allow use** checkbox for the selected employee or guest networks.






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.






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 Wireless Clients in the Site

Connected Clients

The **Connected clients** page displays the list of all active clients in the site. The Connected clients list includes wired, wireless, and infrastructure clients connected to a network in the site. Wireless clients connected to the network are denoted by  icon and wired clients are denoted by  icon. Detailed information about a connected client can be viewed in the [Client Details page](#) by clicking on  icon beside a client name in the **Connected Clients** list. The **Connected clients** list displays the following information:




Column Label	Description
Name	Name of the client. Click on  icon beside the client name from the list to view the Client Details page . The Client Details page lists detailed information about the client.
Network	The network to which the client is connected.
Interface	Denotes the device interface to which the client is connected. The Wireless client will display the radio (2.4 GHz or 5 GHz) to which it is connected.
Device	The network device to which the client is connected.
Duration	Denotes the amount of time that the client has been connected to the network.
Signal / Speed	Indicates the client signal quality. Based on the client's Signal-to-Noise Ratio (SNR), the signal quality is denoted as follows: For Wired Clients  — Good, Signal Strength between 1 to 10 Gbps.  — Fair, Signal Strength between 10 to 100 Mbps. For Wireless Clients  — Good, Signal Strength of 25 dB or higher.  — Fair, Signal Strength between 16 dB and 25 dB.

Column Label	Description
	 — Poor, Signal Strength of 15 dB or lower.
IP Address	IP address of the client.
MAC Address	MAC address of the client.
OS	Operating system (OS) of the client device.
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.
Top Application Category	The most frequently used application type on the device.
Click the  button on the top-right corner of the Connected Clients list to choose the data columns displayed in the list.	

Blocking a Wireless Client

Instant On allows you to block wireless clients from associating with any of the APs on site. Clients can be blocked only if they are already connected to the network. At any point in time, you may choose to [unblock a blocked client](#).


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

1. Click on the **Clients**  tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Connected clients** tab to view the list of connected clients.
3. Hover the cursor over a wireless client. A  button is displayed at the end of the row.
4. Click the  button to block the client. The client is immediately blocked and moved to the **Blocked clients** list.

Sorting Client Information in the Web Application

Client data can be sorted in the Instant On web application to help you locate information efficiently. For example, client data can be sorted in ascending or descending order based on the client name. Click on the column label of the **Connected Clients** or **Blocked Clients** list to sort the list.



Watchlisted Clients

The client watchlist feature allows you to monitor the status of the wired or wireless clients connected to the Instant On devices. After the client is added to the watchlist () , an alert is triggered when the watched client goes offline and is cleared if the client comes back online or removed from the watchlist.





You can add a maximum of 128 wired or wireless clients to the watchlist.

The following procedure describes how to add a client to the watchlist:

1. Click on the **Clients**  tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Connected clients** tab to view the list of connected clients.
3. Hover the cursor over a wired or wireless client. A watchlist icon (☆) is displayed at the end of the row.
4. Click watchlist . The client is added to the **Watchlisted clients**(☆) list.

The following procedure describes how to remove a client from the watchlist:

1. Click on the **Clients**  tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Watchlisted clients** (☆) tab to view the list of clients added to the watchlist.
3. Hover the cursor over a wired or wireless client. An Unwatchlist icon is displayed at the end of the row.
4. Click Unwatchlist . The client is removed from the **Watchlisted clients** list.




Blocked Clients

The **Blocked clients** page lists the details of wireless clients that are barred from joining networks in the site. Clients blocked in a site can be unblocked from this page. The **Blocked clients** page displays the following information:

Column Label	Description
Name	Name of the client.
MAC Address	MAC address of the client.

Unblocking a Blocked Client

Follow these steps to unblock a blocked wireless client:

1. Click on the **Clients**  tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Blocked clients** tab to view the list of blocked clients.
3. Hover the cursor over a blocked client. A  button is displayed at the end of the row.
4. Click the  button to unblock the client. The client is unblocked and moved to the **Connected clients** list.





When a client is blocked, it will not be connected to the network and will not appear in the list of connected clients until the client reconnects to the network, and not directly after unblocking it.

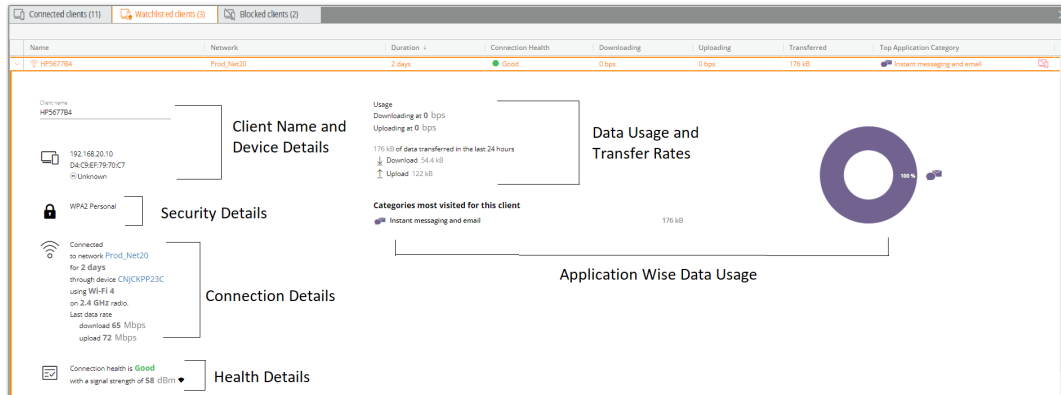
Viewing Client Details

The **Client Details** page provides detailed information about clients in your network. The Client Details page is accessed from the **Connected clients** page. 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. Wired clients are further classified into infrastructure clients. Infrastructure clients are switches and other network devices through which other wired clients are connected to the 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. Select the **Connected clients** tab to view the list of clients to your site.
3. Click on  icon beside the client name from the list to view the **Client Details** page.



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

- [Client Name and Device Details](#)
- [Security Details](#)
- [Connection Details](#)
- [Connection Health](#)
- [Data Usage and Transfer Rates](#)
- [Application Data Usage \(only for wireless clients\)](#)

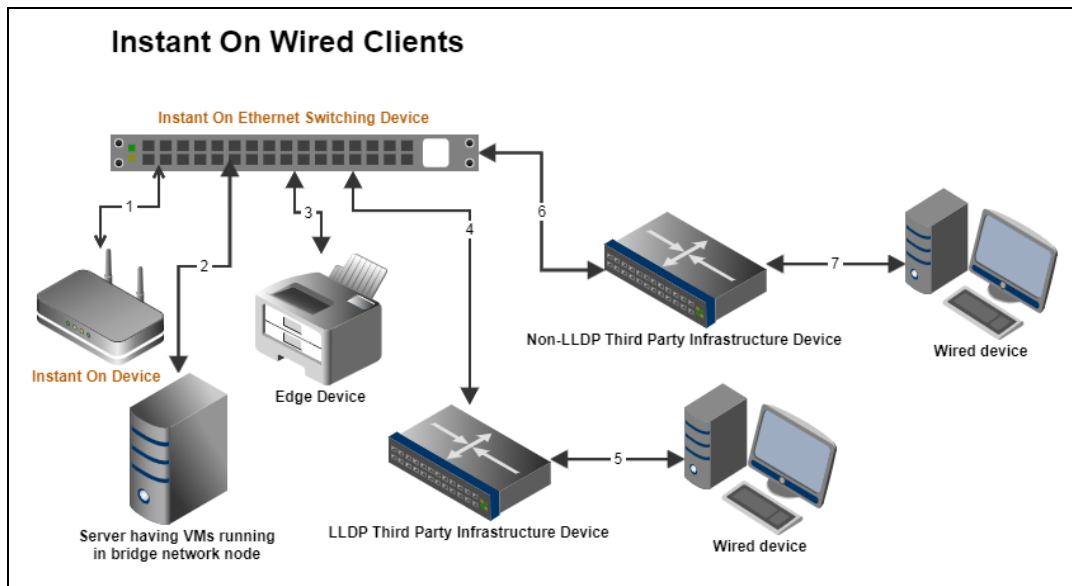
Column Label	Description
Client Name and Device Details	
Client name	Denotes the name of the wireless client. The client name can be edited and updated to a custom name of your choice. The length of the client name can be between 1 to 32 characters. Blank spaces and special characters are accepted as a valid characters in the client name.
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	

Column Label	Description
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: <ul style="list-style-type: none"> ▪ Wi-Fi 5— 802.11ac standard. ▪ Wi-Fi 4— 802.11n standard. NOTE: The Wi-Fi standard will not be displayed for legacy Wi-Fi clients using 802.11b or 802.11g standards.
AP Radio	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: <ul style="list-style-type: none"> ▪ 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
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.
Application Data Usage (only for wireless clients)	
Top Application Category	This section displays the data usage by the client, for various application categories. The categories that are visited by the client is also represented by a pie chart. This is displayed only for wireless clients.

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 5 *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

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

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




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

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.
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.
Connection Health	Denotes the health status of the wired client.
Status	Represents the ratio of the number of error packets on all the packets. <ul style="list-style-type: none"> ■ Good—In full duplex mode, the error rate is less than 0.1%. In half duplex mode, the error rate is less than 2%. ■ 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. Click the **Clients**  tile on the Instant On home page. The **Clients** page is displayed.
2. In the **Connected clients** list, hover the cursor over the wired client. A power cycle () button is displayed at the end of the row.
3. Click the () button to power cycle the wired client. The port will then be sequentially powered off and then be powered on. The **Duration** column displays a message that the client is being power cycled.



The PoE supplier should be an Instant On device.

Watchlisted Clients

The client watchlist feature allows you to monitor the status of the wired or wireless clients connected to the Instant On devices. After the client is added to the watchlist (☆), an alert is triggered when the watched client goes offline and is cleared if the client comes back online or removed from the watchlist.



You can add a maximum of 128 wired or wireless clients to the watchlist.

The following procedure describes how to add a client to the watchlist:

1. Click on the **Clients** (📄) tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Connected clients** tab to view the list of connected clients.
3. Hover the cursor over a wired or wireless client. A watchlist icon (☆) is displayed at the end of the row.
4. Click watchlist (📄). The client is added to the **Watchlisted clients**(☆) list.

The following procedure describes how to remove a client from the watchlist:

1. Click on the **Clients** (📄) tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Watchlisted clients** (☆) tab to view the list of clients added to the watchlist.
3. Hover the cursor over a wired or wireless client. An Unwatchlist icon is displayed at the end of the row.
4. Click Unwatchlist (📄). The client is removed from the **Watchlisted clients** list.

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



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

Changing Account Password

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

1. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. Under **Password and Security** > **Password**, enter your current password, followed by a new password.
3. Click **Change password** to save your changes.

The **Account management** page 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. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. Under **Password and Security** > **Two-Factor Authentication**, select **Set up two-factor authentication**.
3. Under **Validate Password**, enter your current Instant On account password.
4. Tap **Validate password**.
5. Under **Authenticator**, copy the key provided below and manually enter it in the authenticator app, or scan the QR code using the authenticator app.

6. Click **Continue**.
7. Enter a **Recovery email** you can use to sign in when having trouble using the authenticator app.
8. Re-enter the recovery email.
9. Enter the One-time password generated by your authenticator app.
10. Click **Activate two-factor authentication**.



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 web application.

Deactivating Two-Factor Authentication

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

1. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. Under **Password and Security**, click the settings icon (⚙️) beside **Two-Factor Authentication** and select **Disable two-factor authentication** from the drop-down list. A **Confirmation** popup is displayed on the page.
3. Click **Disable**.

Changing the Recovery Email Address

Once the two-factor authentication has been activated, you have the option to change the recovery email address used to sign in when having trouble using the authenticator app.

The following procedure describes how to change the recovery email address:

1. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. Under **Password and Security**, click the settings icon (⚙️) beside **Two-Factor Authentication** and select **Change recovery email** from the drop-down list.
3. Enter the **New recovery email** address.
4. **Confirm new recovery email** by re-entering the new email address.
5. Click **Change recovery email** to apply the changes



Notifications

Notifications are push 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.

Notifications in web application is displayed as an alert (🔔) in the page header. If no action is taken on the alert, the notification remains in the alert 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. Click on the account name displayed on the header and select **Account management** from the drop down menu. The **Account management** page is displayed
2. In the **Account management** page, select **Notifications** to view notifications options.
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. You will receive notifications on your mobile device or email when the selected alert is triggered in the site. For more information on viewing and managing alerts, see:

- [Viewing and Managing Alerts using the Web Application](#)



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](#)
- [Client Watchlisted](#)

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 maximum 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](#).

The user is also notified if a device at the site did not succeed in installing the new software.

Client Watchlisted

Enabling this option will trigger a notification when a watchlisted client goes offline. The notification is triggered individually for each client when its status changes. This alert is cleared from the site when the client reconnects again.

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. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. In the **Account management** page, click **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.



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

- b. Under **Validate your country**, click 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, click 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. Click on the account name displayed on the header and select **Account management** from the drop-down menu. The **Account Management** page is displayed.
2. In the **Account management** page, click **Delete Account**.

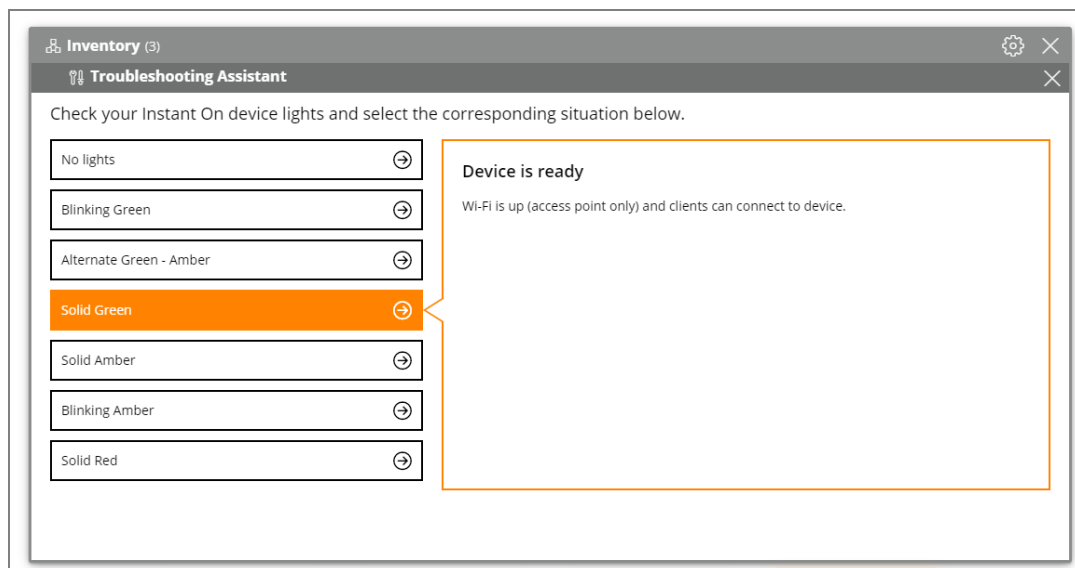
3. In the **Delete Account** page, select the checkbox beside **Permanently delete all my account data, including associated sites and device configurations**. The **Delete Account** button becomes active.
4. Click the **Delete Account** button.
5. A pop-up is displayed on the screen with a warning sign indicating the account will be permanently deleted, in addition to a code.
6. Enter the code in the text box below and click **Delete** to permanently delete your Instant On account.

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.

Figure 6 *Troubleshooting Assistant Page*



5. Check the status of the LED lights on the Instant On and select the corresponding situation in the troubleshooting assistant. The assistant will recommend a troubleshooting action to resolve the alert.
6. If you are unable to find a solution to the problem, navigate to the following link to view additional support options.
 - [Help in the Web Application](#)