

Aruba Instant On 2.1.0

User Guide

MOBILE APP VERSION



Copyright Information

© Copyright 2020 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	7
Aruba Instant On Solution	8
Key Features	8
Supported Devices	8
Whats New in this Release	10
New Features and Hardware Platforms	10
Aruba Instant On Deployment Concepts	12
Wireless Deployment—Access Point Only	12
Wired Deployment—Switch Only	12
Wired and Wireless Deployment—Access Point and Switch	12
Provisioning your Aruba Instant On Devices	14
Downloading the Mobile App	14
Setting Up Your Wireless Network	15
Setting Up Your Wired Network	16
AP Configuration Modes	17
Local Management for Switches	18
IP Assignment for Access Points	20
Discovering Available Devices	21
Multiple Sites	22
Deploying Multicast Shared Services	23
Accessing Aruba Instant On Application	24
Managing Sites Remotely	26
Aruba Instant On User Interface	27
Configuring Menu Items in the Header	28
Configuring Settings in the Modules	29
Site Management	30
Administration Settings	30
Time Zone Settings	31

About Software	31
Monitoring Site Health	33
Alerts	33
Viewing and Updating Inventory	35
Adding a Device	35
Types of Devices	35
Extending your Network	36
Radio Management	38
Access Point Lights	38
Loop Protection	38
Access Point Details	39
Router Details	41
Switch Details	45
Auto-Detection and Auto-Configuring of Switch Ports	50
Configuring Networks	52
Employee Network	53
Guest Network	59
Wired Network	64
Analyzing Application Usage	68
Viewing Application Information	70
Viewing and Blocking Application Access	72
Managing Clients	73
Viewing AP Clients	73
Wired Clients	75
Managing Your Account	78
Modifying Administrator Account Information	78
Alert Categories	79
Managing AP Firmware Upgrades	80
Upgrading the Firmware for an Instant On AP or Switch	80
Instant On Image Server	80
Updating the Software Image on an Instant On Site	80
Verifying Client Connectivity During Upgrade	81
Troubleshooting	82

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 02	Support for AP22 access point and Wi-Fi 6 enabled networks was added.
Revision 01	Initial release.

This User Guide describes the features supported by Aruba Instant On 2.1.0 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 2.1.0 product documentation includes the following:

- [Aruba Instant On Access Point Hardware Documentation](#)
- [Aruba Instant On Release Notes](#)
- Aruba Instant On 1930 Switch Series Management and Configuration Guide
- Aruba Instant On 1930 Installation and Getting Started Guide

Contacting Support

Table 2: *Contact Information*

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

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

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

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

Key Features

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

- [Monitoring Site Health](#)
- [Configuring Networks](#)
- [Analyzing Application Usage](#)
- [Managing Clients](#)
- [Managing Sites Remotely](#)

Supported Devices

Aruba Instant On currently supports the following devices:

Indoor Instant On Access Points

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

Outdoor Instant On Access Points

- Aruba Instant On AP17 Access Points

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

- [Aruba Instant On Hardware Documentation](#)
- [Buy Now from a Local Reseller](#)

Instant On Switches

- Aruba Instant On 1930 8G 2SFP Switch
- Aruba Instant On 1930 8G Class4 PoE 2SFP 124W Switch
- Aruba Instant On 1930 24G 4SFP/SFP+ Switch
- Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch
- Aruba Instant On 1930 24G Class4 PoE 4SFP/SFP+ 370W Switch
- Aruba Instant On 1930 48G 4SFP/SFP+ Switch
- Aruba Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch

Whats New in this Release

This section lists the new features, enhancements, and hardware platforms introduced in Aruba Instant On 2.1.0.

New Features and Hardware Platforms

Instant On WLAN Features

Table 3: *New Features for WLAN Deployments in Instant On 2.1.0*

Feature	Description
Enhancements to Clients Details Page	The security standard, Wi-Fi standard, and radio band information of the client is now displayed in the client details page.
Enhancements to Network Scheduling	Networks can now be scheduled to end at a particular time on the next day. Prior to this release, end time configuration was limited to midnight of the same day.
Radio Power Information	The Instant On UI now displays the radio power information used by the device.
Redirect URL for Internal Captive Portal	Guest clients can now be redirected to a custom URL after accepting the terms and conditions when internal captive portal is used.
Support for New AP Platform	A new Indoor AP platform AP22 is supported by Instant On.
Software Update Enhancements	The software update page now displays the highlights of what is included in the software update and the countdown for the update.
Static IP Configuration for Access Points in the Provisioning Page	IP assignment settings in the provisioning page of the local webUI provides an option to configure a static IP address for the access point.
Wi-Fi 6 Enabled Networks	Wi-Fi 6 (802.11ax) capabilities can be enabled on Instant On networks. This feature is only available when the device inventory has at least one Instant On AP22 access point.
Zoox Captive Portal	Zoox captive portal is added as an external captive portal provider.

Instant On Wired Features

Table 4: *New Features for Wired Deployments in Instant On 2.1.0*

Feature	Description
Connected Clients and Devices on Switch Ports	The Instant On UI now displays the list of clients and devices that are connected to a specific port.
Configuring Network Security on Wired Networks	Network security can be enabled on the Instant On wired network to prevent DHCP and ARP attacks on the switch ports.
Configuring Wired Access Rules	The Network Access option in the Instant On UI allows you to configure network access restrictions for wired clients based on IP destination addresses.

Table 4: *New Features for Wired Deployments in Instant On 2.1.0*

Feature	Description
<u>Enabling or Disabling a Wired Network</u>	The wired networks configured on the site can now be enabled or disabled as required.
<u>Notification Alert When Switch Exceeds Power budget</u>	Instant On now sends a notification when the Switch reaches the maximum power allocated and cannot power new devices through PoE. This alert can be enabled or disabled as required.
<u>Switch Port Auto Detection and Auto Configuration</u>	Instant On now supports auto-detection and auto-configuration if two or more Instant On devices are connected to each other through a common switch port.

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.

This chapter describes the following procedures:

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

Downloading the Mobile App

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

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

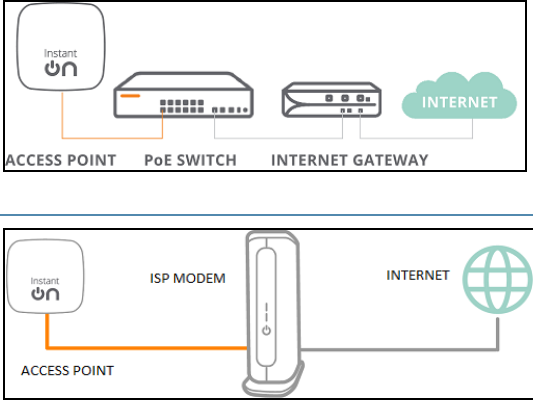
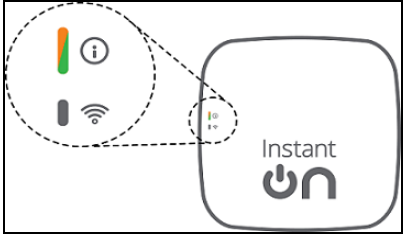


1. Download the app on your smartphone
 - To install the app on iPhone, go to [Apple App Store](#) and search for Aruba Instant On.
 - To install the app on Android phones, go to [Google Play Store](#) and search for Aruba Instant On.
2. Launch the Instant On application and follow the on-screen instructions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

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

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.

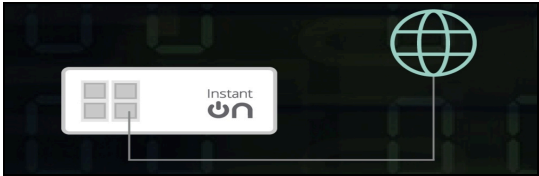
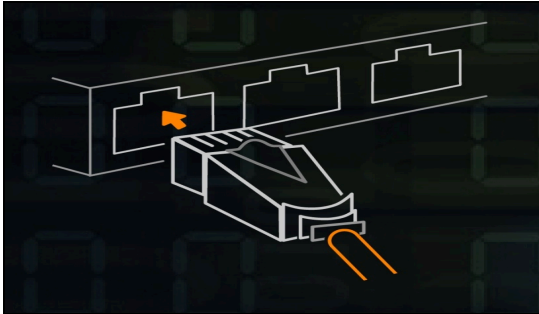
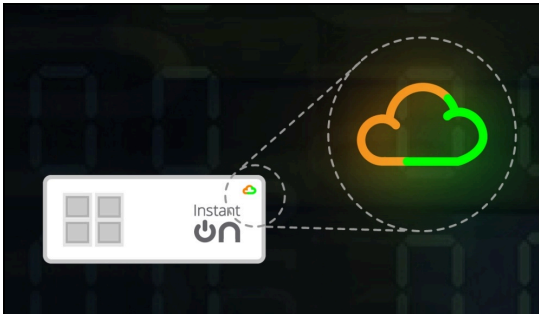


Table 5: *Instant On Wireless Network Provisioning*

SL No	Steps	Illustration
1.	<p>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).</p> <p>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.</p>	
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 6: *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 7: *Cloud LED and AP LED Light Status*

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

AP Configuration Modes

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

- [Private Network Mode](#)
- [Router Mode](#)

Private Network Mode

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

Pre-Requisites

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

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

Configuring Your Instant On Devices in Private Network Mode

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

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

Router Mode

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

Pre-Requisites

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

- A working internet connection provided by your Internet Service Provider (ISP).
- TCP ports 80 and 443 and UDP port 123 should not be blocked by a firewall.
- The Instant On AP must be directly connected to the internet modem with no other device in between. It must therefore be the only AP connected to the internet. Other APs have to be powered down initially and added later through mesh using the extend network capability.

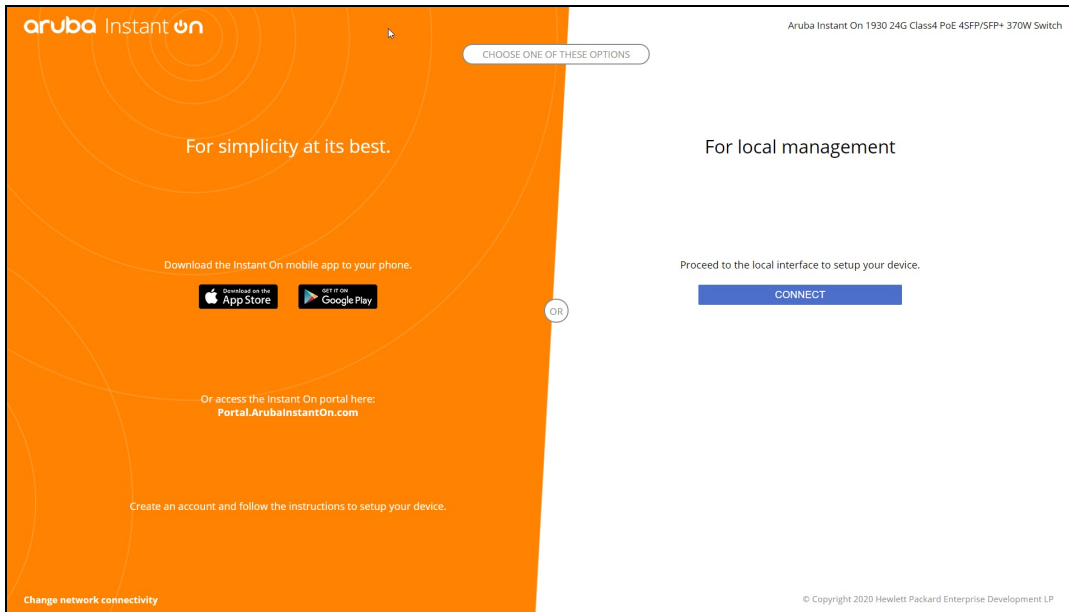
Configuring Your Instant On Device in Router Mode

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

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

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 mobile app once the local management for the switch is selected. The switch needs to be reset to factory default from the local WebUI to switch to the cloud management mode.

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

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

Switch Provisioning Using the Local WebUI

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

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

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

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

IP Assignment for Access Points

The IP address for the access point can be assigned using the local WebUI during onboarding.

The 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 AD:CD:EF corresponds to the last three octets of the MAC address of the AP.
3. Connect your laptop or mobile device to the SSID and access the local web server through **https://connect.arubainstanton.com**. The local WebUI configuration page is displayed.
4. In the **IP addressing** section, configure either of the following options to assign an IP address for the access point:
 - a. **Automatic (default)**: The DHCP server assigns an IP address for the access point. This option is selected by default.
 - b. **Static**: To define a static IP address for the access point, specify the following parameters:
 - i. **IP address**—IP address for the access point.
 - ii. **Subnet mask**—Subnet mask.
 - iii. **Default gateway**—IP address of the default gateway.
 - iv. **DNS server**—IP address of the DNS server.
 - c. **PPPoE**: The ISP assigns an IP address for the access point. This option is configurable only on AP11D access points when it is functioning as the primary router for the network. For more information on configuring PPPoE, see [Setting Up WAN Connectivity for Your Network](#).
5. 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

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

Follow the steps below to configure PPPoE on your network:

1. The Instant On AP should be connected to the ISP provided modem but does not have an IP address provided by the DHCP server.
2. 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 AD: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**, select the **PPPoE** radio button.
5. Enter the PPPoE **Username**, **Password** and **MTU** provided by your ISP, in the respective fields.
6. Click **Apply**. The AP will reboot once the PPPoE configuration is applied.
7. Wait for the LED lights to flash green and orange. This indicates that the PPPoE link is up and stable, you will see the device onboarding status now reads **"Waiting to be onboarded.."**. This step might take an additional five minutes, if the AP upgrades its firmware during the reboot process.
8. You can now proceed to creating a new site and adding devices. For more information, see:
 - [Setup a New Site using the Mobile App](#).



If an AP with the PPPoE configuration is removed from the Inventory or the site is deleted, the AP will move to its 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 or web application scans for nearby devices through BLE and displays the APs discovered, on the screen. Tap or click the **Add devices** button to add the devices discovered to the site. Alternatively, click **Search again** if there are more devices to be displayed. If the BLE scanning fails to discover any devices in the vicinity, tap the **Add devices manually** tab and choose to add devices to your network by entering the serial number or by scanning the barcode of the AP.
- **Serial Number**— Enter the serial number located at the back of your Instant On AP 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.


BLE Troubleshooting

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

Multiple Sites

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




Account Management

In case of multiple sites, select the advanced menu () icon on the **My Sites** screen. Else, tap the icon with an alphabet, on the mobile app header. The **Account Management** page is displayed. For more information, refer to [Managing Your Account](#).



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



Setup a New Site

1. To register a new Instant On site to your account, tap the advanced menu () icon and select  **Setup a new site**. You will be redirected to the initial setup page.
2. Follow the instructions given in [Setting Up Your Wireless Network](#) to add a new Instant On site.
3. If you already have more than one site configured, and would like to setup a new site under your registered account, tap the advanced menu () icon in the **My Sites** screen.

Sign Out

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

Help & Support

Tap the advanced menu () icon and select () help to launch **Help & Support** page. Following are the available technical support options:

- **Help center**—Opens the Aruba Instant On documentation portal. For more information, see <https://www.ArubaInstantOn.com/docs>.
- **Community** - Provide a place for members or participants to search for information, read and post about topics of interest, and learn from each other. For more information, see <https://community.arubainstanton.com/>.
- **Support center**—Opens the Aruba Instant On Support Portal, which provides information on warranty and support policy for the product you selected and also the on-call technical support. For more information, see <https://community.arubainstanton.com/t5/Support/ct-p/Support>.
- **Support resources**—Allows you to generate a support ID by clicking on the **Generate Support ID** button. The ID is then shared with Aruba Support personnel to run a diagnosis on your device.

Deploying Multicast Shared Services

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

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

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

Private Network Mode

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

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



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

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

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



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

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

Router Mode

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

- The networks can be configured either as employee network or guest network.
- Devices offering the service and clients using the service must be connected to the same Wi-Fi Network or different networks with same VLAN ID.

- The **IP and network Assignment** settings must be set to **Same as local network (default)**. You can assign a different network if required by your local network. For information on IP and network settings, see [IP and Network Assignment](#).
- The **Network Access** setting must be set to **Unrestricted access**.
- Alternatively, if an AP11D is used as the primary Wi-Fi router, the clients and services connected to ports E1, E2, E3 are also supported. In the case of wired network, , the cross-vlan services will always be able to access.

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

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



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

Examples

Following are some of the examples for deploying multicast services:

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

Accessing Aruba Instant On Application

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

Mobile OS Requirements

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

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

Browser Requirements

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

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

Create an Instant On Account

Follow these steps to create an Instant On account:

1. Open a browser.
2. Type **https://portal.arubainstanton.com** in the address bar and press the **Enter** key.
3. Click **Create an account** 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 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 **Log 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.

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



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

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.

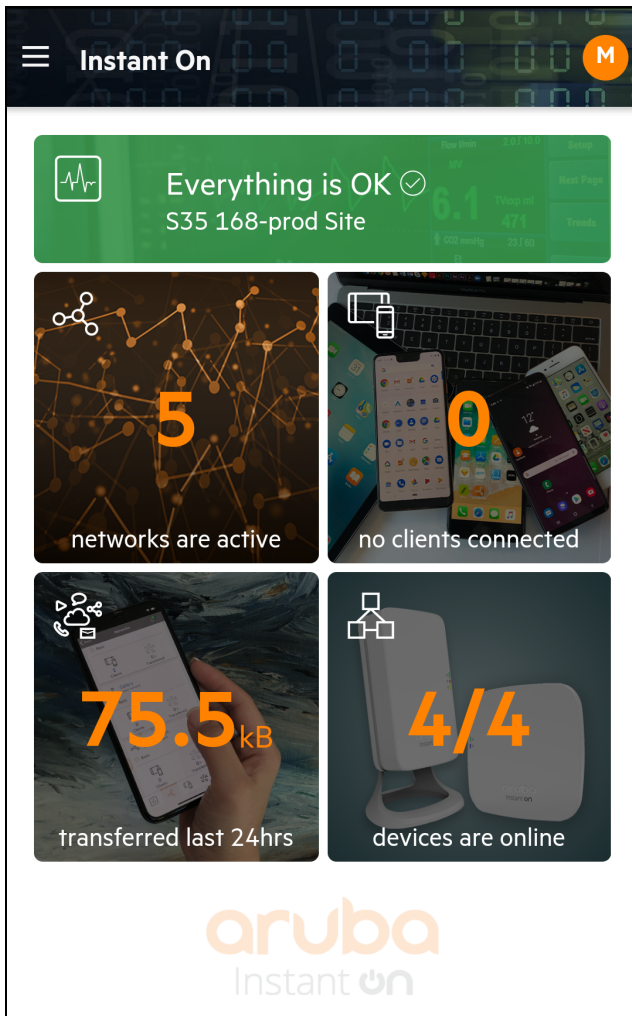
Username and Password Management

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.

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

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

Figure 1 Mobile App User Interface Overview



Configuring Menu Items in the Header

The header includes the following menu items:

Table 8: *Menu Items in the Header*

Header Content	Description
Alert Notification (🔔)	Displays the alerts that are triggered by the system when an unusual activity is observed on the network. See Alerts for more information.
Advanced menu icon (☰)	<p>Displays the site name and provides menu options to administer your account and the sites associated with it.</p> <p>Help & Support (🔍)—Leads you to the Contact support page. Following are the available technical support options:</p> <ul style="list-style-type: none"> ■ Help center—Opens the Aruba Instant On documentation portal. For more information, see https://www.ArubaInstantOn.com/docs. ■ Support center—Opens the Aruba Instant On Support Portal, which provides information on warranty and support policy for the product you selected and also the on-call technical support. For more information, see https://community.arubainstanton.com/t5/Support/ct-p/Support. <p>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.</p> <p>Site management—Allows you to modify various account settings, including time zone and notifications. For more information, see Site Management.</p> <p>Add a new device—Opens the Extend my network page and allows you to add a new device. For more information, see Extending your Network.</p> <p>Connect to another site—Allows you to connect to another Instant On account. After clicking Connect to another site, you are logged out of your account and automatically redirected to the Aruba Instant On login page. Enter the registered email ID and password to access the respective Aruba Instant On. If you have multiples sites configured under the same administrator account, you will be redirected to the My Sites page from where you can select one of the listed sites.</p> <p>Setup a new site—Allows you to setup a new Aruba Instant On site. For more information, see Setting Up Your Network.</p> <p>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/.</p> <p>About—Provides information about the software currently installed on the mobile app, and also the following information:</p> <ul style="list-style-type: none"> ■ End User License Agreement ■ Data Privacy Policy and Security Agreement
Registered email ID NOTE: The alphabet displayed is the first letter of your email ID.	<p>Displays the account username registered email ID and provides options to administer account information and setup notifications or alerts.</p> <p>Account management—Allows you to modify your account information for all associated sites. For more information, see Managing Your Account.</p> <ul style="list-style-type: none"> ■ Change password—Allows you to modify the password for the account. For more information, see Managing Your Account ■ Notifications—Allows you configure the notification settings for the alerts received from the site. For more information, see Alert Categories. <p>Sign out—Allows you to log out of your Aruba Instant On account.</p>

Configuring Settings in the Modules

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






The Instant On user interface consists of the following modules:

- **Site Health:** Provides the health status of devices connected to the network. See [Monitoring Site Health](#) for more information on the **Site Health** module.
- **Networks:** Provides a summary of the networks that are available for primary and guest users. See [Configuring Networks](#) for more information on the **Networks** module.
- **Clients:** Provides connection information for the clients in your network. See [Managing Clients](#) for more information on the **Clients** module.
- **Applications:** Provides daily usage data for the different types of applications and websites accessed by clients in the network. See [Analyzing Application Usage](#) for more information on the **Applications** module.
- **Inventory:** Specifies the number of devices on the site that are UP. This page also allows you to add a new device or remove an existing device. See [Viewing and Updating Inventory](#) for more information on the devices on the site.

Opening a Module

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

Table 9: *Module Tiles*

Module	Tile
Site Health	
Networks	
Clients	
Applications	
Inventory	

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

Closing a Module

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

Site Management

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

- Administration
- Time zone
- 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 provide you with the option to configure Facebook Wi-Fi service to connect to the Internet. This is used in Guest networks without the need for a secured password for authentication. See [Enabling Guest Portal](#), for more information.

Software Update

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

Administration Settings

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

Modifying the Aruba Instant On Site Name

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



1. Tap the advanced menu (☰) icon, and then select **Site management**. The **Site Management** screen displays the account administration settings.
2. Enter a new name for the Aruba Instant On site under **Site name**.



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



Adding a Secondary Account

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

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

Transferring Account Ownership

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

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

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


Time Zone Settings

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

- Displaying daily statistics for your network.
- Enforcing network availability schedules.
- Performing daily image checks on the Aruba Instant On image server.


Setting a Local Time Zone

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

1. Tap the advanced menu () icon on the Aruba Instant On home screen. From the **Site Management** screen, tap **Time zone** to open the **Time Zone** screen.
2. Select a time zone from the **Site local time zone** drop-down list.

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

About Software




The **About** page provides information about the software currently installed on the web application. To view the following information in the **About** page, tap the advanced menu () icon from the title bar and select **About** from the drop-down menu:

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



The **Site Health** page provides a summary of the health status of the Instant On devices connected to the network. It shows a consolidated list of alerts that are triggered from the devices provisioned at the site. It also displays the inventory details of the connected devices and real-time data of active client connections on an hourly basis with the cumulative transfer speed of all the devices.

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

Table 10: *Site Health Messages*

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

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

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

Registered devices send or receive notifications when an alert is triggered by the Instant On due to an unusual activity on the site. For information on how to enable or disable notifications for alerts, refer to [Alert Categories](#).


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



Tap [Show all alerts](#) to view the list of alerts received on the site.

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


Alerts

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

The **Alert** () icon appears on the title bar of the mobile app when there is a pending alert. The number of alerts in the system is displayed as a colored badge on top of the **Alert** (

 icon. The color of the badge determines the severity of the alert present in the system. When there are no alerts present in the system or all the alerts have been acknowledged, the **Alert** () icon will not appear in any of the title bars on the mobile app.

To view the Alert history, follow these steps:


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



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.





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

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

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



The following table lists icons and their corresponding status:

Table 11: *Device Status*

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

Adding a Device

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

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

Types of Devices

Instant On supports three types of devices:

- [Access Points](#)
- [Routers](#)
- [Switches](#)

Extending your Network

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

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

Extend using a cable

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

1. In the **How to Extend your Network** page, choose **Extend using a cable**.
2. To ensure optimal performance, connect your additional Instant On devices to the same switch as the first AP, using network cables. Power on the AP using Power over Ethernet (PoE) or DC power adapter (if you have ordered for it with the installation kit).
3. Wait for the LED lights on the additional Instant On devices to blink alternatively between green and amber.
4. Select **Search for my device** to make the Aruba Instant On scan for both wired and wireless devices. The Instant On device(s) should show up in the list of devices detected in the network.
5. Review the device(s) discovered and add them to your site.
6. If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.

Extend over the air

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

1. In the **How to Extend your Network** page, choose **Extend over-the-air**.
2. Connect at least one Instant On AP to a local wired switch or a router and ensure that the initial setup is complete.
3. Place a wireless Instant On AP in a location within the Wi-Fi range and power it on. For more information, see [Instant On AP Wireless Access Point Placement Guidelines](#).



Ensure the wireless AP is in its factory default state and is not connected to a network using an Ethernet cable.

4. Wait for the LED lights on the wireless Instant On AP(s) to blink alternatively between green and amber.
5. Select **Search for my device** to make the Aruba Instant On scan for both wired and wireless devices. The AP should show up in the list of devices detected in the network.
6. Review the device(s) discovered and add them to your site.
7. If you still cannot find your device, click **I don't see my device** to view the troubleshooting options.

Instant On AP Wireless Access Point Placement Guidelines

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

- **Interfering sources or obstacles**—Check for interfering sources or obstacles and install the APs on a ceiling or a wall.

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



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

Deployment Scenarios for Outdoor Access Points

The versions prior to Instant On 1.4.0, includes both indoor and outdoor APs. However, the user interface did not allow specifying whether an AP is configured for servicing indoor or outdoor environments. In the case of an outdoor AP such as AP17 being setup as a mesh point, it may experience service disruptions if all the surrounding APs are indoor units since many regulatory domains reduce the available channels for outdoor use. The result is that the indoor AP may choose to use a channel that is unavailable to the outdoor AP and hence, the AP17 mesh point will never be able to connect to the mesh portal. The following deployment scenarios for Outdoor APs help mitigate these problems:

Scenario 1: Provision a Site on the Outdoor AP Channel

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

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

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

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

Scenario 3: Existing sites with Mesh outdoor Access Points

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


Scenario 4: Deleting Last Outdoor Mesh Point

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

Radio Management

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


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

1. Tap the **Inventory** tile on the Aruba Instant On Portal home page or tap the **Site Health** banner and select **Show inventory**
2. Tap the advanced menu () icon and select **Radio management**.
3. Choose an option for the **Channel width** and **Channel selection** for the 2.4 GHz and 5 GHz Radios. Based on your **Channel width** selection, the **Channel selection** options will be refreshed and the changes are saved automatically.

Access Point Lights

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

Follow these steps to turn or off the access point lights:

1. Tap the **Inventory** tile on the Aruba Instant On Portal home page or tap the **Site Health** banner and select **Show inventory**
2. Tap the advanced menu () icon and select **Access Point Lights**.
3. Choose one of the following options:
 - **Normal mode (default)**— Use this option to turn on the status and radio lights. This option is selected by default.
 - **Quiet light mode**—Use this option to turn off the status and radio lights. When this option is selected, the device lights are turned off during normal operation.

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

Rapid Spanning Tree Protocol (RSTP)

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

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

Follow these steps to enable RSTP on the network:



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

Access Point Details

The **Access Point Details** page provides details of the selected AP, which includes the AP name, IP address, MAC address, serial number, radio, ports, and model type of the AP. This page also provides a summary of the wireless radios including the number of clients that are currently connected.


Viewing Access Point Details

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

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

Connectivity

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

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

Ports

Every network requires the E0/PT or ENET port of the AP or Router to be connected to the gateway or switch using an Ethernet cable. Each Instant On AP has a single E0/ENET port. To view the details of the port and the uplink status, follow these steps:

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

Port Details

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



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

Connected Clients and Devices

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

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

Radios

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

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

Advanced Menu

Locating Your Instant On AP

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

To locate your Instant On AP, follow these steps:

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

Restarting Your Instant On AP


To restart your AP, follow these steps:

1. Tap the advanced menu (⋮) icon in the title bar of the **Access Points Details** screen.

2. Select **Restart** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Restart**.

Removing an AP from the Inventory

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

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

Follow these steps to remove an AP which is offline:

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



1. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity.
2. To remove the access point from the inventory, follow these steps:
 - a. If the Instant On device is removed from the network, you can choose to remove the device from the inventory by tapping **Remove from inventory** in the **Access Point Details** page. A pop-up box appears on the screen requesting your confirmation.
 - b. Tap **Remove** to delete the device from the inventory.

Router Details

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

Viewing Router Details

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

1. Tap the **Inventory**() tile on the Aruba Instant On home page or tap the **Site Health**() banner and then tap **Show inventory**.
2. Tap any of the AP11D routers listed in the **Inventory** list. The **Router Details** page is displayed with details. View the Router details such as the Router name, IP address, MAC address, Serial number, Router type, radio, and the number of the clients connected on each radio channel.

Connectivity

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

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

1. Under the **Connectivity** section of the **Router Details** page, tap **Internet connectivity**.
2. In the **Internet Connectivity** page choose any of the following options to connect to the Internet.
 - a. **Automatic**: The router will use DHCP protocol and obtain an IP address from your Internet Service Provider. This option is selected by default.
 - b. **Static**: Allows you to specify the IP address for the router and other network parameters for Internet connectivity. You will have to define the following parameters if this option is selected:
 - i. **WAN IP**—Enter a Static IP address.
 - ii. **Subnet mask**—Enter the subnet mask.
 - iii. **Default gateway**—Enter the IP address of the Default Gateway.
 - iv. **DNS server**—Enter the IP address of the DNS server.
 - c. **PPPoE**: Enter the username and the password provided by your ISP to connect to the Internet. This setting cannot be modified through this page. To change PPPoE settings, you must disconnect the device from the Internet and change the credentials through the provisioning page. For more information, see [IP Assignment for Access Points](#).
3. Tap **Ok**.

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

1. Under the **Connectivity** section of the **Router Details** page, tap **Local network connectivity**.
2. Enter the **Base IP address**.
3. Under **Subnet mask**, tap the drop-down arrow (▼) and select the IP address range for the network.
4. Tap **Ok**.

Ports

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

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

Status









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

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

Port Details

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

- Name of the port in read and write mode.

- A toggle switch that allows you to set the port status to **Active** () or **Inactive** (). This field is set to **Active** by default.
- **Port access control (802.1X)**—Configures port-based network access control designed to enhance 802.11 WLAN security. This field consists of a toggle switch which can be active () or inactive ().
 - Inactive ()—The toggle switch is set to inactive by default. This indicates that any client can connect to this port without requiring authentication.
 - Active ()—Indicates that the first device connected to the port must be authenticated prior to using the port. Configure the following RADIUS settings when this option is enabled:
 - **Primary RADIUS Server**—Configure the following parameters for the **Primary RADIUS Server**. If you are using the Instant On mobile app, tap **More RADIUS parameters** to view the below settings.
 - **RADIUS Server IP address**—Enter the IP address of the RADIUS server.
 - **Shared secret**—Enter a shared key for communicating with the external RADIUS server.
 - **Server timeout**—Specify a timeout value in seconds. The value determines the timeout for a RADIUS request. The Instant On device attempts to send the request several times (as configured in the **Retry count**) before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
 - **Retry count**—Specify a number between 1 and 5. Retry count indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
 - **Authentication port**—Enter the authentication port number of the external RADIUS server within the range of 1–65535. The default port number is 1812.
- To configure a **Secondary RADIUS Server**, slide the toggle switch to the right () and update the required fields.
- To **Send RADIUS Accounting** requests, slide the toggle switch to the right ().
- Tap **Done**.
- **Included networks**—This section includes the following configuration settings:
 - **All networks (default)**—The user can assign network traffic based on the VLAN tag or through the default network. By default, all ports assigned traffic from all networks are based on the VLAN tag.
 - **Default network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others.

Networks

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

1. Tap any of the AP11D routers listed in the **Inventory**. The **Router Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the router.
3. From the **Selected network** drop-down list, choose the network you want to map a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
 - **All networks (default)**—The user can assign network traffic based on the VLAN tag or through the default network. By default, all ports assigned traffic from all networks are based on the VLAN tag.
 - **Default network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others.

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

Connected Clients and Devices

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

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

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.

Advanced Menu

Locating Your Instant On Router

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

To locate your Instant On device, follow these steps:

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

Restarting Your Instant On Router

To restart your AP, follow these steps:


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

Replacing a Router from the Inventory

Instant On allows you to replace a router from the inventory when it goes offline. A new AP11D router or any existing router from the site can be used to replace your old router. The old router needs to be manually reset to use as a normal AP.

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

1. Tap the **Inventory** (🏠) tile on the Instant On Solution home page or tap the **Site Health** (📶) banner and then click on **Show inventory**. The **Inventory** page is displayed.



2. Tap the offline router that you want to replace. The **Router Details** page is displayed. A rectangular bar appears below the device name when an alert is triggered.
3. Tap the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the router.
4. In the **Alert Details** page, tap on the replace link. The **Replace router** page is displayed. Alternatively, you can also perform this action by tapping the advanced menu () icon in the title bar of the **Router Details** screen and selecting **Replace hardware** from the menu.
5. Unplug the router you want to replace and plug in your new Instant On AP11D device into your ISP modem.
6. When your device lights are alternating between green and amber, tap **Continue**. The mobile app begins BLE scanning to discover your new router. It usually takes around 4-5 minutes for the router to be detected.
7. Once your router is detected, tap **Replace** to configure the device as your primary Wi-Fi router. **NOTE:** If the mobile app detects more than one primary Wi-Fi router in the area, you will see a message stating that more than one router is detected. In this scenario, keep the preferred router plugged and unplug the remaining routers from the network.
8. If the BLE scanning fails to discover your router in the vicinity, tap the **Add Wi-Fi router manually** button and choose to add your router to your network by entering the serial number or by scanning the barcode of the router.
9. If you still cannot find your device, select **I don't see my Wi-Fi router** button to view the troubleshooting options.

Switch Details

The **Switch Details** page provides details of the selected switch.

Viewing Switch Details

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

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

Power over Ethernet (PoE)



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

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

Ports

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

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

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

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

- Status
- Link Aggregation
- Networks

Status

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

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





The following table displays the status of the switch ports:



Table 12: *Switch Port Status*


Status	Definition
Disconnected	The switch port is enabled, but does not have an Ethernet cable connected.
Inactive	The switch port has been disabled by the administrator.
Suspended	The switch port has encountered an error and may or may not be active.
PoE	The switch port is supplying Power over Ethernet
Loop	A loop is detected on the port
Uplink	The uplink port that is used to connect to the internet.


Port Details

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

- Name of the port in read and write mode.
- A toggle switch that allows you to set the port status to **Active** () or **Inactive** (). This field is set to **Active** by default.
- **Port access control (802.1X)**—Configures port-based network access control designed to enhance 802.11 WLAN security. This field consists of a toggle switch which can be active () or inactive (.


- Inactive ()—The toggle switch is set to inactive by default. This indicates that any client can connect to this port without requiring authentication.
- Active ()—Indicates that the first device connected to the port must be authenticated prior to using the port. Configure the following RADIUS settings when this option is enabled:
 - **Primary RADIUS Server**—Configure the following parameters for the **Primary RADIUS Server**. If you are using the Instant On mobile app, tap **More RADIUS parameters** to view the below settings.
 - **RADIUS Server IP address**—Enter the IP address of the RADIUS server.
 - **Shared secret**—Enter a shared key for communicating with the external RADIUS server.
 - **Server timeout**—Specify a timeout value in seconds. The value determines the timeout for a RADIUS request. The Instant On device attempts to send the request several times (as configured in the **Retry count**) before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
 - **Retry count**—Specify a number between 1 and 5. Retry count indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
 - **Authentication port**—Enter the authentication port number of the external RADIUS server within the range of 1–65535. The default port number is 1812.

To configure a **Secondary RADIUS Server**, slide the toggle switch to the right () and update the required fields.

To **Send RADIUS Accounting** requests, slide the toggle switch to the right ().

Tap **Done**.

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**—This section includes the following configuration settings:
 - **All networks (default)**—The user can assign network traffic based on the VLAN tag or through the default network. By default, all ports assigned traffic from all networks are based on the VLAN tag.
 - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag.
 - **Tagged**—Slide the toggle switch to the right () and tap **Done** to enable this setting. On selecting this option, the port will receive and send traffic from the default network using the management VLAN tag.
 - **Default network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Similar to the **All networks (default)** setting, selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.




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 13: *Switch Ports Aggregation*

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

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

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

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


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

Networks

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

1. Tap any of the switches listed in the **Inventory**. The **Switch Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the switch.
3. From the **Selected network** drop-down list, choose the network you want to map to a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.

6. Select one of the following options, under **Included networks**:

- **All networks (default)**—The user can assign network traffic based on the VLAN tag or through the default network. By default, all ports assigned traffic from all networks are based on the VLAN tag.
 - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag.
 - **Tagged**—Slide the toggle switch to the right (). A popup window appears on the screen. Click **Apply changes** to enable this setting. On selecting this option, the port will receive and send traffic from the default network using the management VLAN tag.
- **Default network only**—On selecting this option, the port's traffic will only be allowed from the default network excluding others. Similar to the **All networks (default)** setting, selecting this option allows you to configure the port settings to **Tagged** or **Untagged**.


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

Connected Clients and Devices

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

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


Advanced Menu

The advanced menu () in the **Switch Details** page provides the following configuration options.

Locating Your Instant On Switch


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

To locate your Instant On switch, follow these steps:

1. Tap the advanced menu () icon in the title bar of the device details page.
2. Tap **Locate**. The locator light is activated on the switch.


Restarting Your Instant On Switch

To restart the device:

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


Removing a Switch from the Inventory

To remove the switch when it is still online:

1. Tap the advanced menu () icon in the title bar of the **Switch Details** screen.

2. Select **Remove from inventory** from the drop-down menu. The appropriate assistant page is displayed.
3. Click **Remove**.


The Instant On switch can be removed from the inventory when it goes offline. On the **Switch Details** page, a rectangular bar appears below the device name when an alert is triggered. The color of the rectangular alert bar will appear according to the alert type.

1. Click the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity.
2. To remove the switch from the inventory, follow these steps:
 - a. If the Instant On switch is removed from the network, you can choose to remove the switch from the inventory by clicking **Remove from inventory** by tapping the advanced menu () icon in the **Switch Details** page.
 - b. Click **Remove** to delete the switch from the inventory.

Switching to Local Management

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

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

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

Connectivity

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

1. Under the **Connectivity** section of the **Switch Details** page, tap **Advanced LAN parameters**.
2. Choose one of the following:
 - **Automatic (default)**: This is the default setting for all APs. The Instant On device will request an IP address from a DHCP service running on the LAN. This option is visible only in the mobile app.
 - **Static**: To specify a fixed IP address on the LAN for your Instant On device, select the **Static** radio button in the mobile app and configure the following parameters:
 - **LAN IP**—Enter a Static IP address.
 - **Subnet mask**—Enter the subnet mask.
 - **Default gateway**—Enter the IP address of the Default Gateway.
 - **DNS server**—Enter the IP address of the DNS server.
3. Tap **DONE** to save the settings.

Auto-Detection and Auto-Configuring of Switch Ports



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

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

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

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

Table 14: Network Information

Parameter	Description
Network Name	Identifies the Instant On network used to connect computers, tablets, or phones together. The network name is also used as the Wi-Fi identifier.
Network type	Indicates if the network is a wired or wireless.
VLAN	Shows the VLAN ID if network is a wired network.
Usage	Indicates if the wireless network is for employees or guests.
Status	Shows the status of the network. Guest networks can be set to Active () or Inactive () by changing the status manually or by creating a network schedule to change the status at a specific day and time. See Guest Network for more details on setting network schedules.
Security	<p>Shows the security option set for the network:</p> <p>Network password (PSK)—Secured using a shared password (PSK). Provides the following security options.</p> <ul style="list-style-type: none"> ■ WPA2 Personal—This is the default setting. ■ WPA2+WPA3 Personal <p>NOTE: The Authentication server (RADIUS) option is displayed only when you click on Use authentication server (RADIUS) instead?.</p> <p>Authentication server (RADIUS)—You must have a RADIUS server available to use this option. Secured using a higher encryption RADIUS authentication server. This option is available only for Employee networks. The following options are available.</p> <ul style="list-style-type: none"> ■ WPA2 Enterprise—This is the default setting. ■ WPA2+WPA3 Enterprise ■ Welcome page—No security. Any user can connect to this network without entering a username or password. This option is available only for guest networks. This network requires Captive Portal to be configured. <p>NOTE: Instant On supports 802.11r and 802.11v fast roaming standards on wireless networks.</p>
Clients	Shows the number of clients currently connected to the network. Tap the 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. Tap the transferred to view an overview of the client and application usage statistics for the network.

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. Tap **Networks** tile on the Instant On mobile app home page.
2. Tap Add (+) and select the **Wireless** tab as the **Network type**. This tab appears only when your site has both wired and wireless networks.
3. Select **Employee**, under Usage to indicate that the network is for an enterprise.
4. Enter a **Network name** for the employee network. This will also be broadcasted as the SSID for the WLAN network.
5. Choose a **Security** level for the network and update the required fields.
 - **Network password (PSK)**—Secures the network using a shared password (PSK). To set the network with password, click the **Password** tab under **Security** and create a password of your choice in the **Network password** field. The following options can be configured.
 - **WPA2 Personal**
 - **WPA2+WPA3 Personal**

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



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


- **Authentication server (RADIUS)**—Secures the network using a higher encryption RADIUS authentication server. Update the following fields:
 - **WPA2 Enterprise**
 - **WPA2 + WPA3 Enterprise**
 - **Server IP address**—Enter the IP address of the RADIUS server.
 - **Shared secret**—Enter a shared key for communicating with the external RADIUS server.
- 6. To configure the other radius parameters, tap **More Radius parameters**. The **Authentication Servers** screen is displayed.
- 7. Configure the following parameters for the **Primary 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.
- **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.



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


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

8. To configure a **Secondary RADIUS Server**, slide the toggle switch to the right () and update the required fields.

9. To **Send RADIUS Accounting** requests, slide the toggle switch to the right () and update the **Accounting Port** field.

10. Click **Save**.





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




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.

11. To configure a **Secondary RADIUS Server**, slide the toggle switch to the right () and update the required fields.

12. To **Send RADIUS Accounting** requests, slide the toggle switch to the right () and enter the —Enter the accounting port number within the range of 1–65,535 in the **Accounting port**. This port is used for sending accounting records to the RADIUS server. The default port number is 1813.

13. Tap the back arrow () to return to the employee network details page.



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

Modifying the Employee Network Name and Password

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

1. Tap **Networks** on the Instant On home screen. The **Networks** screen is displayed.
2. Select the employee network from the **Networks** list to view the **Employee Network Details** screen.
3. Under **Identification**, enter a new name under **Network name** to change the main network name or a new password under **Network password** to change the main network password. A warning message appears, indicating that changes to the network settings will disconnect all clients currently accessing the network.
4. Tap **DONE** to save the settings.

More Options

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

- [IP and Network Assignment](#)
- [Schedule](#)
- [Bandwidth Usage](#)
- [Network Access](#)
- [Wireless Options](#)
- [Shared Services](#)
- [Applications Statistics](#)

IP and Network Assignment

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




- **Same as local network (default)**—This setting is referred to as **Bridged mode**. Clients will receive an IP address provided by a DHCP service on your local network. By default, the default network created during setup is assigned as your local network. To assign other networks, select the network from the **Assigned network** drop-down. The VLAN ID will be assigned to your network based on your network assignment. This option is enabled by default for employee networks.
- **Specific to this 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.

Schedule

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

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



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

3. Slide the toggle switch beside **No schedule** () to the right to enable the network schedule. The **Ruled by a schedule** setting is set to enabled ().
4. Under **Days of the week**, select the day(s) during which the network will be active.
5. Select one of the following options under **Active hours during the day**:
 - **All day**: The network is active throughout the day.
 - **Active between**: The network is only active between the designated **Start Time** and **End Time**. Network access can be configured to end on the same day or the next day. When a time prior to the **Start Time** is selected as the **End Time**, a **Next Day** alert is displayed indicating that the end time is configured on the next day. This enables you to configure scheduled networks for your business when the active hours extend to the early hours of the next day.
6. Tap the back arrow () to return to the **Employee Details** page. Tap **DONE**.

Bandwidth Usage

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



To configure a bandwidth limit, follow these steps:

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

Network Access

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



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

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

Wireless Options



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

Show network

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

Wi-Fi 6

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

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





The Wi-Fi 6 option is only available when the device inventory has at least one Aruba Instant On AP22 access point.

Disable this feature if the client experiences problem connecting to the network.


Radio

Radio settings in the Aruba Instant On 2.1.0 mobile app allows you to configure radio frequencies for your wireless network.

To configure radio frequency, follow these steps:

1. Tap **Networks** () tile on the Instant On home page and select an employee network or guest network from the list.
2. Select the employee or guest network and tap the **More options** drop-down.
3. Tap **Wireless options** and select the radio frequency available under **Radio** tab. The frequency is set to 2.4 GHz and 5 GHz by default. The available frequencies are:
 - **2.4 GHz and 5 GHz (default)**—The AP will broadcast the wireless network on either 2.4 GHz or 5 GHz radio frequencies.
 - **2.4 GHz only**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
 - **5 GHz only**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.
4. The changes are auto saved. Tap the back arrow () to return to the employee or guest network details page.

Extend 2.4 GHz range

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




Enabling this option might slow down the network performance.

Shared Services





Aruba Instant On 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 mobile app. 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 network or guest network, follow these steps:

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




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.

Some of the main services supported are:

- **AirPlay™**—Apple® AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV® and other devices that support the AirPlay feature.
- **AirDrop™**—Apple® Airdrop allows you to share and receive photos, documents and more with other Apple devices that are nearby.
- **Google Cast**—This protocol is built-in to Chromecast devices or Android TV and allow playing audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- **AirPrint™**—Apple® AirPrint allows you to print from an iPad, iPhone or iPod Touch directly to any AirPrint compatible printers.
- **Sharing**—Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple® devices.
- **RemoteMgmt**—Use this service for remote login, remote management, and FTP utilities on Apple® devices.
- **DLNA Media**—Applications such as Windows Media Player use this service to browse and play media content on a remote device.
- **DLNA Print**—This service is used by printers that support DLNA.

Applications Statistics

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

- Tap the down arrow () next to the employee or guest network name and tap on the pie chart displaying the data transferred (in MB).

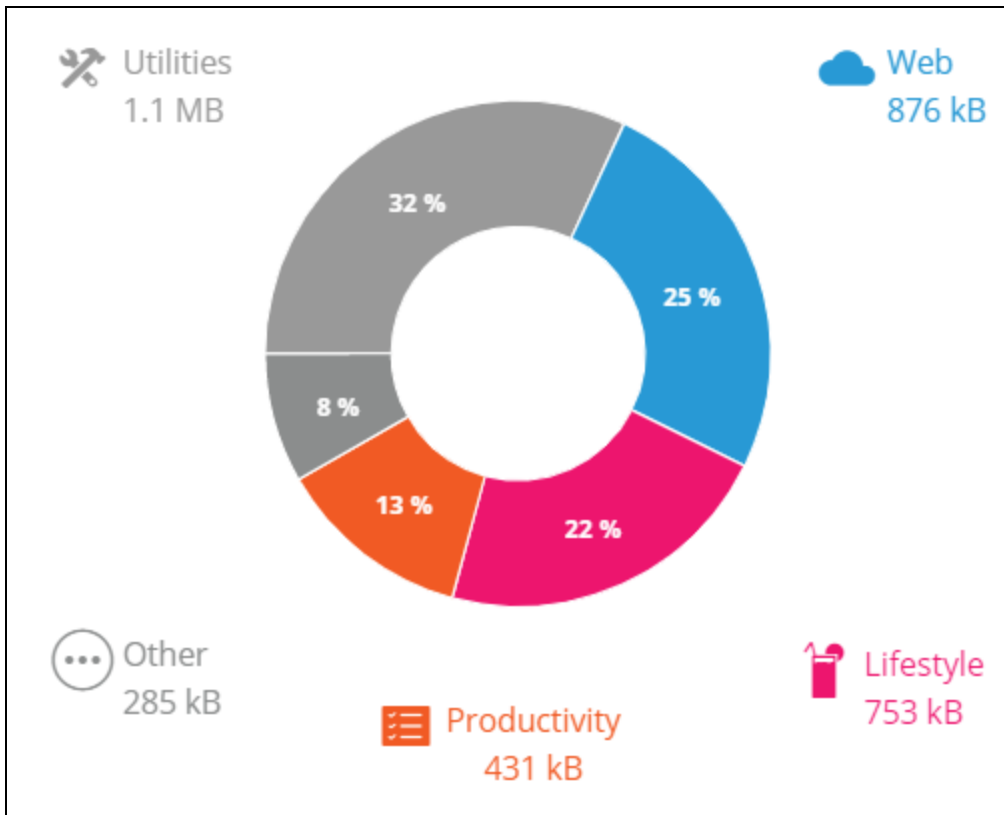
Viewing Client Count

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

Viewing Applications Chart Data

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

Figure 2 Applications Chart



Viewing Total Data Transferred

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





Viewing Blocked and Unblocked Application Categories

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

Guest Network

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

- To create a Guest Network, follow these steps:
 1. Tap **Networks** tile on the Instant On web application home page.

2. Tap Add () and select the **Wireless** tab. This tab appears only when your site has both wired and wireless networks.
3. Select **Guest**, under **Usage** to indicate that the network is for guest users.
4. Select one of the following **Security** levels:
 - a. Tap **Open**, if you want the user to access this network without the requirement of entering a username or password.
 - b. Tap **Portal**, if you do not want to secure the network with a password or if you want to redirect users to your Captive Portal page before accessing the network. For more information, see [Enabling Guest Portal](#).
 - c. Tap **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.
- To change the guest network status manually, follow these steps:
 1. Tap **Networks** () tile on the Instant On home page and select a guest network from the list. The **Guest Details** page is displayed.
 2. Slide the **Inactive** toggle switch () to the right set the network to **Active** ()
 3. Tap **DONE**. The network is marked as **Active**, and all network settings are made visible.


More Options

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

- [IP and Network Assignment](#)
- [Schedule](#)
- [Bandwidth Usage](#)
- [Network Access](#)
- [Wireless Options](#)
- [Shared Services](#)

Enabling Guest Portal

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

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

- [Guest Network](#)
- [Configuring External Captive Portal](#)
- [Facebook Wi-Fi](#)

8. The changes are automatically saved.

Configuring Internal Captive Portal

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

Table 15: *Internal Captive Portal Configuration*

Parameter	Description
Background	Tap the box to view the color palette and choose a color for the background of the internal captive portal page.
Welcome Message	Design the welcome message by updating the following fields: Text —Enter the text for the welcome message. Example: Welcome to Guest Network. Font size —Drag the slider to set the size of the font. Font color —Tap the box to view the color palette and choose a color for the font. Font family —Choose a font type from the drop-down list.
Logo / Image	Tap the image icon to browse and upload an image from your device.
Terms and Conditions	Design the terms and conditions section by updating the following fields: Title text —Enter the title text. Example: Please read the Terms and Conditions before using the Guest Network. Font size —Drag the slider to set the size of the font. Font color —Tap the box to view the color palette and choose a color for the font. Font family —Choose a font type from the drop-down list. Terms content —Enter or paste your terms and conditions in the text box. Agree text —Enter a comment in the text box. For example: I agree to the terms and conditions. <ul style="list-style-type: none"> ■ Font color—Tap the box to view the color palette and choose a color for the font. ■ Font family—Choose a font type from the drop-down list.
Accept Button	Design the Accept Button by updating the following fields: Text —Enter the text for the accept button. Example: I agree to the terms and conditions. Redirect URL —Specify the custom URL to which users should be redirected after clicking the accept button. Border radius —Drag the slider to set the border radius of the accept button. Background color —Tap the box to view the color palette and choose a color for the background. Font color —Tap the box to view the color palette and choose a color for the font. Font family —Choose a font type from the drop-down list.

Configuring External Captive Portal



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

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

Using Third-Party Captive Portal

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

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

1. Select the preferred captive portal provider tile. You must have an account with the selected provider.
2. Configure the following parameters:
 - **Social WiFi identifier**—Enter the social Wi-Fi identifier provided by the provider. This field is applicable only for Aislelabs.
 - **Preferred servers**—Select the preferred server from the drop-down list. This field is applicable only for Aislelabs.
 - **Select your region**—Select the region from the drop-down. This field is not applicable for Aislelabs.
 - **Allowed domains**— Slide the toggle switches to enabled () to allow access to social network domains. Enter a domain name in the **New domain name** and tap  to add additional domains. This allows unrestricted access to additional domains.

Customizing Captive Portal

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

To customize the external captive portal, follow these steps:

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

Table 16: *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.

Table 16: External Captive Portal Configuration

Parameter	Description
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—Enter the IP address of the external RADIUS server. ■ Shared secret—Enter a shared key for communicating with the external RADIUS server. <p>Tap 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 determines the timeout for one RADIUS request. The Instant On AP retries to send the request several times (as configured in the Retry count) before the user gets disconnected. ■ Retry count—Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests. ■ Authentication port—Enter the authorization port number of the external RADIUS server within the range of 1–65,535. The default port number is 1812. ■ Accounting port—Enter the accounting port number within the range of 1–65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813. <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>

Facebook Wi-Fi

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

Configuring the Facebook Wi-Fi Service

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


1. Tap **Networks** from the Aruba Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, tap the **Portal** tab.

4. Click the (✎) **Customize guest portal** link. The **Guest Portal** page is displayed.
5. Tap the drop-down arrow at the right hand corner of the screen and select **Facebook** from the menu.
6. Tap the (✎) **Configure Facebook Wi-Fi** link. You will be redirected to the Facebook page of the business.
7. Log in using your Facebook account and access the internet.

Wired Network

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

The following procedure creates a wired network:

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

Modifying the Network Name or VLAN ID

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



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



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

Enabling or Disabling a Wired Network

The following procedure enables or disables a wired network:

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



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

Important Points to Note:

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

More Options

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

- [Network Access](#)
- [Network Security](#)
- [Shared Services](#)

Network Access

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

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

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

Network Security

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

DHCP Snooping

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

ARP Attack Protection

ARP attack protection is a security feature that validates ARP packets in a network and discards ARP packets with invalid IP-to-MAC address bindings. The system automatically learns the IP to MAC bindings from the

DHCP exchanges in the network and it protects the network from certain man-in-the-middle and impersonation attacks.

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

1. Tap **Networks** (🔗) tile on the Instant On home page and select a wired network from the list. The network details page is displayed.
2. Under **More options**, tap **Network Security**. The **Network Security** screen is displayed.
3. Slide the toggle switch (🔘) to enable the **Network security protections** setting. This setting is disabled by default.
4. Click **Enable** in the pop up window to confirm.
5. Ensure that the **Security protections** setting is also enabled in the **Port Details** page for the port on which the network is configured. For more information on **Security protections**, see [Switch Details](#).
6. Tap **Done**, to save the configuration.

Shared Services

Aruba Instant On 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 mobile app. 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 network or guest network, follow these steps:

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



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.

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.









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 17: *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
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

Application Category	Icon	Instant On Classification
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 & 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 & 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 & 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 —This category contains network protocols that could not be categorized but may be useful to run your network. Therefore, it cannot be blocked. It also includes sites that are uncategorized or no longer exist.		<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
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

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

Viewing Application Information



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

Table 18: Application Information

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

Applications Visibility and Control

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

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

Analyzing Application Usage Data by Category

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

To view the application data based on its category in the mobile app:

- Tap the Applications  tile on the Instant On home page. The **Total Usage** data is displayed in the **Applications** page. Tap on any of the web categories to view the usage data.

The following data is displayed for each category:

- **Websites and applications most visited**—Displays the data for the top five application categories (by usage).
- **Activity for the last 24 hours**—Displays the data for the last 24 hours on the Instant On network.
 - **Network**—Displays the list of employee and guest networks active for the last 24 hours.
 - **Type**—Denotes if the network is an employee or a guest network

Applications Chart

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

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

Applications List

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

Viewing and Blocking Application Access

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


Viewing Applications

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

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

Blocking Application Access

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

1. Tap **Applications** on the Instant On home screen. The various application categories are displayed.
2. Select an application category from the **Applications** list. The selected application category opens.
3. Under **Allow network access to this category**, slide the toggle switch(es) against each employee or guest network to enable restrictions for the selected network(s) ().



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

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

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

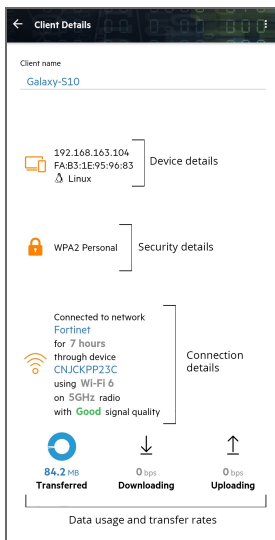
Viewing AP Clients

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

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

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

The following is an example of the Client Details page:



Viewing Details of Active Clients

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

- [Client Name](#)
- [Device Details](#)
- [Security Details](#)

- [Connection Details](#)
- [Data Usage and Transfer Rates](#)

Column Label	Description
Client Name	
Client Name	Name of the client. The client name can be modified as required.
Device Details	
IP Address	IP address of the client.
MAC Address	MAC address of the client.
OS	Operating system (OS) of the client device.
Security Details	
Security Details	This section displays the security standard used by the wireless client to connect to the network.
Connection Details	
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
Duration	Displays the duration for which the client is connected to the network.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Wi-Fi Standard	<p>The Wi-Fi standard of the client connection. The Wi-Fi standard mapping is displayed as follows:</p> <ul style="list-style-type: none"> ■ Wi-Fi 5— 802.11ac client ■ Wi-Fi 4— 802.11n client <p>NOTE: The Wi-Fi standard will not be displayed for legacy Wi-Fi clients using 802.11b or 802.11g standards.</p>
AP Radio	The radio of the AP to which the client is connected.
Signal / Speed	<p>Indicates the client signal quality. Based on the client's Signal-to-Noise Ratio (SNR), the signal quality is denoted as follows:</p> <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. Clicking on the donut chart will take you to the Applications page of the client, where detailed application usage information of the client is displayed.

Viewing Application Information for a Specific Client

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



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

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


Blocking and Unblocking Clients

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

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

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

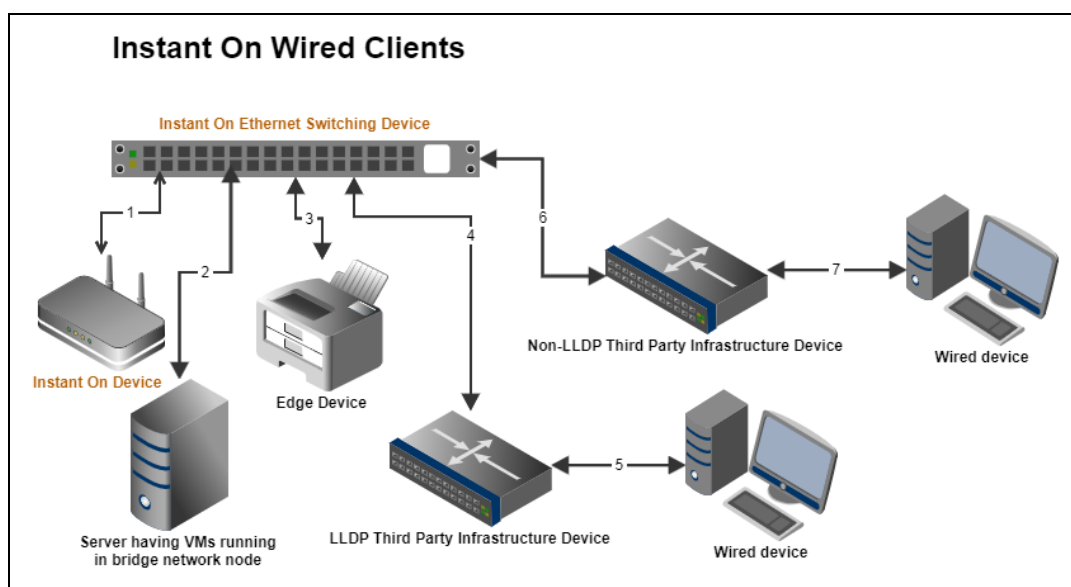
Follow these steps to unblock a blocked client:

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

Wired Clients

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

Figure 3 *Wired Client Scenarios*



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



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

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

Wired Client Details

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

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

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

Table 19: *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.
Type	Denotes the type of the wired client.

Parameter	Description
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.
Speed	Indicates the speed of data transfer at the port. The speed of the port is denoted as follows: <ul style="list-style-type: none"> ■ Good ■ Fair
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.

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

Modifying Administrator Account Information

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

1. From the page header, click the icon next to your account name. The **Account Management** page is displayed.



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

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

The **Account management** screen also allows you to enable or disable alert notifications for the site. For more information, see [Alert Categories](#).



Notifications

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

When you click a notification, your registered device automatically opens the Instant On app and takes you to the corresponding management interface for the Instant On site. If no action is taken on the alert, the notification remains in the notification bar and can still be viewed at anytime until it is cleared. All alerts triggered on the site can be viewed by clicking on **Show all alerts** in the **Site Health** tile.

Enabling or Disabling Alert Notifications

To enable notifications for alerts, follow these steps:

1. Click on the account icon (the alphabet icon) 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**, slide the toggle switch(es) to enable () or disable () the alerts you want to be notified about. The alerts you have enabled will be displayed in the **Site Health** tile in the home page. For more information on viewing and managing alerts, see:

- [Viewing and Managing Alerts using the Mobile App](#)



By default, the notifications are enabled for all three 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](#)

Connection Problem

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

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

Device Problem

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

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

Device Capacity Exceeded

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

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

Upgrading the Firmware for an Instant On AP or Switch

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

Instant On Image Server

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

Updating the Software Image on an Instant On Site

Instant On allows you to control when a software update on the site needs to take place. This is done by configuring a day of the week and time of your preference for the site on the Instant On mobile app. When a new software update is available, an information alert is displayed with sufficient information of when the update will occur. The **Software update** page displays the new version number and the **What's new:** information in the release. The page also includes the scheduled time for the update and the options—**Install now** or **Postpone by a week**.



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

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

1. Tap the advanced menu (☰) icon on the Aruba Instant On home screen. Select **Site management** from the menu.
2. Click the **Software update** tab to view the scheduling options.
3. Select the **Preferred day of the week *** for the software update to be installed automatically.
4. Select a suitable **Time *** from the drop-down menu.

The real-time status of the upgrade is displayed in the **Software update** page, indicating the software update is in progress. When the software is up-to-date, the page will show the current Instant On software version and the date of the last update.

Verifying Client Connectivity During Upgrade

Instant On APs and switches are automatically rebooted with the new version of the Instant On software image during a software upgrade. When an AP goes down during the reboot, the wireless clients connected to that AP are either moved to another AP in the Instant On site or completely dropped from the network. Though this scenario is expected, keep in mind that a firmware upgrade can cause major disruptions for the clients in your network. This is limited to the time-period that the APs take to reboot, which is 3-5 minutes. We recommend that you schedule this activity for when you don't expect users connected to the network actively.

Upgrade Failure

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



Instant On Mobile App Compatibility

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

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

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 **Show all alerts** 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.



Troubleshooting Instant On devices

✓ What the lights mean

The different colors and blinking of the lights on your Aruba Instant On device provide an indication of its status at a glance. The following summarizes the possible states.

Color	Meaning
 No lights	Device has no power Review the different power options and verify that cables are properly connected .
 Blinking Green	Device is starting Wait, it can take up to 8 minutes for the device to be ready.
 Alternate Green - Amber	Device is ready for setup The device is ready to be discovered.
 Solid Green	Device is ready Wi-Fi is up (access point only) and clients can connect to device.
 Solid Amber	Device has detected a problem A problem is preventing the device from being ready. Troubleshoot to learn more.
 Blinking Amber	Device locator Identification of the device has been turned on.
 Solid Red	Device has an issue Unplug and replug the device, contact support if the problem persists.

5. If you are unable to find a solution to the problem, navigate to the following link to view additional support options.

- [Help & Support in the Mobile App](#)