HPE Networking Instant On User Guide

Hewlett Packard Enterprise

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components 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, please check if the code is available in the HPE Software Center at https://myenterpriselicense.hpe.com/cwp-ui/software but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Contents

Contents 3

Revision History 6

About this Guide 7
- Intended Audience 7
- Related Documents 7
- HPE Networking Instant On Release Notes 7
- Contacting Support 8

Instant On Solution 9
- Key Features 9
- Supported Devices 9

Whats New in this Release 11
- New Features 11

Support for Instant On Secure Gateways 12
- Gateway Features 12

Instant On Deployment Concepts 14
- Access Point Only Deployment 14
- Switch Only Deployment 14
- Access Point and Switch Deployment 14
- Gateway Deployment - with AP Switch or Both Devices 15

Provisioning your Instant On Devices 17
- Downloading the Mobile App 17
- Official Cloud URLs for Instant On 18
- Setting Up Your Wireless Network 19
- Setting Up Your Wired Network 20
- Setting Up Your Network Using Gateway 21
- LED Status 22
- AP Operating Modes 24
- Setting Up Your Instant On Secure Gateway 26
- Local Management for Switches 28
- IP Assignment for Access Points 31
- Discovering Available Devices 33
- Cloning a Site 35
- Managing Sites Remotely 35
- Application Error Messages 36

Instant On User Interface 37
- Configuring Menu Items in the Header 38
- Configuring Settings in the Modules 40
- Site Management 41
- About Software 47

Monitoring Site Health 48
Events 50
Alerts 50
Network Tests 52

Devices 54
Adding a Device 54
Adding a Device to an Empty Site 54
Types of Devices 55
Extending your Network 55
Radio Management 58
Loop Protection 59
Power Management 61
Gateway Details 62
Access Point Details 69
Router Details 77
Switch Details 85
Cloud-Managed Stacking 101
Topology 116
Auto-Detection and Auto-Configuring of Switch Ports 119
Wi-Fi 6E Standard 119

Configuring Networks 120
Employee Network 121
Guest Network 129
Enabling Guest Portal 130
Wired Network 134
WAN 141
Latency 142
Packet Loss 143
VPN Network 148

Managing Clients 153
Viewing Wireless Clients 153
Wired Clients 158
Viewing VPN Clients 162

Managing Your Account 164
Changing Account Password 164
Profile 164
Security 165
Notifications 166
Communication Preferences 168
Delete Account 168

Policies 169
Policy Support by Site Topology 169
Policy Deployment 170
Viewing Policies 170
AI-Assisted Policy Creation 171
Manual Policy Creation 172
Schedules 174

Profiles 176
Viewing Port Profiles 176
Creating a Port Profile 176

Port Profile Details 179
RADIUS Profile Page 181
Creating a RADIUS Profile 182
RADIUS Profile Details 183

Security 186
Viewing the Detected Threats 186
Threat Actions 187
Threat Exceptions 187
Threat Management 188
Internet Firewall 188
Restart Firewall 189

Domains 191
Creating a Domain 192
Viewing the Domain Dashboard 192

Analyzing Application Usage 196
Viewing Application Information 200
Viewing Application Access 201

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
About this Guide

This user guide describes the features supported by HPE Networking Instant On 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, switches, and gateways.

Related Documents

In addition to this document, the HPE Networking Instant On product documentation includes the following:

- HPE Networking Instant On Hardware Documentation
- Instant On 1830 Switch Series Management and Configuration Guide
- Instant On 1830 Installation and Getting Started Guide
- Instant On 1840 Installation and Getting Started Guide
- Instant On 1930 Switch Series Management and Configuration Guide
- Instant On 1930 Installation and Getting Started Guide
- Instant On 1940 Installation and Getting Started Guide
- Instant On 1960 Switch Series Management and Configuration Guide
- Instant On 1960 Installation and Getting Started Guide

HPE Networking Instant On Release Notes

The latest HPE Networking Instant On release notes for cloud management and local management are available here:

Cloud Management

- HPE Networking Instant On Release Notes

Local Management

- HPE Networking Instant On 1830 Switch Series - Release Notes
- HPE Networking Instant On 1930 Switch Series - Release Notes
- HPE Networking Instant On 1960 Switch Series - Release Notes

Contacting Support

Table 2: *Contact Information*

Main Site	https://instant-on.hpe.com/
Support Site	https://instant-on.hpe.com/contact-support/
Instant On Social Forums and Knowledge Base	https://community.instant-on.hpe.com/home
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
EULA	https://instant-on.hpe.com/eula/
Security Incident Response Team	Site: https://support.hpe.com/connect/s/securitybulletinlibrary Email: networking-sirt@hpe.com

Chapter 2
Instant On Solution

HPE Networking Instant On is a simple, fast, and secure solution designed for small business networks. It is an affordable to own and easy-to-use solution that is ideal for the businesses with simple technology requirements and setups that do not have IT staff. The product offers the latest Wi-Fi and switching technologies, so that your business can have a fast experience even in a busy office or store. It also includes secure gateways with firewall, IDS/IPS, and WAN resiliency. Access points, switches, and secure gateways together provide an end-to-end, cloud-managed networking solution that delivers performance, security, and simplicity.

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 Instant On app are:

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

Supported Devices

Instant On currently supports the following devices:

Indoor Instant On Access Points

- Instant On AP11 Access Points
- Instant On AP11D Access Points
- Instant On AP12 Access Points
- Instant On AP15 Access Points
- Instant On AP22 Access Points
- Instant On AP25 Access Points
- HPE Networking Instant On AP21 Access Points

- HPE Networking Instant On AP22D Access Points
- HPE Networking Instant On AP32 Access Points

Outdoor Instant On Access Points

- Instant On AP17 Access Points
- HPE Networking Instant On AP27 Access Points

Instant On Switches

- Instant On 1930 8G 2SFP Switch
- Instant On 1930 8G Class4 PoE 2SFP 124W Switch
- Instant On 1930 24G 4SFP/SFP+ Switch
- Instant On 1930 24G Class4 PoE 4SFP/SFP+ 195W Switch
- Instant On 1930 24G Class4 PoE 4SFP/SFP+ 370W Switch
- Instant On 1930 48G 4SFP/SFP+ Switch
- Instant On 1930 48G Class4 PoE 4SFP/SFP+ 370W Switch
- Instant On 1960 24G 2XGT 2SFP+ Switch
- Instant On 1960 24G 20p Class4 4p Class6 PoE 2XGT 2SFP+ 370W Switch
- Instant On 1960 48G 2XGT 2SFP+ Switch
- Instant On 1960 48G 40p Class4 8p Class6 PoE 2XGT 2SFP+ 600W Switch
- Instant On 1960 12XGT 4SFP/SFP+ Switch
- Instant On 1960 8p 1G Class 4 4p SR1G/2.5G Class 6 PoE 2p 10GBASE-T 2p SFP+ 480W Switch
- Instant On 1830 8G Switch
- Instant On 1830 8G 4p Class4 PoE 65W Switch
- Instant On 1830 24G 2SFP Switch
- Instant On 1830 24G 12p Class4 PoE 2SFP 195W Switch
- Instant On 1830 48G 4SFP Switch
- Instant On 1830 48G 24p Class4 PoE 4SFP 370W Switch

Instant On Secure Gateways

- HPE Networking Instant On Secure Gateway 4p Gigabit SG1004
- HPE Networking Instant On Secure Gateway 5p Smart Rate 2.5G Class 4 PoE 64W SG2505P

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

- HPE Networking Instant On Hardware Documentation
- Buy Now from a Local Reseller

Chapter 3
Whats New in this Release

This section lists the new features and enhancements introduced in Instant On 3.4.0.

New Features

Table 3: *New Features Introduced in Instant On 3.4.1*

Feature	Description
Gateway Details Creating a Port Profile Port Profile Details	**Support for Always On and Quick PoE** - Always On PoE and Quick PoE are two different mode of operations supported on the 1840, and 1940 switch series.
Switch Details	**Quiet LED support for 1840 and 1940**- The newly introduced 1840 and 1940 switches support Quiet LED operations. This needs to be documented in the user manuals.
Stack Details	**IP Reservation on Stack members** - It is now possible to reserve an IP address for a stack member through the Mobile interface.
WAN	**WAN latency and packet lost in WAN dashboard** - two new graphs are added to the WAN Dashboard
Monitoring Site Health Alerts	**Updating Symptoms, Probable Causes, Recommended Actions**- the strings associated to the Probable Causes and recommended actions on Conditions and also Alerts are updated.
Quality of Service Wired Options	**QoS on Networks and Policies**- Quality of service is now supported on wireless, wired and VPN networks.
Creating a Port Profile	**Support for 1840 and 1940 in Instant On**-- Introduction of the 1840 and 1940 switches with equivalent support to any other instant on switch.

Chapter 4
Support for Instant On Secure Gateways

HPE Networking Instant On supports deployment, monitoring, and management of Secure Gateways–SG1004 and SG2505P. These Secure Gateways enhance your network's security by providing site-to-site VPN connectivity, advanced firewall protection, and Intrusion Detection and Prevention (IDS/IPS) capabilities.

The following table lists the features that are supported by HPE Networking Instant On Secure Gateways:

Gateway Features

Table 4: *Secure Gateway Features*

Category	Feature	Description
Security	▪ Viewing the Detected Threats ▪ Threat Management ▪ Threat Exceptions ▪ Internet Firewall	Provides threat detection and reporting, firewall configuration, and options to add or block threat exceptions.
Networks	▪ LAN ▪ WAN ▪ WAN Redundancy ▪ WAN Failover	Supports LAN and WAN setup, including WAN Redundancy and WAN Failover.
Devices	Gateway Details	Displays the configuration details of an Instant On gateway deployed at the site and allows the administrator to modify device settings.
Policies	AI-Assisted Policy Creation	Supports AI assisted policy creation for sites that are provisioned with a gateway.
Domains	Domains	Supports site-to-site VPN connections and allows up to eight remote sites to connect to a main site.
Clients	Automated Client Classification	Supports all AP and wired clients when an Instant On Secure Gateway is deployed in the network, including clients connected to a switch, indirectly connected to the gateway as long as the gateway is acting as the DHCP server.
Applications	Deep Packet Inspection	Analyzes incoming traffic to classify it by application and category. This feature is enabled by default.

For information on deployment and setting up the gateway, refer to the following sections:

- Instant On Deployment Concepts
- Setting Up Your Wireless Network
- Setting Up Your Instant On Secure Gateway

Chapter 5
Instant On Deployment Concepts

HPE Networking Instant On supports the following deployment combinations:

- Access Point only
- Switch only
- Gateway only
- Access Point and Switch
- Access Point and Gateway
- Switch and Gateway
- Access Point, Switch, and Gateway

Access Point Only Deployment

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 a gateway, 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.

Switch Only Deployment

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 or a gateway 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.

Access Point and Switch Deployment

This 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

For more information, see AP Operating Modes section to Onboard your devices based on the preferred mode.

Gateway Deployment - with AP Switch or Both Devices

Use this deployment when the Instant On gateway is intended to serve as the primary routing device for the site. The Instant On gateway provides advanced security capabilities such as firewalling, and intrusion detection or prevention (IDS/IPS).

In this deployment, the Instant On gateway offers DHCP, DNS, traffic routing between LAN to WAN interface or WAN to LAN interface and firewall services for your network.

To ensure proper discovery and onboarding, the Instant On Gateway must be directly connected to the internet modem with no other device in between as follows:

- Connect the primary WAN port of the Instant On gateway to the ISP-provided modem or to a device that provides internet access.
  - Port 4 on SG1004 gateway
  - Port 5 on SG2505P gateway
- Connect Instant On APs or Switches to the LAN ports of gateway. This can be done during the initial setup or later by extending your network.

Once connected, the gateway will be discovered and onboarded using Instant On Web application or mobile app. Once the gateway is onboarded, it will provide the DHCP and DNS services, and all traffic will be routed from LAN to the WAN interface.

Once the onboarding is complete, connected devices such as switches and access points are automatically discovered through the LAN ports.

You can also use the secondary WAN port to connect to the secondary internet connection. The following are the secondary WAN ports that can be used for the secondary internet connection:

- Port 3 on SG1004 gateway
- Port 4 or Port 3 on SG2505P gateway. Port 4 is a 2.5G Ethernet port and Port 3 is a 1G Ethernet port.

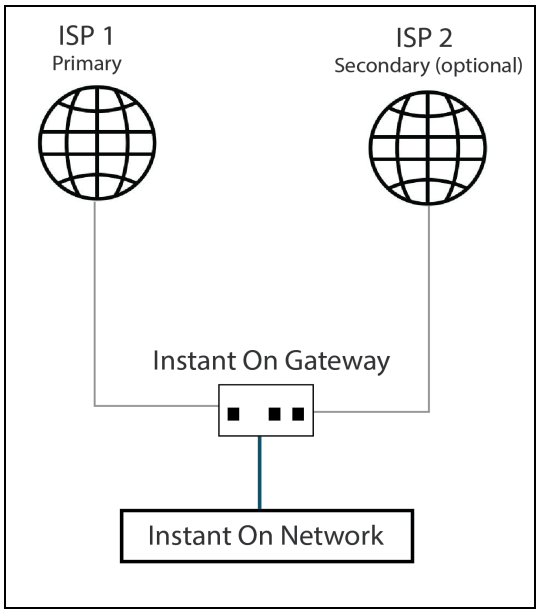
The secondary connection provides backup and failover capabilities in the event when the primary connection is not available.

Direct and Indirect Connection

The Instant On gateway can be connected to the internet either directly or indirectly through an ISP-provided router-modem:

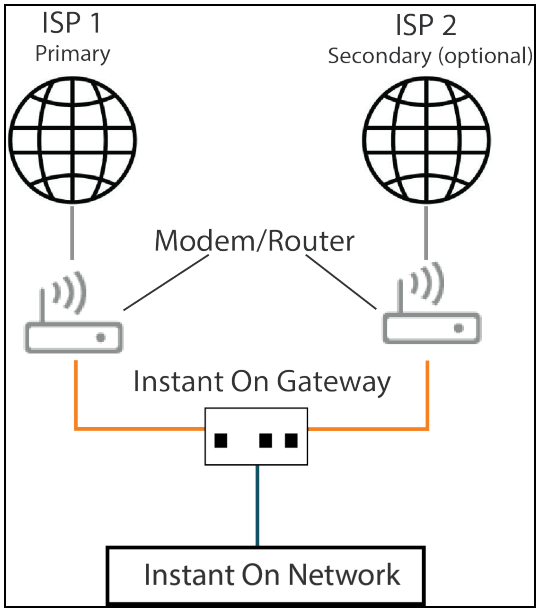
Direct Connection

The Instant On secure gateway connects directly to the internet using an Ethernet cable without any intermediate device.



Indirect Connection

The secure gateway connects to the internet through an intermediate device, such as an ISP-provided router-modem. In an indirect connectivity topology, it is important that the ISP-provided device allows the Instant On gateway to access the internet.



The following additional configurations may be required if the firewall function is active on both systems:

- Client access should be disabled on at least one system. The recommended approach is to disable client access on the ISP-provided device and manage all access using the client access policy on the Instant On Secure gateway.
- By default, remote access is blocked on the Instant On secure gateway. If remote access is required, it must be enabled on both the ISP-provided device and the Instant On secure gateway to allow traffic to pass through both layers.
- If your setup involves two ISP connections and both are indirectly connecting the Instant On secure gateway to the internet, it is recommended to manage all firewall rules on the Instant on gateway.

For more information, see Setting Up Your Instant On Secure Gateway .

Chapter 6
Provisioning your Instant On Devices

This chapter describes the following procedures:

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

Downloading the Mobile App

The 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 HPE Instant On.
   - To install the app on Android phones, go to Google Play Store and search for HPE Instant On.
   - You can also scan the QR code below to download the app directly:

2. Launch the Instant On application and follow the on-screen instructions to complete the setup.

If you are upgrading to HPE Networking Instant On 3.2.0 or later from an earlier version, you must uninstall and reinstall the Instant On mobile app on your device.

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

Mobile OS Requirements

The following mobile OS versions support the HPE Networking Instant On mobile app:

- Android 10 or later versions
- iOS 14 or later versions

Official Cloud URLs for Instant On

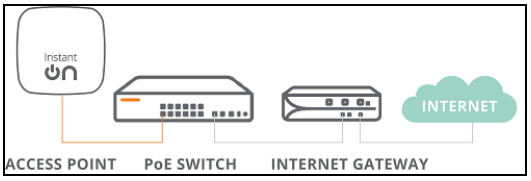
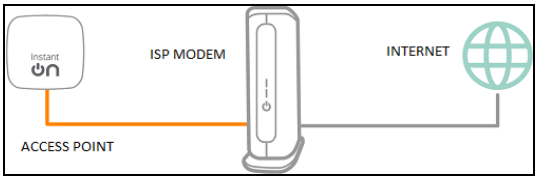
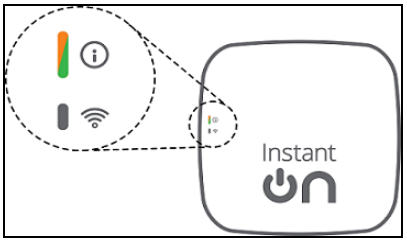
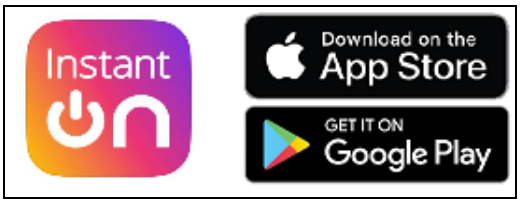
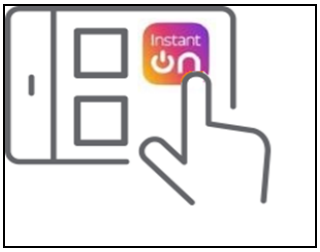
The following cloud URLs are officially used in Instant On to add in the allowed domains list:

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

Setting Up Your Wireless Network

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

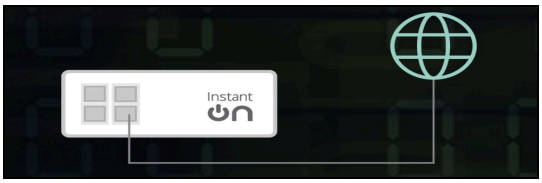
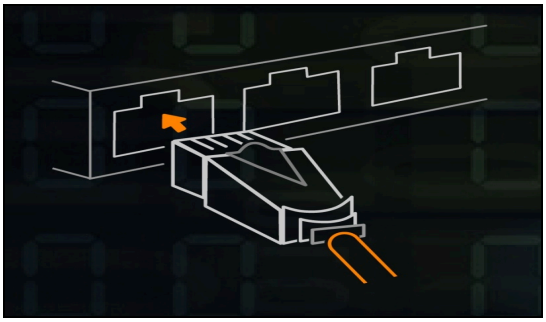
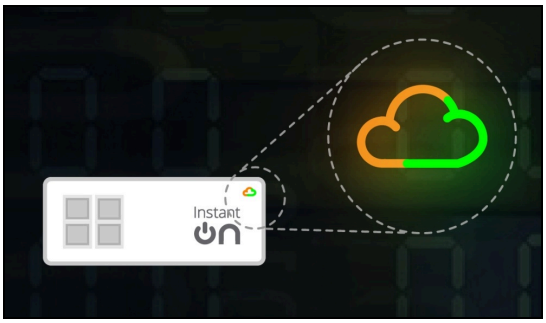
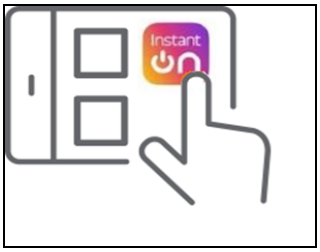
Table 5: *Instant On Wireless Network Provisioning*

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

Setting Up Your Network Using Gateway

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

Table 7: *Instant On Network Provisioning using Instant On Gateway*

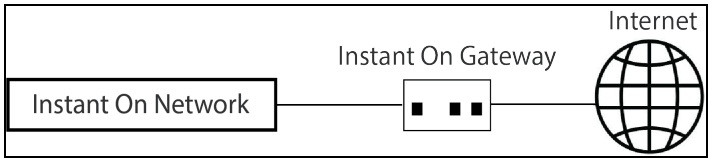
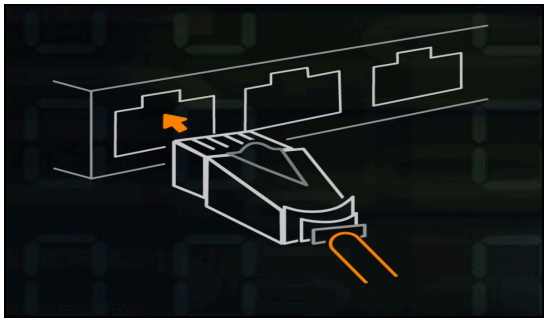
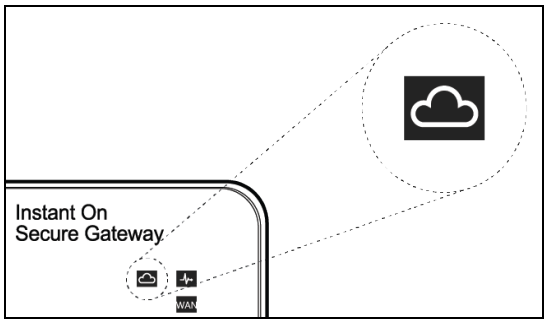
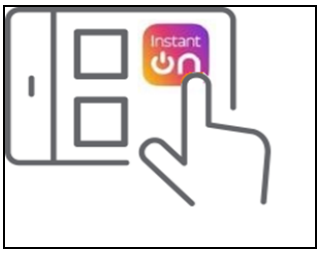
SL No	Steps	Illustration
1.	Ensure that the Instant On gateway is connected to the internet for it to be discovered. The Instant On gateway must be connected to the internet through the WAN port, using either a direct or an indirect connection. For more information about direct and indirect connections, see Direct and Indirect Connection. Primary WAN ports: ■ Instant On Secure Gateway SG1004: Port 4 ■ Instant On Gateway SG2505P: Port 5 **NOTE:** The security gateway must be the primary device for all the Instant On devices.	
2.	Connect the port you want to use as the gateway uplink to your local network using an Ethernet cable, and then power on the gateway. Devices such as switches or access points must be connected to the LAN ports. LAN Ports: ■ SG1004 Gateway: Ports 1, 2, and 3 ■ SG2505P Gateway: Ports 1, 2, 3, and 4 **NOTE:** Only one Instant On gateway is supported per site.	
3.	Power on the Instant On gateway. The Instant On gateway is ready to be discovered when the cloud LED light alternates between green and amber. Devices such as switches and access points connected to the LAN ports are automatically discovered once the Instant On gateway completes the onboarding process.	

Table 7: *Instant On Network Provisioning using Instant On Gateway*

SL No	Steps	Illustration
4.	Configure the Instant On gateway using the web application. For more information, see Accessing 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.	
5.	Launch the Instant On web or mobile application and follow the on-screen instructions to complete the setup.	

LED Status

The following table describes the various LED statuses observed during the onboarding of Instant On APs or switches to a site:

Table 8: *Cloud LED and AP LED Light Status*

Switch Cloud LED or AP LED	Status
No Lights	Indicates that the device has no power. Review the different power options and verify that the cables are properly connected.
Slowly Blinking Green	Indicates that the device is booting or upgrading. It can take up to 8 minutes for the device to be ready.
Rapidly Blinking Green	Indicates that the Instant On device has been powered on.
Solid Amber	Indicates that the device has detected a problem. Click or Tap the **Troubleshoot** link to learn more.
Alternate Green and Amber	Indicates that the device is ready to onboard.
Solid Green	Indicates that the device is connected and configured.
Rapidly Blinking Amber	Indicates that insufficient power is supplied to the device.
Slowly Blinking Amber	Indicates that the Instant On device is connecting. The connection to the Instant On portal is taking longer than expected. This should be temporary and the device will connect as soon as possible. **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.

Table 8: *Cloud LED and AP LED Light Status*

Switch Cloud LED or AP LED	Status
	NOTE: This applies only to Instant On access points and not the switches.

The following table describes the various LED statuses observed during the onboarding of Instant On gateway to a site:

Table 9: *Gateway LEDs*

Gateway LED	State	Status
Global Status	Green (Solid)	Device powered on and operating normally.
	Green (Slow Flash)	Device is booting up.
	Green (Fast Flash)	The locator function has been enabled to help physically locate the standalone unit, stack or a specific unit within the stack.
	Amber (Slow Flash)	System fault detected. Blinks in unison with affected subsystem (PoE or Cloud).
	Off	Device is not powered.
Cloud	Green (Solid)	Device is fully operational and in cloud manage mode.
	Green (Slow Flash)	Device is in the process of establishing a connection to the cloud portal.
	Amber (Solid)	Device is unable to connect to the cloud.
	Amber (Slow Flash)	Onboarding issue. Flashes in unison with the amber Global Status LED.
	Green / Amber (Alternating Flash)	Device is connected to the cloud portal and is ready for setup through the mobile App or web portal. This state is temporary while the device is connected to the cloud portal but not fully setup.
	Off	Onboarding period is over.
WAN	Green (Solid)	WAN mode is selected. Port LEDs indicate WAN status.
	Green (Slow Flash)	WAN mode not selected and at least one WAN is offline or connecting. When the device is not yet onboarded, the default WAN ports are considered offline if the onboarding server is not reachable.
	Off	WAN mode is not selected.
Mode: Link/Act (Default setting)	Green (Solid)	Port is active, blinks for activity proportional to utilization.

Table 9: *Gateway LEDs*

Gateway LED	State	Status
	Amber (Solid)	Fault on the port.
	Off	Port is inactive/unused.
Mode: WAN (Failover/Redundancy)	Green (Solid)	Port is in WAN mode - failover enabled.
	Amber (Solid)	Connectivity fault.
	Off	Port is in LAN mode - no failover.
Mode: PoE (SG2505P only)	Green (Solid)	Port is delivering PoE.
	Green (Slow Flash)	Port denied power or power revoked.
	Amber (Slow Flash)	Port PoE fault with detect or class issue. Flashes in unison with amber Global Status LED.
	Off	Port not delivering PoE.
PoE (SG2505P only)	Green (Solid)	PoE mode is selected and there is no fault. Port LEDs indicate PoE status.
	Green (Slow Flash)	PoE mode has not been selected and there is insufficient power to power all ports. Does not have precedence over Amber (Slow Flash).
	Amber (Solid)	PoE mode is selected and a port has an internal PoE hardware failure. The specific port LED with the fault will also flash.
	Amber (Slow Flash)	PoE mode as not been selected but a port has an internal PoE hardware failure. Flashes in unison with amber Global Status LED. Has precedence over Green (Slow Flash).
	Off	PoE mode is not selected and there are no PoE hardware failres or denied power on ports.

AP Operating Modes

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

- Private Network Mode
- Router Mode

During the initial setup, if one Instant On device is detected when creating the site, the user is prompted to choose if they want to configure the site in the private network mode or router mode.

Private Network Mode

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

Prerequisites

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

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

Configuring Your Instant On Devices in Private Network Mode

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

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

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

5. Review and add the devices to your network.

Router Mode

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

Prerequisites

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

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

Configuring Your Instant On Device in Router Mode

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

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

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

Setting Up Your Instant On Secure Gateway

The Instant On gateway provides DHCP, DNS, traffic routing between LAN and WAN and firewall services for your network. It also supports configuration and establishment of a PPPoE connection with the ISP. There are two methods for connecting the Instant On gateway to the internet. For more information on the connection methods, see Direct and Indirect Connection.

Prerequisites

Before you begin to provision your Instant On gateway as a primary device, complete the following prerequisites:

- An active internet connection from your Internet Service Provider (ISP).
- In an indirect connection, the firewall must be disabled in the ISP provided Modem-Router. The **Threat Management** (Intrusion Detection and Prevention System) feature inspects all incoming and outgoing traffic routed through the gateway and blocks all the critical threats. For more information, see Threat Management.
- In an indirect connection, configure the policy in the router to allow the public IP to reach the Instant On gateway.
- TCP ports 80 and 443 must be open and not blocked by the firewall.
- You must keep the Instant On gateway as the primary device for all the Instant On devices.
- Only one Instant On gateway is supported per site.

Instant On gateway allows you to disable the internal DHCP server on wired networks, but only when a gateway is present.

- By default, the DHCP server is enabled, as the Instant On gateway acts as the default DHCP server on the LAN network.
- When disabled, the application hides sections related to Automatic IP Assignment, DNS Resolution, and IP Address Reservation from the IP Assignment screen.

Configuring Your Instant On Gateway

To add your Instant On gateway to the network, follow these steps:

1. Connect the WAN port of the Instant On gateway to the ISP-provided modem using a standard Ethernet cable:
   - SG1004 Gateway – Use Port 4
   - SG2505P Gateway – Use Port 5
2. Connect other Instant On devices such as switches and access points to the LAN ports on the gateway:
   - SG1004 Gateway – Ports 1, 2, and 3
   - SG2505P Gateway – Ports 1, 2, 3, and 4
3. Power on the Instant On gateway.
4. Observe the LED lights on the Instant On gateway. It may take up to 10 minutes for new devices to complete up firmware updates and boot. The Instant On gateway is ready to be discovered by the Instant On mobile app when the LED light alternates between green and amber.

   Once onboarding is complete, connected devices such as switches and access points are automatically discovered through the LAN ports.

NOTE

By default, the configuration is set to automatic.
To manually assign an IP address using the local web interface, proceed with Step 5 to Step 10.

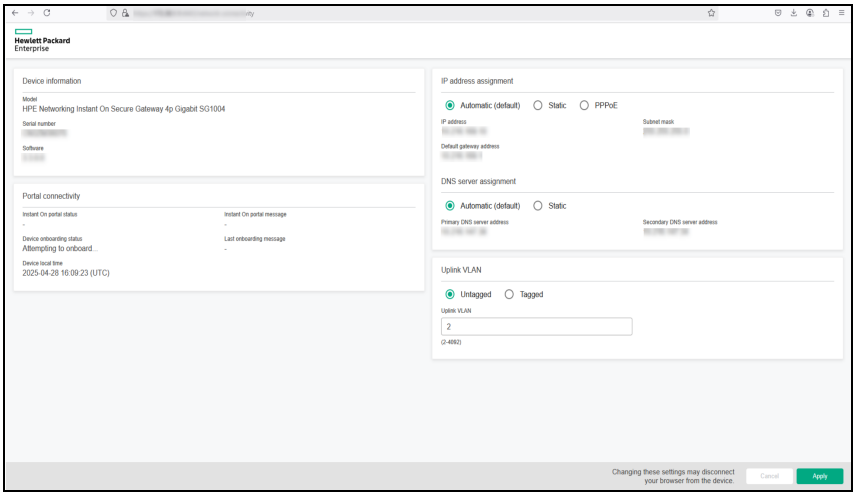
5. Connect your laptop to a LAN port on the Instant On gateway using an Ethernet cable:
   - SG1004 Gateway – Ports 1, 2, or 3
   - SG2505P Gateway – Ports 1, 2, 3, or 4

NOTE

LAN ports are enabled by default.

6. Open a browser and access the local web page using the IP **172.30.1.1**.

   By default, the Instant On gateway assigns an IP address via its built-in DHCP service.



7. In the **IP Address Assignment** section, select one of the following options:
   a. **Automatic (default)**—The DHCP server assigns an IP address for the gateway. Ensure that the IP address and subnet provided by your ISP do not conflict with the gateway's default management network (172.30.1.0/24). If there is a conflict, the gateway may lose internet connectivity, which will prevent it from completing the onboarding process.

b. **Static**: Manually assign a static IP address by entering:
   i. **IP address**–The desired IP for the gateway
   ii. **Subnet mask**–Network subnet
   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 gateway. To configure a PPPoE connection, specify the following parameters:
   - **Username–**Unique identifier provided by your ISP.
   - **Password**–A secret sequence of characters used to verify a username and grant access to the internet
   - **MTU–**Maximum Transmission Unit provided by your ISP.

8. In the **DNS server assignment** section, choose one of the following:
   - **Automatic (default)**–The DNS server details are assigned automatically
   - **Static**–Enter both Primary and Secondary DNS server addresses
9. In the **Uplink VLAN** section, select **Tagged** and enter a **VLAN ID** (between 2 and 4092)
10. Click **Apply**. The Gateway will Reboot to apply the configuration and receive an IP address.

    For PPPoE Setup:
    - Wait for the LED to flash green and orange, indicating a stable link.
    - The onboarding status displays "**Waiting to be onboarded...**"
    - This process may take an additional 5 minutes if a firmware upgrade occurs.
11. You can now proceed to create a new site and add devices. For more information, see:

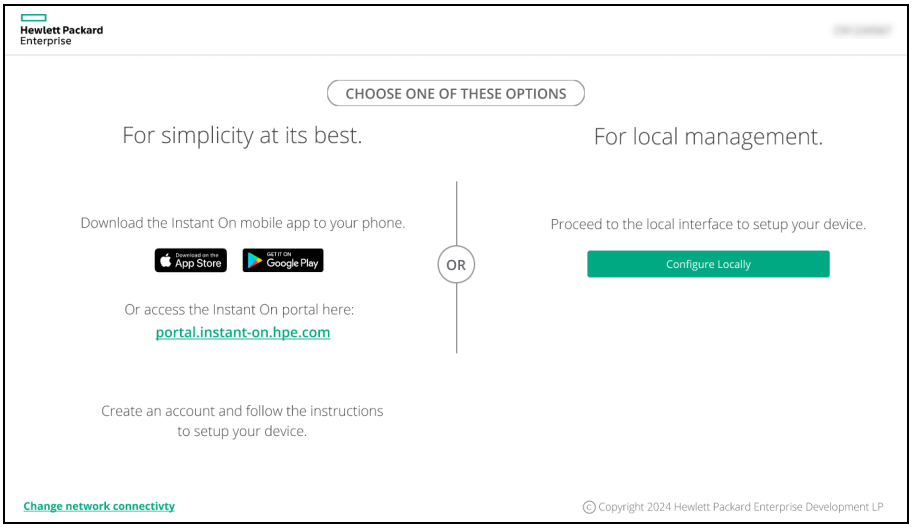
    Setup a New Site using the Mobile App.

If a gateway with a PPPoE configuration is removed from the Inventory or if the site is deleted, the gateway will reset to its factory default state, and the PPPoE configuration will be erased.

Local Management for Switches

The 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.

Figure 1 *Local Management Page*



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.
- The switches will be available to be discovered in the cloud for one week, after this period the switch must be rebooted to be available again. This happens on a switch connected in factory default mode and user does not take any action on it. The local web page will be still available for the switch.

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, follow the instructions provided in *Switching to Local Management*.

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**.

Maintenance

Instant On provides options to restart or reset an offline device on the local WebUI. There are 2 options involved when running a maintenance mode:

- **Restart**- This option restarts te device affecting network services and temporarily disconnects all clients.
- **Reset to Factory Defaults**- This option resets the device to factory settings by removing it from the site to which it belongs and then permanently erases the associated configurations.

Restart or **Reset to Factory Default** options are only available when an on-boarded device is offline.

Recovering an Offline Device Using the Local WebUI

If an onboarded device loses connectivity to the Instant On, you can correct its connectivity settings directly from the device's local WebUI, without performing a factory reset or re-onboarding the device.

The local provisioning page is **read-only while the device is online**. When the device goes **offline**, the connectivity settings become **editable** so that you can recover the device. You can edit the following:

- **Management VLAN and VLAN tagging mode** (Untagged or Tagged on the uplink port)
- **Uplink port** (Switches) – a specific port or All
- **IP Addressing Mode** – **Automatic** (default), **Static**, or **PPPoE**.
- **DNS settings** – Automatic or Static (Primary and Secondary DNS server)

To recover an offline device from the local WebUI:

1. Open a web browser and go to the device's local IP address. If the browser shows a certificate warning (for example, “Your connection is not private”), choose the option to continue to the page.
2. On the local provisioning page, review the **Portal Connectivity** section (Instant On portal status, device onboarding status, and last onboarding message) to confirm why the device is offline.
3. Under **IP addressing**, select **Automatic (default)**, **Static**, or **PPPoE**, and enter the required addressing and DNS information.
4. Under **Uplink**, select **Untagged** or **Tagged**, enter the **Management VLAN** (1–4092), and, on a switch, choose the **Uplink** port (a specific port or **All Ports**).
5. Click **Apply**. Review the warning banner and confirm.

When the device regains connectivity, the Instant On cloud reintegrates it and reconciles your changes with the site's current settings.

Switch-specific Behavior – Uplink Port Selector and Warning Banners

On a switch, applying any change from the local **WebUI wipes the switch's configuration (equivalent to a factory reset) and reboots the switch**. After the reboot:

- If you selected a **specific uplink port**, only that port is enabled and all other ports are disabled.
- If you selected **All Ports**, all ports are tagged to the selected Management VLAN.

The switch remains in this minimal factory-default state (no VLANs, profiles, or port settings) until it reconnects to the cloud. Once it reconnects with no VLAN conflict, it becomes active and all site configurations are pushed to it normally. Before applying, the local WebUI displays a warning banner describing the impact:

- Applying these settings may disconnect your browser from the device.
- Applying these settings configures a specific port as the uplink, shuts down all other ports, and restarts the device. It affects network services and disconnects all clients from the device.
- Applying these settings reconfigures all ports to uplink and restarts the device. It affects network services and disconnects all clients from the device.

Recovering from a Management VLAN Conflict (Suspended State)

When a device reconnects to the cloud after a local Management VLAN change, the cloud compares the device's Management VLAN with the site's Management VLAN. If they do not match, pushing the site configuration would break connectivity, so the device is placed in a Suspended state instead.

A device in the Suspended state:

- Appears explicitly as Suspended on the Devices page.
- Raises a Major alert named Incompatible device management VLAN, and the site health score is reduced while the conflict is active.

To clear the conflict, update the site's Management VLAN or the device's Management VLAN so that the two match. The conflict – and the alert – clear automatically once the Management VLANs match.

- Applying these settings may disconnect your browser from the device.

- Applying these settings may disconnect your browser from the device.
- Applying these settings configures a specific port as the uplink, shuts down all other ports, and restarts the device. It affects network services and disconnects all clients from the device.
- Applying these settings reconfigures all ports to uplink and restarts the device. It affects network services and disconnects all clients from the device.

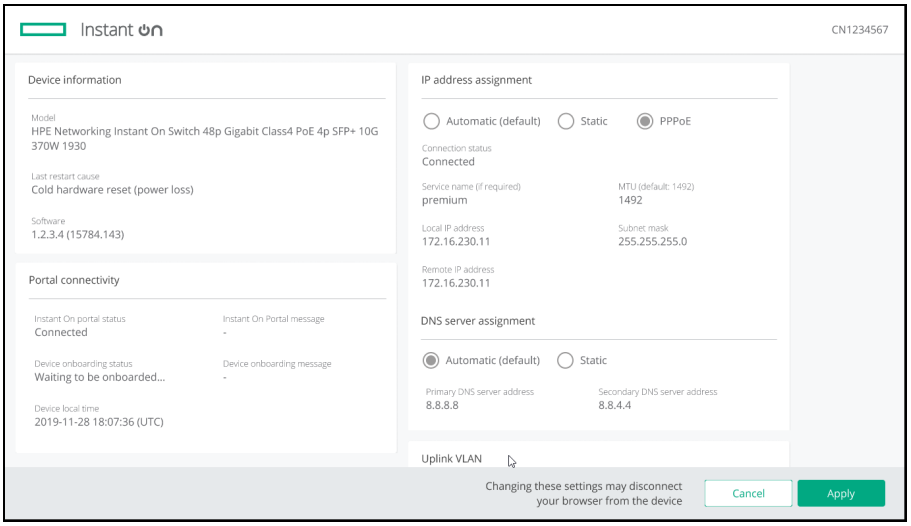
The **Suspended** state affects **Switches** and **Access Points**. Gateways are not subject to this conflict.

IP Assignment for Access Points

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

- Automatic (default)
- Static
- PPPoE

Figure 2 *IP Assignment*



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

DHCP or Static IP Addressing

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

1. Connect the AP to the network.
2. Once the LED on the AP becomes solid orange, the AP will broadcast an open SSID **InstantOn-AB:CD:EF** approximately after one minute, where AB:CD:EF corresponds to the last three octets of the MAC address of the AP.
3. Connect your laptop or mobile device to the SSID and access the local web server through **https://connect.instant-on.hpe.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. For more information on configuring PPPoE, see Setting Up WAN Connectivity for Your Network.
5. a. Under **Uplink VLAN**, select the **Tagged** radio button.
   b. Specify a VLAN ID between 1 and 4092 for the **Uplink VLAN**.
   c. Save the configuration.

   After the uplink VLAN is set, the AP will reboot to apply the new configuration, and the AP will receive an IP address.
6. Once the AP is added to a site, the management VLAN can be modified from Tagged to Untagged and

vice versa in the **Ports** tab of the Instant On AP.

7. Click **Apply**. The AP will restart after the configurations are applied.

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

Setting Up WAN Connectivity for Your Network

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

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

Follow the steps below to configure PPPoE on your network:

1. The Instant On AP should be connected to the ISP provided modem but does not have an IP address provided by the DHCP server.
2. Once the LED on the AP becomes solid orange, the AP will broadcast an open SSID **InstantOn-AB:CD:EF** approximately after one minute, where AB:CD:EF corresponds to the last three octets of the MAC address of the AP.
3. Connect your laptop or mobile device to the SSID and access the local web server through **https://connect.instant-on.hpe.com**. The local WebUI configuration page is displayed. For versions prior to Instant On 3.1.0, access the local web server through **https://connect.instant-on.hpe.com**
4. Under **IP addressing**, click the **PPPoE** radio button.
5. Enter the PPPoE **Username**, **Password**, and **MTU** provided by your ISP in the respective fields.
6. Under **Uplink VLAN**, select the **Tagged** radio button.
7. Specify a VLAN ID between 1 and 4092 for the **Uplink VLAN**.
8. Click **Apply**. The AP will reboot once the PPPoE configuration is applied.
9. Wait for the LED lights to flash green and orange. This indicates that the PPPoE link is up and stable, you will see the device onboarding status now reads "**Waiting to be onboarded...**". This step might take an additional five minutes, if the AP upgrades its firmware during the reboot process.
10. You can now proceed to creating a new site and adding devices. For more information, see:

    Setup a New Site using the Mobile App.

If an AP with the PPPoE configuration is removed from the Inventory or the site is deleted, the AP will move to its factor 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, gateway, 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:

- Serial Number– Enter the serial number located at the back of your Instant On AP, gateway, 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, gateway, or switch.
- QR Code–The Instant On supports QR Code on all switches, gateway and AP21, AP22, AP22D, AP25, AP27, and AP32. This option is available only in the Instant On mobile app, and is available when adding new devices during the initial setup and also in the **Extend network** configuration.
- BLE Scanning–The Instant On mobile app scans for nearby devices through BLE and displays the APs discovered, on the screen. Tap or click the **Add devices** button to add the devices discovered to the site. Alternatively, click **Search again** if there are more devices to be displayed. If the BLE scanning fails to discover any devices in the vicinity, tap the **Add devices manually** tab and choose to add devices to your network by entering the serial number or by scanning the barcode of the AP.

BLE Scanning is supported only on AP11, AP11D, AP12, AP15, AP22, and AP17 access points.

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 Instant On mobile app using your administrator account credentials, the **Managed Sites** page is displayed if multiple Instant On sites are registered to your account. A health icon and health % is is displayed alongside each site. The active alerts generated for each site are also displayed.

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 **Managed Sites** screen and select Account management from the drop-down list. 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 **Create 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 **Managed Sites** screen and click **Create site**.

Sign Out

Click on this field to sign out from your 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 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.instant-on.hpe.com/.
- **Support center**–Opens the 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://instant-on.hpe.com/contact-support/.
- **Support resources**–Allows you to generate a support ID by clicking on the **Generate Support ID** button. The ID is then shared with HPE Networking Support personnel to run a diagnosis on your device.

Cloning a Site

Instant On offers the administrators the possibility of cloning an Instant On site and all its configurations to a new site. This setting is available only in the List View of the managed sites.

Follow these steps to clone an Instant On site:

1. Tap the advanced menu () icon on the Instant On home screen and select **Clone site**.
2. Under **Identify the Site**, enter a **Name** for the new site.
3. The **Location** field displays your current location. To change the location, follow these steps:
   a. Tap on the current location displayed on the screen.
   b. Enter the new location details in the **Search locations** bar.
   c. From the list of locations displayed, select the radio button next to the address you want the site to be tagged to.
   d. Click **DONE**.
4. Tap **Continue**.
5. In the **Add Devices** screen, select one of the following options:
   a. **Add devices**. For more information, see Adding a Device.
   b. **Add devices later**
6. Tap **Continue**. The Cloning Summary details are displayed.
7. Review the summary and tap **Clone site** to complete the process.

Managing Sites Remotely

Remote access allows you to configure, monitor, and troubleshoot 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.

Cloud Service Unavailability Indicator

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

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

When a cloud service outage occurs, you will automatically be informed once the cloud service is fully restored, eliminating the need to manually check the status page.

Application Error Messages

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

Table 10: *Application Error Messages*

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

Chapter 7
Instant On User Interface

The 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 3 *Mobile App User Interface Overview - Without Secure Gateway*

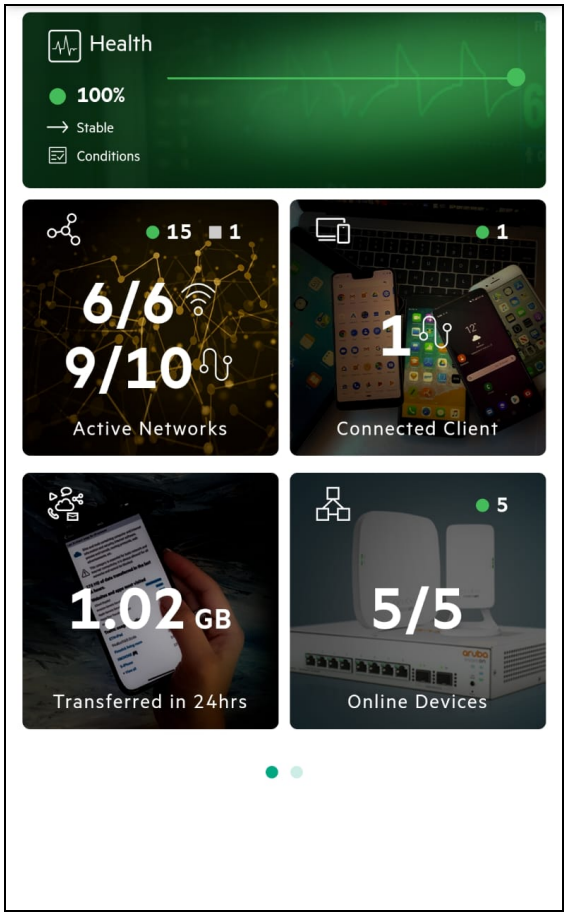
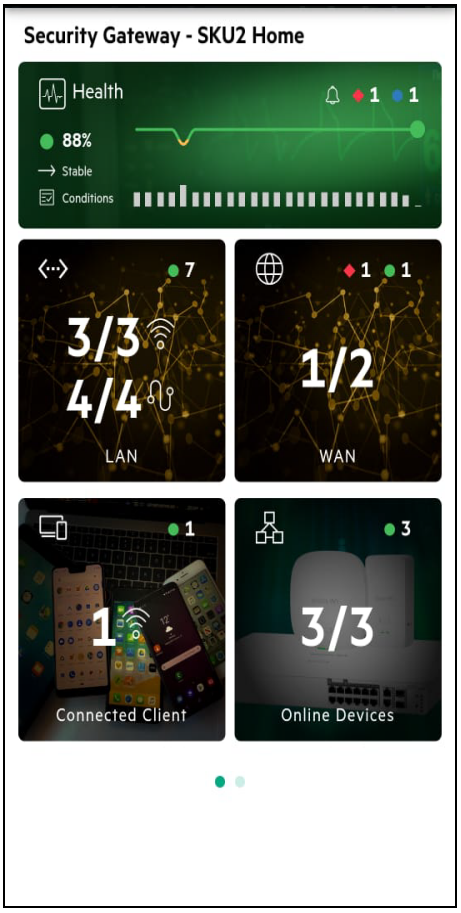


Figure 4 *Mobile App User Interface Overview -With Secure Gateway*



Configuring Menu Items in the Header

The header includes the following menu items:

Table 11: *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.

Table 11: *Menu Items in the Header*

Header Content	Description
Advanced menu icon ()	Displays the site name and provides menu options to administer your account and the sites associated with it.
	Site management–Allows you to modify various account settings, including time zone and notifications. For more information, see Site Management.
	Add new devices–Opens the Extend my network page and allows you to add a new device. For more information, see Extending your Network.
	Sites–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 Instant On login page. Enter the registered email ID and password to access the respective 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.
	Create site–Allows you to setup a new Instant On site. For more information, see Setup a New Site.
	Clone site–Allows administrators to clone an Instant On site and all its configurations to a new site. For more information, see Cloning a Site.
	Help & Support (?)–Leads you to the **Contact support** page. Following are the available technical support options: ■ **Help center**–Opens the HPE Networking Instant On documentation portal. For more information, see https://instant-on.hpe.com/techdocs/en/content/home.htm. ■ **Community**–Opens the HPE Networking Instant On community page. For more information, see https://community.instant-on.hpe.com/support. ■ **Support center**–Opens the HPE Networking Instant On support center. For more information, see https://instant-on.hpe.com/contact-support.
	About–Provides information about the software currently installed on the mobile app, and also the following information: ■ End User License Agreement ■ Data Privacy Policy and Security Agreement
Registered email ID **NOTE:** The alphabet displayed is the first letter of your email ID.	Displays the account username registered email ID and provides options to administer account information and setup notifications or alerts. **Account management**–Allows you to modify your account information for all associated sites. For more information, see Managing Your Account. ■ **Profile**–Allows you to modify the preferred language setting. ■ **Password**–Allows you to modify the password for the account. For more information, see Managing Your Account ■ **Security**–Allows you to configure two-factor authentication for the site. For more information, see Security. ■ **Notifications**–Allows you configure the notification settings for the alerts received from the site. For more information, see Notifications. ■ **Communication Preferences**–Allows you to subscribe to the latest offers and promotions provided by HPE. For more information, see Communication Preferences. ■ **Delete Account**–Allows you to delete the account.
	Sign out–Allows you to log out of your Instant On account.

Configuring Settings in the Modules

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

The Instant On user interface consists of the following modules:

- 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.

  When a security gateway is deployed at the site, the **WAN** tile is displayed. The **WAN** tile displays the number of WAN connections, along with network health, aggregate total usage across all active WAN connections and the availability over the past 24 hours. Both the **LAN** and **WAN** tiles are displayed one next to each other.

  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.
- Devices: 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 Devices for more information on the devices on the site.
- Security: Specifies the number of threats identified and the number of threats blocked from the identified threats. See Security for more information on the Security 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.
- Policies: Provides an unified space for administrators to define and manage rules from a single page and apply them to more than one network or application at the same time. See Policiesfor more information.
- Profiles: The Profile feature allows network administrators to configure and manage Port Profiles and RADIUS Profiles within a site. See Profiles for more information.

Opening a Module

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

Table 12: *Module Tiles*

Module	Tile
Site Health	
Networks	
LAN	
WAN	
Clients	
Applications	
Devices	
Security	

Module	Tile
Policies	

When a secure gateway is deployed at the site, the Networks tile is replaced by separate LAN and WAN tiles.

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 Instant On home screen and tap **Site Management**. The **Site Management** page displays the following user settings that can be modified in the Instant On application:

- Site Addressing
- Administration
- Location
- Software update

Site Addressing

The **Site Addressing** section allows you to manage site registration status within the Instant On DNS infrastructure. It includes options for enabling **Dynamic DNS site addressing**, which provides flexible connectivity for VPN clients and networks.

Choose one of the following options to configure site addressing:

- **No Dynamic DNS site addressing (default)**–When this option is selected, the site will not automatically update its DNS records when its IP address changes. This is the default option.
- **Use Dynamic DNS site addressing**–When this option is selected, the site will automatically update its DNS records whenever its IP address changes. This option is automatically enabled in the following scenarios:
  - A VPN network is created.
  - A port forwarding policy is created.Choose one of the following options to configure site addressing:
  - **No Dynamic DNS site addressing (default)**–When this option is selected, the site will not automatically update its DNS records when its IP address changes. This is the default option.
  - **Use Dynamic DNS site addressing**–When this option is selected, the site will automatically update its DNS records whenever its IP address changes. This option is automatically enabled in the following scenarios:
    - A VPN network is created.
    - A port forwarding policy is created.

      When a port forwarding policy is created, the **Site Hostname** is used instead of a static IP address. This ensures that VPN clients can always connect to the gateway, even if the WAN IP changes or the

primary WAN connection fails. You can click on the **View Policies** hyperlink to view the policy configuration page.

Also, the **Site Hostname** is displayed below the radio buttons when this option is enabled.

Accounts Managing This Site

The **Accounts managing this site** section allows you to modify administrator information, including your 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.

Location

The **Location** can be set during site creation. By default, the location is updated to an approximate address of where the user is located when creating a site. The location settings can be modified from the Site Management page. For more information, see Location.

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.

Support

You can generate a support ID by tapping on the **Generate Support ID** button. The ID is then shared with HPE Networking Support personnel to run a diagnosis on your device.

Administration Settings

The **Site Management** page allows you to modify administrator information, including your Instant On site name and account credentials. You can also add two other administrator accounts to manage the site. All three accounts will have full privileges to the Instant On site configuration and status.

Modifying the Instant On Site Name

To modify the 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 Instant On site under **Site name**.

The site name must be between 1 and 32 alphanumeric characters in length.

Adding Secondary Accounts

Each Instant On site can be managed by five 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. Under **Accounts managing this site**, tap **Add account**, to add a secondary account.
3. Under **Identify Management Account**, enter a valid email ID in the **Email** field.

4. Assign one of the following roles to the account.
   - **Administrator**—Indicates that the account has full access to the site including configuration, monitoring, device maintenance, and all other actions that can be performed on a site, including deleting the site.
   - **Operator**—Indicates that the account has full access to the site including configuration, monitoring, device maintenance, and most actions available on a site. This account does not have the permission to delete the site or manage other accounts.
   - **Delegate**—Indicates that the account has access to limited configurations that do not impact the network infrastructure, and limited actions on clients, networks, and devices. This account does not have the permission to delete the site or manage other accounts.
   - **Viewer**—Indicates that the account only has viewing access to the site but cannot make any modification to the site configurations.
5. Tap **Add account** to add secondary accounts.

Changing Account Role

The **Change Role** setting allows accounts with administrator privileges to change the role of the secondary accounts. The following procedure describes how to change an account role:

1. Tap the advanced menu () icon on the Instant On home screen.
2. Select **Site management** to view the administrator account settings.
3. Under **Account managing this site**, tap the settings () icon beside the secondary account and tap **Change Role**.
4. Select one of the following roles for the user account:
   - **Administrator**
   - **Operator**
   - **Delegate**
   - **Viewer**
5. Tap **Change role** to save the changes.

Removing Account Ownership Access

Instant On allows you to remove the ownership of an existing Instant On account. To remove account ownership of an Instant On site, follow these steps:

1. Tap the advanced menu () icon on the Instant On home screen.
2. Select **Site management** to view the administrator account settings.
3. Under **Account managing this site**, tap the settings () icon beside the administrator account and tap **Remove access**.
4. Tap **Remove access** again in the subsequent screen.

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

Transferring Account Ownership

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

1. Tap the advanced menu () icon on the 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.

Turning on Maintenance Mode

During the maintenance window, you can turn on maintenance mode to disable all email and mobile notifications for all accounts managing the site.

To turn on the maintenance mode, follow these steps:

1. Tap the advanced menu () icon on the Instant On home screen.
2. Tap **Site management** to view the administrator account settings.
3. Tap the () icon in the title bar of the **Site Management** screen.
4. Tap **Turn On Maintenance Mode**. A confirmation window is displayed.
5. Tap **Turn On** in the confirmation window. This disables all email and mobile notifications for all accounts managing the site.

   During this period, an informational message is displayed at the top of the Instant On application screen stating, **This site is under maintenance. Email and mobile notifications are disabled.**
6. Once the site is ready, tap the **View site maintenance** link in the informational message at the top of the Instant On application screen to navigate to the **Site Management** screen.
7. Tap the () icon in the title bar of the **Site Management** screen.
8. Tap **Turn off Maintenance Mode**. This resumes normal operations and reactivates email and mobile notifications for all accounts managing the site.

Deleting a Site

To delete an Instant On site, follow these steps:

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

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

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

Location

The site location is generated after the site is created. By default, the location is automatically geolocated and is based on the location and coordinates of the administrator who created the site.

The following fields are displayed under this section:

- **Location**–Displays the location of the site.
- **Coordinates**–Displays the Latitude and Longitude coordinates of the site.
- **Local Date and Time**–Displays the site local date and time updated in real time and is adjusted if the user selects a different location.

Changing the Location Information of the Site

Follow these steps to modify the location details of the site in the Site Management screen:

1. Under **Site Management** > **Location**, tap on the current location displayed on the screen.
2. Enter the new location details in the **Search locations** bar.
3. From the list of locations displayed, select the radio button next to the address you want the site to be tagged to.
4. Click **DONE**.

Managing Firmware Upgrades

Firmware is the software programmed on Instant On APs, switches and gateways to make sure the devices run and provide functionality to users 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, Switch or Gateway

When an AP, switch, or gateway 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, switch, or gateway 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 HPE Networking. 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 **Schedule update**. Clicking on the **Schedule update** link opens a calendar from which the administrator can pick a specific date on which the update is preferred. The software update can be extended up to a maximum of 30 days from when the alert is generated. If a date is not set in the calendar, the software update will take place based on the **preferred day of the week** setting.

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

1. Tap the advanced menu () icon on the Instant On home screen. Select **Site management** from the menu.
2. Under **Software**, click the **Software update** to view the scheduling options.

3. Select the **Day of the week** for the software update to be installed automatically.
4. Tap on the local time and select a suitable **Site local time**.
5. Under **Installation delay**, move the slider to set the preferred delay for automatic installation of the latest software update. The available options are: No Delay, 1 Week, 2 Weeks, 3 Weeks, and 4 Weeks.

The status of the upgrade is displayed in the **Software update** page by means of a progress bar. The progress bar will be green if the firmware update was successful or yellow if some device(s) failed to install the firmware.

At the end of the software update, a list is displayed that lets the user know how many devices successfully installed the firmware successfully and how many did not complete the installation. If one or more devices failed to update, the Devices Software card displays the warning **Some devices failed to update to new software version**. with a **Retry Installation** link. See **Retrying a Failed Software Update**.

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, a **Device not updated** alert is generated to advise the user about a possible issue on the network. The Instant On APs or switches will continue to operate on the existing software version. You can either wait for the upgrade to be retried automatically during the next maintenance window, or trigger a retry immediately from the Software page. See **Retrying a Failed Software Update**.

Retrying a Failed Software Update

When one or more devices fail to install a new software version during a maintenance window, each affected device raises a **Device not updated** alert and the **Devices Software** card on the **Software** page displays the warning **Some devices failed to update to new software version**. You can trigger another update attempt on demand instead of waiting for the next scheduled maintenance window.

You can open the **Software** page in either of two ways:

- From the alert–Open the **Device not updated** alert and, under **Recommended Actions**, click **Retry software update** to go directly to the Software page.
- From **Site management**–Follow the steps below.

Follow these steps to retry a failed software update from Site management:

1. Click the **Site** icon () at the top-right corner of the UI screen. The **Site management** page is displayed.
2. Click the **Software** tab to view the scheduling options.
3. In the **Devices Software** card, under the **Some devices failed to update to new software version.** warning, click **Retry installation**.
4. The update process restarts for all affected devices in the site. The firmware is downloaded again, if needed, and reinstalled. Track the progress in the progress bar of the **Devices Software** card.

When all devices are updated successfully, the warning and the **Retry installation** link are removed, and the related **Device not updated** alerts are cleared.

The **Retry Installation** action applies to all affected devices in the site, not to an individual device. It is unavailable while a scheduled maintenance window or a previously triggered retry is still in progress.

Instant On Mobile App Compatibility

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

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

About Software

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

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

Chapter 8
Monitoring Site Health

The **Site Health** page provides a summary of the health status of the Instant On devices connected to the network. It shows a consolidated list of alerts that are triggered from the devices provisioned at the site, the health percentage, status, and conditions observed at the site over the last 24 hours.

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

Table 13: *Site Health Messages*

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

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

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

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

Table 14: *Health Conditions*

Condition	Category	Description
Device offline	Device	Raised when a device is offline.
Stack member offline	Device	Raised when one or many members of a stack are online.
Stack offline	Device	Raised when a stack is offline.
PoE fault	Device	Raised when a PoE fault is present on a device.

Table 14: *Health Conditions*

Condition	Category	Description
PoE denied	Device	Raised when there isn't enough PoE power left to power on a client or device on a switch.
Link flapping	Device	Link flapping.
Suboptimal ports health	Device	Raised when many ports are having issues with their connectivity on a specific site device.
Suboptimal clients health	Device	Raised when many clients are having connectivity issues on a specific network.
Suboptimal uplink health	Device	Raised when a device uplink is having connectivity issues.
Suboptimal client performance	Client	Raised when a client is having connectivity issues.
Suboptimal clients health	Client	Raised when a client is having connectivity issues.
Network password connection failure	Network	Raised when clients connect to a network with a bad password.
Authentication failures	Network	Raised when clients experience authentication failure (802.1X or MAC).
Limited network availability	Network	Raised when the network coverage is impacted by one or many site devices offering the network being unexpectedly offline.
WAN connection offline	Network	WAN connection is offline.
Suboptimal WAN connection health	Network	Raised when WAN health is poor.
Connection to Domain Offline	Domain Offline	Device Underpowered

Click on the name of the condition to view additional details about the condition. The side panel displays the information listed in the following table.

Table 15: *Health Conditions- Side Panel*

Parameter	Description
Name	Name of the condition.
Severity	Severity of the condition.
Source	Denotes the device or network for which the health condition is displayed.
Alert	This field is displayed when an alert is triggered. Click on **View Alert** to see the details of the alerts. For more information, see Alerts.

Table 15: *Health Conditions- Side Panel*

Parameter	Description
Symptoms	Displays potential symptoms associated with the condition.
Probable Causes	Displays the probable cause of the condition.
Recommended Actions	Displays the recommended actions the user can perform.

Events

The **Health** > **Events** page lists all the events recorded for the site. The different types of events are classified as follows:

- Network events –Real-time occurrences within the site.
- Audit events–Administrative actions or configuration changes on the site.

Table 16: *Events Information*

Parameter	Description
Event	Description of the event.
State	Displays the status of the event. Listed below are the supported values: ■ Success–Indicates that the event was successful. ■ Failure–Indicates that the event failed.
Occurred	Displays when the event occurred.
Category	Displays the category of the event. Listed below are the supported values: ■ Client ■ Device ■ Network ■ Site ■ Stack ■ Policy ■ Schedule
Source	Displays the source type of the event.
Type	Displays the type of user, **System** or **User**.
Account	Displays the associated email address.
Attributes	Displays additional details like device name, operation type, or previous IP addresses.

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.

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 table below shows the list of possible alerts:

Table 17: *List of Alerts*

Name	Severity	Description
Software available	Informational	A new software has been released
Site offline	Major	When all devices are offline
Device offline	Minor	Minor at first, becomes major after 5 minutes
Device underpowered	Major	When an AP does not receive enough power
Device not updated	Minor	Device failed the software update after repeated attempts. Check that the device is connected. Check the configuration of network services (such as DHCP, DNS, and firewalls). Make sure the instant-on.hpe.com domain is allow-listed. Restart the device or Internet gateway. Review the software update status and try to reinstall the software version(click View software update/ Retry software update to open the Software page).
Domain offline	Major	All connections to the domain are down (main site)
Domain connection offline	Minor	The connection to the domain is down (connected site). Minor at first, becomes major after 5 minutes
Stack member offline	Minor	Minor at first, becomes major after 5 minutes
Stack members offline	Minor	Minor at first, becomes major after 5 minutes
Stack offline	Minor	Minor at first, becomes major after 5 minutes
Miswired stack	Major	Recabling does not allow the stack to function properly
Stack topology changed	Informational	Recabling change the type of stack topology (ring vs daisy chain)
Device power unit failure	Major	No longer delivering PoE
Device power budget exceeded	Minor	Not enough power remaining in the budget
Stack member power unit failure	Major	A stack member can no longer deliver PoE

Name	Severity	Description
Stack members power unit failure	Major	Multiple stack members can no longer deliver POE
Stack member power budget exceeded	Minor	Not enough power remaining in the budget for a stack member
Stack members power budget exceeded	Minor	Not enough power remaining in the budget for stack members
Stack member not updated	Minor	A stack member failed the software update after repeated attempts. Check that the device is connected. Check the configuration of network services (such as DHCP, DNS, and firewalls). Make sure the instant-on.hpe.com domain is allow-listed. Restart the device or Internet gateway. Review the software update status and try to reinstall the software version(click View software update/ Retry software update to open the Software page).
Stack members not updated	Minor	Multiple stack members failed the software update. Check that the device is connected. Check the configuration of network services (such as DHCP, DNS, and firewalls). Make sure the instant-on.hpe.com domain is allow-listed. Restart the device or Internet gateway. Review the software update status and try to reinstall the software version(click View software update/ Retry software update to open the Software page).
Watchlisted client offline	Minor	A watchlisted client went offline
Uplink type changed	Informational	The device uplink has changed from a wired connection to an over-the-air connection
Domain offline	Major	All tunnels are down (main site)
Connection to domain offline	Minor	Tunnel down (connected site).
WAN offline	Minor	WAN connection is offline.
Incompatible device management VLAN	Major	The management VLAN provisioned on the device differs from the one configured on the site. The device is Suspended until the VLANs match.

Alert Triggered When Instant On AP25 Access Point is Underpowered

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

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

Network Tests

The **Test Connectivity** option is used to test the reachability of an Instant On device. To perform a network test, you need to enter a **Network Destination** to be reached.

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

1. Tap the **Site Health** banner () on the Instant On home page.
2. Tap the () icon in the title bar of the **Site Health** screen and then tap on **Test Connectivity** from the drop-down menu. The **Connectivity** screen is displayed.
3. Under **Source**, select an Instant On device from the drop-down list.

   Only active devices of a site can be selected in this field. It could be a Switch or an AP.
4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

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

Table 18: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Chapter 9
Devices

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

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

1. Tap the Devices () tile on the Instant On mobile app home page.
2. The **Devices** page lists the gateways, APs, secure gateways, and switches added in the network and their operational status. Tap on a gateway, AP, or switch to view the details of the device.

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

Adding a Device

Instant On allows you to add up to 125 devices to a site. To add a device to the inventory list, follow these steps:

1. Click the Devices () tile on the Instant On mobile app home page.
2. Tap add () at the bottom right corner of the page. The **Extend Network** page is displayed.
3. Place your Instant On device in its destination area and make sure it is powered on and connected to the Internet. (Optional) To include devices which are connected over-the-air, select the **Include outdoor over-the-air devices** checkbox.
4. Tap **Search for my devices**. 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.
5. Review the device(s) discovered and add them to your site.

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

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

Adding a Device to an Empty Site

If the Instant On site does not have any devices or has only offline devices in the inventory, you will be required to manually select an option to add a new device.

1. Tap the Devices () tile on the Instant On mobile app home page.
2. Tap add () at the bottom right corner of the page. The **Extend Network** page is displayed.
3. Place your Instant On device in its destination area and make sure it is powered on and connected to the Internet. Tap **Continue**.

4. Enter the **Serial Number** of the device which you choose to add to the inventory, or select one of the following options:
   - **Search for devices**–Initiates the LLDP automatic search. It usually takes around 4-5 minutes for the Instant On devices to be detected.
   - **Scan barcode or QR code**–Use the barcode or QR code scan method to add your devices. For more information, see Discovering Available Devices.
   - **Automatic (Bluetooth devices only)**–Initiates the BLE search to add Instant On devices that have the bluetooth function.

Types of Devices

Instant On supports four types of devices:

- Access Points
- Routers
- Switches and Switch stacks
- Gateway

Extending your Network

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

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

Extend using a cable

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

1. Tap the Devices () tile on the Instant On mobile app home page.
2. Tap add () at the bottom right corner of the page. The **Extend Network** page is displayed.

   (Optional) To include devices which are connected over-the-air, select the **Include outdoor over-the-air devices** checkbox in the **Extend Network** page.
3. Tap **How to extend my network**.
4. In the **Extend Network** screen, tap **Extend using a cable**.
5. 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).
6. Wait for the LED lights on the additional Instant On devices to blink alternatively between green and amber.
7. Select **Search for my devices** to make the 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.

8. Review the device(s) discovered and add them to your site.

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

9. 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 Instant On scan for both wired and wireless devices. The AP should show up in the list of devices detected in the network.
6. Review the device(s) discovered and add them to your site.

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

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

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.

Scenarios That Trigger Error Messages When Adding Devices in the Inventory

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

Table 19: *Scenarios and Error Messages*

Scenario	Error Message
Entering a serial number of a device that is already onboarded on another site	Already assigned to another site.

Scenario	Error Message
Adding a device that is connected between the ISP modem and the Instant On router	Upon clicking Search for devices, the system will recognize and display the devices along with the following error message: A new Instant On device that is connected between the ISP modem and the Instant On router shall not be allowed to be added to the network.
Entering the serial number of a device that is connected to another site, but not yet assigned	Device is on the same network as another site

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

Radio Management

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

Changing these settings may disconnect clients from the network.

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

1. Tap the Devices **()** tile on the Instant On home page.
2. Tap the advanced menu () icon and select **Radio management**.
3. If you have an AP32 access point, deployed at the site, select the preferred frequency from the **Radio frequencies (AP32 only)** drop-down list.

- For AP32 access points, mesh configuration is possible under the 5 GHz and 6 GHz radios. When using AP32 as a mesh point on 5 GHz radio and the user decides to change the radio frequency to either 2,4 GHz + 6 GHz globally or locally, the mesh point will go offline and the user will have to connect it using an Ethernet cable instead of mesh to bring it back online in the site. User can then change back radio frequencies drop-down list for AP32 to include 5 GHz to re-establish the mesh link.
- For AP32 access points, mesh link is possible on the 6 GHz radio only between two or more AP32 access points.
- If the user decides to select 2.4 GHz and 6 GHz, a message will be displayed to alert the user that mesh devices might be affected as they are operating under 5 GHz. Additional confirmation from the user is not required to proceed.

4. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio–**20 MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio–**20 MHz**, **20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.
   c. 6 GHz Radio–**20/40/80 MHz** or **20/40/80/160 MHz (default)**.

- The 6 GHz radio spectrum is currently available only on AP32 access points.
- The channel width of 160 MHz is available as a global setting only after an AP25 or an AP32 access point is added to the inventory for the first time. However, the **20/40/80/160 MHz** setting will still be available after all the AP25 and AP32 access points are removed from the inventory.
- The channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for AP32 access points. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.

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

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

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

The changes made in the above procedure are saved automatically.

Loop Protection

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

- Instant On Proprietary Mechanism
- Spanning Tree Loop Protection

Instant On Proprietary Mechanism

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

Spanning Tree Loop Protection

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 Devices **()** tile on the Instant On home page.
2. Tap the advanced menu () icon in the **Devices** page and select **Loop protection**.
3. Slide the **Spanning Tree Loop Protection** toggle switch to enabled ( ), to configure loop protection on the network. The page lists the spanning tree diagnostics such as the **Root bridge device** connected to the network and its **priority** value. It also indicates the duration and number of times the **Topology changed** for the root switch device on the network.

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

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

Bridge Priority Assignments

The **Bridge Priority** page displays the participating spanning tree devices and their bridge priority. The priority will be automatically determined using the topology and the position of the devices related to each other. The root bridge is assigned to the Instant On switch or router that is closest to the internet router or entry point to a private network. The root bridge priority is assigned the default value of 28762. All subsequent Instant On switches and routers are assigned priority values based on their distance from the root bridge.

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

- Instant On 1 would be assigned priority 28762 (root)
- Instant On 2 would be assigned priority 36864
- Instant On 3 would be assigned priority 40960

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

1. Tap the Devices **()** tile on the Instant On home page.
2. Tap the advanced menu () icon in the **Devices** page and select **Loop protection**.
3. Slide the **Spanning Tree Loop Protection** toggle switch to enabled ( ), to configure loop protection on the network.

4. Tap the **Bridge priority assignments** link. The details of the **Base priority** and **Bridge priority** are displayed.
5. To modify the **Base priority**, tap the drop-down arrow and select a priority from the list.
6. If you choose to recalculate the bridge priority, tap the advanced menu () on the header and then tap **Recalculate bridge priority**.

   The changes are auto saved.

Power Management

The **Power Management** screen allows you to enable or disable the **Energy Efficient Ethernet** (EEE) or Green Port Management reduces power consumption on switch ports when data activity is low or idle. Regular heartbeats are sent to gauge port activity. Ports are fully enabled when data activity resumes. This function allows you to manage all site-wide Energy Efficiency features and is enabled by default.

Energy Efficient Ethernet displays a warning message immediately upon the user enabling the EEE mode.
Warning Message: Changing power efficiency preferences will reset all device ports and temporarily affect network services.

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

The **Power Schedule** configuration is applied to every PoE port with or without connected site devices.

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

1. Tap the Devices **()** tile on the Instant On home page.
2. Tap the advanced menu () icon in the **Inventory** page and select **Power Schedule**.
3. Under **Ruled by a schedule**, select one of the following options:
   a. **Fixed**–Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) during which the switch enables the power supply for the PoE ports.
   - Select the days on which the switch should supply power to PoE ports.
   - Select one of the following options under **Active hours during the day**:
     - **All day**: The switch provides power to the PoE ports throughout the day.
     - **Active between**: The switch provides power to the PoE ports for the specified time period. Configure the **Start Time** and **End Time** for PoE supply as required.

   b. **Variable**–Indicates the schedule configuration that allows users to set up a different time range on a daily basis.
   - Follow these steps to enable the power schedule for specific days of the week:
     i. Tap the () icon for the day of the week for which you need to configure a schedule.
     ii. Set the toggle switch to **Active** ( ).
     iii. Select one of the following options under **Active hours during the day**:
       - **All day**: The switch provides power to the PoE ports throughout the day.
       - **Active between**: The switch provides power to the PoE ports for the specified time period. Configure the Start Time and End Time for PoE supply as required.

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

4. You can also configure the PoE power schedule on multiple ports for devices in the inventory.
   a. Tap the **Power schedule assignment** link.
   b. Tap on an Instant On router or switch from the list of devices displayed.
   c. Tap on the ports for which the power schedule should be enabled. Alternatively, you can also tap on **Assign to All**, to enable the power schedule for all the available PoE ports on that device.
5. Tap the back arrow () to return to the **Devices** screen. The Instant On devices will automatically begin to synchronize after the new configuration.

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

Gateway Details

The gateway details page displays the configuration details of an Instant On secure gateway deployed at the site and allows the administrator to modify some basic settings related to the device.

Viewing Gateway Details

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap any of the gateways listed in the **Devices** list. The **Gateway Details** page is displayed with details.

   View the gateway details such as the gateway name, IP address, MAC address, Serial number, SKU.

   To reset the device name to its default name, select the device name text field, tap the reset icon and then tap **Update** to save the change. The reset icon is displayed only when the device is assigned a custom device name.

Connectivity

The Instant On gateway is connected as a primary device connected to the internet or 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 gateway. The Instant On gateway acts as a DHCP service on the local network and provides IP addresses to requesting devices.

The connectivity section contains the following information:

- **Uplink–** Displays the name of the WAN Network the gateway is connected. Tap on the link to view the uplink **Network Details** screen. For more information, see WAN .
- **Internet IP**–IP Address of the Instant On gateway.
- **IP Assignment**–By default, the IP Address Assignment for the Instant On gateway is set to automatic. The Instant On gateway will inherit the IP address assigned by the DHCP in the network.

  To configure the network settings on an Instant On gateway complete the following steps:

1. Under the **Connectivity** section of the **Gateway Details** page, tap **IP assignment**.
2. Configure the **Base IP address**—The **Base IP address** is used to configure the LAN IP address for the gateway interface.
3. Configure the **Subnet mask**—Tap the drop-down arrow (▼) and select the IP address range for the network.
4. Under **Automatic IP address assignment**, configure the following parameters:
   - Start IP address
   - End IP address
5. Under the **DNS resolution**, configure the following parameters:
   - Domain suffix—Part of a domain name that comes after the main domain.
   - Automatic (default) – The IP address for the gateway is assigned by the DHCP server.
   - Static—Assign a static IP address for the gateway. To configure a static IP address enter the IP address of the primary and secondary DNS server.
6. Tap **Reserve an IP address** under the **IP address reservations for Management Network**, to view the **Reserve an IP Address** screen.
7. In the **Reserve an IP Address** screen select the device for which you want to reserve the DHCP IP addresses for clients and devices.

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

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

To configure a static IP address , under **IP Assignment** > **DNS resolution**, select **Static** and type the **Primary DNS server** and **Secondary DNS Server** details.

Power over Ethernet

Displays information about the **Total Budget** and **Ports Consumption**.

Ports

The **Ports** section in the **Gateway Details** page visually represents the physical ports for the gateway 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.

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

- Status
- Networks
- Port Details
- Clients and Devices

Status

The **Status** tab view under **Ports** is selected by default when you arrive on the **Gateway 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 gateway and displays its current status. Port 5 for SG2505P gateway and Port 4 for SG1004 gateway is always selected by default and acts as the default uplink port for the gateway. Tap on any of the gateway ports to view the following details:

- Port number—The physical port number of the gateway.
- 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.
- Connected to—Displays the name of the device the port is connected. Tap on clicking the device name and the selected devices detail screen is displayed.
- Port details—A hyperlink that redirects you to the **Port Details** screen of the selected port, where you can access configuration options.

Networks

In the **Networks** tab, choose the network from the **Selected network** drop-down list. It displays the network details for the selected port.

Port Details

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 gateway can be assigned a separate VLAN ID and configured to manage the network traffic.

You must connect the primary WAN port (Port 4 – SG1004 or Port 5 – SG2505P) of the Instant On gateway to the ISP modem or a device that provides the Internet connection.

The primary WAN ports supports up to 2.5 Gbps. Both gateways are provisioned to allow one LAN port to be converted into a secondary WAN port. For more information on secondary WAN, see WAN.

Secondary WAN Port Details:

- SG1004 Gateway:
  - Port 3 can be converted into a secondary WAN port.
  - Port 3 supports speeds of up to 1.2 Gbps.
- SG2505P Gateway:
  - Either Port 3 or Port 4 can be converted into a secondary WAN port.
  - Only one port can be used as a secondary WAN port at a time.
  - Port 4 supports up to 2.5 Gbps.
  - Port 3 supports up to 1.2 Gbps.

Select a port in the **Gateway Details** page and tab on **Port Details** to view the **Port Details** screen.

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

- Name of the port in read and write mode.
- The **Enable port** toggle switch allows you to enable the port status. This field is set to enabled by default. Clients and devices are allowed to draw power and connect to the port when it is set to enabled.
- **Port profile**—Allows the administrator to assign a port profile.
  - **Use port profile**—Enable the **Use port profile** to view the **Port profile** drop-down list.
  - **Port profile**—To assign a port profile to the select port, select a port profile from the drop-down list and tab **Ok**. After assigning a port profile, tab on **View port profile** to view and update the port profile configuration.

- **Port Options** > **Power Management**
  - **No Power over Ethernet**–No power is allocated to the port.
  - **Usage (default)** – The power allocated to the port is based on usage and is unrestricted.
  - **Class** – The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts
Class 2	7 Watts
Class 3	15.4 Watts
Class 4	30 Watts

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

- When two ports belonging to the same priority are demanding power, the port with the least port number is given priority. Example: When port 2 and 3 are assigned **Critical** class and the gateway has a power budget constraint, device on port 2 will receive full power and the remaining power budget will be allocated to the device on port 3.
- PoE priority cannot be configured for Instant On devices. By default, Instant On devices are configured with **Usage** mode and **Critical** for **Port Priority.**

  - **Power Mode**–Determines how the switch delivers Power over Ethernet (PoE) to connected devices during a reboot. Select one of the following options:
    - **Always On** (default)–PoE remains active on eligible ports throughout a reboot. Power is maintained from the moment the hardware restarts until the switch is fully operational and the ports complete initialization, unless input power is lost.
    - **Quick**–The hardware restores PoE to eligible ports as soon as it restarts, with no software dependency, so power is delivered as quickly as possible–before the switch has fully started.
    - **Normal**–The standard power behavior, in which power is applied to the ports only after the configuration is restored.

Power Mode is supported only on the Instant On 1840 and 1940 Switch Series, and is not displayed on other devices.

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

- **Included Networks**
  - **Untagged**–This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
  - **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
    - **All Wired Networks**–Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
    - **Selected Wired Networks**–Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.

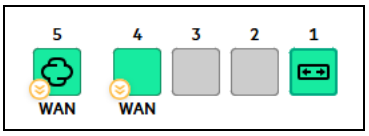
Clients and Devices

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

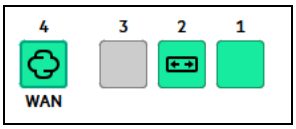
Clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. For indirectly connected clients, only their MAC address is displayed.

The following section describes the different behaviors of the gateway ports.

Figure 5 *Gateway Ports*



SG2505P Gateway



SG1004 Gateway

Color of the Ports

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

The color of the port will be:

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

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

Device Lights

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

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

1. Tap the **Devices** tile on the HPE Networking Instant On Portal home page.
2. Select the gateway from the devices inventory.
3. In the **Gateway Details** screen, scroll down to the **Device Lights** section and choose one of the following options:
   - **Normal mode (default)**– Use this option to turn on the status lights. This option is selected by default.
   - **Quiet light mode**–Use this option to turn off the status lights. When this option is selected, the device lights are turned off during normal operation.

Network tools

The **Test Connectivity** option is used to test the reachability of an Instant On device. To perform a network test, you need to enter a **Network Destination** to be reached.

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the gateway listed in the **Devices** inventory. The **Gateway Details** screen is displayed with details.
3. Tap on the **Network tools** accordion on the **Gateway Details** screen to view the tools available.
4. Tap on **Test connectivity** from the drop-down menu. Displays the **Connectivity** screen.
5. Under **Source**, select an Instant On device from the drop-down list.

   Only active devices of a site can be selected in this field. It could be a Switch or an AP.
6. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
7. Tap **Start connection test**.

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

Table 20: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>

Connectivity Rating	Roundtrip Time	Test Results Format
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Advanced Menu

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

- Locate
- Restart Device
- Restart Device
- Restart Device

Locate

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

To locate your Instant On gateway, follow these steps:

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

Restart Device

To restart the device:

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

Replace Device

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

NOTE

- This option is visible only when the Instant On gateway is offline.
- When a higher-model gateway is replaced with a lower-model gateway, certain configurations may not be carried over to the newly replaced gateway.
- It is recommended to replace the failed gateway with a working gateway of the exact same model to ensure all device configurations are successfully transferred to the replaced gateway.

1. In the devices inventory, tap the failed Instant On gateway. The **Gateway Details** screen is displayed.
2. Tap the advanced menu () icon in the title bar of the **Gateway Details** screen.
3. Tap **Replace device**.
4. In the **Replace Device** screen, tap **Search** when the device lights are alternating between green and amber.
5. Enter the **Serial Number** of the device which you choose to add to the inventory, or select one of the following options:
   - **Search for devices**–Initiates the LLDP automatic search. It usually takes around 4-5 minutes for the Instant On devices to be detected.
   - **Scan barcode or QR code**–Use the barcode or QR code scan method to add your devices. For more information, see Discovering Available Devices.
6. Tap the Instant On gateway to replace with the failed switch in the inventory.
7. Tap **Replace**.
8. Tap **Finish**.

Remove from inventory

To remove the gateway from the inventory, follow these steps:

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

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 Devices() tile on the Instant On home page.
2. Tap any of the APs listed in the **Devices** 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, SKU, AP type, radio, and the number of the clients connected on each radio channel.

   To reset the device name to its default name, select the device name text field, tap the reset icon and then tap **Update** to save the change. The reset icon is displayed only when the device is assigned a custom device name.

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** screen, tap **Advanced LAN parameters**.
2. Choose one of the following:
   - **Automatic (default)**: This is the default setting for all APs. The Instant On device will request an IP address from a DHCP service running on the LAN. This option is visible only in the mobile app.
   - **Static**: To specify a fixed IP address on the LAN for your Instant On device, select the **Static** radio button in the mobile app 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.
     - **Primary DNS server**–Enter the IP address of the Primary DNS server.
     - **Secondary DNS server**–Enter the IP address of the Secondary DNS server.
3. Tap **DONE** to save the settings.

802.1X Authentication

Allows you to select the RADIUS profile for the access point.
In the RADIUS Profile drop-down list, select either none, or an existing RADIUS profile.
For more information on creating a radius profile, see Creating a RADIUS Profile.

Ports

Every network requires the E0/PT or ENET port of the AP or Router to be connected to the gateway or switch using an Ethernet cable. Each Instant On AP has a single port, except for the AP11D or AP22D devices which have an additional 3 LAN ports–E1, E2, and E3 respectively. These ports can be used to connect additional APs in the network. The ports are visually represented on the page in the same manner as the actual physical ports on the device. The E0/PT or ENET port is always selected by default and acts as the default uplink port for the router. To view the details of the port and the uplink status, follow these steps:

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

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.

Depending on the Access point and the port selected, the **Port details** screen display the following:

- Name–Name assigned to the port.
- **Enable port**–Allows the administrator to enable or disable the device port.
- **Port profile**–Allows the administrator to assign a port profile.
  - **Use port profile**–Enable the **Use port profile** to view the Port profile drop-down list.

- **Port profile**–To assign a port profile to the select port, select a port profile from the drop-down list and tab **Ok**. After assigning a port profile, tab on **View port profile** to view and update the port profile configuration.

- **Authentication**–The authentication option is available only when **Use Port Profile** is disabled. By default, **No Authentication** is selected. To select **Port-based** authentication, you must select a RADIUS profile listed under **802.1X Authentication**. The RADIUS server configuration is part of the RADIUS profile. From the **Overview** page, you can assign a RADIUS profile to the device.
- **Port Options** > **Power Management**
  - **No Power over Ethernet**–No power is allocated to the port.
  - **Class (default)** – The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts
Class 2	7 Watts
Class 3	15.4 Watts
Class 4	30 Watts

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

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 OnAP11D or AP22D device can be assigned a separate VLAN ID and configured to manage the network traffic. The following procedure describes how to map a network to a VLAN port:

1. Tap any of the AP11D or AP22D routers listed in the **Inventory**. The **Router Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the router.
3. From the **Selected network** drop-down list, choose the network you want to map a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Untagged**–This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
   - **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:

- **All Wired Networks**–Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
- **Selected Wired Networks**–Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Networks** checkbox removes the tagged status from all eligible LAN networks.

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

Clients and Devices

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

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

Radios

This section provides details on the clients operating on the 2.4 GHz, 5 GHz, and 6 GHz radios of the device:

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

Radio Details

The **Radio Details** page overrides the radio settings configured at the site level and allows you to configure 2.4 GHz, 5 GHz, and 6 GHz radio settings which are specific to the selected Instant On device. All active wireless networks associated with different radios are enabled by default. To disable broadcasting of the wireless networks on a specific radio band, deselect the **Enable Networks on This Radio** checkbox.

Mesh configuration continues to operate on the 5GHz or 6GHz band even if the **Enable Networks on This Radio** checkbox is unchecked.

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

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

1. Under **Radios**, tap on **Radio details**.
2. Slide the toggle switch ( ) beside **Specific radio management** for **2.4 GHz Radio**, **5 GHz Radio**, and **6 GHz Radio** respectively to view the device specific radio settings.

NOTE

The 6 GHz radio spectrum is currently available only on AP32 access points.

3. If you have an AP32 access point, deployed at the site, select the preferred frequency from the **Radio frequencies (AP32 only)** drop-down list. This setting overrides the radio selection in the global radio management configuration for AP32 access points.

NOTE

- For AP32 access points, mesh configuration is possible under the 5 GHz and 6 GHz radios. When using AP32 as a mesh point on 5 GHz radio and the user decides to change the radio frequency to either 2,4 GHz + 6 GHz globally or locally, the mesh point will go offline and the user will have to connect it using an Ethernet cable instead of mesh to bring it back online in the site. User can then change back radio frequencies drop-down list for AP32 to include 5 GHz to re-establish the mesh link.
- For AP32 access points, mesh link is possible on the 6 GHz radio only between two or more AP32 access points.
- If the user decides to select 2.4 GHz and 6 GHz, a message will be displayed to alert the user that mesh devices might be affected as they are operating under 5 GHz. Additional confirmation from the user is not required to proceed.

4. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio–**20 MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio–**20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.
   c. 6 GHz Radio–**20/40/80 MHz** or **20/40/80/160 MHz (default)**.

NOTE

The channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for AP32 access points. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.

5. Based on your selection for each radio, the **Channel selection** options are refreshed. All channels are enabled by default and are displayed in orange. The disabled channels are displayed in gray.
6. Configure the **Transmit power** range for the 2.4 GHz, 5 GHz, and 6 GHz radios by adjusting the slider between a minimum and maximum value. For example, if the slider is set between **Very high** and **Max**, the radio transmits between 30 dBm and maximum power. The available values are:

Transmit Power Level	Threshold for 2.4 GHz Radio (in dBm)	Threshold for 5 GHz Radio (in dBm)
Low	6 dBm	15 dBm
	9 dBm	18 dBm
	12 dBm	

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

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

The changes made in the above procedure are saved automatically.

Dynamic Channel Display

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

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

Network Assignment

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

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

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

   The **Network Assignment** screen is displayed.
2. Under **Wireless networks supporting client connections through this device**, tap the checkbox next to a network name to assign the AP to that network.

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

Access Point Lights

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

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

1. Tap the **Devices** tile on the HPE Networking Instant On Portal home page.
2. Select an AP from the devices inventory.
3. In the **Device Details** screen, choose one of the following options:
   - **Normal mode (default)**– Use this option to turn on the status and radio lights. This option is selected by default.
   - **Quiet light mode**–Use this option to turn off the status and radio lights. When this option is selected, the device lights are turned off during normal operation.

Advanced Menu

Locating Your Instant On AP

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

To locate your Instant On AP, follow these steps:

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

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 Device Inventory

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

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

Follow these steps to remove an AP which is offline:

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

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

Replacing a Failed AP from the Inventory

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

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

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

1. Tap the **Devices** tile () on the Instant On home page.
2. Tap the failed AP that you want to replace. The **AP Details** page is displayed. A rectangular bar appears below the device name when an alert is triggered.
3. Tap the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the AP.
4. On the **Alert Details** page, tap on the replace link. The **Replace Access Point** page is displayed. Alternatively, you can also perform this action by tapping the advanced menu () icon in the title bar of the **Access Point Details** screen and selecting **Replace device** from the menu.
5. Unplug the AP you want to replace and plug in your new AP to the network.
6. Tap **Search** when the device lights are alternating between green and amber.
7. In the **Replace Device** page, enter the **Serial Number** of the device which you choose to add to the inventory, or select one of the following options:
   - **Search for devices**–Initiates the LLDP automatic search. It usually takes around 4-5 minutes for the Instant On devices to be detected.
   - **Scan barcode or QR code**–Use the barcode or QR code scan method to add your devices. For more information, see Discovering Available Devices.
   - **Automatic (Bluetooth devices only)**–Initiates the BLE search to add Instant On devices that have the bluetooth function.
8. Once your AP is detected, tap **Replace**.
9. If you still cannot find your device, select **I don't see my device** button to view the troubleshooting options.

Network tools

The **Test Connectivity** option is used to test the reachability of an Instant On device. To perform a network test, you need to enter a **Network Destination** to be reached.

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the gateway listed in the **Devices** inventory. The **Access Point Details** screen is displayed with details.
3. Tap on the **Network tools** accordion on the **Access Point Details** screen to view the tools available.
4. Tap on **Test connectivity** from the drop-down menu. Displays the **Connectivity** screen.
5. Under **Source**, select an Instant On device from the drop-down list.

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

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

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

Table 21: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Reserving an IP Address for a Device

In addition to reserving an IP address from the network's **IP Assignment** tab, you can also reserve or remove a client's IP address directly from the device's page for both online and offline devices.

To reserve an IP Address for a device:

1. Tap the advanced menu () icon in the title bar of the **Switch Details** screen.
2. Select **Add IP Address Reservation** from the list. To remove it, tap **Remove IP Address Reservation**.

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 APs can act as a Wi-Fi router, but only AP11D or AP22D device can have wired configuration.

Viewing Router Details

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

1. Tap the **Devices**() tile on the Instant On home page.
2. Tap the router listed in the **Devices** list. The **Router Details** page is displayed with details. View the Router details such as the Router name, IP address, MAC address, Serial number, SKU, Router type, radio, and the number of the clients connected on each radio channel.

To reset the device name to its default name, select the device name text field, tap the reset icon and then tap **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.

Connectivity

The Instant OnAP11D or AP22D device is connected as a primary Wi-Fi router to the ISP provided modem, using an Ethernet cable. The **Connectivity** section lists the gateway IP address of the uplink and the **Internet IP** forwarded by the ISP provided modem to the router. The Instant On router acts as a DHCP service on the local network and provides IP addresses to requesting devices.

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

The connectivity section contains the following information:

- **Uplink–** Displays the name of the WAN Network the router is connected. Tap on the link to view the uplink **Network Details** screen. For more information, see WAN .
- **Internet IP**–IP Address of the Instant On gateway.
- **IP Assignment**–By default, the IP Address Assignment for the Instant On gateway is set to automatic. The Instant On gateway will inherit the IP address assigned by the DHCP in the network.

  To configure the network settings on an Instant On gateway complete the following steps:

  1. Under the **Connectivity** section of the **Gateway Details** page, tap **IP assignment**.
  2. Configure the **Base IP address**–The **Base IP address** is used to configure the LAN IP address for the gateway interface.
  3. Configure the **Subnet mask**–Tap the drop-down arrow (▼) and select the IP address range for the network.
  4. Under **Automatic IP address assignment**, configure the following parameters:
     - Start IP address
     - End IP address
  5. Under the **DNS resolution**, configure the following parameters:
     - Domain suffix–Part of a domain name that comes after the main domain.
     - Automatic (default) – The IP address for the gateway is assigned by the DHCP server.
     - Static–Assign a static IP address for the gateway. To configure a static IP address enter the IP address of the primary and secondary DNS server.
  6. Tap **Reserve an IP address** under the **IP address reservations for Management Network**, to view the **Reserve an IP Address** screen.
  7. In the **Reserve an IP Address** screen select the device for which you want to reserve the DHCP IP addresses for clients and devices.

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

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

  To configure a static IP address , under **IP Assignment** > **DNS resolution**, select **Static** and type the **Primary DNS server** and **Secondary DNS Server** details.

802.1X Authentication

Allows you to select the RADIUS profile for the router.
In the RADIUS Profile drop-down list, select either none, or an existing RADIUS profile.
For more information on creating a radius profile, see Creating a RADIUS Profile.

Ports

Every network requires the E0/PT or ENET port of the AP or Router to be connected to the gateway or switch using an Ethernet cable. Each Instant On AP has a single port, except for the AP11D or AP22D devices which have an additional 3 LAN ports–E1, E2, and E3 respectively. These ports can be used to connect additional APs in the network. To view the details of the ports and the uplink status, follow these steps:

1. Tap any of the AP11D or AP22D 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 or AP22D 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 enable or disable the port. This field is set to enable by default.
- **Port profile**–Allows the administrator to assign a port profile.
  - **Use port profile**–Enable the **Use port profile** to view the **Port profile** drop-down list.
  - **Port profile**–To assign a port profile to the select port, select a port profile from the drop-down list and tab **Ok**. After assigning a port profile, tab on **View port profile** to view and update the port profile configuration.
- **Authentication**–The authentication option is available only when **Use Port Profile** is disabled. By default, **No Authentication** is selected. To select **Port-based** authentication, you must select a RADIUS profile listed under **802.1X Authentication**. The RADIUS server configuration is part of the RADIUS profile. From the **Overview** page, you can assign a RADIUS profile to the device.

Networks

After creating your network, you have the option to map the network to a VLAN port which, either allows traffic from all networks or only for a specific network. Each port in the Instant On AP11D or AP22D device can be assigned a separate VLAN ID and configured to manage the network traffic. The following procedure describes how to map a network to a VLAN port:

1. Tap any of the AP11D or AP22D routers listed in the **Inventory**. The **Router Details** page is displayed.
2. Select the **Networks** tab, under **Ports** to view the ports on the router.
3. From the **Selected network** drop-down list, choose the network you want to map a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
   - **Tagged networks assignment**—The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
     - **All Wired Networks**—Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
     - **Selected Wired Networks**—Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.
7. Tap **Done** to finish mapping the network to the port.

Clients and Devices

The following procedure describes how to view the clients and devices connected to a specific port on the AP11D or AP22D router:

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

Radios

This section provides details on the clients operating on the 2.4 GHz, 5 GHz, and 6 GHz radios of the device:

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

Radio Details

The **Radio Details** page overrides the radio settings configured at the site level and allows you to configure 2.4 GHz, 5 GHz, and 6 GHz radio settings which are specific to the selected Instant On device. All active wireless

networks associated with different radios are enabled by default. To disable broadcasting of the wireless networks on a specific radio band, deselect the **Enable Networks on This Radio** checkbox.

NOTE

Mesh configuration continues to operate on the 5GHz or 6GHz band even if the **Enable Networks on This Radio** checkbox is unchecked.

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

NOTE

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

1. Under **Radios**, tap on **Radio details**.
2. Slide the toggle switch ( ) beside **Specific radio management** for **2.4 GHz Radio**, **5 GHz Radio**, and **6 GHz Radio** respectively to view the device specific radio settings.

NOTE

The 6 GHz radio spectrum is currently available only on AP32 access points.

3. If you have an AP32 access point, deployed at the site, select the preferred frequency from the **Radio frequencies (AP32 only)** drop-down list. This setting overrides the radio selection in the global radio management configuration for AP32 access points.

NOTE

- For AP32 access points, mesh configuration is possible under the 5 GHz and 6 GHz radios. When using AP32 as a mesh point on 5 GHz radio and the user decides to change the radio frequency to either 2,4 GHz + 6 GHz globally or locally, the mesh point will go offline and the user will have to connect it using an Ethernet cable instead of mesh to bring it back online in the site. User can then change back radio frequencies drop-down list for AP32 to include 5 GHz to re-establish the mesh link.
- For AP32 access points, mesh link is possible on the 6 GHz radio only between two or more AP32 access points.
- If the user decides to select 2.4 GHz and 6 GHz, a message will be displayed to alert the user that mesh devices might be affected as they are operating under 5 GHz. Additional confirmation from the user is not required to proceed.

4. Choose a **Channel width** for each of the following:
   a. 2.4 GHz Radio–**20 MHz (default)** or **20/40 MHz**.
   b. 5 GHz Radio–**20/40 MHz**, **20/40/80 MHz (default)**, or **20/40/80/160 MHz**.
   c. 6 GHz Radio–**20/40/80 MHz** or **20/40/80/160 MHz (default)**.

NOTE

The channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for AP32 access points. However, these access points when deployed as mesh points will operate only on **20/40 MHz** or **20/40/80 MHz (default)**.

5. Based on your selection for each radio, the **Channel selection** options are refreshed. All channels are enabled by default and are displayed in orange. The disabled channels are displayed in gray.
6. Configure the **Transmit power** range for the 2.4 GHz, 5 GHz, and 6 GHz radios by adjusting the slider between a minimum and maximum value. For example, if the slider is set between **Very high** and **Max**, the radio transmits between 30 dBm and maximum power. The available values are:

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

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

The changes made in the above procedure are saved automatically.

Dynamic Channel Display

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

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

Network Assignment

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

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

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

   The **Network Assignment** screen is displayed.

2. Under **Wireless networks supporting client connections through this device**, tap the checkbox next to a network name to assign the AP to that network.

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

Advanced Menu

Locating Your Instant On Router

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

To locate your Instant On device, follow these steps:

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

Running a Connectivity Test

The **Test Connectivity** option is used to test the reachability of an Instant On device. To perform a network test, you need to enter a **Network Destination** to be reached.

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

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

   Only active devices of a site can be selected in this field. It could be a Switch or an AP.
4. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
5. Tap **Start connection test**.

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

Table 22: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>

Connectivity Rating	Roundtrip Time	Test Results Format
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Restarting Your Instant On Router

To restart your router, follow these steps:

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

Replacing a Router from the Inventory

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

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

1. Tap the **Devices** () tile on the Instant On Solution home page.
2. Tap the offline router that you want to replace. The **Router Details** page is displayed. A rectangular bar appears below the device name when an alert is triggered.
3. Tap the **Alerts** link. You will be directed to the **Alert Details** page which provides more information about the unusual activity and a link to replace the router.
4. In the **Alert Details** page, tap on the replace link. The **Replace router** page is displayed. Alternatively, you can also perform this action by tapping the advanced menu () icon in the title bar of the **Router Details** screen and selecting **Replace device** from the menu.
5. Unplug the router you want to replace and plug in your new Instant On AP11D device into your ISP modem.
6. Tap **Continue** when the device lights are alternating between green and amber.
7. In the **Replace Device** page, enter the **Serial Number** of the device which you choose to add to the inventory, or select one of the following options:
   - **Search for devices**–Initiates the LLDP automatic search. It usually takes around 4-5 minutes for the Instant On devices to be detected.
   - **Scan barcode or QR code**–Use the barcode or QR code scan method to add your devices. For more information, see Discovering Available Devices.
   - **Automatic (Bluetooth devices only)**–Initiates the BLE search to add Instant On devices that have the bluetooth function.
8. 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.
9. If you still cannot find your device, select **I don't see my Wi-Fi router** button to view the troubleshooting options.

Switch Details

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap any of the switches listed in the Devices 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, SKU, switch model, and ports.

   To reset the device name to its default name, select the device name text field, tap the reset icon and then tap **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.

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

- Connectivity
- Power over Ethernet (PoE)
- Ports
- Network tools

Connectivity

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

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

Power over Ethernet (PoE)

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

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

Power Usage Details

The **Power Usage** option allows to you to view a 24-hour view of PoE power consumption and related events. The graph displays historical usage alongside event indicators, with interactive features such as tool tips on hover, detailed information on selection, and horizontal scrolling for navigation across the full day.

A **Power Events** link has been added under the **Health** > **Events** page, allowing you to view a consolidated list of all relevant power events. This enhancement enables quick navigation and ensures that all relevant power events are accessible in one consolidated location, improving visibility and ease of monitoring.

- The **Power Usage** graph displays historical data over the past 24 hours for clients using PoE.
- Each data point includes a tooltip with detailed information and a list of clients consuming PoE at that specific time.
- The vertical axis represents the power budget of the Instant On PoE device, while the horizontal axis represents the corresponding timestamps.
- The graph line indicates usage in green under normal conditions and shifts to yellow when consumption exceeds 80% of the available power.

The list of devices below the graph displays the PoE client list and provides a tooltip with details such as power usage, number of PoE clients, related events, and the corresponding time period.

Notifications for device capacity issues are grouped to highlight high power usage or PoE port denials without sending multiple alerts.

802.1X Authentication

Allows you to select the RADIUS profile for the device.
In the RADIUS Profile drop-down list, select either none, or an existing RADIUS profile.

If 802.1X Authentication on a port is set to either Port-based or Client-based, the None option is not available.

For more information on creating a radius profile, see Creating a RADIUS Profile.

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 Devices() tile on the Instant On home page.
2. Tap any of the switches listed in the Devices list. The **Switch Details** screen is displayed with details.

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

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

Status

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

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

Networks

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

1. Tap any of the switches listed in the Devices 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 the following options, under **Included networks**:
   - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
   - **Tagged networks assignment**—The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
     - **All Wired Networks**—Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
     - **Selected Wired Networks**—Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Networks** checkbox removes the tagged status from all eligible LAN networks.
7. Tap **Done** to finish mapping the network to the port.

Aggregation

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

Table 23: *Switch Ports Aggregation*

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

Table 23: *Switch Ports Aggregation*

Number of Ports per Switch	Number of LAG Supported	Number of LAG members supported
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 Devices inventory. The **Switch Details** page is displayed.
2. Under the **Ports** section, select the **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.
   - **Enable link aggregation** ( )–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.
   - **Port Profile**–Assign a port profile the selected list of port members, to enable the **Use Port Profile** option slide the toggle switch to enable. From the **Port Profile** drop-down list, select an existing port profile.

     For more information on creating a port profile, see Creating a Port Profile.

     After a port profile is assigning, the **View Port Profile** is displayed. Tap the **View Port Profile** to view the **Port Profile Details** screen.

NOTE

If a port profile is selected, then **Security** section is not displayed. . These parameters are configured in the port profile.

   - **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.
   - **Security**–This section includes the following configuration settings:
     - **DHCP and ARP protections (untrusted port)**–Under **Security**, enable this option to protect DHCP and ARP. This must be enabled on at least one wired network to take effect. This option is enabled by default.
     - **Port isolation (protected port)**–Under **Security**, enable this option to provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that belong to the same broadcast domain (VLAN). This ensures that the specific ports can be isolated from others within the same VLAN. When this option is enabled, the port can only send traffic to unprotected ports. Any packets received on a protected port are filtered at the egress of other protected ports, preventing communication between them. This option is disabled by default. Protected ports are not supported on Instant On 1830 switches.

- **Spanning tree protections**—Under **Security**, enable this option to protect spanning tree configurations from interference. BPDU protection is a security feature designed to protect the active MSTP topology by preventing spoofed BPDU packets from entering the MSTP domain. The options listed under **Spanning tree protections** are:
  - **No spanning tree protections (default)**—The default spanning tree protection settings without the BPDU option.
  - **Filter spanning tree protocol (BPDU filter)**—Filters incoming and outgoing BPDUs on the port.
  - **Block spanning tree protocol (BPDU guard)**—Stops the incoming and outgoing BPDUs received on the port.
  - **Root bridge protection (Root guard)**—Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge.

- **Included networks**—This section includes the following configuration settings:
  - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
  - **Tagged networks assignment**—The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
    - **All Wired Networks**—Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
    - **Selected Wired Networks**—Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.
- **Port options**—Under **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

5. Click **Done**.

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

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

Transceiver Details

Instant On switches are capable of detecting an SFP transceiver. When a transceiver is connected to a switch, the details of the transceiver are displayed under the **Ports** section in the **Switch Details** page. The details of the transceiver may not always be displayed completely, if the transceiver used is unsupported or provided by a third-party. It is possible that the transceiver details are displayed even if the port state is up, down, loop detected, or link flapping.

Follow these steps to view the details of the transceiver connected to the Instant On switch:

1. Tap any of the switches listed in the Devices inventory. The **Switch Details** page is displayed.
2. Under the **Ports** section, tap the port to which the transceiver is connected. The transceiver details are displayed:

Line No	Transceiver Details
Line 1	Denotes the transceiver compatibility in the following categories: ■ **Supported transceiver**–Official transceiver models recommended by HPE Networking and appearing on the switch datasheet. ■ **Unsupported transceiver**–Third party transceiver models that are compatible with the switch. ■ **Incompatible or faulty**–Third party transceiver models that are unsupported and incompatible with the switch. The transceiver information is unavailable in this case.
Line 2	Name of the Vendor
Line 3	Type of transceiver
Line 4	Serial number of the transceiver.
Line 5	Model number of the transceiver.

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

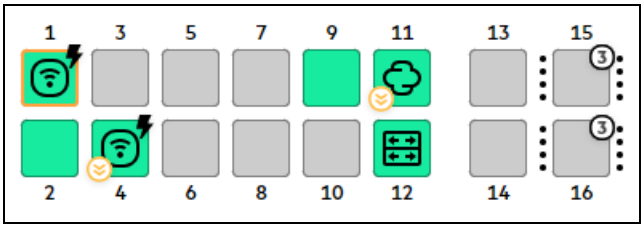
Port Details

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

- Name of the port in read and write mode.
- The **Enable port** toggle switch allows you to enable the port status. This field is set to enabled by default. Clients and devices are allowed to draw power and connect to the port when it is set to enabled. This setting is available for PoE ports with or without connected site devices.
- **Port profile**–Allows the administrator to assign a port profile.
  - **Use port profile**–Enable the **Use port profile** to view the **Port profile** drop-down list.
  - **Port profile**–To assign a port profile to the select port, select a port profile from the drop-down list and tab **Ok**. After assigning a port profile, tab on **View port profile** to view and update the port profile configuration.

The following section describes the different behaviors of the switch ports.

Figure 6 *Switch Ports*



Color of the Ports

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

The color of the port will be:

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

Port Icons

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

Table 24: *Port Icons*

Symbol	Definition
	Powered by PoE.
	PoE denied, indicating that the port is disconnected.
	PoE fault
	Transceiver issue.
	Link flapping
	Loop detected

Security

The **Security** section is displayed only when a port profile is not assigned to the selected port.

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

- **DHCP and ARP protections (untrusted port)**–Enable this option to protect DHCP and ARP. This must be enabled on at least one wired network to take effect. This option is enabled by default.
- **Port isolation (protected port)**–Enable this option to provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that belong to the same broadcast domain (VLAN). This ensures that the specific ports can be isolated from others within the same VLAN. When this option is enabled, the port can only send traffic to unprotected ports. Any packets received on a protected port are filtered at the egress of other protected

ports, preventing communication between them. This option is disabled by default. Protected ports are not supported on Instant On 1830 switches.

- **Spanning tree protections**–Under **Security**, enable this option to protect spanning tree configurations from interference. BPDU protection is a security feature designed to protect the active MSTP topology by preventing spoofed BPDU packets from entering the MSTP domain. The options listed under **Spanning tree protections** are:
  - **No spanning tree protections (default)**–The default spanning tree protection settings without the BPDU option.
  - **Filter spanning tree protocol (BPDU filter)**–Filters incoming and outgoing BPDUs on the port.
  - **Block spanning tree protocol (BPDU guard)**–Stops the incoming and outgoing BPDUs received on the port.
  - **Root bridge protection (Root guard)**–Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge.

Authentication

The authentication option is available only when **Use Port Profile** is disabled. By default, **No Authentication** is selected. To select **Port-based** or **Client-based** authentication, you must select a RADIUS profile listed under **802.1X Authentication**. The RADIUS server configuration is part of the RADIUS profile. From the **Overview** page, you can assign a RADIUS profile to the device.

The **802.1X Authentication** section consists of the following options:

These settings are available only for ports that do not have devices connected to it. However, the authentication mode can be updated regardless of the connected clients.

- **No authentication**–Instant On devices and clients can connect to the port without authenticating. This is the default setting.
- **Port-based**–All Instant On devices and clients connected to the port are authorized after the initial 802.1x RADIUS authentication is successful.
- **Client-based**–Requires each Instant On device or client connecting to the port to separately authenticate to the 802.1x RADIUS server to gain access.

  This is an optional setting. When **Client-based** is selected as the **802.1X Authentication** type, an additional **Authentication Options** section is displayed. You can select one of the following options:
  - **802.1X + MAC Authentication**–Enables a secondary attempt at MAC-based authentication if the initial 802.1X request times out. If 802.1X is explicitly refused by the server (for example, during an invalid credentials), MAC authentication is not attempted.
  - **Unauthenticated User Guest Access**–Enables a fallback to a wired guest network for clients that fail 802.1X authentication. This requires a wired Guest Network to be configured on the Instant On site. On enabling this option the guest network is displayed as **Untagged guest network** under the **Network Assignment** > **Included Networks** section of the port configuration.

The **Port-based** and **Client-based** authentication methods, require configuration a RADIUS profile to determine how authentication behaves across all access controlled ports.

Port Option

The **Port Option** option displays the link speed and how the port handles the traffic in both directions (Half or Full-Duplex). The data volume is displayed in **Mbps**.
The configurations displayed under **Speed/Duplex** are:

- **Auto Negotiated(default)**–displays the recommended setting for almost all devices.
- **Manual**–displays the port to a specific speed and duplex values by selecting **Manual Speed / Duplex Options** from the drop-down list. (e.g., 100 Mbps Half-Duplex, 100 Mbps Full-Duplex, 1 G Full-Duplex, 2.5 G Full-Duplex).

Select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Tap on Power Management to configure the power settings.

Power Management

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

- **Power Allocation** – Select either one of the following options to configure a power supply policy for the port:
  - **No Power over Ethernet**–No power is allocated to the port.
  - **Usage(default)** – The power allocated to the port is based on usage and is unrestricted.
  - **Class** – The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Table 25: *Power Class of Devices*

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts
Class 2	7 Watts
Class 3	15.4 Watts
Class 4	30 Watts

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

- When two ports belonging to the same priority are demanding power, the port with the least port number is given priority. Example: When port 2 and 3 are assigned **Critical** class and the gateway has a power budget constraint, device on port 2 will receive full power and the remaining power budget will be allocated to the device on port 3.
- PoE priority cannot be configured for Instant On devices. By default, Instant On devices are configured with **Usage** mode and **Critical** for **Port Priority.**

- **Schedule** – Toggle this switch beside **Use site power schedule** to either enable ( ) or disable ( ) power schedule on the port. If enabled, the PoE supply to the port will be determined by the power schedule

defined. To change the power schedule, tap on **View power schedule**. For more information on configuring **Power Schedule**, see Power Management.

Clients and Devices

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

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

Allowed Clients and Devices

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

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap any of the switches listed in the Devices inventory. The **Switch Details** screen is displayed with details.
3. Under **Ports**, tap the **Clients and devices on this port** link.
4. Tap the advanced menu () in the **Clients and Devices** page and tap **Allowed clients and devices**.
5. Set the **Specific clients** toggle switch to enabled ( ).
6. Tap **Allowed clients and devices list**.
7. Tap the add icon () at the bottom of the **Allowed Clients and Devices** screen.
8. Tap on the **Search for new clients and devices** button and connect new clients and devices to the port to be discovered.
9. Once the search is complete, select the checkbox next to the clients and devices you want to add to the Allowed list and tap the **Add clients and devices** button.
10. Tap **< Back** to return to the previous screen. The changes are automatically saved.

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

Network tools

The **Network tools** section in the **Switch Details** page contains different diagnostics tools and include items related to the device port and shall give access to a dedicated page. On a switch, **Network Tools** is used to send a copy of network packets from one port, several ports, or a network (VLAN) to another switch port. This is used to inspect and analyze traffic.

The Network tools option provides the following diagnostics tools:

- Port Mirroring
- Connectivity Test
- Test Cable

Port Mirroring

The Instant On switches have the ability to trace the packets sent and received from a port, by mirroring the data and sending it to a destination port. This feature is useful to troubleshoot network issues. Only one port mirroring session can be configured for each Instant On switch. If a site has multiple switches, there can be multiple port mirroring sessions active at the same time on different devices. When a port mirroring session is active, a destination port cannot be selected as a member of a Link aggregation group.

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

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the switch listed in the **Devices** inventory. The **Switch Details** screen is displayed with details
3. Tap on the **Network tools** accordion on the **Switch Details** screen to view the tools available.
4. Tap on **Port mirroring** from the drop-down list.
5. In the **Port Mirroring** screen, select a switch port from the drop-down list, to which the traffic should be mirrored. This setting is configured as the destination port. The destination can be any port on the switch, except for the following:
   - The uplink port
   - A port where the Instant On device is connected.
   - A port that is configured as part of a trunk.
   - A port that uses 802.1x
6. Under **Source**, select one of the following options:
   a. **Network**–Select one of the available networks from the drop-down list.
   b. **Ports**–Select the port(s) to be used as the source port(s).

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

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

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

Connectivity Test

The **Test Connectivity** option is used to test the reachability of an Instant On device. To perform a network test, you need to enter a **Network Destination** to be reached.

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the switch listed in the **Devices** inventory. The **Switch Details** screen is displayed with details.

3. Tap on the **Network tools** accordion on the **Switch Details** screen to view the tools available.
4. Tap on **Test connectivity** from the drop-down menu. Displays the **Connectivity** screen.
5. Under **Source**, select an Instant On device from the drop-down list.

   Only active devices of a site can be selected in this field. It could be a Switch or an AP.
6. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
7. Tap **Start connection test**.

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

Table 26: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Test Cable

The **Test Cable** diagnostics on a switch detects potential cable issues on the copper links. To run the **Test Cable** wizard on a switch, you must select the port to run the test.

- On starting the cable test, the selected port is temporarily shut down and other ports on the device stop receiving requests until the cable test finishes.
- For accurate results, you must perform the cable test on a cable longer than 3 meters.

To run a cable test on an Instant On switch, follow the steps below:

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the switch listed in the **Devices** inventory. The **Switch Details** screen is displayed with details.
3. Tap on the **Network tools** accordion in the **Switch Details** screen to view the tools available.
4. Tap on the **Test Cable**.
5. In **Select Port to Test** page, select the port on which you want to run the cable test.
6. Tap on the **Start cable test**. Initiates the cable test for the selected port.

The table below shows the possible test results from the cable test:

Table 27: *Possible Cable Test Results*

Category	Icon	Result
Diagnostic	Spinner	Cable test in progress.
	Green circle	Good cable.
	Amber triangle	Two-pairs 10/100 Mbps cable.
	Red rhombus	Bad cable.
	Red rhombus	Electrical short in cable.
	Red rhombus	Impedance mismatch in cable.
	Red rhombus	Open cable.
	Gray square	Cable test failed. Message–Cable test could not start on the selected device. Try again later.
	Gray square	No cable detected.
Distance to Fault	None	In case of a cable fault, it displays the distance to the fault.
Cable Length	None	Displays the cable length only in case of a successful cable test. The minimum cable length is 50 meters and is provided within a 30 meter range. The cable length falls into one of the following categories: less than 50 meters, 50 and 80 meters, 80 and 110 meters, or greater than 110 meters. **NOTE:** Cable length is not available for ports with traffic rates below 1 Gbps.

Device Options or Switch Lights

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

Device Options are supported only on the Instant On 1840 and 1940 Switch Series. This section is not displayed for other Instant On switches

Follow these steps to modify the status of the switch lights:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left. The Device **Overview** page is displayed.
2. Use one of the following methods to view the switch details:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop down list.

3. Under **Overview** > **Device Options** > **Device Lights**, select one of the following options:
   a. **Normal**–Use this option to turn on the status lights. This option is selected by default.
   b. **Quiet**–Use this option to turn off the status lights. When this option is selected, the device lightsare turned off during normal operation.
4. Click **Update**.

Advanced Menu

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

- Locate
- Restart
- Routing
- Jumbo Frames
- Switching to Local Management
- Replace Device
- Remove from Inventory

Locate

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

To locate your Instant On switch, follow these steps:

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

Restart

To restart the device:

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

Routing

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

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

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

- A minimum of two wired networks must be configured in the site to perform routing.
- The Instant On switch must be online to configure routing.
- Routing can be performed by only one Instant On switch in a site.

Jumbo Frames

Jumbo frames improve data transmission efficiency by reducing the number of frames and overheads for switches to process. Configuring jumbo frames is supported on all Instant On switches and can be enabled on each switch individually.

The following procedure allows you to configure jumbo frames on an Instant On switch:

1. Tap the advanced menu () icon in the title bar of the **Switch Details** page.
2. Tap on **Jumbo frames** from the drop-down list. The **Jumbo Frames** screen is displayed.
3. Slide the toggle switch next to Jumbo frames to the right ( ) to enable the setting and allow transmission of large data through the switch.
4. Tap **Done**.
   The Instant On switch reboots automatically to apply the changes.

Switching to Local Management

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

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

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

Replace Device

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

- This option is visible only when the Instant On switch is offline.
- When a higher-model switch is replaced with a lower-model switch, certain configurations may not be carried over to the newly replaced switch.
- It is recommended to replace the failed switch with a working switch of the exact same model to ensure all device configurations are successfully transferred to the replaced switch.

1. In the devices inventory, tap the failed Instant On switch. The **Switch Details** screen is displayed.
2. Tap the advanced menu () icon in the title bar of the **Switch Details** screen.
3. Tap **Replace device**.
4. In the **Replace Device** screen, tap **Search** when the device lights are alternating between green and amber.
5. Enter the **Serial Number** of the device which you choose to add to the inventory, or select one of the following options:
   - **Search for devices**–Initiates the LLDP automatic search. It usually takes around 4-5 minutes for the Instant On devices to be detected.
   - **Scan barcode or QR code**–Use the barcode or QR code scan method to add your devices. For more information, see Discovering Available Devices.
6. Tap the Instant On switch to replace with the failed switch in the inventory.
7. Tap **Replace**.
8. Tap **Finish**.

Remove from Inventory

To remove the switch when it is still online:

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

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

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

Reserving an IP Address for a Device

In addition to reserving an IP address from the network's **IP Assignment** tab, you can also reserve or remove a client's IP address directly from the device's page for both online and offline devices.s

To reserve an IP Address for a device:

1. Tap the advanced menu () icon in the title bar of the **Switch Details** screen.
2. Select **Add IP Address Reservation** from the list. To remove it, tap **Remove IP Address Reservation**.

Cloud-Managed Stacking

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

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

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

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

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

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

Creating a New Stack– During Initial Setup

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

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

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

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

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

Creating a New Stack– After Initial Setup

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

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

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

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

Adding an Instant On 1960 Series Switch to an Existing Stack

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

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

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

Stack Details

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

1. Tap the Devices() tile on the Instant On home screen.
2. Tap on the stack listed in the Devices list. The **Stack Details** screen is displayed with details. The summary details include the **Stack name** and **Device name** of all the devices in the stack. It is followed by the details of each of the devices.

To reset the device name to its default name, select the device name text field, tap the reset icon and then tap **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.

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

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

Stack Management

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

Assigning a Role for a Switch in the Stack

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

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

Removing a Switch from the Stack

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

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

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

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

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

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

Connectivity

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

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

802.1X Authentication

Allows you to select the RADIUS profile for the switch stack.
In the RADIUS Profile drop-down list, select either none, an existing RADIUS profile, or create a new RADIUS profile.
For more information on creating a radius profile, see Creating a RADIUS Profile.
On assigning a RADIUS profile, **View RADIUS Profile** is displayed. Click **View RADIUS Profile**, opens the RADIUS profile detail panel on the left.
To edit an existing RADIUS profile, click **View Details**, which displays the RADIUS profile configuration page.

Power over Ethernet (PoE)

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

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

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

Ports

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

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the stack listed in the devices list. The **Stack Details** screen is displayed with details.

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

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

Status

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

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

Networks

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

1. Tap on the stack listed in the Devices list. The **Stack Details** screen is displayed
2. Select the **Networks** tab, under **Ports** to view the ports on the switch.
3. From the **Selected network** drop-down list, choose the network you want to map to a specific port.
4. Tap the port to which you want to assign the selected network.
5. Tap the **Port details** link.
6. Select one of the following options, under **Included networks**:
   - **Untagged**–This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
   - **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
     - **All Wired Networks**–Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
     - **Selected Wired Networks**–Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port

profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.

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

Aggregation

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

Table 28: *Switch Ports Aggregation*

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

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

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

NOTE

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

4. The **Link Aggregation Details page** provides the following configuration options:
   - Provide a custom name for the Link aggregation in the text box.
   - **Enable line aggregation** ( )–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.
   - **Port Profile**–Assign a port profile the selected list of port members, to enable the **Use Port Profile** option slide the toggle switch to enable. From the **Port Profile** drop-down list, select an existing port profile.
     For more information on creating a port profile, see Creating a Port Profile.
     After a port profile is assigning, the **View Port Profile** is displayed. Tap the **View Port Profile** to view the **Port Profile Details** screen.

NOTE

If a port profile is selected, then **Security** section is not displayed. . These parameters are configured in the port profile.

- **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.
- **Security**—This section includes the following configuration settings:
  - **DHCP and ARP protections (untrusted port)**—Under **Security**, enable this option to protect DHCP and ARP. This must be enabled on at least one wired network to take effect. This option is enabled by default.
  - **Port isolation (protected port)**—Under **Security**, enable this option to provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that belong to the same broadcast domain (VLAN). This ensures that the specific ports can be isolated from others within the same VLAN. When this option is enabled, the port can only send traffic to unprotected ports. Any packets received on a protected port are filtered at the egress of other protected ports, preventing communication between them. This option is disabled by default. Protected ports are not supported on Instant On 1830 switches.
  - **Spanning tree protections**—Under **Security**, enable this option to protect spanning tree configurations from interference. BPDU protection is a security feature designed to protect the active MSTP topology by preventing spoofed BPDU packets from entering the MSTP domain. The options listed under **Spanning tree protections** are:
    - **No spanning tree protections (default)**—The default spanning tree protection settings without the BPDU option.
    - **Filter spanning tree protocol (BPDU filter)**—Filters incoming and outgoing BPDUs on the port.
    - **Block spanning tree protocol (BPDU guard)**—Stops the incoming and outgoing BPDUs received on the port.
    - **Root bridge protection (Root guard)**—Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge.
- **Port options**—Select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.
- **Included networks**—This section includes the following configuration settings:
  - **Untagged**—This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
  - **Tagged networks assignment**—The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
    - **All Wired Networks**—Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
    - **Selected Wired Networks**—Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site has more than one LAN network. Select **All Networks**

checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.

5. Click **Done**.

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

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

NOTE

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

Port Details

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

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

Port profile

Assign a port profile the selected list of port members, to enable the **Use Port Profile** option slide the toggle switch to enable. From the **Port Profile** drop-down list, select an existing port profile.

For more information on creating a port profile, see Creating a Port Profile.

After a port profile is assigning, the **View Port Profile** is displayed. Tap the **View Port Profile** to view the **Port Profile Details** screen.

NOTE

If a port profile is selected, then **Security** section is not displayed. . These parameters are configured in the port profile.

Security

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

- **DHCP and ARP protections (untrusted port)**–Enable this option to protect DHCP and ARP. This must be enabled on at least one wired network to take effect. This option is enabled by default.
- **Port isolation (protected port)**–Enable this option to provide Layer 2 isolation between interfaces (Ethernet ports and LAGs) that belong to the same broadcast domain (VLAN). This ensures that the specific ports can be isolated from others within the same VLAN. When this option is enabled, the port can only send traffic to unprotected ports. Any packets received on a protected port are filtered at the egress of other protected ports, preventing communication between them. This option is disabled by default. Protected ports are not supported on Instant On 1830 switches.
- **Spanning tree protections**–Under **Security**, enable this option to protect spanning tree configurations from interference. BPDU protection is a security feature designed to protect the active MSTP topology by preventing spoofed BPDU packets from entering the MSTP domain. The options listed under **Spanning tree protections** are:
  - **No spanning tree protections (default)**–Disables spanning tree protection.
  - **Filter spanning tree protocol (BPDU filter)**–Filters incoming and outgoing BPDUs on the port.
  - **Block spanning tree protocol (BPDU guard)**–Stops the incoming and outgoing BPDUs received on the port.

- **Root bridge protection (Root guard)**–Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge

Authentication

The **802.1X Authentication** section consists of the following options:

These settings are available only for ports that do not have devices connected to it. However, the authentication mode can be updated regardless of the connected clients.

- **No authentication**–Instant On devices and clients can connect to the port without authenticating. This is the default setting.
- **Port-based**–All Instant On devices and clients connected to the port are authorized after the initial 802.1x RADIUS authentication is successful.
- **Client-based**–Requires each Instant On device or client connecting to the port to separately authenticate to the 802.1x RADIUS server to gain access.

  This is an optional setting. When **Client-based** is selected as the **802.1X Authentication** type, an additional **Authentication Options** section is displayed. You can select one of the following options:
  - **802.1X + MAC Authentication**–Enables a secondary attempt at MAC-based authentication if the initial 802.1X request times out. If 802.1X is explicitly refused by the server (for example, during an invalid credentials), MAC authentication is not attempted.
  - **Unauthenticated User Guest Access**–Enables a fallback to a wired guest network for clients that fail 802.1X authentication. This requires a wired Guest Network to be configured on the Instant On site. On enabling this option the guest network is displayed as **Untagged guest network** under the **Network Assignment** > **Included Networks** section of the port configuration.

The **Port-based** and **Client-based** authentication methods, require configuration a RADIUS profile to determine how authentication behaves across all access controlled ports.

Port Options

The **Port Option** option displays the link speed and how the port handles the traffic in both directions (Half or Full-Duplex). The data volume is displayed in **Mbps**.
The configurations displayed under **Speed/Duplex** are:

- **Auto Negotiated(default)**–displays the recommended setting for almost all devices.
- **Manual**–displays the port to a specific speed and duplex values by selecting **Manual Speed / Duplex Options** from the drop-down list. (e.g., 100 Mbps Half-Duplex, 100 Mbps Full-Duplex, 1 G Full-Duplex, 2.5 G Full-Duplex).

Limit Broadcast and Multicast Storms– Select the checkbox to limit excessive broadcast and multicast traffic.

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

- **No Power over Ethernet**–No power is allocated to the port.
- **Usage (default)** – The power allocated to the port is based on usage and is unrestricted.
- **Class** – The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

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

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

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

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

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

Included Networks

- **Untagged**–This is the default setting. The port will receive and send traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, tap the **Untagged network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
  - **All Wired Networks**–Select this option to include all tagged networks. When this option is selected, then the list of tagged networks is not displayed.
  - **Selected Wired Networks**–Select this option to manually select the tagged VLAN networks. When this option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time. **All Networks** option is available only when the site

has more than one LAN network. Select **All Networks** checkbox marks all eligible LAN networks as tagged. Clear **All Network**s checkbox removes the tagged status from all eligible LAN networks.

Connected Clients and Devices

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

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

Allowed Clients and Devices

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

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap any of the switches listed in the Devices inventory. The **Stack Details** screen is displayed with details.
3. Under **Ports**, tap the **Clients and devices on this port** link.
4. Tap the advanced menu () in the **Clients and Devices** page and tap **Allowed clients and devices**.
5. Set the **Specific clients** toggle switch to enabled ( ).
6. Tap **Allowed clients and devices list**.
7. Tap the add icon () at the bottom of the **Allowed Clients and Devices** screen.
8. Tap on the **Search for new clients and devices** button and connect new clients and devices to the port to be discovered.
9. Once the search is complete, select the checkbox next to the clients and devices you want to add to the Allowed list and tap the **Add clients and devices** button.
10. Tap **< Back** to return to the previous screen. The changes are automatically saved.

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

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

Network tools

The **Network tools** section in the **Switch Details** page contains different diagnostics tools and include items related to the device port and shall give access to a dedicated page. On a switch, **Network Tools** is used to send a copy of network packets from one port, several ports, or a network (VLAN) to another switch port. This is used to inspect and analyze traffic.

The Network tools option provides the following diagnostics tools:

- Port Mirroring
- Test Connectivity
- Test Cable

Port Mirroring

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

NOTE

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

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

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

NOTE

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

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

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

Test Connectivity

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

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

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the switch stack listed in the **Devices** inventory. The **Stack Details** screen is displayed with details.

3. Tap on the **Network tools** accordion on the **Stack Details** screen to view the tools available.
4. Tap on the **Test Connectivity**.
5. Under **Source**, select an Instant On stack from the drop-down list.
6. Under **Destination**, enter the **hostname or IP address** of the device to which the source device should connect.
7. Tap **Start connection test**.

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

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

Table 29: *Possible Test Results*

Connectivity Rating	Roundtrip Time	Test Results Format
Good	All network tests passed with a latency of less than 150 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Hostname resolved to <IP address> **Line 4**: Fast connectivity to destination. **Line 5**: Roundtrip Time: Minimum, Maximum, Average <time in milliseconds> **Line 6**: Connection Path Analysis <logs>
Fair	Some network tests passed with a latency between 150 and 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: DNS Server. **Line 3**: Slow connectivity to <host / IP address> **Line 4**: <hostname / IP address> **Line 5**: Connection Path Analysis <logs>
Poor	Ping network passed with a latency greater than 400 milliseconds.	**Line 1**: Network Destination < hostname / IP address>. **Line 2**: Reachability > Unable to reach IP address **Line 3**: Connection Path Analysis <logs>

Test Cable

The **Test Cable** diagnostics on a switch stack detects potential cable issues on the copper links. To run the **Test Cable** wizard on a switch stack, you must select a stack member and a member port to run the test.

- On starting the cable test, the selected port is temporarily shut down and other ports on the device stop receiving requests until the cable test finishes.
- For accurate results, you must perform the cable test on a cable longer than 3 meters.

To run a cable test on an Instant On switch stack, follow the steps below:

1. Tap the Devices() tile on the Instant On home page.
2. Tap on the stack listed in the Devices inventory. The **Stack Details** screen is displayed with details.
3. Tap on the **Network tools** accordion in the **Stack Details** screen to view the tools available.
4. Tap on the **Test Cable**.
5. In the **Select Source Member and Port to Test** page, select a stack member and the member port on which you want to run the cable test.
6. Tap on the **Start cable test**. Initiates the cable test for the selected port.

The table below shows the possible test results from the cable test:

Table 30: *Possible Cable Test Results*

Category	Icon	Result
Diagnostic	Spinner	Cable test in progress.
	Green circle	Good cable.
	Amber triangle	Two-pairs 10/100 Mbps cable.
	Red rhombus	Bad cable.
	Red rhombus	Electrical short in cable.
	Red rhombus	Impedance mismatch in cable.
	Red rhombus	Open cable.
	Gray square	Cable test failed. Message—Cable test could not start on the selected device. Try again later.
	Gray square	No cable detected.
Distance to Fault	None	In case of a cable fault, it displays the distance to the fault.
Cable Length	None	Displays the cable length only in case of a successful cable test. The minimum cable length is 50 meters and is provided within a 30 meter range. The cable length falls into one of the following categories: less than 50 meters, 50 and 80 meters, 80 and 110 meters, or greater than 110 meters. **NOTE:** Cable length is not available for ports with traffic rates below 1 Gbps.

Advanced Menu

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

- Locate
- Restart
- Routing
- Unstack
- Replace Device

Locate

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

To locate your Instant On switch, follow these steps:

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

Restart

To restart the device:

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

Routing

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

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

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

The Instant On switch must be online to configure routing.

Jumbo Frames

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

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

1. Tap the advanced menu () icon in the title bar of the **Stack Details** screen.
2. Tap on **Jumbo frames** from the drop-down list. The **Jumbo Frames** screen is displayed.

3. Slide the toggle switch next to Jumbo frames to the right ( ) to enable the setting and allow transmission of large data through the switch.
4. Tap **Done**.
   The Instant On switches in the stack automatically reboot to apply the changes.

Unstack

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

1. Tap the advanced menu () icon in the title bar of the **Stack Details** screen.
2. Tap **Unstack**. The **Unstack** screen is displayed, requiring your confirmation.
3. Tap **Unstack**.
   The stack is removed and the switches will now appear as standalone devices in the inventory.

Replace Device

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

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

1. Tap the advanced menu () icon in the title bar of the **Stack Details** screen.
2. Tap **Replace device**. The offline Instant On switch is displayed.
3. Tap the offline Instant On switch.
4. In the **Replace Device** screen, tap **Search**.
   The standalone Instant On 1960 switches connected to the network are displayed.
5. Tap the Instant On 1960 switch to replace with the offline switch in the stack.
6. Tap **Replace**.
7. Tap **Finish**.

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

Reserving an IP Address for a Device

In addition to reserving an IP address from the network's **IP Assignment** tab, you can also reserve or remove a device's IP address directly from the device's page for both online and offline devices.

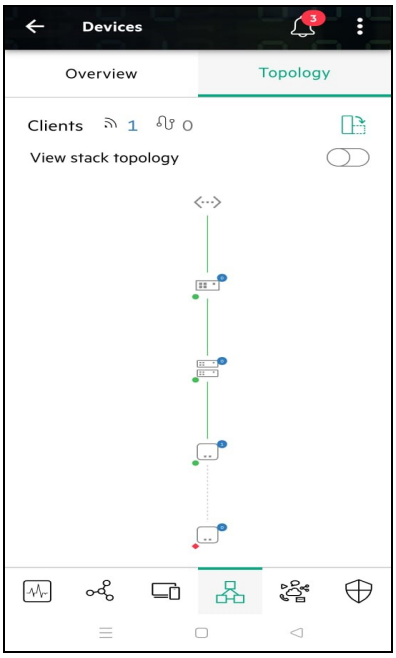
To reserve an IP Address for a device:

1. Tap the advanced menu () icon in the title bar of the **Stack Details** screen.
2. Select **Add IP Address Reservation** from the list. To remove it, tap **Remove IP Address Reservation**.

Topology

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

An example of the topology page is displayed below:

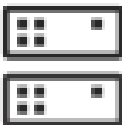


NOTE

Pinch to zoom in or zoom out.

Description of Topology Icons

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

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

Stack Topology

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

1. Tap the **Devices** () tile on the Instant On mobile app home page.
2. Tap **Topology** .
3. Slide the **View stack topology** toggle switch to the right ( ).

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

The stack topology displays the following details:

- Interconnections between the devices in the stack.
- Devices in the stack which are connected to another Instant On device that is not part of the stack.
- Connectivity status between devices.
- Third party devices that are connected to the stack, resulting in an invalid topology.
- Displays the connections between a device of the stack and another Instant On device in the inventory.
- Displays the summary details for each device of the stack and stand-alone devices.

Auto-Detection and Auto-Configuring of Switch Ports

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

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

Wi-Fi 6E Standard

The Wi-Fi 6E standard adds support for 6 GHz spectrum, with more channels and channel width up to 160 MHz, thereby ensuring faster wireless speeds and lower latencies. Clients supporting Wi-Fi 6E can now connect to the 6 GHz spectrum using Wi-Fi 6 (802.11ax) technology. Wi-Fi 6E is currently supported only on Instant On AP32 access points. The support of 6 GHz spectrum will be available when an AP32 access point is added to an Instant On site. The AP32 access point has 2 radios that can operate in the tri-bands—2.4 GHz, 5 GHz, and 6 GHz. It is up to the user to decide on which spectrum the 2 radios should operate. The default radio choice is 2.4 GHz and 5 GHz.

There are four conditions under which the 6 GHz option is made available for a wireless network.

- An AP32 access point must be added to the site.
- Wireless Network Security should be enabled on:
  - WPA2 + WPA3 Personal authentication for Employee Networks. For more information, see Employee Network
  - OWE (enhanced open) for Guest Networks. For more information, see Wi-Fi Enhanced Open (OWE)
- Wi-Fi 6 option should be enabled in the wireless options section. For more information, see Quality of Service.
- Only a maximum of two wireless networks should be configured with the 6 GHz option in a site.

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

When a gateway is deployed at a site, then the following tabs are displayed in the Networks page:

- LAN
- WAN

To view the **Networks** page, tap the Networks () tile on the Instant On home page:

Figure 7 *Networks Page - Without Secured gateway*

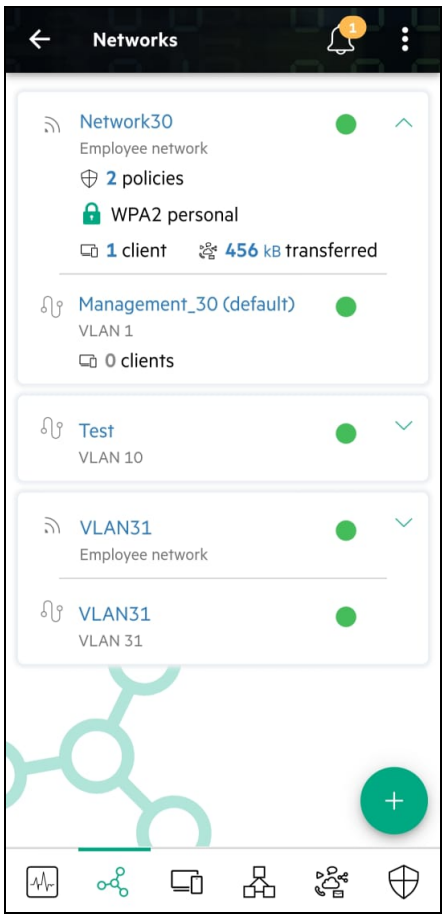
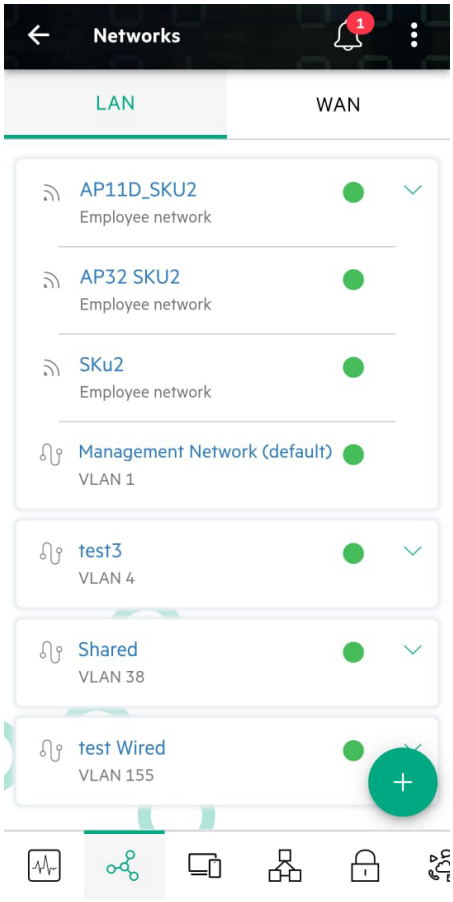


Figure 8 *Networks Page - With Secured Gateway*



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

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

- Employee Network
- Guest Network
- Wired Network
- WAN

Employee Network

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

NOTE

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

To configure an employee network:

1. Tap the 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. Under **Identification**, enter a **Name** for the employee network. This will also be broadcasted as the SSID for the WLAN network.
5. Under **Security**, select one of the following **Network Security** options:
   a. **WPA2 Personal**–Uses PSK password authentication. **WPA2 Personal** is enabled by default.
   b. **WPA2 + WPA3 Personal**–Uses PSK password authentication. Select **WPA2 + WPA3 Personal** to enable this option.
   c. **WPA2 Enterprise**–Uses Radius authentication. Select the **WPA2 Enterprise** radio button to select this option.
   d. **WPA2 + WPA3 Enterprise**–Uses Radius authentication. Select the **WPA2 + WPA3 Enterprise** radio button to select this option.
6. Selecting the **WPA2 Enterprise** or **WPA2 + WPA3 Enterprise** options, displays the RADIUS Server configuration and Network Access Attributes options. This enables you to secure the network using a higher encryption RADIUS authentication server. Configure the following settings:

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

   - Enter the **RADIUS server IP address or domain name.**
   - Enter the **Shared Secret**.
7. Click **More RADIUS parameters** and configure the following settings:
   - **RADIUS Accounting**–Slide the toggle switch to send RADIUS accounting messages.
   - **Primary RADIUS Server**–Configure the following parameters for the **Primary RADIUS Server**.
     - **Server IP Address or domain name**–Enter the IP address or fully qualified domain name of the RADIUS server.
     - **Shared secret**–Enter a shared key for communicating with the external RADIUS server.
     - **Server timeout**–Specify a timeout value in seconds. The value determines the timeout for a RADIUS request. The Instant On AP attempts to send the request several times (as configured in the **Retry count**) before the user gets disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds.
     - **Retry count**–Specify a number between 1 and 5. Retry count indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests.
     - **Authentication port**–Enter the authentication port number of the external RADIUS server within the range of 1-65535. The default port number is 1812.
   - **Secondary RADIUS Server**–Slide the toggle switch to configure a secondary RADIUS server.
     - **Server IP Address or domain name**–Enter the IP address or fully qualified domain name of the secondary RADIUS server.
     - **Shared secret**–Enter a shared key for communicating with the secondary RADIUS server.
     - **Server timeout**–Specify a timeout value in seconds. The value determines the timeout for a secondary 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 secondary RADIUS server within the range of 1-65535. The default port number is 1812.

8. Under **Network Access Attributes**, configure the following settings if you wish to proxy all RADIUS requests from the Instant On AP to the client.
   - **NAS identifier**–Enter a string value for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server.
   - **NAS IP address**–Select one of the following options if your Instant On devices are configured in a private network mode. The options below determine how the RADIUS authentication takes place across all networks. This option is grayed out if the Instant On AP is configured as a primary Wi-Fi router on the network. In which case each AP in the network will send RADIUS requests to the server with a matching Source IP address and NAS IP address.
     - **Use device IP (default)**–This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients.
     - **Use a single IP**–The RADIUS and NAS IP address will originate from a single IP address representing the site. Enter the **NAS IP address** for the site.
9. Tap close () to return to the employee details page.

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

Modifying the Employee Network Name and Password

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

1. Tap the Networks () tile 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 **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 Instant On mobile app allows you to configure following settings for clients on employee networks:

- IP Assignment
- Network Access Schedule
- Bandwidth Usage
- Network Access
- Quality of Service

IP Assignment

The **IP assignment** setting in the 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.

By default, a guest network is configured as **NAT**. You can select Specific to this network to automatically assign IP addresses to the DHCP server.

Automatic IP Address Assignment

The **Automatic IP Address Assignment** section allows you to refer to the use of DHCP and NAT to automatically assign IP addresses to clients and devices connecting to network, without manual configuration.

Follow these steps to configure the Automatic IP address assignment for clients:

1. Under **Start IP Address**, enter the IP address of the network.
2. Under **End IP Address**, enter the last IP address of the network.

The **Available IP addresses** will display the range of IP addresses available for allocation.

DNS Resolution

The **DNS Resolution** section allows you to configure servers assigned to clients and devices to resolve domain names.

Follow these steps to configure the DNS resolution for clients:

1. Under **IP Assignment** > **DNS Resolution**, select one of the following options.
   - **Automatic(default)**—This is the default setting. The DNS settings are automatically configured.
   - **Static**—Use this setting to configure a custom DNS server.
     - **Primary DNS Server**—Enter the hostname or IP address of the primary DNS server.
     - **Secondary DNS Server**—Enter the hostname or IP address of the secondary DNS server.

Network Access Schedule

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

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

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

3. Choose from the following options:
   - If the network is controlled by a policy, the policy name is displayed. To modify the policy tap on the policy name to view the **Policy Details** page. For more information on policies, see Policies topic.
   - If the network is not controlled by a policy, complete the following procedure:
     1. Tap on **View policies**, in the **Network Access Schedule** page. Displays the **Policies** page.
     2. If no policy is configured, create a new policy. To create a new policy tap the () icon. The **Create Policy** screen is displayed. For more information on creating a policy, see Creating a Network Policy topic.

Bandwidth Usage

The bandwidth consumption for an employee or guest network can be limited based on the client MAC address. The configured limit will be maintained even when the client roams from one AP to another within the network. As an alternative, you can choose to set the bandwidth on an entire network, instead of restricting the usage per client.

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

1. Tap the Networks () tile on the Instant On home page and select an employee network or guest network from the list.
2. Tap the **More options** drop-down.
3. Tap **Bandwidth Usage**.
4. Set the **Limit bandwidth usage** toggle switch to enabled ( ).
5. Tap the **Client** radio button and move the slider to set the speed limit between 1 Mbps to 1 Gbps for the employee or guest network. The limit is set to **1 Gbps** by default.
6. The changes are auto saved. Tap the back arrow () to return to the employee or guest network details page.

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

1. Tap the Networks () tile on the Instant On home page and select an employee network or guest network from the list.
2. Select the employee or guest network and tap the **More options** drop-down.
3. Tap **Bandwidth Usage**.
4. Set the **Limit bandwidth usage** toggle switch to enabled ( ).
5. Tap the **Network** radio button and move the slider to set the speed limit between 1 Mbps to 1 Gbps for the employee or guest network. The limit is set to **1 Gbps** by default.
6. 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 the Networks () tile on the Instant On home page and select an employee or guest network from the list. The network details page is displayed.
2. Under **More options**, tap **Network access**. The **Network Access** screen is displayed.

3. Configure one of the of the following settings on your network:
   - **Unrestricted access (default)**–This is the default setting for Employee networks. This option allows users to access any destination available to the network.
   - **Restricted access**–This is the default setting for Guest networks. This option restricts users to access only the internet and prevents them from accessing internal network resources. To allow the users to access specific network resources, enter the **IP address** in the list of IP addresses and tap .

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

       Enter the **IP address** in the list of IP addresses and tap .

Allowed Clients

The **Specific Clients** feature is used to provide network access only to the clients that are added to the list. This feature is available only on employee networks that are configured with a network password (PSK) authentication. The **Specific Clients** setting is disabled by default. This setting can be enabled per-network and not globally. Each applicable network can have its own list of allowed clients. You can add a maximum of 256 wireless clients to the **Allowed Clients** list.

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

1. Tap the Networks () tile on the Instant On home page and select an employee network with from the list. The network details page is displayed.
2. Under **More options**, tap **Network access**. The **Network Access** screen is displayed.
3. Under **Allowed Clients**, slide the toggle switch ( ) next to **Use allowed client list** to enable the setting.
4. Tap **Edit allowed client list**.
5. Tap the add () icon and then tap on **Search for new clients**. The Instant Ondevices begins scanning for nearby clients that are available to connect to the network.
6. Choose the clients that should be added to the **Allowed Clients** list.

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

7. Tap **Done**.

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

Quality of Service

Quality of Service (**QoS**) determines how the network's traffic is treated when the network connection is congested. It controls the priority of the network's traffic relative to other networks, and can limit the download and upload bandwidth available to the network.

These settings define the default Quality of Service for all of the network's traffic. For more advanced scenarios, policies provide options to prioritize or limit the bandwidth of specific traffic – for example, specific clients, applications, or traffic flows. See Policies.

Network-level Quality of Service settings are evaluated after any applicable policies. A policy that sets the priority or bandwidth limits for specific traffic therefore takes precedence over these network-level defaults.

Network Options

Select one or both of the following:

- **Multicast-to-Unicast Conversion**–Converts multicast streams into unicast streams over the wireless network to improve the quality and reliability of streaming video, while preserving the bandwidth available to non-video clients. This option is disabled by default, because some wireless clients may not be compatible with it.
- **Network Priority**–Assigns a Quality of Service priority to the network's traffic, so that higher priority networks are favored over lower-priority networks when the connection is congested. When selected, choose a priority level under Network Priority.

Under Network Priority, select one of the following priority levels:

- **Low**–The lowest priority, for bulk transfers and other non-critical traffic that can tolerate delay.
- **Medium**(default)–The default priority, for traffic that is not time-sensitive, such as most standard applications (best effort).
- **High**–A higher priority for latency-sensitive traffic, such as video streaming and video conferencing.
- **Very High**–The highest priority, for traffic that is highly sensitive to delay and jitter, such as voice (VoIP).

Bandwidth Control

Bandwidth Control limits the bandwidth available to the network. Under Bandwidth Limits, select one or both of the following, and then set the rate with the corresponding slider (maximum 1 Gbps):

- **Download**–Sets the maximum download rate for the network.
- **Upload**–Sets the maximum upload rate for the network.

Under Usage Controlled by, select how the limit is applied:

- **Client**(default)–Applies the limit to each client connected to the network, based on the client MAC address. The limit is maintained even when a client roams from one access point to another within the network.
- **Network**–Applies the limit to the network as a whole rather than to each individual client.

Wireless Options

The Wireless Options tab is available on wireless networks and contains the Wi-Fi Technologies settings.

Wi-Fi Technologies

Under Wi-Fi Generations, select one or more of the following standards:

- **Wi-Fi 5**–The mandatory default standard for every wireless network. Wi-Fi 5 cannot be disabled, as it is required for the network to operate.
- **Wi-Fi 6**–Enables the Wi-Fi 6 (802.11ax) capabilities of the network. When selected, 802.11ax capable clients can make use of the enhanced throughput and transmission capabilities of the 802.11ax standard. This setting is enabled by default. To disable it, clear the Wi-Fi 6 checkbox.

NOTE

The Wi-Fi 6 option is available only when the device inventory includes at least one Wi-Fi 6 capable access point (for example, AP22, AP25, or AP32).

Wi-Fi 6 Options

The Wi-Fi 6 Options are available only when Wi-Fi 6 is enabled for the network.

- **Multiple Client Optimization** (OFDMA)—Improves channel efficiency when multiple Wi-Fi 6 clients are connected, by enabling OFDMA (Orthogonal Frequency-Division Multiple Access). This setting is disabled by default.

Multiple Clients Optimizations

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

Optimize for Video Streaming

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

NOTE

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

To configure optimization for video streaming, follow these steps:

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

Radio

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

To configure radio frequency, follow these steps:

1. Tap the 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**—The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
   - **5 GHz**—The AP will broadcast the wireless network only on the 5 GHz radio frequency.
   - **6 GHz**—The AP will broadcast the wireless network only on the 6 GHz radio frequency.

When only the 6 GHz option is selected for a wireless network, the **Wi-Fi 6** checkbox and the **6 GHz** checkbox under **Radio** settings will be grayed out until the user selects a second radio spectrum.

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

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.

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 the Networks () tile on the Instant On mobile app home screen.
2. Tap Add () and select the **Wireless** tab. This tab appears only when your site has both wired and wireless networks.
3. Select **Guest**, under **Usage** to indicate that the network is for guest users.
4. Enter a name for the guest network.
5. Under **Security**, select one of the following security levels:
   - **None**–if you want the user to access this network without the requirement of entering a username or password.
   - **Wi-Fi Enhanced Open**–Wi-Fi Enhanced Open (OWE) is the open security type derived from WPA3. It runs concurrently with an equivalent legacy Open SSID. For more information, see Wi-Fi Enhanced Open (OWE).
   - **WPA2 Personal**–This option allows you to secure the network using a shared password (PSK) encryption. Enter a password of your choice in the **Network password** field.
   - **WPA2 + WPA3 Personal**–This is the default setting when creating a new guest network. This option allows you to secure the network using a shared password (PSK) encryption. Enter a password of your choice in the **Network password** field.

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

6. To configure a guest portal in addition to the security levels, enable the **Guest portal** toggle switch ( ) and follow the instructions provided in Guest Network.

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

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

2. Slide the **Inactive** toggle switch ( ) to the right set the network to **Active** ( ).
3. Tap **DONE**. The network is marked as **Active**, and all network settings are made visible.

Wi-Fi Enhanced Open (OWE)

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

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

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

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

More Options

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

- IP Assignment
- Network Access Schedule
- Bandwidth Usage
- Network Access
- Quality of Service

Enabling Guest Portal

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

1. Tap the Networks () tile on the Instant On home page.
2. Select an active Guest Network connection.
3. Under **Security**, enable the **Guest portal** toggle switch ( ).
4. Tap **View 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** settings.
6. Tap **Ok**.

7. Based on your selection, enter values in the required fields. For more information, see:
   - Configuring Internal Captive Portal
   - Configuring External Captive Portal
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 31: *Internal Captive Portal Configuration*

Parameter	Description
Background	Tap the box to view the color palette and choose a color for the background of the internal captive portal page.
Welcome Message	Design the welcome message by updating the following fields: ■ **Text**–Enter the text for the welcome message. Example: Welcome to Guest Network. ■ **Font size**–Drag the slider to set the size of the font. ■ **Font color**–Tap the box to view the color palette and choose a color for the font. ■ **Font family**–Choose a font type from the drop-down list.
Logo / Image	Tap the image icon to browse and upload an image from your device. **NOTE:** Ensure that you upload the image only in the png, jpg, gif, or bmp formats.
Terms and Conditions	Design the **terms and conditions** section by updating the following fields: **Title text**–Enter the title text. Example: Please read the Terms and Conditions before using the Guest Network. **Font size**–Drag the slider to set the size of the font. **Font color**–Tap the box to view the color palette and choose a color for the font. **Font family**–Choose a font type from the drop-down list. **Terms content**–Enter or paste your terms and conditions in the text box. **Agree text**–Enter a comment in the text box. For example: **I agree to the terms and conditions**. ■ **Font color**–Tap the box to view the color palette and choose a color for the font. ■ **Font family**–Choose a font type from the drop-down list.
Accept Button	Design the **Accept Button** by updating the following fields: ■ **Text**–Enter the text for the accept button. Example: I agree to the terms and conditions. ■ **Redirect URL**–Specify the custom URL to which users should be redirected after clicking the accept button. ■ **Border radius**–Drag the slider to set the border radius of the accept button. ■ **Background color**–Tap the box to view the color palette and choose a color for the background. ■ **Font color**–Tap the box to view the color palette and choose a color for the font. ■ **Font family**–Choose a font type from the drop-down list.

Configuring External Captive Portal

You can configure an external captive portal for your guest network by configuring RADIUS authentication and accounting parameters

Customizing Captive Portal

To customize the external captive portal, follow these steps:

1. Select **External** from the **Guest Portal** page.
2. The **Custom** external captive portal offers two types of user accessibility to the Internet through the guest portal under Guest user access. Choose one of the following options.
   - **User authentication (default)**–Users are required to enter their credentials in the guest portal page to access the Internet. The credentials entered by the user are sent to the RADIUS server for validation. This is the default setting for the custom external captive portal.
   - **Guest portal acknowledgement**–The guest portal must return a predefined string **InstantOn.Acknowledge** to grant user access to the Internet. When selected, a predefined authentication text is returned by the external server after successful user authentication.

Guest portal acknowledgment is not available on the guest wired network.

3. Configure the following external captive portal configuration parameters:

4. **Table 32:** *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.
Require RADIUS Message Authenticator	Slide the toggle switch to enabled ( ) for the AP to discreetly discard packets from the RADIUS servers that does not have the Message Authenticator.
RADIUS Accounting	Slide the toggle switch to enabled ( ) to ensure the Instant On AP sends a status-server request to determine the actual state of the accounting server before marking the server as unavailable.
Primary RADIUS Server	Configure a primary RADIUS server for authentication by updating the following fields: ■ **Server IP address or domain name**–Enter the IP address or fully qualified domain name of the external RADIUS server. ■ **Shared secret**–Enter a shared key for communicating with the external RADIUS server. Tap the **More RADIUS parameters** link to configure the following parameters: ■ **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

Table 32: *External Captive Portal Configuration*

Parameter	Description
	disconnected. ■ **Retry count**–Specify a number between 1 and 5. Indicates the maximum number of authentication requests that are sent to the server group, and the default value is 3 requests. ■ **Authentication port**–Enter the authorization port number of the external RADIUS server within the range of 1-65,535. The default port number is 1812. ■ **Accounting port**–Enter the accounting port number within the range of 1-65,535. This port is used for sending accounting records to the RADIUS server. The default port number is 1813. Configure the following settings under **Network Access Attributes**, if you wish to proxy all RADIUS requests from the Instant On AP to the client. ■ **NAS identifier**–Enter a string value for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server. ■ **NAS IP address**–Select one of the following options if your Instant On devices are configured in a private network mode. The options below determine how the RADIUS authentication takes place across all networks. **Use device IP (default)**–This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients. **Use a single IP**–The RADIUS and NAS IP address will originate from a single IP address representing the site. Enter the **NAS IP address** for the site. **NOTE:** This option is grayed out if the Instant On AP is configured as a primary Wi-Fi router on the network. In which case each AP in the network will send RADIUS requests to the server with a matching Source IP address and NAS IP address.
Secondary RADIUS Server	To configure a Secondary RADIUS Server, slide the toggle switch to the right ( ). **NOTE:** The configuration parameters for the **Secondary RADIUS Server** and the **Primary RADIUS Server** are the same.
Network Access Attributes	This option is available only if **User authentication (default)** is selected under **Guest user access**. Configure the following parameters under network access attributes: ■ **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**–Tap on NAS IP Address and select one of the following options if your Instant On devices are configured in a private network mode. The options below determine how the RADIUS authentication takes place across all networks. This option is grayed out if the Instant On AP is configured as a primary Wi-Fi router on the network. In which case each AP in the network will send RADIUS requests to the server with a matching Source IP address and NAS IP address. a. **Use device IP (default)**–This is the default setting. The RADIUS requests and NAS IP address will originate from each device authenticating the clients. b. **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.

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 the Networks () tile 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. Select **Employee (default)** or **Voice** as **Usage**.
5. Under **Identification**, enter a **Network name** and **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 the Networks () tile 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 () tile 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. 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.

Configuring a Voice Network

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

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

1. Tap the Networks () tile 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. Select **Voice** as **Usage**.
5. Enter a **Network name** for the network.
6. Enter a **VLAN** for your network.
7. Tap **Done**.

To change the voice network, you need to delete the existing voice network and then create a new one.

Configuring a Guest Wired Network

Instant On allows you to create a guest wired network when the secure gateway is deployed at a site. You can create only one guest network per site.

1. Tap theNetworks () tile 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. Select **Guest** as **Usage**..
5. Under **Identification**, enter a **Network name** and **VLAN** for your network.
6. Tap **Done**.

Important Points to Note:

- Only one Voice network can be configured per site. The Voice network toggle switch will remain visible on other wired networks, but will be grayed out, preventing the user from enabling it. A message is displayed in the network details page indicating that the network is configured as a Voice network.
- The Voice network cannot be assigned to the management VLAN.
- The Voice network feature is available only for IP phones that are directly connected to the switch.
- If you connect a phone on a dedicated port with restricted access, the restricted access configuration will also be applied to the Voice VLAN.

Energy Efficient Ethernet

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

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

More Options

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

- Network Security
- Network Access
- Network Assignment
- Wired Options

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 the 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.

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 the 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 + .

Important Points to Note

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

IP Assignment Reservation

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

IP Address Reservation

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

In addition to managing reservations here, you can add or remove an IP address reservation directly from the Clients and Devices pages. See Reserving an IP Address for a Clientand Reserving an IP Address for a Device.

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

Add an IP Address Reservation

The following procedure defines the steps to add an IP Address Reservation on Instant On devices:

1. Click the **IP Assignment** tab.
2. Under **IP Address Reservation**, click **Add**. The **Add IP Address Reservation** dialog is displayed.
3. Under **Reserve to**, select one of the following options:
   a. **Client** – Select a client from the **Client** dropdown list. The list displays all online and offline within the last 24 hours, excluding watched clients unless connected or last seen on the network.
   b. **Device** – Select a device from the **Device** dropdown list. The list displays all online and offline devices connected or last seen on the network.
   c. **MAC Address** – Enter the MAC address of the client or device in the **MAC Address** field. The **IP Address** field is pre-populated with the next available IP address from the DHCP range.
4. Modify the pre-populated IP address in the **IP Address** field. The IP address must be within the DHCP subnet range and must not be already leased or assigned as a static IP.
5. Click **Add IP Reservation**.

NOTE

The Device option is only available on the management network of a site.
If the MAC address is tied to a known client or device (online or offline), the client or device name will be resolved and displayed in the IP address reservation table after the reservation is saved.

NOTE

A maximum of 128 IP address reservations is supported on the network.

Change an IP Address Reservation

The following procedure defines the steps to change an IP Address Reservation on Instant On devices:

1. Under **IP Address Reservation**, click on the reservation entry you wish to modify. The **Change IP Address Reservation** dialog is displayed, showing the MAC address and the current reserved IP address.
2. Enter the new IP address in the **IP Address** field.
3. Click **Change IP Reservation**.

Remove an IP Address Reservation

The following procedure defines the steps to remove an IP Address Reservation on Instant On devices:

1. Under **IP Address Reservation**, click on the reservation entry you wish to remove, and select the remove option. The **Remove IP Address Reservation** dialog is displayed.
2. A warning message dialog box is displayed.
3. Click **Remove IP Reservation** to confirm, or **Cancel** to keep the reservation.

NOTE

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

DNS Resolution

The **DNS Resolution** section allows you to configure servers assigned to clients and devices to resolve domain names.

Follow these steps to configure the DNS resolution for clients:

1. Under **IP Assignment** > **DNS Resolution**, select one of the following options.
   - **Automatic (default)**–This is the default setting. The DNS settings are automatically configured.
   - **Static**–Use this setting to configure a custom DNS server.
     - **Primary DNS Server**–Enter the IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
2. Click **Update**.

Network Assignment

Network Assignment for Wired Networks

The **Network Assignment** page facilitates the assignment of wired networks to Instant On devices at the site. All the ports on an Instant On AP11D or AP22D router or an Instant On switch can now be configured at the same time and assigned to a particular VLAN network. The **Network Assignment** page provides a global view of the wired network and displays all the devices deployed at the site. Every port on the Instant On devices at the site can be assigned in bulk to a particular VLAN, expect for the following:

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

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

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

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

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

Network Assignment for Wireless Networks

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

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

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

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

Wired Options

The **Wired Options** section in the mobile app allows you to configure the multicast optimization setting.

Multicast Optimizations

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

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

1. Tap the Networks () tile on the Instant On home page and select a wired network from the list.
2. Tap the **More options** drop-down.
3. Tap **Wired Options**.
4. Set the **Multicast Optimizations** toggle switch to enabled ( ).
5. The changes are auto saved. Tap the back arrow () to return to the network details page for the wired network.

NOTE

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

Quality of Service

Quality of Service (**QoS**) determines how the network's traffic is treated when the network connection is congested. It controls the priority of the network's traffic relative to other networks, and can limit the download and upload bandwidth available to the network.

These settings define the default Quality of Service for all of the network's traffic. For more advanced scenarios, policies provide options to prioritize or limit the bandwidth of specific traffic – for example, specific clients, applications, or traffic flows. See Policies.

NOTE

Quality of Service is not supported on access point LAN ports, or on the Instant On 1830, 1930, and 1960 switch series. On a site where only these products are present, the Quality of Service tab is not displayed.

NOTE

Network-level Quality of Service settings are evaluated after any applicable policies. A policy that sets the priority or bandwidth limits for specific traffic therefore takes precedence over these network-level defaults.

Network Options

Select Network Priority to assign a Quality of Service priority to the network's traffic. Higher-priority networks are favored over lower-priority networks when the connection is congested.

Under Network Priority, select one of the following priority levels:

- **Low**—The lowest priority, for bulk transfers and other non-critical traffic that can tolerate delay
- **Medium** (default)—The default priority, for traffic that is not time-sensitive, such as most standard applications (best effort).
- **High**—A higher priority for latency-sensitive traffic, such as video streaming and video conferencing.
- **Very High**—The highest priority, for traffic that is highly sensitive to delay and jitter, such as voice (VoIP).

Bandwidth Control

Bandwidth Control limits the bandwidth available to the network. Under Bandwidth Limits, select one or both of the following, and then set the rate with the corresponding slider (maximum 1 Gbps):

- **Download**—Sets the maximum download rate for the network.
- **Upload**—Sets the maximum upload rate for the network.

WAN

The Wide Area Network (WAN) is an IP network that provides access to the internet. It is used to forward traffic to and from an Internet Service Provider (ISP).

By default, the WAN interface is set as a DHCP client and uses an untagged VLAN by default.

WAN Dashboard

The WAN Dashboard provides default chart-based visualizations of key metrics over the past 24 hours for up to two Secure Gateway WAN connections.

A toggle button is available at the top-right corner of the WAN Networks page to switch between two viewing modes:

- **Dashboard View**—Displays chart-based visualizations of WAN metrics over a rolling 24-hour period. This view is enabled by default.
- **List View**—Displays the tabular WAN status and configuration.

Dashboard Charts

HPE Networking Instant On supports three metric charts in the **Dashboard View**.

Health & Availability

The **Health and Availability** chart displays the WAN health state and online or offline availability over time using horizontal status bars.

Table 33: *Health Bar*

	Description
Good	The WAN health score is good. The connection is performing within expected parameters.
Fair	The WAN health score is sub-optimal. The connection may be experiencing

	Description
	degraded performance.
Poor	The WAN health score is poor. The connection is experiencing significant issues.
None	The WAN connection is in unknown state.

Table 34: *Availability Bar*

	Description
Online	The WAN connection is online and operational.
Offline	The WAN connection is offline.

Hover the cursor over the **Health And Availability** chart, the following information is displayed at the selected point in time:

- **WAN Connection Name**–Displays the name of the connection.
- **Health state**–Displays the health of the connection is good, fair, or poor.
- **Connection state**–Displays the connection is online or offline.
- **Timestamp**–Displays the time stamp of the selected data point.

Usage

The **Usage** chart displays upstream (upload) and downstream (download) traffic volume per WAN connection as a line chart.

- **Single WAN**–For a single WAN site, the chart displays uploads above zero and downloads below using an inverted scale to clearly separate them.
- **Multi WAN**–For a multi WAN site, the chart displays upload and download data per connection with distinct line colors, and a stacked layout to differentiate traffic.

Hover the cursor over the **Usage** chart, the following information is displayed at the selected point in time:

- **WAN Connection Name**–Displays the name of the WAN connection.
- **Download Value**–Displays the download traffic volume at the selected point in time.
- **Upload Value**–Displays the upload traffic volume at the selected point in time.
- **Timestamp**–Displays the time stamp of the selected data point.

For multi WAN sites, the tool tip displays the health and availability state for each WAN connection.

Latency

Latency is the time it takes for a data packet to travel from a source to a destination across the network, and is typically measured in milliseconds (ms). It reflects the responsiveness of a connection: lower latency results in a faster, more responsive network, while higher latency introduces delays that can degrade the quality of real-time applications such as voice and video calls, video conferencing, and online gaming. Latency can be affected by the distance to destination, network congestion, and the quality of the WAN connection provided by the Internet Service Provider (ISP).

The Latency chart displays the network latency, measured in milliseconds (ms), per WAN connection as a line chart.

- **Single WAN**–For a single WAN site, the chart displays the latency values for the WAN connection over the past 24 hours.
- **Multi WAN**–For a multi WAN site, the chart displays the latency data per connection with distinct line colors to differentiate the connections.

Hover the cursor over the Latency chart, the following information is displayed at the selected point in time:

- **WAN Connection Name**–Displays the name of the WAN connection.
- **Latency**–Displays the latency, in milliseconds, at the selected point in time.
- **Timestamp**–Displays the time stamp of the selected data point.

For multi WAN sites, the tool tip displays the latency value for each WAN connection.

Packet Loss

Packet loss occurs when one or more data packets traveling across the network fail to reach their destination. It is expressed as the percentage of packets lost out of the total number of packets sent. Packet loss is commonly caused by network congestion, unreliable or overloaded links, and faulty hardware or cabling. Even a small percentage of packet loss can noticeably degrade performance, resulting in choppy audio, frozen or pixelated video, and slower or interrupted data transfers, which is why it is an important indicator of WAN connection quality.

The Packet Loss chart displays the percentage of packets lost per WAN connection as a line chart.

- **Single WAN**–For a single WAN site, the chart displays the packet loss percentage for the WAN connection over the past 24 hours.
- **Multi WAN**–For a multi WAN site, the chart displays the packet loss data per connection with distinct line colors to differentiate the connections.

Hover the cursor over the Packet Loss chart, the following information is displayed at the selected point in time:

- **WAN Connection Name**–Displays the name of the WAN connection.
- **Packet Loss**–Displays the packet loss percentage at the selected point in time.
- **Timestamp**–Displays the time stamp of the selected data point.

For multi WAN sites, the tool tip displays the packet loss value for each WAN connection.

WAN Connections

HPE Networking Instant On supports two WAN connections in a site.

Primary WAN Connection

The primary WAN connection is created during the initial setup and its priority is automatically assigned as **Primary**. The primary WAN is assigned to WAN physical port of secure gateway and cannot be assigned to any other port. It supports DHCP, static IP, and PPPoE configurations along with DNS and VLAN settings.

Secondary WAN Connection

The secondary connection can be designated as the secondary WAN. It provides backup and failover capabilities in the event when primary connection is not available. The priority for the secondary WAN is assigned as **Secondary**.

WAN Details

To view the **WAN** details, follow these steps:

1. Tap the WAN () tile on the Instant On mobile app home page.
2. Tap any of the WAN connections in the **WAN** tab. This tab appears only when a secure gateway is deployed at a site.

Table 35: *WAN Information*

	Description
Name	Displays the name of the WAN. By default, the name of primary WAN connection is displayed as Internet.
Health	Displays the health status of the network: ■ Good – Indicates that the overall health score of the network is good. ■ Fair – Indicates that the overall health score of the network is sub-optimal. ■ Poor – Indicates that the overall health score of the network is poor. ■ None – Indicates that the network is in unknown state.
Status	Shows the status of the network, whether Online or Offline.
Connection	
Priority	Indicates the primary or secondary role of the WAN connection.
Connection Type	Indicates the connection type. The supported connection type is Ethernet.
Speed/Duplex	Displays the speed of the port and indicates whether the client is connected in a full duplex or half duplex mode.
Uplink	
Uplink VLAN	Specifies the VLAN ID associated with the network.
More Options	
IP Assignment	Specifies how the IP address is assigned to the WAN connection. Tap on **IP assignment** to change the settings.
Network Assignment	Specifies the IP address assigned to the WAN connection

More Options

The **More options** drop-down in the Instant On mobile app allows you to configure following settings for the WAN connection:

- IP Assignment
- Network Assignment

IP Assignment

The **IP assignment** setting in the Instant On mobile app allows you to configure DHCP and NAT for clients on the WAN. You can configure one of the following settings on your device:

- **Automatic(default)** – Select this option to automatically assign the IP address through the DHCP server.
- **Static** – Select this option to manually assign a static IP address for the WAN connection. Configure the following parameters:
  - **IP Address**–Enter a Static IP address.
  - **Subnet Mask**–Enter the subnet mask.
  - **Default Gateway**–Enter the IP address of the Default Gateway.
  - **Primary DNS Server**–Enter the IP address of the primary DNS server.
  - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
- **PPPoE**– Establishes the WAN connection to use Point-to-Point Protocol over Ethernet (PPPoE) for IP assignment.
  - Under **PPPoE Service**, configure the following parameters:
    - **Username**–Enter the user name provided by your ISP.
    - **Password**–Enter the password provided by your ISP.
    - **Service Name**–Enter the name of your ISP.
    - **MTU**–Enter the MTU in bytes for the PPoE connection. The default MTU value is 1492 bytes.
  - Configure one of the following **DNS Server Assignment** options:
    - **Automatic(default)** – Select this option to automatically assign the IP address through the DHCP server.
    - **Static** – Select this option to manually assign a static IP address for the WAN connection. Configure the following parameters:
      - **Primary DNS Server**–Enter the IP address of the primary DNS server.
      - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.

DNS Resolution

The **DNS Resolution** section allows you to configure servers assigned to clients and devices to resolve domain names.

Follow these steps to configure the DNS resolution for clients:

1. Under **IP Assignment** > **DNS Resolution**, select one of the following options.
   - **Automatic(default)**–This is the default setting. The DNS settings are automatically configured.
   - **Static**–Use this setting to configure a custom DNS server.
     - **Primary DNS Server**–Enter the hostname or IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the hostname or IP address of the secondary DNS server.

DNS Resolution

The **DNS Resolution** section allows you to configure servers assigned to clients and devices to resolve domain names.

Follow these steps to configure the DNS resolution for clients:

1. Under **IP Assignment** > **DNS Resolution**, select one of the following options.
   - **Automatic(default)**–This is the default setting. The DNS settings are automatically configured.
   - **Static**–Use this setting to configure a custom DNS server.
     - **Primary DNS Server**–Enter the hostname or IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the hostname or IP address of the secondary DNS server.

Network Assignment for WAN

The **Network Assignment** page allows you to select an available port to assign the WAN connection and define whether the selected port will be tagged or untagged.

You can use the secondary WAN port to connect to the secondary internet connection. The following are the ports the can be used for the both LAN and secondary WAN connection:

- SG1004 Gateway:
  - Port 3 can be converted into a secondary WAN port.
  - Port 3 supports speed of up to 1 Gbps.
- SG2505P Gateway:
  - Either Port 3 or Port 4 can be converted into a secondary WAN port.
  - Only one port can be used as a secondary WAN port at a time.
  - Port 4 supports speed up to 2.5 Gbps.
  - Port 3 supports speed up to 1 Gbps.

Every port on the Instant On devices at the site can be assigned in bulk to a particular VLAN, expect for the following:

- WAN ports
- A port where an Instant On device is connected.

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

Creating a Secondary WAN

You can create a secondary WAN connection after the site creation. The secondary WAN connection is always assigned with the secondary priority.

To create the secondary WAN, follow these steps:

1. Tap the **WAN** () tile on the Instant On mobile app home page.
2. Tap add () at the bottom right corner of the page. The Create Network screen is displayed.
3. Under **Identification**, enter a name for the WAN connection.
4. Under **Connection**, set the priority to the WAN connection. By default, the priority value is set to **Secondary**.
5. Under **Uplink VLAN**, assign an Uplink VLAN for network routing. The value must be between 2 and 4092.
6. Under **Assign Network**, select an available port to assign the WAN connection to and select whether the port is tagged or untagged.

- SG1004 Gateway
  - Port 3 can be converted into a secondary WAN port.
  - Port 3 supports speed of up to 1 Gbps.
- SG2505P Gateway
  - Either Port 3 or Port 4 can be converted into a secondary WAN port.
  - Only one port can be used as a secondary WAN port at a time.
  - Port 4 supports speed up to 2.5 Gbps.
  - Port 3 supports speed up to 1 Gbps.

7. Under **More Options**, configure one of the following **IP Address Assignment** options:
   - **Automatic(default)** – Select this option to automatically assign the IP address through the DHCP server.
   - **Static** – Select this option to manually assign a static IP address for the WAN connection. Configure the following parameters:
     - **IP Address**–Enter a Static IP address.
     - **Subnet Mask**–Enter the subnet mask.
     - **Default Gateway**–Enter the IP address of the Default Gateway.
     - **Primary DNS Server**–Enter the IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
   - **PPPoE**– Establishes the WAN connection to use Point-to-Point Protocol over Ethernet (PPPoE) for IP assignment.
     - Under **PPPoE Service**, configure the following parameters:
       - **Username**–Enter the user name provided by your ISP.
       - **Password**–Enter the password provided by your ISP.
       - **Service Name**–Enter the name of your ISP.
       - **MTU**–Enter the MTU in bytes for the PPoE connection. The default MTU value is 1492 bytes.
     - Configure one of the following **DNS Server Assignment** options:
       - **Automatic(default)** – Select this option to automatically assign the IP address through the DHCP server.
       - **Static** – Select this option to manually assign a static IP address for the WAN connection. Configure the following parameters:
         - **Primary DNS Server**–Enter the IP address of the primary DNS server.
         - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
8. Tap the back arrow () on the title bar of the mobile app to save and exit the screen.
9. Tap **Done**. The secondary WAN is created and displayed in the **WAN** tab.

WAN Redundancy

WAN Redundancy provides an intelligent, automated way to ensure continuous network availability. It uses multiple WAN connections and offers seamless failover to maintain uninterrupted business operations.

The **WAN Redundancy** page is displayed only when a secondary WAN connection is configured.

To configure WAN redundancy, follow these steps:

1. Tap the **WAN** (tile on the Instant On mobile app home screen.
2. In the **Networks** screen, tap the advanced menu () icon and tap **WAN Redundancy**.

3. Under **WAN Redundancy**, select one of the following options:
   - **Active / Backup Failover (default)**–Prioritizes the primary WAN connection for all traffic. The secondary WAN connection is used only if the primary connection fails. For more information, see WAN Failover.
   - **Active / Active Load Balancing**– Distributes traffic between the primary and secondary WAN connections evenly.

WAN Failover

WAN Failover ensures continuous internet connectivity by automatically switching to the secondary WAN connection if the primary connection fails. The secure gateway monitors the status of both the primary and secondary WAN connections. If the primary WAN goes offline, the failover is triggered, and the secondary WAN (backup) takes over. The switch from primary to secondary occurs within two minutes. Once the primary WAN is back online, it takes around three minutes to switch back to the primary connection.

VPN Network

A Virtual Private Network (VPN) is suitable for users who require secure and encrypted connections across their network infrastructure. It enables encrypted communication between remote clients and a secure gateway, allowing users to access resources on the local network.

Remote clients must have proper authorization on their device to establish a remote connection through a VPN tunnel. They can access networks and services based on site-specific and VPN network policies.

You can create only one VPN network per site. A VPN network can be created only when a secure gateway is deployed at the site.

The following procedure creates a VPN network:

1. Tap the **LAN** tile 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 **VPN** as **Network type**.
4. Under **Identification**, enter a **Name** for your network.
5. Under **Properties**, enter the **Listening port** for the VPN server. The default port is 51820.

When the UDP protocol on the WAN port is already in use by an existing port forwarding policy, the following error banner message is displayed: **The UDP protocol on WAN port (portID) is used by the (policyName) policy**.

6. Under **IP Addressing**, enter the **Network address** of the VPN server. The **Subnet mask** is auto-generated based on the secured gateway SKU model and displayed as read-only.

   This step defines how clients and devices will obtain IP addresses when connecting to the VPN network.

7. Under **Tunneled destination Networks**, define which LAN networks are accessible through the VPN tunnel by selecting one of the following options:
   - **All wired networks**–Select this option to include all available wired LAN networks in the VPN tunnel. This is the default option.
   - **Selected Wired Networks**–Select this option to allow only selected wired LAN networks to be included in the VPN tunnel. Select at least one network from the list.

8. Tap **Done**.

   Once completed, a VPN network is created, and the corresponding policy is automatically created to allow access to the selected destinations.

Network Options

Select Network Priority to assign a Quality of Service priority to the network's traffic. Higher-priority networks are favored over lower-priority networks when the connection is congested.

Under Network Priority, select one of the following priority levels:

- **Low**—The lowest priority, for bulk transfers and other non-critical traffic that can tolerate delay
- **Medium** (default)—The default priority, for traffic that is not time-sensitive, such as most standard applications (best effort).
- **High**—A higher priority for latency-sensitive traffic, such as video streaming and video conferencing.
- **Very High**—The highest priority, for traffic that is highly sensitive to delay and jitter, such as voice (VoIP).

Bandwidth Control

Bandwidth Control limits the bandwidth available to the network. Under Bandwidth Limits, select one or both of the following, and then set the rate with the corresponding slider (maximum 1 Gbps):

- **Download**—Sets the maximum download rate for the network.
- **Upload**—Sets the maximum upload rate for the network.

Viewing VPN Network Details

The following procedure is used to view or modify an existing VPN network:

1. Tap the LAN tile on the Instant On home screen. The **Networks** screen is displayed.
2. Select the VPN network from the **Networks** list to view the **Network Details** screen.

Table 36: *VPN Network Details*

	Description
Name	Displays the name of the VPN network.
Enable Network	Indicates whether the network is enabled or disabled. Slide the **Enable network** toggle switch to the right ( ) to enable the VPN network, or to the left ( ) to disable the VPN network.
Health	Displays the health status of the network: ■ Good – Indicates that the network in active and online. ■ Poor – Indicates that the network is offline. ■ None – Indicates that the network is inactive.
State	Shows the operational state of the network, indicating whether it is **active** or **inactive**.
Site hostname	Displays the site host name. The site host name is automatically assigned by the system and displayed in a read-only format.
Listening Port	Displays the listening port of the VPN server. The default port is 51820. You can update the value if needed.
Public key	Displays the cryptographic keys associated with the VPN network. You can copy the displayed public key to the clipboard by clicking the **Copy public key** icon. To generate a new key, click the **Regenerate** icon. **NOTE:** Generating a new public key for the network disconnects all clients using it.

3. Tap **Done**.

More Options

The **More options** drop-down in the Instant On mobile app allows you to configure following settings for the VPN network

- IP Assignment
- Client Configurations

IP Assignment

The **IP assignment** configuration in the Instant On mobile app allows you to configure IP addressing for clients and devices connecting to the VPN network.

The following procedure configures the IP assignment on Instant On VPN network:

1. Tap the **LAN** tile on the Instant On home page and select a VPN network from the list. The network details page is displayed.

2. Under **More options**, tap **IP assignment**. The **IP Assignment** screen is displayed with the following information:
   - **Network Address**–Displays the network address assigned to VPN. This network address is different from the base IP address, which is always reserved for the WireGuard interface.

Changing the network address disconnects all clients and invalidates all existing client configurations for this network.

   - **Subnet Mask**–Displays the subnet mask, which varies based on the Secure Gateway SKU:
     - SG1004 gateway–The subnet mask is set to /24 (255.255.255.240), supporting up to 10 clients.
     - SG2505P gateway–The subnet mask is set to /24 (255.255.255.224), supporting up to 25 clients.

Client Configurations

The **Client Configurations** screen allows you to create and manage the client configurations for a VPN network.

Clients must have proper authorization using the WireGuard VPN application on their devices to establish a remote connection through a VPN tunnel.

You can download the WireGuard application for your operating system from the official WireGuard Installation page.

The maximum number of client configurations depends on the SKU:

- SG1004 gateway supports a maximum of 10 client configurations.
- SG2505P gateway supports a maximum of 25 client configurations.

Creating a Client Configuration

The following procedure creates the client configuration Instant On VPN network:

1. Tap the LAN tile on the Instant On home page and select a VPN network from the list. The network details page is displayed.
2. Under **More options**, tap **Client configurations**. The **Client configurations** screen is displays the list of VPN client configurations.
3. Tap ( ) to create a new network. The **Create Client Configuration** screen is displayed.
4. Under **Client Properties**, enter the name of the client. Under **Connectivity**, the IP Address of the client is displayed automatically. This IP address is auto-calculated based on the first available address within the subnet.
5. Click **Continue**.
6. Under **Cryptographic Client Identity**, select one of the following options to specify how to generate the key pair of the VPN client.
   - **Automatic (default)**–Select this option to automatically generate the key pair. This is the default option.
   - **User Defined**–Select this option to manually define the public key in the **Public Key (Base64**) field.
7. Click **Create Client Configuration**. The **Client configuration** screen is displayed with the client configuration. You can import the configuration into the WireGuard application in one of the following methods:

- QR Code–Scan the QR code using your mobile phone to import the full client configuration.
- Copy–Tap the **Copy** icon ( ) to copy the WireGuard configuration to the clipboard.
- Download–Tap the **Download** icon () to download the WireGuard configuration file.

Client Configuration Details

The Client Configuration details screen contains the following sections:

- Identification
- Connectivity
- Public Key
- Client Configuration
- Delete Client Configuration

To view the details of the client configuration, follow these steps:

1. Tap the **LAN** tile on the Instant On home page and select a VPN network from the list. The network details page is displayed.
2. Under **More options**, tap **Client configurations**. The **Client configurations** screen is displays the list of VPN client configurations.
3. Tap on the client configuration for which you want to view the details. The following information is displayed

Identification

The **Identification** section provides the basic details of the selected VPN client.

Under **Overview** > **Identification** section displays the following details:

- **Name**–Displays the name of the client. You can edit the name if required.
- **Enable client**–Indicates whether the client configuration is enabled or not. Use the toggle switch to enable or disable the client configuration.
- **State**–The current operational state of the client.

Connectivity

The **Connectivity** section displays the IP address of the client. This IP address is auto-calculated based on the first available address within the subnet.

Public Key

The **Public Key** section displays the cryptographic public key associated with the client.

Client Configuration

The **Client Configuration** section displays the most recently generated WireGuard configuration. You can use the **Regenerate** icon () to generate a new WireGuard client configuration.

Delete Client Configuration

Tap the advanced menu () icon, and then tap **Delete client** to delete the client configuration.

Chapter 11
Managing Clients

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, watchlisted clients, and blocked clients in separate pages. To view the **Clients** page, tap the **Clients** () tile on the Instant On home page.

The following sections are available in the Clients page:

- **Overview**–Displays the list of clients that are actively connected in the site.
- **Watchlisted**–Displays the list of offline and online watchlisted clients in every network of the site.
- **Blocked**–Displays the list of clients blocked in the site by the administrator.
- **Classification Tags**–Displays the list of classification tags that has accessed the site.

Viewing Wireless 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, wireless, and VPN.

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. Tap the Clients () tile on the Instant On home page. The **Clients** page is displayed.
2. Click on the client name from the list connected clients (). 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:

- Viewing Wireless Clients
- Device Details
- Security Details
- Connection Details
- Connection Health
- Data Usage and Transfer Rates

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

Column Label	Description
	To reset the client name to its default name, select the client name text field, tap the reset icon and then tap **Update** to save the changes. The reset icon is displayed only when the client is assigned a custom device name.
Device Details	
IP Address	IP address of the client.
MAC Address	MAC address of the client.
OS	Operating system (OS) of the client device.
Security Details	
Security Details	This section displays the security standard used by the wireless client to connect to the network.
Connection Details	
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
State Duration	Displays the duration for which the client remains in their current state, including both online and offline periods, for the entire span of the session.
Device Uptime	Denotes the continuous duration that the client has been powered on and processing traffic.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Device Connected On	Displays the details of the Instant On 1960 Series switch in a stack to which the client is connected to. **NOTE:** This information is displayed only for clients connected to a stack.
Wi-Fi Standard	The Wi-Fi standard of the client connection. The Wi-Fi standard mapping is displayed as follows: ▪ **Wi-Fi 6**– 802.11ax client ▪ **Wi-Fi 5**– 802.11ac client ▪ **Wi-Fi 4**– 802.11n client **NOTE:** The Wi-Fi standard will not be displayed for legacy Wi-Fi clients using 802.11b or 802.11g standards.
Interface	The radio of the AP to which the client is connected.
Last data rate	The latest download and upload rates of the client in Mbps.
Connection Health	
Status	The general health status of the client.
Signal / Speed	Indicates the client signal quality. Based on the client's Signal-to-Noise Ratio (SNR), the signal quality is denoted as follows: ▪ Good – Signal Strength of 25 dB or higher.

Column Label	Description
	■ 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 the Clients () tile 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.

Adding or Removing Clients from a Watchlist

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

You can add a maximum of 256 wired, wireless, or VPN clients to the watchlist.

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

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. The list of connected clients is displayed. Swipe from right to left on the client from and tap on the watchlist icon.

Alternatively, you can perform the following steps:

1. Tap on the wired, wireless, or VPN client you want to add to the watchlist (☆). The **Client Details** page for the selected client is displayed.
2. Tap the advanced menu icon () and select **Add to watchlist** from the drop-down menu. The client is added to the watchlisted clients (☆) list.

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

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. The list of connected clients is displayed.
2. Tap the watchlist icon (☆). The list of watchlisted clients is displayed.

3. Swipe left on the wired, wireless, or VPN client to be removed from the watchlist and tap the () icon. The client is removed from the watchlist.

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

Follow these steps to unblock a blocked client:

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

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

You can enable the **Multi-select Mode** either by performing a long press on a client row or by navigating through **Advanced Menu** > **Select**. Once enabled,you can choose multiple client rows simultaneously to perform bulk actions suchas **Add to Watchlist**, **Block Clients**, or **Power cycle**.

- **Add to Watchlist** option will be inactive, once the Watchlist category reaches its maximum capacity of 128 clients.
- **Block Clients** option will be inactive, once the Watchlist category reaches its maximum capacity of 256 clients.
- **Power Cycle** option will be inactive, once the Power Cycle allows bulk actions to simultaneously restart all selected wired PoE clients, but is only available when every device on the site running Instant On 3.4.0 or later versions and at least one wired PoE client is chosen. It requires the same permissions as individual client power cycling.

Filtering and Sorting of Active Clients

The **Filter** category tab displays the count of selections of that category. If the combination of active filters and search queries yields zero results, the system displays a **No clients found** empty state.

The **Filter** page lists the following information:

Column Label	Description
Health	
None	Select the checkbox if the health of the client is unknown.
Poor	Select the checkbox if the health of the client is poor.
Fair	Select the checkbox if the health of the client is fair.
Good	Select the checkbox if the health of the client is good.
State	
Online	Select the checkbox if the client is online.
Offline	Select the checkbox if the client is offline.
Network	
Wireless	Select the checkbox if the network is a wireless client.
Wired	Select the checkbox if the network is a wired client.
VPN	Select the checkbox if the network is a VPN client.
Classification - This option allows you to select or unselect the client tags.	
Sort By	
Name (A-Z)	This option will sort the name of the active clients in ascending order.
Name (Z-A)	This option will sort the name of the active clients in descending order.
Health: Poor to Good	This option will sort the health of the active clients from poor to good.
Health: Good to poor	This option will sort the health of the active clients from good to poor.

Classification Tag Details

The Instant On mobile app displays all classification tags applied to the client.

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

1. Select the desired client on the **Clients** screen. The **Client Details** page opens.
2. To change the current associated tag, click **Edit**. You can view the list of clients associated with the classification tag.
3. To add or remove classification tag for the client, tap on **Search Classification Tags** and enter the tag name.
4. Click **Done** to save the changes.

Alternatively, you can perform the following steps:

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. Select the Classification Tags option from the **More** menu on the top. The **Classification Tags** screen appears.
2. Click on a classification tag to open the details page. You can view the number of clients and rename the currently selected tag.

Client Classification option under **Actions** allows you to update classification tags for multiple clients simultaneously by selecting them directly from the **Clients** page.

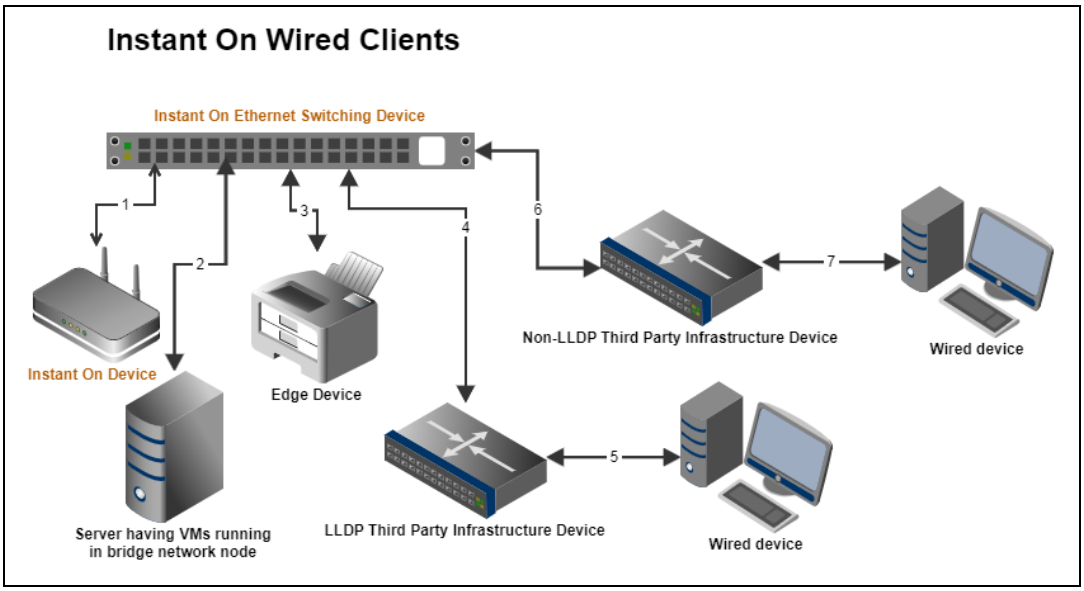
NOTE

- When two or more clients are selected, the section **Assign classification tags to the [N] selected clients** is displayed.
- When a single client is selected, the process shall follow the same flow as when accessing the tag through **Client Details** > **Classification Tags**.

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 9 *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.

NOTE

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

- **Scenario 3:** The edge device will be shown as an edge wired client.
- **Scenario 4:** The third-party infrastructure device will be shown as an infrastructure wired client.

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

Wired Client Details

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

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

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

Table 37: *Wired Client Details Information*

Parameter	Description
Client name	Denotes the name of the wired client. The client name can be edited and updated to a custom name of your choice. The length of the client name can be between 1 to 32 characters. Blank spaces and special characters are accepted as a valid characters in the client name. To reset the client name to its default name, select the client name text field, tap the reset icon and then tap **Update** to save the changes. The reset icon is displayed only when the client is assigned a custom device name.
Type	Denotes the type of the wired client. The client can either be an infrastructure client or a voice client.
IP Address	IP address of the client.
MAC Address	Denotes the MAC address of the wired client.
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
Interface	Denotes the device interface to which the client is connected. The Wired client will display the port ID or the custom port name to which it is connected.
State Duration	Displays the duration for which the client remains in their current state, including both online and offline periods, for the entire span of the session.
Device Uptime	Denotes the continuous duration that the client has been powered on and processing traffic.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Port	Denotes the switch port through which the wired client is connected to the network.
Client Health	Denotes the health status of the wired client.
Status	Represents the ratio of the number or error packets on all the packets. ■ Good–In full duplex mode, the error rate is less than 0.1%. In half duplex mode, the error rate is less than 2%. ■ Fair–In full duplex mode, the error rate is above 0.1%. In half duplex mode, the error rate is above 2%.

Parameter	Description
Duplex Mode	Denotes if the wired client is connected in a full duplex or half duplex mode.
Downloading	Shows the download throughput within the last 30 seconds, in bytes per second.
Uploading	Shows the upload throughput within the last 30 seconds, in bytes per second.
Transferred	Shows the total amount of data transferred during the client session, in bytes.

PoE Power Cycle

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

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

NOTE

The PoE supplier should be an Instant On device.

Power Cycle Multiple Clients

You can power-cycle several wired PoE clients at once from the Clients **Overview** or **Watchlist** table.

The following procedure is used to power cycle multiple clients:

1. Click the **Clients** ( ) tile on the Instant On home page. The **Clients** page is displayed.
2. Long press on the client row to enable the **Multi-select Mode**, or through **Advanced Menu** > **Select**.
3. Select the wired PoE clients you want to power-cycle, then select **Power Cycle**. Each selected client is powered off and then back on in sequence.

NOTE

The **Power Cycle** bulk action appears only when all devices on the site are running Instant On 3.4.0 or later versions and at least one wired PoE client (a client connected to a PoE port on an Instant On router or switch) is selected.

Adding or Removing Clients from a Watchlist

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

NOTE

You can add a maximum of 256 wired, wireless, or VPN clients to the watchlist.

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

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. The list of connected clients is displayed. Swipe from right to left on the client from and tap on the watchlist icon.

Alternatively, you can perform the following steps:

1. Tap on the wired, wireless, or VPN client you want to add to the watchlist (☆). The **Client Details** page for the selected client is displayed.
2. Tap the advanced menu icon () and select **Add to watchlist** from the drop-down menu. The client is added to the watchlisted clients (☆) list.

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

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. The list of connected clients is displayed.
2. Tap the watchlist icon (☆). The list of watchlisted clients is displayed.
3. Swipe left on the wired, wireless, or VPN client to be removed from the watchlist and tap the () icon. The client is removed from the watchlist.

Classification Tag Details

The Instant On mobile app displays all classification tags applied to the client.

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

1. Select the desired client on the **Clients** screen. The **Client Details** page opens.
2. To change the current associated tag, click **Edit**. You can view the list of clients associated with the classification tag.
3. To add or remove classification tag for the client, tap on **Search Classification Tags** and enter the tag name.
4. Click **Done** to save the changes.

Alternatively, you can perform the following steps:

1. Tap the Clients () tile in the Instant On homepage of the Instant On mobile app. Select the Classification Tags option from the **More** menu on the top. The **Classification Tags** screen appears.
2. Click on a classification tag to open the details page. You can view the number of clients and rename the currently selected tag.

Client Classification option under **Actions** allows you to update classification tags for multiple clients simultaneously by selecting them directly from the **Clients** page.

NOTE

- When two or more clients are selected, the section **Assign classification tags to the [N] selected clients** is displayed.
- When a single client is selected, the process shall follow the same flow as when accessing the tag through **Client Details** > **Classification Tags**.

Reserving an IP Address for a Client

In addition to reserving an IP address from the network's **IP Assignment** tab, you can also reserve or remove a client's IP address directly from the Clients page, for both online and offline clients.

The following procedure reserve or remove a client's IP address directly from the Clients list:

1. Tap the **Clients** ( ) tile on the Instant On home screen, select the desired client to view the details.
2. Tap the advanced menu icon and tap **Add IP Address Reservation**. The current IP address is reserved by default, adjust it if needed, then tap **Add IP Address Reservation**.
3. To remove a reservation, open the advanced menu and tap Remove **IP Address Reservation**.

Reserving an IP Address on Multiple Networks- When a wired client is connected to more than one network, the **Add IP Address Reservation** dialog lets you reserve a separate IP address for the client on each eligible network in a single operation.

NOTE

Under **Wired Networks**, select the checkbox for each network on which you want to reserve an IP address. For each selected network, the client's current IP on that network is reserved by default; you can adjust it within the network's DHCP range.

- Networks that have already reached the maximum of 128 IP address reservations (cannot be selected).
- Networks that already have an IP address reserved for this client. Click **Add IP address reservation** to apply all selected reservations at once.

Viewing VPN Clients

The VPN Client details page provides detailed information about clients connected to the VPN network.

NOTE

You cannot block the VPN client.

VPN clients include laptops, personal computers, tablets, mobile phones, etc. that connect to the Instant On network through a VPN tunnel.

To view the VPN client details page for a specific client, follow these steps:

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

Table 38: *VPN Client Details*

Column Label	Description
Identification	
Hostname	Displays the hostname of the client.
Health	Displays the health status of the connected clients: ■ Good –Indicates that the health of the client is good. ■ Fair – Indicates that the health of the client is fair. ■ Poor – Indicates that the health of the client is poor.
State	Denotes the state of the connected client, whether Online or Offline.
Online Since	Displays the time since the client is connected to the network. You can click on the **View client configuration** to view the client configuration details page.

Column Label	Description
Connectivity	
IP Address	The IP address of the client.
Remote IP Address	The IP address of the remote server.
Remote Port	The port number used by the VPN client to connect to the remote server.
Connection	
Network	The network to which the client is connected. Clicking on the network name will take you to the Network Details page.
Device	The network device to which the client is connected. Clicking on the device name will take you to the Device Details page.
Port Usage	
Downloading at	The download throughput of the device in the last 30 seconds, in kilobits per second.
Uploading at	The upload throughput of the device in the last 30 seconds, in kilobits per second.

Chapter 12
Managing Your Account

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

Changing Account Password

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

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

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

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

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

Profile

The **Account Management** > **Profile** screen contains the following sections:

- Identification
- Preferences

Identification

The Identification section displays the primary administrator email account used to manage the operations for the site.

Preferences

The **Preferences** section provides the option to change the preferred language for the interface, notifications, and other communications. To change the language preference, select the language from the **Language** drop-down list.

The administrator of the account can modify the language to one of the following supported languages:

- German
- English
- French
- Spanish
- Italian

- Japanese
- Korean
- Portuguese
- Chinese, Simplified
- Chinese, Traditional

Security

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

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

Activating Two-Factor Authentication

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

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Security**.
3. Tap **Set up two-factor authentication**.
4. Under **Validate Password**, enter your current Instant On account password.
5. Tap **Validate password**.
6. Under **Authenticator**, copy the key provided below and enter it in the authenticator app.
7. Tap **Continue**.
8. Enter a **Recovery email** you can use to sign in when having trouble using the authenticator app.
9. Re-enter the recovery email.
10. Enter the One-time password generated by your authenticator app.
11. Tap **Activate two-factor authentication**.

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

Deactivating Two-Factor Authentication

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

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Security**.
3. The **Security** screen displays that **Two-Factor Authentication** is currently enabled on your account.
4. Tap the advanced menu () icon in the header and tap **Disable two-factor authentication**. A popup is displayed on the screen.
5. Tap **Disable**.

Changing the Recovery Email Address

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

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

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Security**.
3. Tap the advanced menu () icon in the header and tap **Change recovery email address**.
4. Enter the **New recovery email** address.
5. **Confirm new recovery email** by re-entering the new email address.
6. Tap **Change recovery email** to apply the changes.

Notifications

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

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

Enabling or Disabling Alert Notifications

To enable notifications for alerts, follow these steps:

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Notifications**.
3. Under **Notification Preferences**, you have the option to choose notification preferences by selecting one or both of the following options:
   - **Notify When a Situation Arises**–Receive alerts when an issue or event occurs. This option is enabled by default.
   - **Notify When a Situation Clears**–Receive alerts when the issue is resolved.
4. Under notification categories, you have the option to enable either **Mobile** or **Email** notifications, or both. Slide the toggle switch(es) to enable ( ) or disable ( ) the alerts you want to be notified about as mobile or email notifications. The alerts you have enabled will be displayed in the **Site Health** tile in the home page. For more information on viewing and managing alerts, see:
   - Viewing and Managing Alerts using the Mobile App

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

Alert Categories

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

- Connectivity
- Device
- Capacity
- Watchlisted Client
- Software

Connectivity

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

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.
- Deployment issue.
- Instant On Device is restarting due to an unexpected condition.

Capacity

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.

Watchlisted Client

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

Software

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

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

Communication Preferences

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

1. Tap the account icon (the alphabet icon) displayed on the header. The **Account management** screen is displayed.
2. In the **Account management** screen, tap **Communication Preferences**.
3. Under **Country**, tap the drop-down icon and select the country you reside in, from the list.
4. Under **Offers and promotions**, select the **May HPE provide you with personalized communications about HPE and select partner products, services, offers, and events** checkbox.

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

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

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

Delete Account

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

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

Chapter 13
Policies

The Policies page provides a unified space for administrators to define and manage rules from a single page and apply them to more than one network or application at the same time. The task of firewall configuration, blocking application access and wireless network availability schedules are managed as policies. You can create a maximum of 32 policies for an Instant On site. If more than once policy is created and activated, the policy with the higher priority will be applied first on the site. If there are many rules about the same element, the rule with the highest priority is applied and the remaining policies are discarded, using the smallest common factor:

- A category for an application policy.
- A network for a network schedule policy.

Instant On supports policy creation using the following methods:

- AI-Assisted policy creation—Policies are created using prompts in an interactive, text-based format. The **Edit** option allows you to modify the policy generated by the AI. AI-assisted policy creation is available on all site topologies, including sites with or without a secure gateway. For more information, see AI-Assisted Policy Creation.
- Manual policy creation—Sites without a secure gateway supports only the manual policy creation. You need to manually define the required parameter to configure the policy. Manual policy creation is available on all site topologies. For more information, see Manual Policy Creation.

Policy Support by Site Topology

Policies can be created on any site, but the available actions, sources, and destinations depend on the devices present in the site:

- On sites with a secure **Gateway**, the full set of policy capabilities is available, including client policies, application-category policies, Internet or domain or network destinations, port forwarding, and network routing.
- On switch-only sites (switches but no secure gateway), you can create network firewall policies with the **Allow**, **Block**, and **Restrict** acions. The source can be a specific IP address or subnet, or a wired network; the destination is a specific IP address or subnet.
- On **AP-only** sites, wireless network-to-application-category policies and IP-to-IP rules (IP address or subnet based) are supported. For APs with wired and wireless capabilities (such as AP11D and AP22D), wired network-to-IP address or subnet policies are also supported. Other wired-network firewall policies are not available.

The following capabilities require a secure gateway and are not available on gateway-less sites:

- Destinations such as the **Internet**, **Domains**, or **Networks**.
- The **Same Network** destination type, which is supported only with Secure Gateway.
- Client-to-network policies, port forwarding, and network routing.

Wireless access points generally do not support using a wired network as the policy source; however, this capability is available on APs that support wired networks, such as the AP11D and AP22D. The 1830 switch series does not support firewall policies.

Policy Deployment

In HPE Networking Instant On network, policies are dynamically applied based on the site's topology, ensuring rules, configurations, and settings are optimized based on network infrastructure and operational requirement. Wherever possible, the system is designed to automatically enforce the policies on the Instant On edge devices—devices situated at the periphery of the network topology. This automated enforcement enhances efficiency and responsiveness by minimizing latency and reducing reliance on centralized Instant On devices.

The system intelligently balances policy enforcement between edge and centralized devices through techniques such as tiered enforcement, lightweight processing, and cloud-assisted solutions. This approach ensures that each site operates optimally within its unique environment while maintaining a balance between performance and resource utilization.

The HPE Networking Instant On network applies the configured rules for a site in the following order:

1. **Configured Policies**—These are the custom rules defined by administrators within the **Policies** section. They are applied first, following the priority order specified in the policy list.
2. **Default rules**—Applicable only to sites with a deployed secure gateway, a set of default rules is automatically enforced. These rules are not visible in the user interface and include the following rule:
   - All LAN ports are granted access to the internet by default.
   - Communications between LAN networks are blocked by default.
   - All application categories are permitted on all networks by default.
3. **Network Access Controls**—Within the Access Control section, administrators can configure network access restrictions for wired or wireless clients based on destination IP addresses. For detailed instructions, refer to the Configuring Networks documentation.

Viewing Policies

The **Policies** page displays the list of policies created for the site, in order of their highest to lowest priority. To view the details of a policy, follow these steps:

1. Tap the Policies () tile on the Instant On mobile app home page. The list of policies created by the administrator are displayed here in order of their highest priority.
2. Tap on any of the policies in the list to view its details. The **Policy Details** page is displayed.

Reordering Priority

The list of policies are displayed in order of their highest to lowest priority. To change the order of the priority, follow these steps:

1. Tap the Policies () tile on the Instant On mobile app home page. The list of policies created by the administrator are displayed here in order of their highest priority.
2. Press the **=** icon next to the policy and drag it above or below the policy you want to position it.
3. Click **Done**.

AI-Assisted Policy Creation

AI-Assisted policy creation simplifies the process of setting up policies by allowing you to generate them through natural language prompts. Instead of manually configuring each setting, you can describe your requirements in plain text, and the system will automatically generate a policy based on your input.

AI-assistance is limited to policy creation only. Other Instant On configurations or any information beyond the scope of policy creation is not supported by the AI-assistance.

Policies can be created using the AI assistant (Assistant) or manual policy creation on any site topology. The categories of policies the assistant can create depend on the devices present in the site. A site with a secured gateway supports the following categories of policies:

- Site Policy–Allow or block port forwarding.
- Client Policy–Control destinations that can be accessed by clients on the network.
- Network Policy–There are three types of network policies:
  - Network Activation–Activate or deactivate the network during specific times.
  - Network Firewall–Allow or block incoming and outgoing traffic to protect against unauthorized access and threats.
  - Network Access–Control destinations that can be reached from the network.
- Application Policy–Allow or block specific applications from being used on the network.

On a **Switch-only** site, the assistant creates network firewall policies (Allow, Block, Restrict) between IP/subnet or wired-network sources and IP or subnet destinations.

Limitation of AI-Assistance

- Policies cannot be edited using the AI-assistance. To edit an existing policy, tap on the policy to view the **Policy Details** screen.
- Creation of new schedule is not supported, only exciting schedules can be applied during new policy creation.
- To ensure that domain policy rules are correctly implemented for site clients within an HPE Networking Instant On environment, the clients must use the Secure Gateway as their DNS server.

Creating a Policy Using AI-Assistance

The following procedure describes how to create an AI-assisted policy:

1. Tap the Policies () tile on the Instant On mobile app home page.

   The **Policies** screen is displayed.
2. Tap the ( ) icon.

   The **Create Policies** screen is displayed.
3. In the **State a Policy by Intention** text box, enter the policy requirement as a prompt.

   You can also select from predefined suggestions displayed above the **State a Policy by Intention** text box. Swipe left to view the full list of predefined suggestions.
4. Tap the **Submit** icon.

   The AI assistant analyzes the input and initiates a conversation to gather all necessary details.
5. Interact with the AI-assistant to refine and complete the policy details.

6. The AI assistant generates the policy based on the interaction.
7. To review and edit the AI-generated policy tap on the suggested policy.

   The **Policy Details** screen is displayed.
8. In the **Policy Details**, you can do the following:
   a. Manual edits to the suggested policy.
      - After editing the policy, tap **Done** to save the changes and return to the **Create Policies** screen.
      - Tap the Cancel **X** icon to discard the changes done to the policy and return to the **Create Policies** screen.
   b. Review the policy details.

      After reviewing the generated policy, tap the back arrow icon to return to the **Create Policies** screen.
9. In the **Create Policies** screen, tap **Start Over** icon to delete the current conversation and begin again. This is an optional setting.
10. In the **Create Policies** screen, tap **Delete** icon next to the policy to delete the proposed policy. This is an optional setting.
11. Tap **Accept** to confirm.
12. Tap **Create Policies**.

    The newly created policy is added at the end of the policy table.

Manual Policy Creation

Instant On supports manual policy creation on all site topologies. The available categories and rule options depend on the devices present in the site.

Creating a Network Policy

Instant On allows you to assign a single schedule to many different wireless networks instead of configuring a schedule per wireless network.

The following procedure describes how to create a network schedule policy:

1. Tap the Policies () tile on the Instant On mobile app home page. The **Policies** screen is displayed.
2. Tap the ( ) icon. The **Create Policy** pop-up screen is displayed.
3. Select **Assistant** to open the page using AI Assistant.
4. Select **Advanced** to open the page without AI Assistant.
5. The **Create Policy** screen is displayed.
6. Under **Set Policy Type**, tap on the **Networks** tile.
7. Tap **Continue**.
8. Under **Set Rule and Condition**, configure the following settings:
   a. **Action**–Select one of the following actions for the rule:
      - **Enable**–Makes a wireless network available for users to connect when the provided schedule is enabled.
      - **Disable**–Makes a wireless network unavailable when the provided schedule is disabled.

b. Under **Networks**, select one of the following:
   - **All Wireless Networks**–Policy applicable on all the wireless networks.
   - **Selected Wireless Networks**–Select networks from the **Select networks** list to which the rule will be applied. At least one network must be selected.

c. Tap the back arrow () to return to the **Set Policy Type** screen. This is an optional setting.

9. Tap **Continue.** The **Set Policy Applicability** screen is displayed.
10. Under **Set Policy Applicability**, configure the following settings:
    - **Identification**, enter a name for the policy.
    - Set the **Priority** for the policy.
      1. Under **Position**, select either **Lower** or **higher**.
      2. Under **Policy**, select a policy from the drop-down list.
    - Under **Schedule**, select one of the following options:
      1. **Always Active**–Select this option to make the wireless network always available for users to connect.
      2. **Existing Schedules**–Select this option to use the existing schedules.
    - Tap the back arrow icon, to return to the **Set Rule and Condition** screen. This is an optional setting.
11. Any time during policy creation, tap **Cancel creation** to cancel the policy creation. This is an optional setting.
12. Tap **Create Policy**.

Creating an Application Policy

It is possible to allow or deny access to application categories for some or all wireless networks. Additionally, the Network condition can be configured. If the Network condition is not provided, the policy will be applied on all wireless networks.

The following procedure describes how to create an application policy:

1. Tap the Policies () tile on the Instant On mobile app home page. The **Policies** screen is displayed.
2. Tap the ( ) icon. The **Create Policy** screen is displayed
3. Under **Actions**, tap on the **Applications** tile.
4. Tap **Continue**.
5. Under **Set Rule and Conditions**, configure the following settings:
   a. **Rule**–Select one of the following actions for the rule:
      i. **Allow**–Allows traffic matching the specified application categories and wireless networks pass.
      ii. **Block**–Blocks traffic matching the specified application categories and wireless networks.
   b. Under **Networks**, select one of the following:
      - **All Wireless Networks**–Policy applicable on all the wireless networks.
      - **Selected Wireless Networks**–Select networks from the **Select networks** list to which the rule will be applied. At least one network must be selected.
   c. Under **To Access** or **From Accessing** > **Applications Categories**–Select the application categories from the **Applications Categories** list for which the action needs to be applied. Tap the back arrow icon to save the application list. For the current list of application categories, see Applications List.
   d. Tap the back arrow () to return to the **Set Policy Type** screen. This is an optional setting.

6. Tap **Continue**.

   Displays **Set Policy Applicability** screen.
7. Under **Set Policy Applicability**, configure the following settings:
   - **Identification**, enter a name for the policy.
   - Set the **Priority** for the policy.
     1. Under **Position**, select either **Higher** or **Lower**.
     2. Under **Policy**, select a policy from the drop-down list.
   - Tap the back arrow icon, to return to the **Set Rule and Condition** screen. This is an optional setting.
8. Any time during policy creation, tap **Cancel creation** to cancel the policy creation. This is an optional setting.
9. Tap **Create Policy**.

Schedules

Instant On allows you to enable or disable a network for users at a particular time of the day. You can now create a time range schedule specific to the employee or guest network, during which access to the Internet or network is restricted. This feature is particularly useful if you want the Wi-Fi network to be available to users only during a specific time, for example, only when your business is operational. The **Policies** > **Schedules** screen lists all the schedules that have been created to be included in the policies for the site.

Creating a Schedule

Follow these steps to create a new schedule:

1. Tap the Policies () tile on the Instant On mobile app home page.
2. Tap the advanced menu icon () and select **Schedules**.
3. In the **Schedules** screen, tap the () icon.
4. Under **Create Schedule** > **Identification**, enter a name for the schedule you are creating.
5. Under **Network Access Schedule**, select one of the following values for **Type**:
   a. **Fixed**–Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) equally to those of the employee or guest network schedule.
      - Select one of the following options under **Daily Operating Hours**:
        - **Active All day**: The network is active throughout the day for the selected days.
        - **Active between a Start and End Time**: The network is only active between the designated **Start Time** and **End Time**. Network access can be configured to end on the same day or the next day. When a time prior to the **Start Time** is selected as the **End Time**, a **Next Day** alert is displayed indicating that the end time is configured on the next day. This enables you to configure scheduled networks for your business when the active hours extend to the early hours of the next day.

   b. **Variable**–Indicates the schedule configuration that allows users to set up a different time range on a daily basis.
      - Follow these steps to enable the network schedule for specific days of the week:
        - After selecting **Variable**, click on the day of the week for which you need to configure a schedule.

- Select one of the following options under **<Day> Operating Hours**:
  - **Inactive All Day**: The network is inactive throughout the selected day.
  - **Active All day**: The network is active throughout the selected day.
  - **Active between a Start and End Time**: 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 **Done**.

Chapter 14
Profiles

The **Profiles** screen allows network administrators or operators to configure and manage **Port** profiles and **RADIUS** profiles within a site. This centralized interface simplifies profile management by ensuring that any changes made to a profile are automatically applied to all ports, networks, and devices using 802.1X authentication that are associated with the respective Port Profile or RADIUS profile.

This section outlines the necessary features and functionality of these profiles including profile creation, configuration, and management across various system components.

The profile screen consists of the following tabs:

- **Ports**—Port Profiles are reusable configuration that defines a set of settings applied to one or more network ports. They enable the administrators to standardize and simplify the deployment of common port configurations across multiple interfaces. You can create up to 32 port profile.
- **RADIUS**—A RADIUS profile is a predefined set of configuration parameters used to integrate a network device with a RADIUS server for authentication, authorization, and accounting (AAA) services. You can create up to 16 RADIUS profile per site. Each device supports only one RADIUS profile for port 802.1X authentication.

Viewing Port Profiles

The **Profiles** screen displays the list of profiles created for the site. To view the details of a profile, follow these steps:

1. Tap the **Profiles** ( ) on the Instant On mobile app home screen.

   The list of all configured port profiles are displayed.
2. Tap on any of the port profiles, to view the profile details screen.

Creating a Port Profile

The port profile screen displays the list of port profiles configured. It displays the name of the port profile and the count of ports the port profile is assigned.

The following procedure describes how to create a port profile:

1. Tap the **Profiles** ( ) on the Instant On mobile app home screen.

   The port profile screen is displayed.
2. Tap the () icon. The **Create Port Profile** screen is displayed.
3. Under **Identify the Profile**, configure the following:
   - **Name**—Enter a name for the port profile.
   - **Port Options**—The **Limit broadcast and Multicast Storms** configuration is an optional setting, and is enabled by default. Use the toggle button to enable or disable the **Limit broadcast and Multicast Storms** configuration. This configuration does not apply to the gateways.

4. Tap **Continue**.

   The **Port Security and Authentication** screen is displayed.

5. This is an optional setting. Under **Port Security and Authentication** > **Security**, select a security option.

   You can select multiple options for port security type. The different types of port securities options are:

   - **DHCP and ARP Protections (untrusted Port)**–Requires at least one wired network to be enabled with DHCP and ARP attack protections. Not applicable to gateways, access points, and 1830 series switches.
   - **Port Isolation (protected port)**– Not applicable to gateways, access points, and 1830 series switches.

6. Under **Port Security and Authentication** > **Spanning Tree Protection**, select a Spanning Tree Protection (STP) option.

   It is a security feature that disables a port if it receives Bridge Protocol Data Units (BPDUs), which are control packets used by (STP). You must select one option for the list of **Spanning Tree Protection** options. STP does not apply to gateways and access points.

   - **No spanning tree protections (default)**–The default spanning tree protection settings without the BPDU option.
   - **Filter spanning tree protocol (BPDU filter)**–Filters incoming and outgoing BPDUs on the port.
   - **Block spanning tree protocol (BPDU guard)**–Stops the incoming and outgoing BPDUs received on the port.
   - **Root bridge protection (Root guard)**–Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge.

7. Under **Port Security and Authentication** > **Authentication**, you must select the authentication type from the list of options displayed:

   - **No authentication (default)**–No authentication is applied. This is the default option selected.
   - **Port-based**–Enables port-based 802.1X authentication. Port-based authentication is not applicable to gateways, and 1830 series switches.
   - **Client-based**–Enables client-based 802.1X authentication. Client-based authentication does not apply to gateways, access points, and 1830 series switches.

     This is an optional setting. When **Client-based** is selected as the **802.1X Authentication** type, an additional **Authentication Options** section is displayed. You can select one of the following options:

     - **802.1X + MAC Authentication**–Enables a secondary attempt at MAC-based authentication if the initial 802.1X request times out. If 802.1X is explicitly refused by the server (for example, during an invalid credentials), MAC authentication is not attempted.
     - **Unauthenticated User Guest Access**–Enables a fallback to a wired guest network for clients that fail 802.1X authentication. This requires a wired Guest Network to be configured on the Instant On site. On enabling this option, the guest network is displayed as **Untagged guest network** under the **Network Assignment** > **Included Networks** section of the port configuration.

8. Tap **Continue**.

   The **Power Management** screen is displayed. The **Power Management** screen allows you to configure the Power over Ethernet (PoE) functionality and related power settings for ports that power other devices.

9. Under **Power Management** > **Power allocation**, select the PoE option.

   Power management options allow you to configure PoE supply to devices connected to the switch. The different power allocation options available are:

- **No Power over Ethernet**–The PoE supply to devices connected to the switch is disabled. Only on selecting **No Power over Ethernet**, other power management options are not displayed such as **Port Priority**, and **Power Management Options**.
- **Usage (default)**–The power allocated to the port is based on usage and is unrestricted. By default, usage is selected.
- **Class**–Allocates power based on the device's PoE standard.

Power allocation by usage does not apply to access points, which always use class.

10. Under **Power Management** > **Port priority**, assigns a priority level to the port profile.

    Determines PoE delivery order during budget constraints **Critical** > **High** > **Low**.

Port priority does not apply to access points.

11. Under the **Power Management** > **Power Mode**, select the power behavior applied to eligible ports during a reboot.

    The available options are:

    - **Always On**(default)–Maintains PoE on eligible ports throughout a reboot, unless input power is lost.
    - **Quick**–Restores PoE on eligible ports as soon as the hardware restarts, before the switch has fully started.
    - **Normal**–Applies power to the ports only after the configuration is restored.

Power Mode applies only to the Instant On 1840 and 1940 Switch Series.

12. This is an optional setting. Under **Power Management** > **Power Management Options**, use the toggle button to enable or disable power schedule.

    If enabled, the PoE supply to the port profile is determined by the power schedule. When the **Power Schedule** option is enabled, the **View Power Schedule** link is displayed. Click **View power schedule** option to view the power schedule applicable to this port profile.

13. Tap **Continue**.
14. Under **Network Assignment** screen, select the networks the port profile supports.
    - **Untagged network**–The traffic received and sent from the default network without using a VLAN tag. To custom map the port profile to an untagged VLAN, click the untagged network drop-down list and select a network. Only one untagged network can be assigned to a port profile.
    - **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
      - **All networks**–To select all the tagged networks. If **All networks** option is selected, then the list of tagged networks is not displayed.
      - **Select networks**–Allows you to manually select the tagged VLAN networks. When **Select networks** option is selected, the **Tagged Networks** list is displayed. To custom map the port profile to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time.
15. Tap **Continue**.

16. Under **Port Assignment**, tap on expand arrow (⌄) next to the device.

    The port associated with the device is displayed. Select the port to which you want to assign the port profile.

    You can assign the port profile to multiple devices and ports. The selected ports are highlighted and the port gets added to the **Selected Ports** list.

    - **Assign to All**–Apply the profile to all ports on the device.
    - **Remove All**–Remove the profile from all ports on the device.

17. Tap **Create port profile**.

    The new port profile is displayed in the port profile screen.

Port Profile Details

Tap on an exciting port profile to view the **Port Profile Details** screen.

The port profile screen displayed the following:

- **Name**–Displays the name assigned to the port profile by the administrator.
- **Reference**–Displays the count of physical ports currently using the port profile.
- **Security**–Displays the security configuration applied to the port profile.

  The different types of **Port Security** options are:

  - **DHCP and ARP protections (untrusted port)**–Requires at least one wired network to be enabled with DHCP and ARP attack protections. Not applicable to gateways, access points, and 1830 series switches.
  - **Port isolation (protected port)**– Not applicable to gateways, access points, and 1830 series switches.
- **Security** > **Spanning tree protections**–This section displays the Spanning Tree Protections (STP) configuration applied to the port profile. Not applicable to gateways and access points. You must select a one of the following options:
  - **No spanning tree protections (default)**–The default spanning tree protection settings without the BPDU option.
  - **Filter spanning tree protocol (BPDU filter)**–Filters incoming and outgoing BPDUs on the port.
  - **Block spanning tree protocol (BPDU guard)**–Stops the incoming and outgoing BPDUs received on the port.
  - **Root bridge protection (Root guard)**–Protects the designated root bridge by preventing unauthorized ports from becoming a root bridge.
- **Authentication**–Displays the 802.1X authentication method configured for the port profile.

  The different types of authentications are:

  - **No authentication**–Is the default option selected.
  - **Port-based**–Enables port-based 802.1X authentication. Port-based authentication is not applicable to gateways, and 1830 series switches.
  - **Client-based**–Enables client-based 802.1X authentication. Client-based authentication does not apply to gateways, access points, and 1830 series switches.

    This is an optional setting. When **Client-based** is selected as the **802.1X Authentication** type, an additional **Authentication Options** section is displayed. You can select one of the following options:

- **802.1X + MAC Authentication**–Enables a secondary attempt at MAC-based authentication if the initial 802.1X request times out. If 802.1X is explicitly refused by the server (for example, during an invalid credentials), MAC authentication is not attempted.
- **Unauthenticated User Guest Access**–Enables a fallback to a wired guest network for clients that fail 802.1X authentication. This requires a wired Guest Network to be configured on the Instant On site. On enabling this option, the guest network is displayed as **Untagged guest network** under the **Network Assignment** > **Included Networks** section of the port configuration.

- **Power Management**–Provides options to configure Power over Ethernet (PoE) supply for connected devices. Power management options are unavailable for ports that are part of an LACP group.
- **Power Management** > **Power allocation**–Select one of the following PoE supply policies for the port profile:
  - **No Power over Ethernet**–Disables PoE for devices connected to the port assigned with the port profile.
  - **Usage (default)**–Allocates power based on device usage with no restrictions.
  - **Class**–The power allocated to the port is based on the PoE standard of the device. The power class of devices is categorized as follows:

Table 39: *Power Class of Devices*

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

- **Power Management** > **Port priority**–Assigns a priority level to the port profile. When PoE budget is limited, power is allocated based on priority in the following order: **Critical** > **High** > **Low**.

When two ports belonging to the same priority request power, the port with the lower port number is given priority. Example: If port 2 and 5 is assigned Critical class and the switch has a power budget constraint, port 2 receives full power before port 5.

- **Power Mode**–Determines how the switch delivers Power over Ethernet (PoE) to connected devices during a reboot. Select one of the following options:
  - **Always On**(default)–PoE remains active on eligible ports throughout a reboot. Power is maintained from the moment the hardware restarts until the switch is fully operational and the ports complete initialization, unless input power is lost.
  - **Quick**–The hardware restores PoE to eligible ports as soon as it restarts, with no software dependency, so power is delivered as quickly as possible–before the switch has fully started.
  - **Normal**–The standard power behavior, in which power is applied to the ports only after the configuration is restored.

NOTE

Power Mode is applicable only to the Instant On1840 and 1940 Switch Series

- **Power Management** > **Power management options**–This is an optional setting. Toggle the **Power schedule** option to enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule. When the **Power Schedule** option is enabled, the **View Power Schedule** link is displayed. Tap the **View power schedule** option to view the power schedule applicable to the port profile.
- On expanding the **More options** displays the following port profile configurations:
  - **Limit Broadcast and Multicast Storms**
  - **Network Assignment**
  - **Port Assignment**
- Tap on **Network assignment** to view the **Network Assignment** screen.

  Select the networks that the port profile supports.
  - **Untagged network**–The traffic received and sent from the default network without using a VLAN tag. To custom map the port profile to an untagged VLAN, tap on the untagged network drop-down list and select a network. Only one untagged network can be assigned to a port profile at a time.
  - **Tagged networks assignment**–The port receives and sends traffic from the default network using the management VLAN tag. Select one of the options:
    - **All networks**–To select all the tagged networks. If **All networks** option is selected, then the list of tagged networks is not displayed.
    - **Select networks**–Allows you to manually select the tagged VLAN networks. When **Select networks** option is selected, the **Tagged Networks** list is displayed. To custom map the port to a tagged VLAN, select the check boxes against the networks listed under **Tagged Networks**. A maximum of 22 tagged networks can be mapped to a port at a time.
- Tap the back arrow ← icon to return to the **Port Profile Details** screen.
- Tap on **Port Assignment** to view the **Port Assignment** screen.

  The port profile can be assigned to multiple devices and ports. Tap on the down arrow (⌄) next to the device to view the device's port image. On selecting the port, the port number gets added to the **Selected Ports** list.
  - **Assign to All**– Apply the profile to all ports on the device.
  - **Remove All**– Remove the profile from all ports on the device.
- Tap the advanced menu () icon in the title bar of the **Port Profile Details** screen.
  - **Delete port profile**–Allows you to permanently delete the port profile. In the **Confirm Profile Deletion** pop-up, tap **Delete Profile**.
  - **Duplicate port profile**–Allows you to create a duplicate port profile from the existing port profile using the same configuration. You must assign the port profile name for the duplicate port profile.

After changing any configuration for of the port profile, tap **Done** to save the changes, or tap the Cancel (**X**) icon to discard changes.

RADIUS Profile Page

The **RADIUS** profile screen lists all the configured RADIUS profilesand displays the following information:

Hover the cursor over a policy, click the ••• button, and select one of the following options:

- NAME–Displays the name assigned to the RADIUS profile by the administrator.
- Primary Server–Displays the primary server IP address configured for the RADIUS profile.

Viewing RADIUS Profiles

The **Profiles** page displays the list of profiles created for the site. To view the details of a profile, follow these steps:

1. Tap the **Profiles** ( ) on the Instant On mobile app home page.
2. The list of all port profiles created by the administrator.
3. Tap on the **RADIUS** tab to view the list of RADIUS profiles created by the administrator.
4. Tap on any of the profile (ports profile or RADIUS profile), to view the profile details screen.

Creating a RADIUS Profile

To create a RADIUS Profile, complete the following steps:

1. Tap the **Profiles** ( ) on the Instant On mobile app home screen.

   The port profile screen is displayed.
2. Tap on the **RADIUS** tab on the **Profiles** screen.
3. Tap the () icon.

   The **Create RADIUS Profile** screen is displayed.
4. Under the **Identify the Profile** section, assign a name to the RADIUS profile.
5. Tap **Continue**.

   The **Set Authentication Servers** screen is displayed.
6. This is an optional setting. Under **Security** > **RADIUS Security** section, use the toggle button to enable or disable the **Require RADIUS Message-Authenticator** option.
7. This is an optional setting. Under **Authentication Servers** section, configure the RADIUS authentication servers. Use the toggle button to select or deselect the RADIUS authentication server configuration.

   You can select multiple options. The available options are:
   - **RADIUS Accounting**–Tracks and logs user activity on a network. When enabled, it collects accounting data is collected from network devices and sent to the RADIUS server. On enabling RADIUS Accounting feature, you must configure the **Accounting Port**.
   - **Secondary RADIUS Server**–A backup authentication server used if the primary is unavailable.
8. Under the **Primary RADIUS Server** section, configure the following:
   - **Server IP Address or Domain Name**–The IP address or fully qualified domain name (FQDN) of the primary RADIUS server.
   - **Shared Secret**–Password or key used to encrypt and authenticate communication between the RADIUS client and the primary RADIUS server.
   - **Authentication Port**–Port number used by the primary RADIUS server for authentication requests. The port range is between 1-65535.
   - **Accounting Port**–Port number used by the primary RADIUS server for accounting request. The **Accounting Port** parameter is displayed only if **RADIUS Accounting** is selected under **Authentication Servers** settings. The port range is between 1-65535.

9. Under the **Secondary RADIUS Server** section, configure the following:
   - **Server IP Address or Domain Name**–The IP address or fully qualified domain name (FQDN) of the secondary RADIUS server.
   - **Shared Secret**–Password or key used to encrypt and authenticate communication between the RADIUS client and the secondary RADIUS server.
   - **Authentication Port**–Port number used by the secondary RADIUS server for authentication requests. The port range is between 1-65535.
   - **Accounting Port**–Port number used by the secondary RADIUS server for accounting request. The **Accounting Port** parameter is displayed only if **RADIUS Accounting** is selected under **Authentication Servers** settings. The port range is between 1-65535.

The **Secondary RADIUS Server** section is displayed only when you enable **Secondary RADIUS Server** option listed under the **Authentication Servers** section.

10. Under the **Server Failure Detection** section, configure the following:
    - **Server Timeout**–The maximum amount of time (in seconds) the RADIUS client waits for a response from the RADIUS server after sending a request. The range is between 1-30 seconds.
    - **Retry Count**–The number of times the RADIUS client resend a request to the same authentication server before considering it unreachable. The range is between 1-3 attempts.
11. Tap **Continue**.

    The **Set Network Access Attributes** screen is displayed.
12. Under the **NAS Identifier Assignment** section, configure how the NAS is identified in RADIUS communications. The two options available are:
    - **Use Device IP Address (default)**–The NAS is identified by its IP address.
    - **Use Specific NAS Identifier**–The NAS is identified by a custom NAS identifier.

    On selecting **Use Specific NAS Identifier**, you must specify the **NAS Identifier**.
13. Under the **Network Access Attributes** > **NAS IP Address Assignment** section, configure the NAS IP address used for RADIUS communication. The following options are available:
    - **Use Device IP Address (default)**–The NAS uses its device IP address.
    - **Use a Single IP Address**–The NAS uses a single, specified IP address.

    On selecting **Use a Single IP Address**, you must specify the **NAS IP Address**.
14. Tap **Create RADIUS Profile**.

    The new RADIUS profile is displayed in the RADIUS Profile screen.

RADIUS Profile Details

The RADIUS profile details screen displays the following information:

- **NAME**– Displays the name assigned to the RADIUS profile by the administrator.
- **Security** (Optional)–Under **RADIUS Security**, displays the authentication mode used in RADIUS packets. Currently RADIUS profile supports **Require RADIUS Message-Authenticator**. The authentication is done using the message-authenticator attribute in RADIUS packets.
- **Authentication Servers** (Optional) –Under **RADIUS Options**, displays information about authentication server configuration and allows you to configure the connectivity and security settings for RADIUS authentication servers. You can select multiple options for the authentication server. Available authentication server types are:

- **RADIUS Accounting**—Tracks and logs user activity on a network. When enabled, it collects accounting data is collected from network devices and sent to the RADIUS server. On enabling RADIUS Accounting feature, you must configure the **Accounting Port**.
- **Secondary RADIUS Server**—A backup authentication server used if the primary is unavailable.

- **Primary RADIUS Server**—Is the main authentication server that a network device (RADIUS client) interacts with for Authentication, Authorization, and Accounting (AAA) services. The Primary RADIUS server configurations include:
  - **Server IP Address or Domain Name**—The IP address or fully qualified domain name (FQDN) of the RADIUS server.
  - **Shared Secret**—Password or key used to encrypt and authenticate communication between the RADIUS client and the RADIUS server.
  - **Authentication Port**—Port number used by the RADIUS server for authentication requests. The port range is between 1-65535.
  - **Accounting Port**—Port number used by the RADIUS server for accounting requests. The Accounting Port parameter is displayed only if RADIUS Accounting is selected under Authentication Servers settings. The port range is between 1-65535.
- **Secondary RADIUS Server**—Is a backup authentication server a network device (RADIUS client) interacts with for Authentication, Authorization, and Accounting (AAA) services when the main authentication server is not reachable.

The **Secondary RADIUS Server** configurations are displayed only if **Secondary RADIUS Server** is select under **Authentication Servers.**

The secondary RADIUS server configurations include:

- **Server IP Address or Domain Name**—The IP address or fully qualified domain name (FQDN) of the secondary RADIUS server.
- **Shared Secret**—Password or key used to encrypt and authenticate communication between the RADIUS client and the secondary RADIUS server.
- **Authentication Port**—Port number used by the secondary RADIUS server for authentication requests. The port range is between 1-65535.
- **Accounting Port**—Port number used by the secondary RADIUS server for accounting requests. The Accounting Port parameter is displayed only if RADIUS Accounting is selected under Authentication Servers settings. The port range is between 1-65535.

- **Server Failure Detection**—Is used to monitor the RADIUS server's responsiveness for Authentication, Authorization, and Accounting (AAA) services. The configuration includes:
  - **Server Timeout**—The maximum amount of time (in seconds) the RADIUS client waits for a response from the RADIUS server after sending a request. The range is between 1-30 seconds.
  - **Retry Count**—The number of times the RADIUS client resend a request to the same authentication server before considering it unreachable. The range is between 1-3 attempts.
- **Network Access Attributes**—Configure the access rights, restrictions, and connection. These attributes include:
  - **NAS Identifier Assignment**—Determines how the RADIUS servers identify the NAS in RADIUS communications. The two options available under NAS Identifier Assignment are **Use Device IP Address** (default), and **Use Specific NAS Identifier**.

    On selecting **Use Specific NAS Identifier**, you must specify the **NAS Identifier**.

- **NAS IP Address Assignment**–Determines the IP address associated with the NAS, which the RADIUS server uses for communication. The two options available under NAS IP Address Assignment are Use Device IP Address (default), and Use a Single IP Address.

  On selecting **Use a Single IP Address**, you must specify the **NAS IP Address**.

- On expanding the **More options** displays the following RADIUS profile configurations:
  - **Network Assignment**
  - **Port Assignment**
- Tap on **Network Assignment**, to view the network assignment configuration for the RADIUS profile.
  - **Network using the RADIUS Profile**–The drop-down list allows you to select a network referencing the RADIUS profile.
  - **Identification**–The Identification section includes:
    - **Name**–Displays the network name that is selected from the list of networks referencing this RADIUS profile. Tap over the network name, displays the network details page. For more information, see Configuring Networks.
    - **Health**– Displays the current network health status, such as Good, Fair, and Poor.
    - **State**–Displays if the network is Active or Inactive.
    - **Network Usage**–Displays the user type for which the network is configured.
  - **Security**–The security section displays information regarding the network security configuration.
  - **Authentication**–The Authentication section displays the RADIUS profile configured for the network. Tap on the RADIUS profile name, displays the RADIUS profile detail screen.
- Tap the back arrow icon to return to the **RADIUS Profile Details** screen.
- Tap the advanced menu () icon in the title bar of the **RADIUS Profile Details** screen, and tap **Delete profile**.

  Allows you to permanently delete the RADIUS profile. In the **Delete Profile** pop-up, tap **Delete Profile**.

After changing any configuration for of the RADIUS profile, tap **Done** to save the changes, or tap the Cancel (**X**) icon to discard changes.

Chapter 15
Security

The **Security** page serves as a centralized location for configuring and monitoring threat-related security and Internet firewall settings. This page is visible only when a secure gateway is deployed at a site.

The Instant On secure gateway provides an Intrusion Detection and Prevention System (IDPS) for real-time threat detection and protection. IDPS continuously analyzes network traffic to identify suspicious activities or potential attacks. It helps protect the network from cyber threats, including malware communication and intrusion attempts.

Threat detection and prevention is enabled by default. Threats with a critical severity level are reported in the **Threats** table and blocked. The threats with other severity levels are reported in the **Threats** table but are not blocked. You have the option to add an exception to the threat to revert the default action taken.

The **Security** page provides visibility and control over the following threat-related functions:

- Threats
- Threat Exceptions
- Threat Management
- Internet firewall

The **Security** page is displayed only on sites containing security gateways. It is accessible only to users with administrative privileges.

Viewing the Detected Threats

The **Security** > **Threats** screen displays the list of threats detected on the site.

To view the detected threats, complete the following steps:

1. Tap the **Security** () tile on the Instant On mobile app home page. The list of threats detected on the site is displayed.
2. Under the **Threats** () tab, tap on any of the threats in the list, to view its details. The **Threat Details** screen is displayed with the following information:

Table 40: *Threats Details*

Field	Description
Name	Name of the threat.
Severity	Denotes the severity of the generated threat. The severity of threats is determined based on the severity level corresponding to the threat. The severity levels are categorized as follows: ■ Critical–Refers to vulnerabilities that can cause significant disruptions, system failure, or data loss. ■ Major–Refers to high-risk threats that could impact the system or data.

Field	Description
	■ Minor–Refers to low-risk threats that usually do not require immediate action. ■ Info–The alert is for reference only and has little to no impact on the system. ■ Unknown–The system could not determine the threat's severity.
State	Denotes the current state of the threat whether it is blocked or allowed.
Occurred	Indicates when the threat was detected in the time zone of the site.
Category	Denotes the type or classification of the threat.
Source	Denotes the source host or origin of the threat.
Protocol	Denotes the application-layer protocol associated with the detected threat.
Destination	Denotes the destination host of the threat.

Threat Actions

You can allow or block exception to a threat to override the default action taken by threat management.

To add an allow or block exception, follow these steps:

1. Tap the **Security** () tile on the Instant On mobile app home page.
2. Under the **Threats** () tab, swipe from right to left over the threat to perform one of the following actions:
   - **Add Block Exception**–Adds a block exception to the threat.
   - **Add Allow Exception**–Adds an allow exception to the threat.

   Alternatively, you can tap on the threat, and in the **Threat Details** screen, tap the advanced menu () icon and tap **Add block exception** or **Add allow exception** to add a block or allow exception.

Threat Exceptions

The **Threat Exceptions** tab lists all the exception made to a threat to override the default action taken by the threat management.

To view the threat exceptions details, follow these steps:

1. Tap the **Security** ()tile on the Instant On mobile app home page.
2. Under the **Threat Exceptions** () tab, tap on the threat to view the exception details.

Table 41: *Threat Exception Details*

Field	Description
Threat	Name of the Threat identifier.
Category	Denotes the type or classification of the threat.
Severity	Denotes the severity of the generated threat. The severity of threats is determined based on the severity level corresponding to the threat. The severity levels are categorized as follows: ■ Critical–Refers to vulnerabilities that can cause significant disruptions, system failure,

Field	Description
	or data loss. ■ Major—Refers to high-risk threats that could impact the system or data. ■ Minor—Refers to low-risk threats that usually do not require immediate action. ■ Info—The alert is for reference only and has little to no impact on the system. ■ Unknown—The system could not determine the threat's severity.
Action	Indicates the current state of the threat, which can either be Blocked or Allowed.
Added	Indicates when the threat was added to the exceptions, in the time zone of the site.

Removing Threat Exceptions

To remove the threat from the exceptions list, follow these steps:

1. Tap the **Security** ()tile on the Instant On mobile app home page.
2. Under the **Threat Exceptions** () tab, swipe from right to left over the threat and tap the delete icon to remove the exception.

Alternatively, you can tap on the threat from the **Threat Exceptions** screen, and in the **Threat Exception Details** screen, tap the advanced menu () icon, and then tap **Remove exception** to remove the exception.

Threat Management

The **Threat Management** page allows you to enable or disable the threat detection and prevention. This setting is enabled by default. Threats with a critical severity level are reported in the **Threats** table and blocked. The threats with other severity levels are reported in the **Threats** table but are not blocked.

To enable or disable the threat management function, follow these steps:

1. Tap the **Security** ()tile on the Instant On mobile app home page.
2. In the **Threats** screen, tap the advanced menu () icon and tap **Threat Management**.
3. Under **Threat Management**, select one of the following options:
   - **Threat Detection and Prevention (default)**—Activates the threat management function. This option is enabled by default. When enabled, all incoming and outgoing traffic routed by gateway is inspected by Intrusion Detection and Prevention System (IDPS).
   - **No Threat Management**—Disables threat detection. When this option is selected, the **Threats** and **Threat Exceptions** pages will not be displayed.

Internet Firewall

The **Firewall** tab allows you to define rules for incoming traffic from the Internet and outgoing traffic from within the site.

By default, all incoming traffic is blocked and all outgoing traffic is allowed.

The following policies can be configured to manage the firewall:

- Application Access—Allows or blocks applications that can be used on the network.
- Client Access—Controls destinations that can be reached by clients on the network.

- Network Access—Controls destinations that can be reached from this network.
- Remote Access—Allows or blocks port forwarding during specific times.

To navigate to the **Internet Firewall** screen, follow these steps:

1. Tap the **Security** () tile on the Instant On mobile app home page.
2. In the **Threats** screen, tap the Internet Firewall () icon.
3. To configure one or more policies for the firewall, click the **View policies**. You will be redirected to the Policies page.
4. To view the configured firewall policies, click the policy name or number of policies (in the case of two or more policies) hyperlink below **Controlled by**. You will be redirected to the Policies page. The **Policies** page is filtered to only show the firewall policies.

For more information on creating policies, see Policies.

Application Layer gateway (ALG)

The Application Layer Gateway (ALG) section lets you control which protocol helpers the secure gateway uses to inspect and rewrite protocol-specific traffic so it can traverse NAT. ALG helpers are enabled by default and benefit most networks. In some deployments a helper can interfere with applications that perform their own NAT traversal—for example, a VoIP provider using STUN/TURN/ICE—so you can disable individual protocols for troubleshooting.This section is available only on sites with a secure gateway and applies to every LAN network on the site.

Under Protocols, select or clear the checkbox for each protocol to enable or disable its ALG helper. All protocols are enabled by default.

The following policies can be configured to manage the firewall:

- **Session Initiation Protocol (SIP)**—Manages voice and video signaling. Disabling may lead to silent calls or dropped connections.
- **H.323**—Handles legacy video conferencing traffic. Disabling may lead to failed calls or one-way audio.
- **Real-Time Streaming Protocol (RTSP)**—Controls media streams for cameras and players. Disabling may lead to frozen video or broken playback.
- **File Transfer Protocol (FTP)**—Coordinates data exchange between clients and servers. Disabling may lead to timed-out transfers or hidden file lists.
- **Trivial File Transfer Protocol (TFTP)**—Supports simple file transfers for device booting and configuration updates. Disabling may lead to firmware update or PXE boot failures.

Changes are applied to the secure gateway without rebooting the device. Because existing sessions continue under their previous behavior, HPE recommends restarting the firewall (see **Restart Firewall**) so the change also takes effect on active session.

Restart Firewall

Whenever a new policy is created, it applies only to new sessions. Existing sessions continue without any changes. To make sure all connections follow the latest policy, you can restart the firewall. Restarting the firewall will terminate all active sessions and ensure that all new sessions operate according to the policy applied to the secure gateway.

This action may temporarily affect network services and client connections.

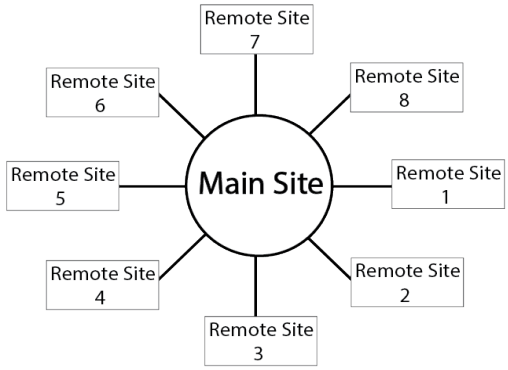
To restart the firewall, follow these steps:

1. Tap the **Security** ()tile on the Instant On mobile app home page.
2. In the **Security** screen, tap the advanced menu () icon and tap **Restart Firewall**. A popup appears on the screen requiring confirmation.
3. Tap **Restart Firewall** in the confirmation pop-up.
4. Under **Threat Management**, select one of the following options:

Chapter 16
Domains

A domain represents a site-to-site VPN connection. The VPN connection must use the IPsec protocol to establish a secure, encrypted tunnel over the internet. It is mandatory to use port 4500 (for IPSEC NAT-Traversal mode) and UDP protocol.

A site can be connected to a domain only if a gateway is assigned to it. To create a domain, at least two sites are required and each must contain a gateway. A domain supports up to eight remote sites connected to a single main site. In this configuration, all remote sites are connected directly to the main site in a star topology. Each remote site maintains a point-to-point connection with the main site, and there are no direct connections between remote sites. The remote site can also be referred to as the Connected Site.



NOTE

Once a domain is created, the main site cannot be converted to a remote site or vice versa. To make such changes, you must delete the existing domain and create a new one.

The **Domains** tab in the **Site Management** view displays the list of domains configured.

The details of the domains in the **Domains** page are listed under the following categories:

Category	Description
Domain (number of connected sites)	Displays the domain name and the total number of connected sites. The site count includes the main site and all additional connected sites.
Alerts	Next to the **Alerts** ( ) icon the count of major ,minor and informational alerts are displayed.
Health Score	Displays the health percentage of the domain. The health score is calculated based on the operational status of VPN connections and the presence of valid communication-enabling policies. ■ Good–Indicates that the health score of the sites in the domain is between 67% - 100%. ■ Fair–Indicates the health score of the sites in the domain is between 34% - 66%. ■ Poor–Indicates the health score of the sites in the domain is between 0% - 33%.

Creating a Domain

To create a domain, there must be a minimum of two sites available, and each site must have at least one gateway device.

Follow these steps to create a new Instant On domain:

1. Login to your Instant On account using your administrator credentials.

   The **Site Management** screen is displayed.
2. Choose one of the following options:
   - If the setup has an existing domain, complete the following steps:
     a. Tap on **Domains**.
     b. Tap the advanced menu () icon and select **Create domain**.
   - If there are no existing domains created in the setup, then tap the advanced menu () icon and select **Create domain**.

   The **Identify the Domain** page is displayed.
3. In **Identify the Domain** page, enter a name for the domain.

   The name of the domain must not exceed 64 characters.
4. Select a main site to which other sites will connect.

   The list displays only the sites that contain at least one gateway mapped to them. You can select only one site as the main site.
5. Tap **Continue.**
6. In the **Select Sites to Connect** page, select a site that will connect to the main site.

Only one remote site can be configured at a time to connect to the main site. This limitation applies when creating a domain or when adding sites using the **Site Connections** tab. You can connect up to eight remote sites to a main site. The system enforces this limit by disabling the selection of more sites once the maximum is reached.

7. Tap **Continue.**
8. In the **Specify Network Access** screen, expand the network list and select the wired networks to allow access between the **Connected site** and the **Main site** networks.

VLANs with the same IP subnet cannot be selected as the wired network to create the connection between the remote site and the main site.

9. Tap **Create Domain**.

Viewing the Domain Dashboard

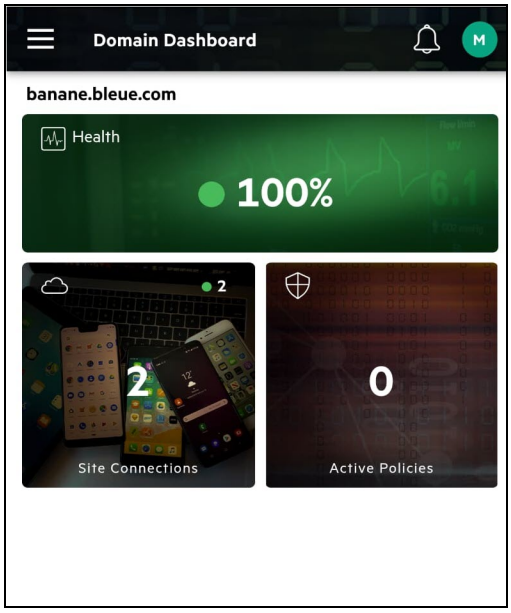
To view the Domain Dashboard screen, complete following the steps:

1. Login to your Instant On account using your administrator credentials. The sites **Overview** screen is displayed.
2. Tap on **Domains**.

   The list of domains configured are displayed.
3. Tap on the domain name.

   The **Domain Dashboard** screen is displayed.

Figure 10 *Domain Dashboard*



The domain details page comprises of the following components:

Content	Description
Advanced menu icon ()	Displays the domain name and provides menu options to administer your domain.
	Domain Management–The **Domain Management** page displays the domain name. To delete a domain from the **Domain Management** screen, tap the () icon and select **Delete domain**.
	Sites–Navigates to the **Managed Sites** screen. The **Manages Sites** screen displays the list of sites.
	Domains–Navigated to the **Domains** page. The **Domains** page displays the list of domains.
Alert Notification ( )	Displays the alerts that are triggered by the system when an unusual activity is observed on the domain.
Health	Displays the overall health status of the domain. The health card includes a visual indicator with the value as a percentage and a count of active alerts. The health score is calculated based on the operational status of VPN connections and the presence of valid communication-enabling policies.
Site Connection	The **Site Connection** card displays the total number of independent sites connected to the domain (including the main site and connected sites) and health for all the connected sites. On tapping on the **Site Connection** card displays the following information: ▪ **Overview** page–Displays the list of connected sites. Tap on any site in the list to view the site connection details. In the Overview page you can connect additional remote sites to the main site. To connect a remote site to the main site complete the following procedure: 1. Tap on the **Add** icon.

Content	Description
	2. In the **Select Sites to Connect** page, select site(s) to connect to the main site. You can select up to eight sites to connect to the main site. 3. Tap **Continue**. 4. In the **Specify Network Access** screen, expand the network list and select the wired networks to allow access between the **Connected site** and the **Main site** networks. 5. Tap **Add Site**. ▪ **Main site** page–Displays site connection information for the main site.
Policies	Displays the number of active and total policies configured for the domain. The **Policies** screen provides a unified space for administrators to define and manage rules for a domain. Domain policies support network access policies by enabling the wired network at a remote site to connect with the wired network at the main site. Each remote site connected to the main site creates an individual domain policy. By default, the name of the remote site is assigned as the domain policy name. The domain policies are created automatically based on the configuration selected while creating a domain or when a new site is added to the domain using the **Site Connections**. The domain policy details screen allows the administrators to view the policy details and manage or update the **Network Access** policy. To view the domain policy details screen tap on the policy name. The domain policy screen displays the following information: ▪ **Identification** section displays the basic details of the selected domain policy, which includes the following: ◦ **Name**–Displays the name of the domain policy. By default, the remote site name is assigned as the domain policy name. Tap on the **Name** text and update the name for the domain policy. ◦ **State**–Refers to the current operational condition of a policy ◦ **Type**–Only Network Access is supported as the connection type. ▪ **Rule**–The rule section displays the **Action** status of the selected domain policy. By default, the **Action** is set to **Allow**, and the value is non-editable. ▪ **LAN network types** section displays the policy rule applies to which network categories–**Wireless**, **Wired**, and **VPN**, which includes the following: ◦ **Wireless**–When **Wireless networks** is **ON**, choose either **All networks** or **Selected networks** (only one at a time), **Selected networks** displays a list of configured wireless networks. ◦ **Wired**–When **Wired networks** is **ON**, choose either **All networks** or **Selected networks** (only one at a time), **Selected networks** displays a list of configured wired networks. ◦ **VPN**–When **VPN networks** is **ON**, the **VPN Network** name is displayed below the **VPN networks** label. ▪ **Connected Site**–Expand the accordion to view all the **Wired Networks** available in the remote site. To enable a wired connection to connect to the main site, selecting the checkbox adjacent to the specific wired network. ▪ **Main Site**–Expand the accordion to view all the **Wired Networks** available in the main site. To enable a wired connection to connect to the remote site, selecting the checkbox adjacent to the specific wired network. After updating the domain policy, tab on the following options:

Content	Description
	■ **Done**—To save the configuration. ■ Cancel **X** icon—To cancel the updates done to the domain policy.

Chapter 17
Analyzing Application Usage

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

The Instant On solution classifies the traffic into a large number of categories, to reduce the complexity of the feature in the 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 42: *Application Categories and their Classification*

Application Category	Icon	Instant On Classification
Adult Content–Adult content applications include websites with graphic adult content or illegal subjects.		▪ Abortion ▪ Abused Drugs ▪ Adult and Pornography ▪ Death and Gore ▪ Gambling ▪ Gross ▪ Illegal ▪ Marijuana ▪ Nudity ▪ Porn ▪ Violence
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.		▪ Business and Economy ▪ Financial Institutions ▪ Financial Services ▪ Real Estate ▪ Stock Advice ▪ Tools ▪ Stock Market
Education–Sites about education information like schools, college, universities, and online training tools like Linda.com, LinkedIn learning, etc.		▪ University ▪ Education ▪ Schools ▪ Colleges ▪ Online Learning ▪ Online Training ▪ Training Tools
Explicit Content–Restricted content applications include websites with sensitive information or graphic content.		▪ Alcohol and Tobacco ▪ Cult and Occult ▪ Cheating ▪ Hate ▪ Questionable Racism

Application Category	Icon	Instant On Classification
		▪ Sex Education ▪ Swimsuits and Intimate Apparel ▪ Violence ▪ Weapons
Gaming–Sites containing information about gaming, mostly referred as video games. Video games that are played partially or exclusively through the internet.		▪ Online Gaming
Government & Politics–Military and government applications include websites on military and government information and services.		▪ Philosophy and Political Advisory ▪ Military ▪ Public Services
Instant Messaging & Email–Websites and applications where users can send and receive messages and emails.		▪ Email ▪ Instant Messaging ▪ Mail ▪ SMTP (Simple Mail Transfer Protocols) ▪ Telephony ▪ Web Conferencing Software ▪ Webmail
Kids and Family–Sites aimed for kids and families with learning, educational and interactive content.		▪ Educations ▪ Kids ▪ Learning
Lifestyle–Sites that cover beauty and fashion trends, dining, entertainment and arts, maps and navigation, religion, society and travel.		▪ Beauty ▪ Dating ▪ Dining ▪ Entertainment and Arts ▪ Fashion ▪ Forum ▪ GPS ▪ Maps ▪ Motor Vehicles ▪ Navigation ▪ Online Greeting Cards ▪ Personal Blogs ▪ Religion ▪ Society ▪ Transportation ▪ Travel ▪ Local Information
Malicious and Risk–High security risk applications include websites that contain known malicious Internet tools that can harm devices and damage the internal network.		▪ Bot Nets ▪ Frauds ▪ Hacking ▪ High Risk Sites ▪ Keyloggers and Monitoring

Application Category	Icon	Instant On Classification
		■ Malware Sites ■ Moderate Risk Sites ■ Phishing ■ Proxy Avoidance and Anonymizers ■ SPAM URLs ■ Spyware and Adware
News & Media–Sites containing local and world news, breaking news, online newspapers, crowdsourced news, general information, and weather.		■ News ■ Weather ■ Reddit ■ Buzzfeed
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.		■ Antivirus ■ Application Service ■ Automation Protocol ■ Collaborative Software ■ Enterprise Apps ■ ERP ■ Local Network ■ Mobile App Store ■ Printer ■ Productivity Software ■ Reference and Research ■ Search Engine ■ Translation ■ Web Conferencing Software ■ Web Search
Shopping–Shopping applications include websites for online shopping.		■ Auctions ■ Shopping ■ Buy and Sell ■ Pay to Surf
Social Network–Social applications include websites for social networking and media.		■ Social Networking ■ Dating ■ Personal sites and Blogs ■ News and Media
Sports and recreation–Recreational applications include websites on personal activities and interests.		■ Travel ■ Home and Garden ■ Entertainment and Arts ■ Local Information ■ Hunting and Fishing ■ Society ■ Sports ■ Music ■ Fashion and Beauty ■ Recreation and Hobbies ■ Motor Vehicles

Application Category	Icon	Instant On Classification
		■ Kids ■ Online Greeting cards ■ Religion
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.		■ Audio/Video ■ Media ■ Movies ■ Music ■ Videos
Uncategorized–This category contains network protocols that could not be categorized but may be useful to run your network. Therefore, it cannot be blocked. It also includes sites that are uncategorized or no longer exist.		■ Dead Sites ■ Parked Domains **NOTE:** The data in these categories is negligible, they will be ignored in the data transferred calculation and nothing will be displayed about them in Instant On.
Utilities–Sites about tools and services that ease internet usage and navigation, such as search engines, cloud storage, and file transfer.		■ Authentication ■ Behavioral ■ Cloud Storage ■ Compression ■ Content Delivery Network ■ Database ■ Document and Media Sharing ■ Downloading Files ■ Encrypted ■ File Hosting ■ File Hosting Service ■ File Server ■ Host and Share Files ■ Internet Portals ■ Network Management ■ Network Protocols ■ Network Service ■ Peer to Peer ■ Routing ■ Shareware and Freeware ■ Standard ■ Terminal ■ Thin Client ■ Upload and Share Files ■ Wap ■ Web Hosting ■ Analytics
Web–Sites and tools containing computer and internet information and security, internet software, proxies and tunnels, routing protocols, web advertisements, etc.		■ Computer and Internet Information ■ Computer and Internet Security ■ Internet Protocols (IPv4, IPv6, DHCP, ■ Ethernet)

Application Category	Icon	Instant On Classification
		■ Internet Service Provider ■ Internet Software ■ Parked Domains ■ Proxies and Tunnels ■ Tunneling ■ Routing Protocol ■ Security Service ■ TELNET (remote login process) ■ Web Advertisements
Wired—This category is essential for basic network and Internet connectivity. It is always allowed for all networks and cannot be blocked. **NOTE:** The wired application category will not be available for sites with a gateway.		■ Wired networks

Viewing Application Information

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

To navigate to the Application screen, tap the Applications () tile on the Instant On home screen.

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**.

Table 43: *Application Information*

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

Applications Visibility and Control

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

1. To navigate to the **Visibility and Control** page, tap the Applications () tile on the Instant On home screen. Tap the advanced menu () icon in the **Applications** page and select **Visibility and control**. The **Visibility and Control** page is displayed.
2. Select one of the available options:
   - **Application details (default)**—Provides a detailed view of date usage by different applications and websites accessed by clients in the network. Applications chart and Applications list are displayed

only when this option is selected. This option is enabled by default.

- **Application activity summary**—Provides only an overview of uploaded and downloaded data of all the networks for the last 24 hours in the Applications page. Choose this option for better network performance. Selecting this option hides the Applications tab in the mobile app.

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

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

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.

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:

- Policies that control the selected category
- Amount of data transferred in the last 24 hours
- Websites and apps most visited
- Traffic usage per client
- Network access

Viewing 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.

Due to the complexity of application fingerprinting, such as obfuscation or encryption of traffic, dynamic application behavior, and secure DNS masking of domain names, the accuracy of application classification and filtering is not guaranteed.

Viewing Applications

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

1. Tap the Applications () tile on the Instant On home screen.
2. Select an application category from the Applications list to view the details of the application.

   The following data is displayed for each category:
   a. Policies that control the selected category
   b. Amount of data transferred in the last 24 hours
   c. Websites and apps most visited
   d. Traffic usage per client
   e. Network access

Blocking Application Access

The 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.