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
- Setting Up Your Wireless Network 18
- Setting Up Your Wired Network 19
- Setting Up Your Network Using Gateway 20
- LED Status 21
- Accessing Instant On Application 23
- AP Operating Modes 25
- Local Management for Switches 27
- Setting Up Your Instant On Secure Gateway 29
- IP Assignment for Access Points 32
- Discovering Available Devices 34
- Managing Sites Remotely 37
- Application Error Messages 38

Instant On User Interface 39
- Site Management 41

Monitoring Site Health 48
- Alerts 49
- Events 52

Devices 54

Adding a Device 55
Topology 55
Extending your Network - APs 57
Extending Your Network - Gateway 60
Radio Management 60
Loop Protection 62
Power Management 63
Gateway Details 64
Access Point Details 73
Router Details 84
Switch Details 93
Cloud-Managed Stacking 114
Auto-Detection and Auto-Configuring of Switch Ports 132
Wi-Fi 6E Standard 132

Networks 134
135
Creating a Network 135
Configuring a Wired Network 135
Configuring a Wireless Network 137
Configuring a VPN Network 139
Modifying an Employee Network 140
Modifying a Guest Network 147
Modifying a Wired Network 157
Modifying a VPN Network 163
WAN 167
Latency 168
Packet Loss 169

Applications 175
Applications Overview 175
Application Category Details 179
Application Visibility and Control Settings 180
Application Usage Summary 180

Managing Clients 181
Viewing Clients List 181
Blocked Clients 184
Watchlisted Clients 184
Viewing Wireless Client Details 185
Viewing Wired Client Details 188
Viewing VPN Client Details 192
Classification Tags 193

Security 194
Threats 194
Threat Actions 195
Threat Exceptions 195
Threat Management 196
Firewall 196

Managing Your Account 198
Identification 198
Changing Account Password 198
Two-Step Verification 198
Changing the Recovery Email Address 199
Preferences 199

Communications 200
Delete Account 200
Notifications 201

Policies 203
Policy Support by Site Topology 203
Policy Deployment 204
Overview 204
Deleting a Policy 205
AI-Assisted Policy Creation 206
Manual Policy Creation 207
Updating a Policy 209
Schedules 212

Profiles 215
Ports Profile Page 215
Duplicating a Port Profile 216
Creating a Port Profile 217
Port Profile Details 219
RADIUS Profile Page 222

Domains 228
Creating a Domain 229
Overview 230
Domain Management 231
Alerts 231
Site Connections 233
Policies 234

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 web application are:

- Monitoring Site Health
- Networks
- Applications
- Managing Clients
- Managing Sites Remotely
- Managing Threats
- Managing Domains

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 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

HPE Networking 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
Ports Creating a Port Profile Overview	**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.
Overview	**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.
	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 Network Assignment	**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	▪ Threats ▪ Threat Management ▪ Threat Exceptions ▪ 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.

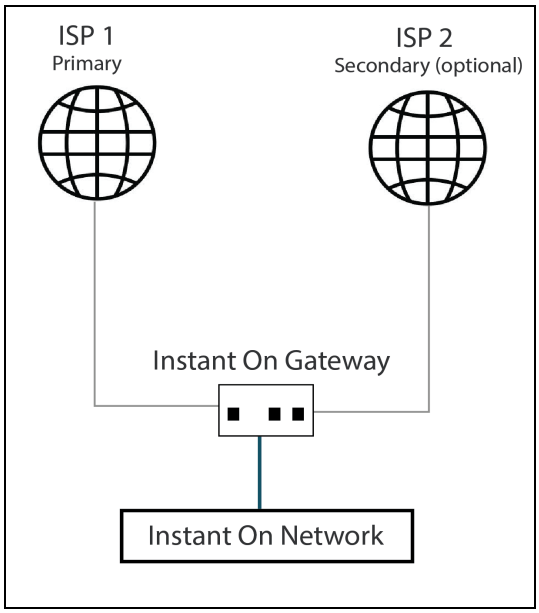
The secondary connection provides backup and failover capabilities in the event when the primary connection is not available.

Direct and Indirect Connection

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

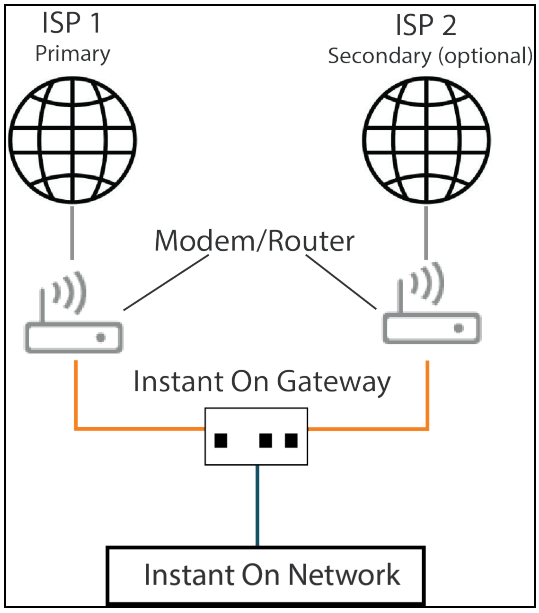
Direct Connection

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

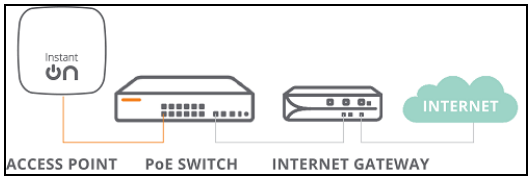
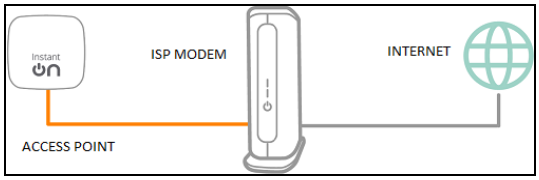
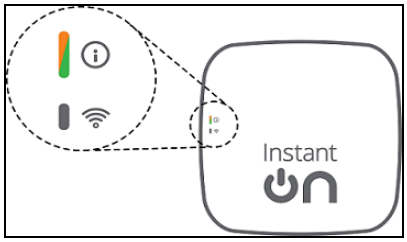
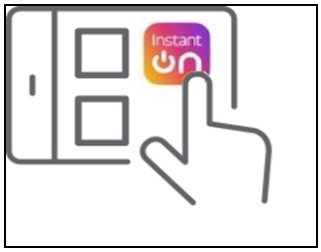
This chapter describes the following procedures:

- Setting Up Your Wireless Network
- Setting Up Your Wired Network
- Setting Up Your Network Using Gateway
- LED Status
- AP Operating Modes
- Setting Up Your Instant On Secure Gateway
- Discovering Available Devices
- Accessing Instant On Application
- Managing Sites Remotely

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.

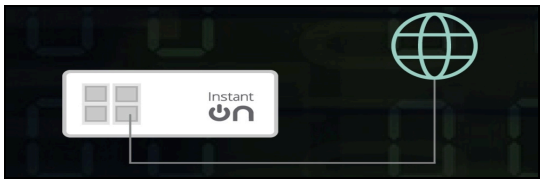
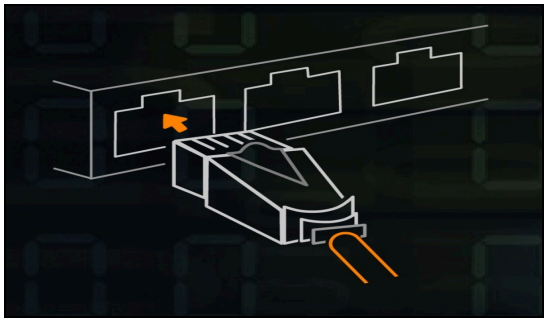
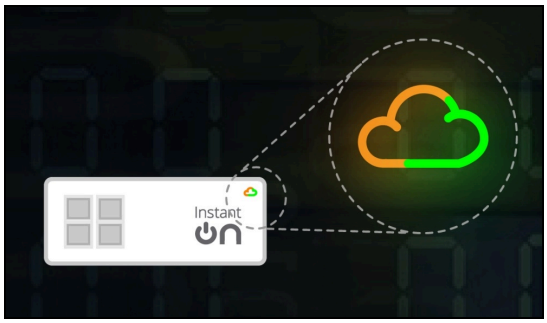
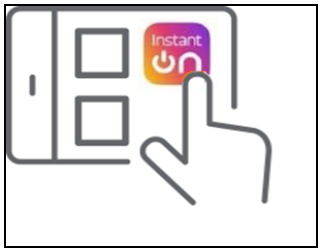
Table 5: *Instant On Wireless Network Provisioning*

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*

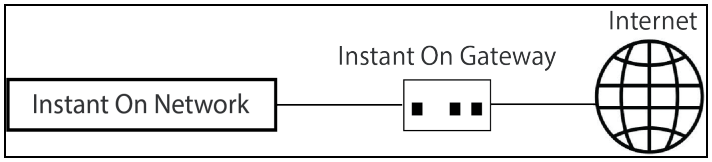
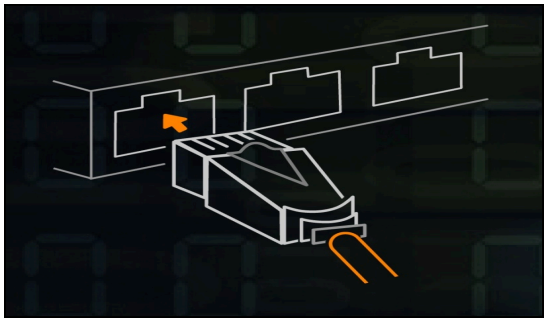
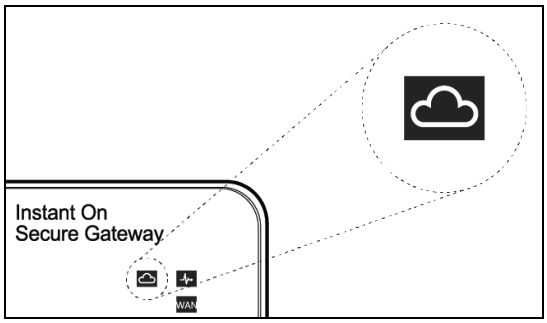
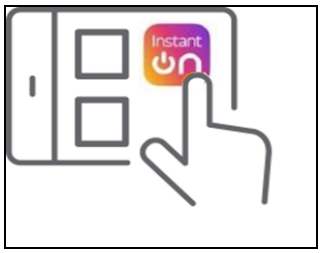
SL No	Steps	Illustration
1.	Ensure that the Instant On gateway is connected to the internet for it to be discovered. The Instant On gateway must be connected to the internet through the WAN port, using either a direct or an indirect connection. For more information about direct and indirect connections, 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.

Accessing Instant On Application

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

Browser Requirements

The following web browsers support the Instant On web application:

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

Create an Instant On Account

Follow these steps to create an Instant On account:

1. Open a browser.
2. Type **https://portal.instant-on.hpe.com/login** in the address bar and press the **Enter** key.
3. Click **Create an account** to create a new Instant On account.
4. Enter an email ID in the **Email** field. The email ID should not be associated with another Instant On account.
5. Enter a password in the **Password** field.
6. Select a country from the **Country** drop-down list.
7. Under **Product Updates and Offers**, select the **Receive personalized communications about Instant On and select partner products, services, offers, and events according to** HPE Privacy Statement checkbox to receive periodic updates.
8. Under **Terms and Conditions**, select the End User License Agreement **and** Data Privacy Policy and Security Agreement checkbox.
9. Click **Create Account**.
10. A verification email is sent to your email account. Follow the instructions in the email to activate your Instant On account.

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

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

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

Logging in to Instant On

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

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

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

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

Resetting Your Account Password

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

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

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

Official Cloud URLs for Instant On

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

- Onboarding URL used by 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**

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.

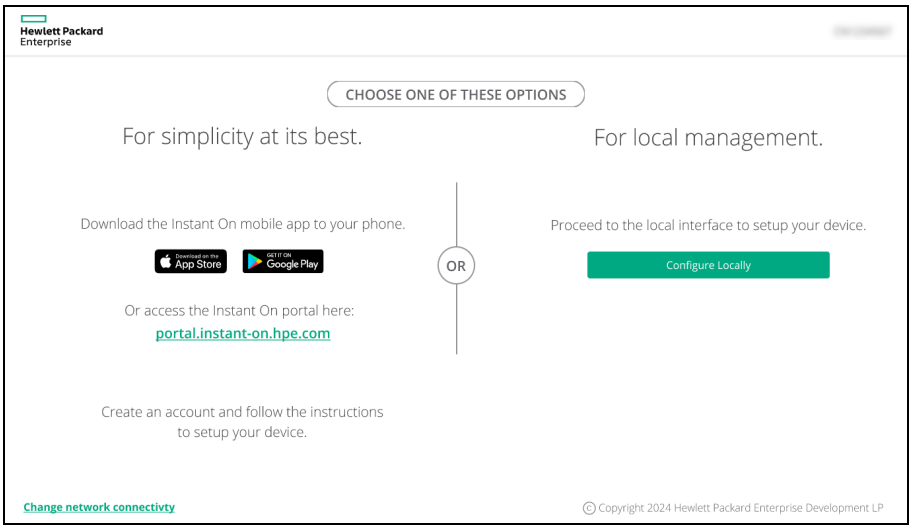
4. In the mobile app–Enable location and bluetooth services and set the Instant On app permissions to use location and bluetooth services in order to automatically discover nearby Instant On devices.

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

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.

NOTE

- The switch cannot be onboarded or managed from the Instant On web interface once the local management for the switch is selected. The switch needs to be reset to factory default from the local WebUI to switch to the cloud management mode.
- 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 web application), 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.

NOTE

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

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.

By default, the configuration is set to automatic.

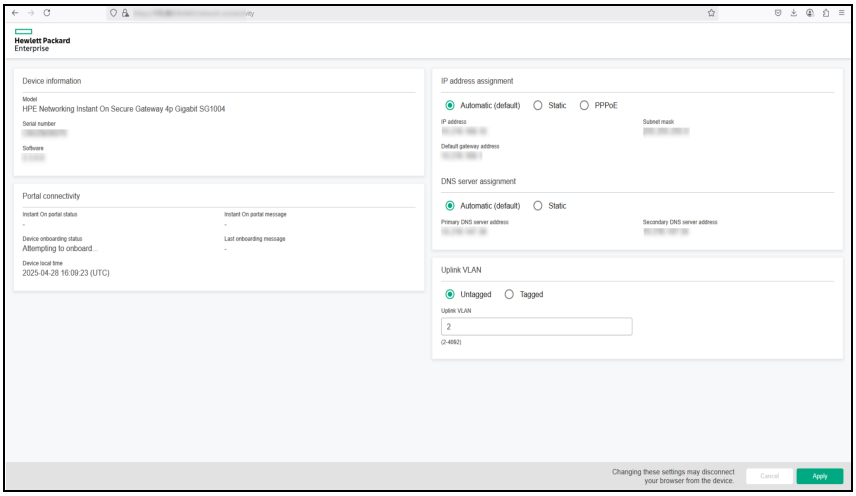
To manually assign an IP address using the local web interface, proceed with Step 5 to Step 10.

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

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 Web Application

NOTE

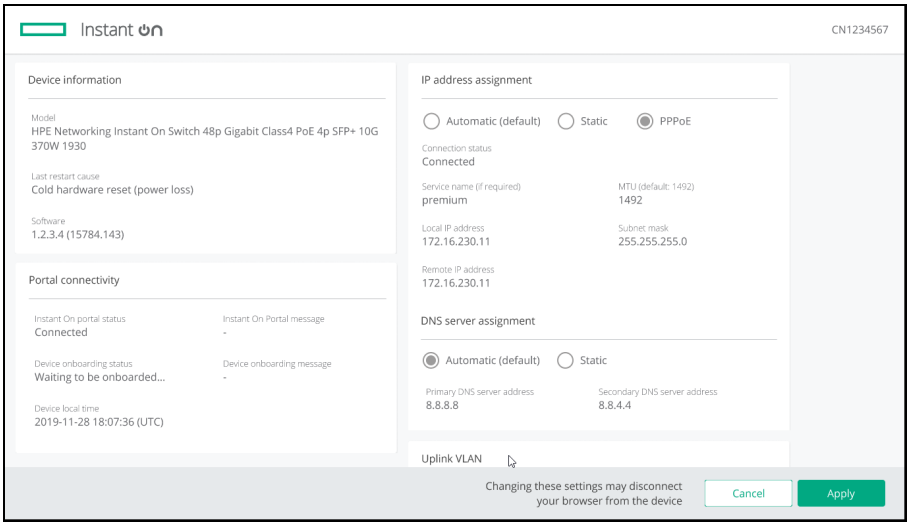
If a gateway with a PPPoE configuration is removed from the Inventory or if the site is deleted, the gateway will reset to its factory default state, and the PPPoE configuration will be erased.

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 Web Application

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

Managed Sites

When you login to the Instant On application using your administrator account credentials, the **Managed Sites** page is displayed if multiple Instant On sites are registered to your account. The sites created for your Instant On account are displayed based on the following customized views:

- Card View
- List View
- Map View

Card View

This is the default view. The sites registered to the account are displayed as separate cards and provide an overview of the overall health status of the site and active alerts.

Follow these steps to view the sites in the Card View:

1. Login to your Instant On account using your administrator credentials. The Managed Sites screen is displayed.
2. Click the Card View icon ( ) on the top-right corner of the screen to view the sites in the card view.

   Each site is displayed as a separate card.
3. Click on any of the cards listed on this page, to view or manage the settings of that particular site.

List View

The sites **Overview** page displays site information such as site name, health, health trend, alerts, and location. The details displayed in each column can be sorted by clicking on the column name.

Follow these steps to view the sites in the List View:

1. Login to your Instant On account using your administrator credentials. The **Managed Sites** screen is displayed.
2. Click the List View icon ( ) on the top-right corner of the screen to view the sites in the list view. Each site is displayed in a list, arranged in alphabetical order of the site name.
3. Use one of the following methods to view the details:
   a. Clicking on the site name.
   b. Hover the cursor to the end of the row of the site you want to view, click the ••• button, and select **View Details** from the drop-down list.

Exporting the Sites Table

The administrators can export the sites table in a .csv format.

To export the sites table, complete the following steps.

1. In the List View, click on the **Actions** drop-down.
2. Click **Export**.
3. The sites table is successfully exported. The downloaded .csv file contains site information such as site name, health, health trend, alerts, and location.

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. Hover the cursor to the end of the row of the site you want to clone, click the ••• button, and select **Clone** from the drop-down list.
2. Under **Identify the Site** > **Identification**, enter a **Name** for the new site.

3. Follow these steps to change the location settings:
   a. Click the **Change** button, next to **Location**. The Map View is displayed.
   b. In the subsequent screen, enter the new location details, or use the cursor to drag the location pin to the new location..
   c. Click **Change Location**.
4. Click **Next**.
5. Click the **Add Devices** button in the next screen, if you choose to add new Instant On devices to the cloned site. For more information, see Devices.
6. Click **Clone Site** to complete the process.

Map View

In this view all the Instant On sites associated with your administrator account are displayed on a map based on their site location. Use the (+) and (—) buttons to zoom in or zoom out on the site locations in the map view. The ( ) button resets the map view back to its original setting.

Follow these steps to view the sites in the Map View:

1. Login to your Instant On account using your administrator credentials. The **Managed Sites** screen is displayed.
2. Click the Map View icon ( ) on the top-right corner of the screen to view the sites in the map view.

   Each site is displayed on the map, based on the location settings configured by the administrator.
3. To view the details of a particular site, in the map view, follow these steps:
   a. Enter the Site Name in the **Search Sites** search bar and click on the site name when it appears in the search results. The site panel is displayed on the right.
   b. Click **View Details**, to view the complete site details information.
4. To view the map in the satellite view, select the **Satellite** radio button.
5. To display the names of the Instant On sites on the map, click the **Names** radio button.
6. To display the site health details on the map, click the **Health** radio button.

Account Management

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

Sign Out

Click the alphabet icon in the page header and selection **Sign out** to sign out from your Instant On account.

Help

Click the button in the page header to view the following options.

- **Help**–Displays the contextual help in the side panel. You can click on the **View in Help Center** link to access the Instant On Online Help. For more information, see https://instant-on.hpe.com/techdocs/en/content/home.htm.
- **Support**–The following options are available to reach Instant On support:
  - **Contact support**–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.

- **Community**—Provides 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.
- **Resources**—Opens the Instant On resource page. For more information, see https://instant-on.hpe.com/resources.

- **Legal**—Provides information on the privacy, terms of service, legal disclaimers and other important information.
  - Privacy
  - Terms of Service
  - End User License Agreement
  - Do Not Sell My Personal Information

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.

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.

Figure 3 *Web Application User Interface Dashboard - Without Secure Gateway*

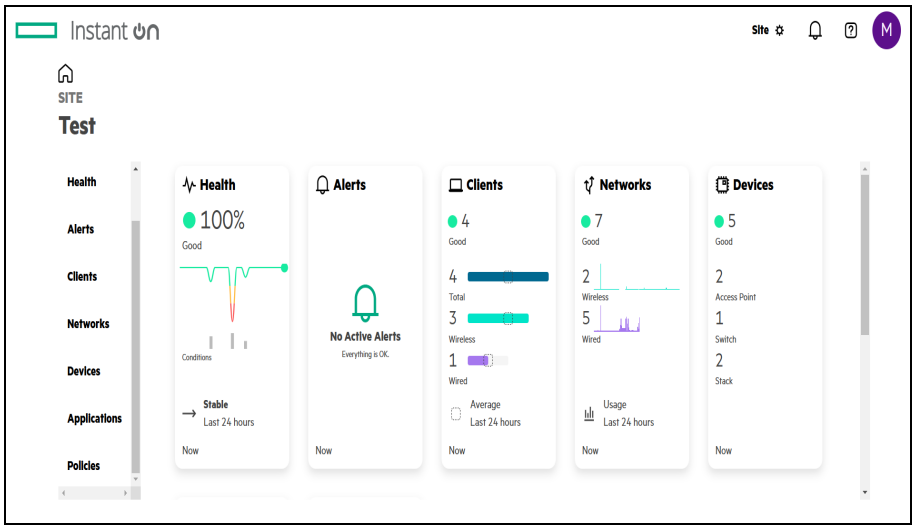
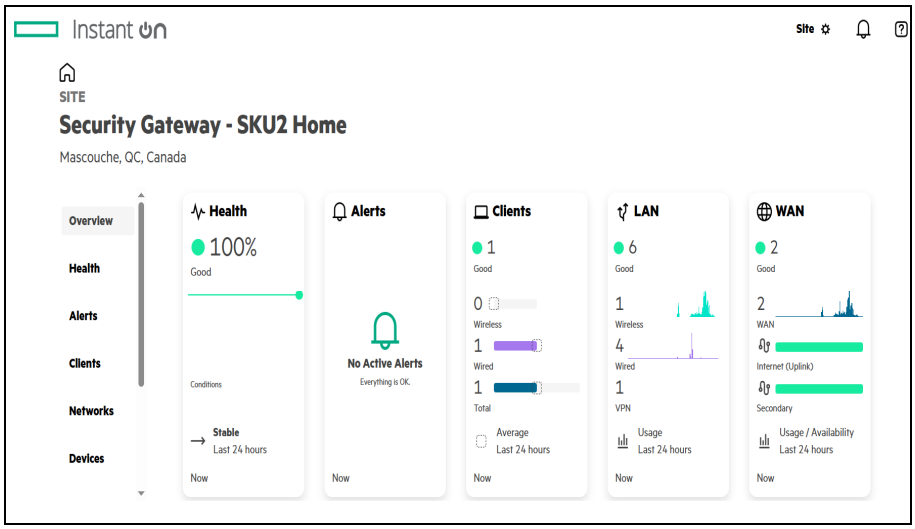


Figure 4 *Web Application User Interface Dashboard - With Secure Gateway*



The Instant On user interface comprises of the following components:

Table 11: *Instant On User Interface Dashboard Components*

Content	Description
Instant On logo	Displays the Instant On logo and functions as a button to return to the Instant On home page.
Alerts ( )	Displays the alerts that are triggered by the system when an unusual activity is observed on the network. See Alerts for more information.
Site ()	Clicking this icon takes you to the **Site management** page. For more information, see Site Management.
Account options ( )	Displays the registered email ID and provides options to administer account information and setup notifications. The first letter of your e-mail id will be displayed in the circle. Account options allows you to perform the following actions: ■ **Account Details**–Allows you to modify your account information for all associated sites. For more information, see Managing Your Account. ■ **Sign Out**–Allows you to log out of your Instant On account.
Help ( )	Provides the following options to reach Instant On support and additional details of the product: ■ **Help**–Opens the Instant On documentation portal. For more information, see https://instant-on.hpe.com/techdocs/en/content/home.htm. ■ **Support**–Listed below are the options available: ◦ **Contact support** - 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. ◦ **Community** - Provides 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/home. ◦ **Resources**– Opens Instant On resource page. For more information, see https://instant-on.hpe.com/resources. ◦ **Version**– Displays the software version. ◦ **View Notes**–Opens the release notes. ◦ **Product Tour**–Provides an overview of the Instant On WebUI and its features. Click the **Product Tour** button to view the information popups for different screens in the UI. ■ **About** - Provides information about the software currently installed on the web application, and also the following information: ◦ End User License Agreement ◦ Data Privacy Policy and Security Agreement
Modules- Modules allow you to configure and monitor network components such as application usage and system alerts. Clicking on a module tile allows you to configure settings relevant to the module. The Instant On user interface consists of the following modules:	
Health	Displays the site health details and trends for the last 24 hours. See Monitoring Site Health for more information.
Alerts	Displays the list of alerts generated at the site. See Alerts for more information.
Clients	Provides connection information for the clients in your network. See Managing Clients for more information on the **Clients** module.

Table 11: *Instant On User Interface Dashboard Components*

Content	Description
Networks	Specifies the number of wired, wireless and VPN, networks available at a site, along with network health, aggregate total usage, and availability over the last 24 hours. When a secure gateway is deployed at the site, then **Networks** tile is renamed to the **LAN** tile, and a **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 Networks for more information on the **Networks** 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. This is available only when a Instant On secure gateway is deployed at a site. 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 Applications for more information on the **Applications** module.
Policies	Specifies the number of policies that govern the site, clients, firewall, network schedules and application category access. See Policies for 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.

Site Management

Click the site management icon () at the top-right corner of the UI screen. The **Site Management** page displays the following user settings that can be modified in the Instant On application:

- Identification
- Management Accounts
- Software
- Support

Identification

The **Identification** page allows you to modify administrator information, including your Instant On site name, change the Location settings associated to the local time zone, date, and time for your Instant On site. For more information, see Identification.

Management Accounts

The Management Accounts page allows you to add additional accounts to manage the site, and also modify the roles assigned to each user account. For more information, see Management Accounts.

Software

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

Support

The Support page allows you to generate a support identifier and device token. The support identifier and device token are then shared with HPE Networking Support personnel to run a diagnosis on your device. For more information, see Support .

Identification

The **Identification** page allows you to modify administrator information, including your Instant On site name, site addressing, location, turn on maintenance mode, and deleting a site.

Modifying the Instant On Site Name

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

1. Click the site management icon () at the top-right corner of the UI screen. The **Site Management** page is displayed.
2. Enter a new name for the Instant On site, under **Name**.

The site name must be between 1 and 64 alphanumeric characters in length.

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.

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

To modify the location details of the site, click **Change**. The location of the site is displayed as a pin on a map. To view the satellite image of the map, click the radio button next to the **Satellite** field. You can use the **+** and **-** controls to zoom in or zoom out on the site location on the map.

1. You can either move the pin on the map by mouse click to change the location, or enter specific coordinates or a location name in the **Search Locations** text box.

Clearing the field does not change the site pin on the map nor affects the site location.

2. Click **Change Location** to save the changes.

Clicking on **Cancel** keeps the current site address and returns to the previous page without making any changes.

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, click **Turn On** next to **Turn On Maintenance Mode**. During this window, all email and mobile notifications for all accounts managing the site will be disabled and a banner is displayed at the top of the page stating, **This site is under maintenance. Email and mobile notifications are disabled.**

Once the site is ready, click the **View site maintenance** link in the banner to navigate to the **Site Management** page, and click **Turn off** next to **Turn off Maintenance Mode**. This resumes normal operations and reactivates email and mobile notifications for all accounts managing the site.

Delete Site

To delete an Instant On site, follow these steps:

1. Click the **Delete** button, next to **Delete Site**.
2. To **Confirm Site Deletion**, enter the **Confirmation Code** displayed on the screen in the text box.
3. Click **Delete Site** to permanently delete the site.

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.

Management Accounts

The **Management Accounts** page lists all the accounts that are added to gain access to the site. You can add a maximum of 25 user accounts to access the site. The accounts are classified as follows:

- **Account**–Displays the email address of the user account.
- **State**–Denotes if the email address of the user account is verified or not.
- **Management Role**–Indicates the access level role assigned to the user account.

The **Management Accounts** page also allows you to add other administrator accounts to manage the site. Once they are added, you can perform additional functions such as Changing Role, Transfer Access, and Remove Access.

Adding Accounts

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

1. Click the site management icon () displayed on the header. The **Site Management** page is displayed.
2. Click the **Management Accounts** section.
3. To add an administrator account, click **Add Account**.
4. Under **Identify Management Account**, enter a valid email ID in the **Email** field.
5. 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.
6. Click **Add account** to save the changes.

Changing Account Role

This page allows accounts with administrator privileges to change the role of the accounts. The following procedure describes how to change an account role:

1. Click the site management icon () displayed on the header. The **Site Management** page is displayed.
2. Click the **Management Accounts** section. The list of user accounts associated with the site is displayed.
3. Hover the cursor over the user account, click the more options icon (•••), and select **Change Management Role**.
4. In the **Change Management Role** pop-up window, select one of the following roles for the user account:
   a. **Administrator**
   b. **Operator**
   c. **Delegate**
   d. **Viewer**
5. Click **Change Role**. The new role information is displayed under the **Role** column for the account.

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. Click the site management icon () displayed on the header. The **Site Management** page is displayed.
2. Click the **Management Accounts** section. The list of user accounts associated with the site is displayed.
3. Hover the cursor over the user account, click the more options icon (•••), and select **Transfer Access**.
4. Enter the email address of the new user account that will receive the access and the management role from the current user account.
5. Click **Next**.
6. Click the **Transfer Access** button to confirm the action. A confirmation message is displayed, stating that ownership has been transferred successfully.

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. Click the site management icon () at the top-right corner of the UI screen. The **Site Management** page is displayed.
2. Click the **Management Accounts** section. The list of user accounts associated with the site is displayed.
3. Hover the cursor over the user account, click the more options icon (•••), and select **Remove Access**.
4. Click the **Remove Access** button on the next screen. The account is signed out immediately and can no longer be used to access the site.

Managing Firmware Upgrades

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

Upgrading the Firmware for an Instant On device

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

Instant On Image Server

Every version of the Instant On software image is uploaded and stored in a cloud-based image server that is hosted by 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 using the Instant On web application. When a new software update is available, an information alert is displayed with sufficient information of when

the update will occur. In the **Software update** section click **View Notes** to view information about the new software version and date when the last software push completed. The page also includes the scheduled time for the update and the options—**Install Now**, **Schedule**, or **Reschedule**. Clicking on the **Schedule** or **Reschedule** link opens a calendar from which the administrator can pick a specific date on which the update is preferred. The software update can be extended up to a maximum of 30 days from when the alert is generated. If a date is not set in the calendar, the software update will take place based on the preferred day of the week setting.

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

1. Click the **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. Under **Automatic Updates**, select a day from the **Day of the week** drop-down list for the software update to be installed automatically.
4. Under **Site Local Time**, click on a suitable time from the clock and click **Ok**.
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 (Default), 2 Weeks, 3 Weeks, and 4 Weeks.
6. Click **Update**.

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 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.

Support

The **Support** page allows you to generate a support identifier and device token. The support identifier and device token are then shared with HPE Networking Support personnel to run a diagnosis on your device.

Generating a Support Identifier and Device Token

To generate a support identifier and device token, follow these steps:

1. Click the site management icon () at the top-right corner of the UI screen. The **Site Management** page is displayed.
2. Click the **Support** section.
3. To generate a support identifier, click **Get** next to **Get Support Identifier**. The support identifier is used by HPE Networking Support personnel to access diagnostic and support information.
4. To generate a device token, click **Get** next to **Get Device Token**. The device token is used by HPE Networking Support personnel to access local device information.
5. Copy the support identifier and device token, and share them with HPE Networking Support personnel to run a diagnosis on your device.

Chapter 8
Monitoring Site Health

The **Health** > **Overview** 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 Site Health page also shows a line graph and bar chart combination which captures changes in values over a specified period of time.

The **Health** > **Overview** page displays the following Site Health attributes:

- Condition–Denotes the health condition alerts or status generated from the devices or networks. The list of health conditions and their descriptions are listed in Monitoring Site Health.
- Category–Denotes the three categories for which the health condition is displayed:
  - Clients
  - Networks
  - Devices
- Source–Denotes the device or network for which the health condition is displayed.
- Severity/Health–Denotes the severity of the alert generated.

For more information, see Alerts.

Table 12: *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.
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.

Table 12: *Health Conditions*

Condition	Category	Description
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 13: *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.
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.

Alerts

Alerts are triggered by the system when an unusual activity is observed with the network devices on the site. To view the **Alerts** page, click the **Alerts** ( ) tile on the site home page or from the navigation pane on the left.

The **Overview** tab in the Alerts page displays the list of alerts under the following:

Category	Description
Alert	Displays the short summary of the alert generated.
Severity	Displays the severity of the alert generated.
Source	Displays the network or device details for which the alert is generated.
State	Displays if the alert is active or cleared.
Raised	Displays the time at which the alert was received.
Cleared	Displays the time at which the alert was cleared.

The different types of alerts are classified as follows:

Table 14: *Types of Alerts and its Severities*

Alert Type (Severity)	Icon	Description
Major		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		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.
Informational		The information alert indicates a change has occurred in the site topology, but there are no interruptions to the connectivity.

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 **Alerts ( )** tile on the site home page will display a **No Active Alerts** message.

The table below shows the list of possible alerts:

Table 15: *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.

Name	Severity	Description
		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
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).

Name	Severity	Description
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.

Viewing Alert History

To view the Alert history, follow these steps:

1. Click the **Alerts** ( ) tile on the Instant On home page, or click **Alerts** from the navigation pane on the left.
2. The **Overview** tab on the **Alerts** page displays the history of the alerts generated on the site. This list includes the active alerts and the ones that have been cleared.

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

Alert Triggered When Instant On AP25 Access Point is Underpowered

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

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

Events

The **Site 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.

The **Export** option exports the list of events in CSV format. You can also search for an event in the search bar.

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.

Chapter 9
Devices

The **Devices** page displays the list of devices in the network, their current operational status, and other details.

To view the list of devices, follow these steps:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left.
2. The **Overview** section of the **Devices** page lists the APs and switches added in the network. Click an AP or switch to view the details of the device.

The details of the devices in the **Overview** page are listed under the following categories:

Table 17: *Device Details*

Category	Description
Device	Displays the name of the Instant On device set by the administrator.
Health	Displays the health status of the Instant On devices connected at the site: ■ Good – Indicates that the health of the device is good. ■ Fair – Indicates the health of the device is fair. ■ Poor – Indicates the health of the device is poor.
State	Denotes the state of the Instant On device, such as Online, Offline, Restarting, Updating, or Synchronizing.
State Duration	Denotes the amount of time the device 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.
Type	Denotes the type of Instant On device - Gateway, AP, switch, or stack.
Model	Displays the model type of the Instant On device.
MAC Address	Displays the MAC address of the Instant On device.
IP Address	Displays the IP address currently used by the Instant On device.
Clients	Denotes the number of clients connected to the Instant On device.

Hover the cursor over a device, click the ••• button and select one of the following options:

- **View Details**–Allows you to view the details of the device.
- **Restart**–Restarts the device.
- **Remove**–Removes the device.

Adding a Device

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

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. Click **Add devices**.
3. Place your Instant On device in its destination area and make sure it is powered on and connected to the Internet. Click the **Include outdoor over-the-air devices** checkbox, to include outdoor devices (AP17 and AP27) that are connected as mesh.
4. Select **Next**. It usually takes around 4-5 minutes for the Instant On devices to be detected.
5. Review the device(s) discovered and click **Add Devices** to add them to your site.

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

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

To extend your network with a gateway, see Extending Your Network - Gateway

Types of Devices

Instant On supports four types of devices:

- Gateways
- Access Points
- Routers
- Switches and Switch Stacks

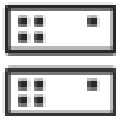
Topology

The **Topology** tab in the Devices 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. Clicking on a device opens up a panel which displays the device information card. Click **View Details** to view the complete details of the connected device.

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

Table 18: *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.

Icon	Description
	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, AP25, AP22, or AP32 access point.
	Indicates an AP17 or AP27 access point.
	Indicates an AP11D or AP22D 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 gateway.
	Indicates that the network is connected to a private network.

Icon	Description
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. An icon is displayed next to the stack and its member devices to indicate their health status. To view the topology of the stack, follow these steps:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left.
2. Click the **Topology** tab.
3. Slide the **View stack topology** toggle switch to right ( ).

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

The stack topology displays the following details:

- Interconnections between the devices in the stack.
- Devices in the stack which are connected to another Instant On device that is not part of the stack.
- Connectivity status between devices.
- Third party devices that are connected to the stack, resulting in an invalid topology.
- Displays the 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.

Extending your Network - APs

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

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

Extend using a Cable

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

1. Click the **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. Click **Add devices**.
3. 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).

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

Extend Over the Air

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

1. Connect at least one Instant On AP to a local wired switch or a router and ensure that the initial setup is complete.
2. 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.
3. Wait for the LED lights on the wireless Instant On AP(s) to blink alternatively between green and amber.
4. Review the device(s) discovered and add them to your site.

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

Scenarios That Trigger Error Messages When Adding Instant On Devices

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.
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.

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

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

Scenario 1: Provision a Site on the Outdoor AP Channel

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

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

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

If the user chooses to discover outdoor APs as part of the search by selecting the **Include over-the-air outdoor devices in search** checkbox:

- A warning message is displayed to indicate that the Wi-Fi network will be temporarily unavailable when search for over-the-air outdoor devices. All APs in the site are forced to the outdoor channel and power plan. All APs discovered in the search regardless of their type or connectivity status will be displayed and can be added to the inventory. If there are no outdoor APs discovered in this process, the site will revert to the default channel plan.

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

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

Scenario 3: Existing sites with Mesh outdoor Access Points

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

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

Scenario 4: Deleting Last Outdoor Mesh Point

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

Extending Your Network - Gateway

You can add a secure gateway to any type of site, whether it is in bridged mode or router mode. The secure gateway can be added when existing devices are online or offline.

If the existing devices are online, the gateway will be automatically discovered. If the devices are offline, you can manually add the gateway by entering its serial number.

To ensure proper discovery and onboarding, the gateway must be placed at the top of the network 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 APs or Switches to the LAN ports of gateway.

Bridged Mode

In the bridged mode, once the secure gateway is added, it becomes the primary routing device for the site. It will provide the DHCP and DNS services, and all traffic will be routed from LAN to the WAN interface.

Router Mode

In the router mode, once the secure gateway is added, the existing Wi-Fi router device becomes a bridged device, and the secure gateway becomes the primary routing device for the site.

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 APs in the site use only the selected channels and allowed channels for the channel width.

Important Considerations 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 dropdown for AP32 to include 5 GHz to re-establish the mesh link.
- 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.
- The 6 GHz radio spectrum is currently available only on AP32 access points.

Changing these settings might disconnect clients from the network.

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

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left
2. Click the **Radio Management** tab.
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.
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 channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for 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.

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.
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:

Table 20: *Transmit Power Levels and Threshold Values*

Transmit Power Level	Threshold for 2.4 GHz Radio	Threshold for 5 GHz Radio	Threshold for GHz Radio
Low	6 dBm	15 dBm	15 dBm
	9 dBm	18 dBm	18 dBm
	12 dBm		21 dBm
Medium	15 dBm	21 dBm	24 dBm
	18 dBm		
High	21 dBm	24 dBm	27 dBm
	24 dBm	27 dBm	30 dBm
	27 dBm		
Very high	30 dBm	30 dBm	33 dBm
Max	This is the default setting.	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
- Rapid Spanning Tree Protocol (RSTP)

Instant On Proprietary Mechanism

This mechanism is in-built on AP11D and AP22D access points to protect them against loops or storms. This mechanism cannot be disabled on the device using the Instant On web application. The device sends out a proprietary packet and blocks any port that receives the same packet. The device will recover in 60 seconds once the fault is removed.

Rapid Spanning Tree Protocol (RSTP)

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

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

Follow these steps to enable RSTP on the network:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left.
2. Click the **Loop Protection** tab.
3. Click the **Spanning Tree Loop Protection** checkbox to enable 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 bridge device on the network.

RSTP is enabled by default when a stack is present in the device inventory and the checkbox selection cannot be disabled. However, if the stack is removed from the inventory, RSTP will still be enabled, but the checkbox becomes available to enable or disable the setting.

Bridge Priority Assignments

The **Bridge Priority** page displays the participating spanning tree devices and their bridge priority. The priority will be automatically determined using the topology and the position of the devices related to each other. The root bridge is assigned to the Instant On switch or router that is closest to the internet router or entry point to a private network. The root bridge priority is assigned the default value of 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. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left.
2. Click the **Loop Protection** tab.
3. Click the **Rapid Spanning Tree (RSTP)** checkbox to enable loop protection. The details of the **Base priority** and **Root bridge** are displayed.
4. Under **Priority Assignment**, click the drop-down arrow and select a priority from the **Base Priority** list.
5. If you choose to recalculate the bridge priority, click the **Recalculate** button next to **Priority Assignment** and then click **Recalculate Priorities**.

   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 Management** page allows you to configure a schedule for Instant On gateway (SG2505P), 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, PoE capable access points and gateway SG2505P. Starting with Instant On 2.8.0, the power schedule configuration is applied to every PoE port with or without connected site devices.

The Power Schedule feature does not take effect on:

- Uplink port
- Link aggregation ports

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

1. Click the **Devices** ( ) tile on the Instant On web application home page or click **Devices** from the navigation pane on the left.
2. Click the **Power Schedule** tab.
3. Under **Power Schedule Assignment** > **Devices**, click on an Instant On device from the list displayed to configure the PoE power schedule on multiple ports for devices in the inventory.
4. Alternatively, you can also click on **Assign to All**, to enable the power schedule for all the available PoE ports on that device, or **Remove All** to deselect the selected options.
5. Under **Power Schedule** > **Type**, click one of the following options:
   a. **Fixed**–Indicates the schedule configuration for only recurring durations (day/hour on a weekly basis) during which the switch enables the power supply for the PoE ports.

- Under **Active Days**, select the days on which the switch should supply power to the PoE ports.
- Select one of the following options under **Daily Operating Hours**:
  - **Active All day**: The switch provides power to the PoE ports throughout the day.
  - **Active between a Start and End Time**: 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. After selecting **Variable**, click on the day of the week for which you need to configure a schedule.

ii. Select one of the following options under **<Day> Operating Hours**:
- **Inactive All Day**: The PoE power supply is disabled for the selected day of the week.
- **Active All day**: The switch provides power to the PoE ports throughout the day.
- **Active between a Start Time and End Time**: The switch provides power to the PoE ports for the specified time period. Configure the **Start Time** and **End Time** for PoE supply as required.

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

6. You can also configure the PoE power schedule on multiple ports for devices in the inventory.
7. Click **Update**. The configuration is automatically saved.

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

The gateway details are displayed under the following categories:

- Overview
- Ports
- Network Assignment
- Network Tools

Overview

The **Overview** tab of the gateway details page contains the following sections:

- Identification
- Hardware
- Uplink
- Connectivity
- Power over Ethernet (PoE)

- Restart Device
- Replace Device
- Device Options

To view the details of the gateway, follow these steps:

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 gateway details:
   a. Clicking on the gateway name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

Identification

The **Identification** section provides the basic details of the selected gateway, which includes the gateway name, status, and health.

The **Overview** > **Identification** section displays the following details:

- **Name**–Denotes the device name specified by the administrator or the Serial Number of the device. The maximum number of characters supported is 32.

  To reset the device name to its default name, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.
- **Health**–Displays the health status of the device:
  - Good–Indicates that the health of the device is good.
  - Fair–Indicates the health of the device is fair.
  - Poor–Indicates the health of the device is poor.
- **State**–Denotes if the device is Online, Offline, Synchronizing, Rebooting, and Updating.
- **Online Since**–Denotes the time duration for which the device has been online.
- **Locator Light**–Used to locate your device when there are many devices in the site. Slide the **Locator Light** toggle switch to right ( ) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.
- **View in topology**–Used to view the device connections in the topology view. To view the topology view, click the link.

Hardware

The hardware section displays the following details:

- **Model**–The model number of the device.
- **MAC Address**–The MAC address of the device.
- **Serial Number (S/N)**–The Serial number of the device.
- **Part Number**–The part number assigned to the device.
- **Software**–The Instant On software version.

Uplink

The uplink section displays the name of the WAN Network. You can click on the link to view the uplink network details page.

For more information about WAN Network, see Overview.

Connectivity

The connectivity section contains the following information:

- **IP Address Assignment**–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.
- **IP Address**–IP Address of the Instant On gateway.
- **Subnet Mask**–Subnet Mask of the Instant On gateway.
- **Default Gateway**–IP Address of the Instant On default gateway.
- **Primary DNS Server**–IP Address of the primary DNS server. The primary DNS server is the main, authoritative server for a domain, responsible for storing and managing the domain's DNS zone file.
- **Secondary DNS Server**–IP Address of the secondary DNS server.

Power over Ethernet (PoE)

The **Power over Ethernet** section is available only on SG2505P gateway that supports PoE technology. The PoE section provides the following information:

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

Restart Device

Instant On allows you to restart the device (AP, Gateway or Switch) if you suspect any problem with it.

To restart your device, follow these steps:

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 select and restart the device:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Restart** from the dropdown list.
3. Under **Overview** > **Restart Device**, click the **Restart** button.
4. Click **Restart Device** in the popup window that appears on the screen.

Replace Device

The **Replace Device** option is displayed only when the gateway is in a offline state.

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.

- 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.

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

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. Select the offline gateway you want to replace from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Replace** from the dropdown list.
3. Under **Overview** > **Replace Device**, click the **Replace** button.
4. Unplug the gateway you want to replace and plug in your new gateway to the network. When your device's lights are alternating between green and amber, click **Next**.
5. Enter the serial number located on your new Instant On gateway and click **Discover**.
6. Once your gateway is detected, select **Replace Device**.
7. Click **Finish** when your new gateway is added to your network.

Device Options

The **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.

Follow these steps to modify the status of the gateway 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 gateway 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** > **Lights**, select one of the following options:
   - **Normal**–Use this option to turn on the status and radio lights. This option is selected by default.
   - **Quiet**–Use this option to turn off the status and radio lights. When this option is selected, the device lights are turned off during normal operation.
4. Click **Update**.

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 IP address directly from the device's page for both online and offline devices.

Follow these steps to reserve reserving an IP address from the device list:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click , or click **Inventory** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation**.

   To remove it, select **Remove IP Address Reservation**.

Follow these steps to reserve reserving an IP address from the device details:

1. Select the device from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the device IP address directly from the details, select **Remove**.

NOTE

IP Reservation is only supported when Instant On functions as the DHCP server on the network, which occurs only when a Secure Gateway configured as a Wi-Fi Router is present at the site.

Ports

The ports are visually represented on the page in the same manner as the actual physical ports on the device. Each port is numbered according to the port number on the switch and displays its current status. Select a port to open the port configuration.

NOTE

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 port supports speed up to 2.5 Gbps. Both gateways are provisioned to allow one LAN port to be converted into a secondary WAN port. To create a secondary WAN, seeCreating a Secondary WAN .

Secondary WAN Port Details:

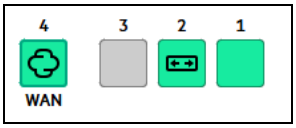
- SG1004 Gateway:
  - Port 3 can be converted into a secondary WAN port.
  - Port 3 supports speeds of up to 1 Gbps.
- SG2505P Gateway:
  - Either Port 3 or Port 4 can be converted into a secondary WAN port.
  - Only one port can be used as a secondary WAN port at a time.
  - Port 4 supports speed up to 2.5 Gbps.
  - Port 3 supports speed up to 1 Gbps.

Viewing Port Details

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

Identification

Under **Identification**, when a port is selected the following options are displayed:

- Name of the port in read and write mode.
- **Enabled** –Select the checkbox to enable the port. To disable the port, unselect the checkbox. 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.
- **State**–State of the port. Displays information such as upload speed, download speed, and maximum speed during full-duplex communication.
- **Use Port Profile**–Allows you to assign a port profile to the selected port.
- **Port Profile**–On enabling **Use Port Profile**, the **Port Profile** field is displayed.

  From the **Port Profile** drop-down list, select either an existing port profile or create a new port profile.
  For more information on creating a port profile, see Creating a Port Profile.
  After a port profile assigning, **View Port Profile** is displayed. On clicking the **View Port Profile**, opens the port profile detail panel on the left.
  Click **View Details**, to navigate to the port profile configuration page.

If a port profile is assigned, then the **Power Management** section is not displayed. This parameter is configured in the port profile.

Power Management

Power management options allow you to configure PoE supply to devices connected to the gateway. One SG2505P gateway supports PoE. 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 is categorized as follows:

Table 21: *Power Class of Devices*

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts

Class	Maximum Power from PSE
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 ports 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.

- **Power schedule**– Select this checkbox to either enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **View power schedule**. For more information on configuring **Power Schedule**, see Power Management.

Port Options

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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Port Usage

Port Usage option displays the total accumulated data over the past 24-hour period. The data volume is displayed in **bytes**.
The configurations displayed under **Power Management** are:

- **Downloaded**—displays the total accumulated download data over the previous 24-hour period.
- **Uploaded**—displays the total accumulated upload data over the previous 24-hour period.

Port Usage option includes the total number of packets processed during the 24-hour period.

- **pkts** for values less than 1,000,000 packets. Values between 1,000 and 999,999 packets represents standard decimal notation (i.e. 1.5 pkts for 1,500 packets).
- **M pkts** for values from 1,000,000 up to (but not including) 1,000,000,000 packets.
- **G pkts** for values of 1,000,000,000 packets and greater.

Connected Clients and Devices

On selecting the port, the **Connected Clients and Devices** section displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address. To filter the clients and devices connected to a specific network, select a network from the **Wired Network** drop-down list.

Network Assignment

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.

To assign network to a port, click on **Select network** drop-down list and choose the network you want to map to the port.

Identification

Under **Identification**, when a port is selected the following options are displayed:

- Name of the port in read and write mode
- **State**—State of the port.

Uplink Network

Displays information about the network, such as name of the WAN network, number of uplink, and VLAN tagging.

Included Networks

The Include Networks section is displayed only when port profile is not assigned to the selected port.

Select the following options:

- **Untagged Default Network**–This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged 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.

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. 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 gateway details:
   a. Clicking on the device name of the gateway.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Connectivity**.
5. Specify a destination hostname or IP address to reach on the network in the **Network Destination** text box.
6. Click **Next**. The test begins to run on the gateway and the test results are displayed on the screen.
7. Click **Close Connectivity Test** to complete the 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.

Connectivity Rating	Roundtrip Time	Test Results Format
		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>

Access Point Details

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

The page details are displayed under the following categories:

- Overview
- Radios
- Ports
- Network Assignment
- Network Tools

Overview

The Access Point Details > **Overview** page comprises of the following sections:

- Identification
- Hardware
- Uplink
- Uplink
- 802.1X Authentication
- Restart Device
- Remove Device
- Replace Device
- Device Options

To view the details of the AP, follow these steps:

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 AP details:
   a. Clicking on the AP name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

Identification

The **Identification** section provides the basic details of the selected AP, which includes the AP name, status, and health.

The **Overview** > **Identification** section displays the following details:

- **Name**–Denotes the device name specified by the administrator or the Serial Number of the device. The maximum number of characters supported is 32.

  To reset the device name to its default name, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.
- **Health**–Displays the health status of the device:
  - Good–Indicates that the health of the device is good.
  - Fair–Indicates the health of the device is fair.
  - Poor–Indicates the health of the device is poor.
- **State**–Denotes if the device is Online, Offline, Synchronizing, Rebooting, and Updating.
- **Online Since**–Denotes the time duration for which the device has been online.
- **Locator Light**–Used to locate your device when there are many devices in the site. Slide the **Locator Light** toggle switch to right ( ) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.
- **View in topology**–Used to view the device in the topology view. To view the topology view, click the link.

Hardware

The hardware section displays the following details:

- **Model**–The model number of the device.
- **MAC Address**–The MAC address of the device.
- **Serial Number (S/N)**–The Serial number of the device.
- **Part Number**–The part number assigned to the device.
- **Software**–The Instant On software version.

Uplink

The uplink section displays the following information:

- **Device**– The name of the uplink device. You can click on the link to view the uplink device details page.
- **Uplink Device IP Address**–The IP address of the uplink device.

Connectivity

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

1. Click the **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 AP 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 dropdown list.
3. Under **Overview** > **Connectivity**, select any one of the following options to assign an IP address for the AP:
   - **Automatic(default)** – The IP address for the AP is assigned by the DHCP server.
   - **Static** – Assign a static IP address for the AP and configure the following parameters:
     a. **IP Address**–Enter a Static IP address.
     b. **Subnet Mask**–Enter the subnet mask.
     c. **Default Gateway**–Enter the IP address of the Default Gateway.
     d. **Primary DNS Server**–Enter the IP address of the primary DNS server.
     e. **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
4. Click **Update**.

802.1X Authentication

Allows you to select the RADIUS profile for the device.

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.

Click **View Details**, to view and edit an existing RADIUS profile.

Restart Device

Instant On allows you to restart the device (AP, Gateway or Switch) if you suspect any problem with it.

To restart your device, follow these steps:

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 select and restart the device:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Restart** from the dropdown list.
3. Under **Overview** > **Restart Device**, click the **Restart** button.
4. Click **Restart Device** in the popup window that appears on the screen.

Remove Device

Follow these steps to remove an Instant On device (AP or Switch) which is still online:

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. Select the device you want to remove from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Remove** from the dropdown list.
3. Under **Overview** > **Remove Device**, click the **Remove** button.
4. Click **Remove Device** in the popup window that appears on the screen.

Replace Device

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

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

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

1. Click the **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. Select the offline AP you want to replace from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Replace** from the dropdown list.
3. Under **Overview** > **Replace Device**, click the **Replace** button.
4. Unplug the AP you want to replace and plug in your new AP to the network. When your device's lights are alternating between green and amber, click **Next**.
5. Enter the serial number located on your new Instant On AP and click **Discover**.
6. Once your AP is detected, select **Replace Device**.
7. Click **Finish** when your new AP is added to your network.

Device Options

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

Follow these steps to modify the status of the access point 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 AP 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 dropdown list.

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

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 IP address directly from the device's page for both online and offline devices.

Follow these steps to reserve reserving an IP address from the device list:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click , or click **Inventory** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation**.

   To remove it, select **Remove IP Address Reservation**.

Follow these steps to reserve reserving an IP address from the device details:

1. Select the device from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the device IP address directly from the details, select **Remove**.

IP Reservation is only supported when Instant On functions as the DHCP server on the network, which occurs only when a Secure Gateway configured as a Wi-Fi Router is present at the site.

Radios

The **Radios** tab provides an option to override 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.

Important Considerations 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 dropdown for AP32 to include 5 GHz to re-establish the mesh link.
- 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.
- The 6 GHz radio spectrum is currently available only on AP32 access points.
- 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. In the **Radios** page, click the **Use Specific Channels and Power** checkbox for **2.4 GHz Radio**, **5 GHz Radio**, and **6 GHz Radio** respectively to view the device specific radio settings.
2. Under the respective **2.4 GHz Radio** and **5 GHz Radio** sections, select the **Specific Configurations** checkbox for each of the radios, to modify their channel and power values.
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.
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 channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for AP32 access points.

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:

Table 23: *Transmit Power Level and Threshold Values*

Transmit Power Level	Threshold for 2.4 GHz Radio	Threshold for 5 GHz Radio	Threshold for 6 GHz Radio
Low	6 dBm	15 dBm	15 dBm
	9 dBm	18 dBm	18 dBm
	12 dBm		21 dBm
Medium	15 dBm	21 dBm	24 dBm
	18 dBm		
High	21 dBm	24 dBm	27 dBm
	24 dBm	27 dBm	30 dBm
	27 dBm		
Very high	30 dBm	30 dBm	33 dBm
Max	This is the default setting.	This is the default setting.	This is the default setting.

NOTE

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.

7. Click **Update** to save the changes.

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** section allows you to assign an Instant On AP to the wireless networks configured on site.

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

1. Click the **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 AP details:
   a. Clicking on the AP name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Under **Radios** > **Network Assignment** , click the checkbox next to a network name to assign the AP to that network.

NOTE

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

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.

Identification

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

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

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 Router details:
   a. Clicking on the device name of the AP configured as the primary Wi-Fi router..
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Under the **Ports** tab, select any of the ports to view the following details:
   - Port number–The physical port number of the router.
   - Port status–The speed of the trunk is displayed if the port is the member of a trunk.
   - Upstream and Downstream throughput – The upstream and downstream throughput of the trunk is displayed when the port is the member of a trunk.
   - **Use Port Profile**–Allows you to assign a port profile to the selected port.
   - **Port Profile**–On enabling **Use Port Profile**, the **Port Profile** field is displayed.

     From the port profile drop-down list, select either an existing port profile or create a new port profile.
     For more information on creating a port profile, see Creating a Port Profile.
     After a port profile assigning, **View Port Profile** is displayed. On clicking the **View Port Profile**, opens the port profile detail panel on the right.
     Click **View Details**, to navigate to the port profile configuration page.

If a port profile is assigned, then the **Authentication** section is not displayed. This parameter is configured in the port profile.

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

- Name of the port in read and write mode.
- **Enabled**–Select **Enabled** checkbox to enable the port.

Authentication

The Authentication option is available only when **Use Port Profile** is disabled. By default, **802.1X Authentication** is set to **No Authentication (default)**. To select **Port-based** authentication, RADIUS profile must be assigned to the access point under **Overview** > **802.1X Authentication.**

Power Management

Power Management options allow you to configure PoE supply to devices connected to the switch. Select the checkbox to enable power management. After enabling, click on the View power schedule link to view the **Power Schedule Assignment**. The configurations displayed under **Power Management** are:

- **Power Allocation**
  - **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

- **Power Schedule** – Select this checkbox to either enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **View power schedule**. For more information on configuring **Power Schedule**, see Power Management.

Port Options

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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Port Usage

Port Usage option displays the total accumulated data over the past 24-hour period. The data volume is displayed in **bytes**.
The configurations displayed under **Power Management** are:

- **Downloaded**–displays the total accumulated download data over the previous 24-hour period.
- **Uploaded**–displays the total accumulated upload data over the previous 24-hour period.

Port Usage option includes the total number of packets processed during the 24-hour period.

- **pkts** for values less than 1,000,000 packets. Values between 1,000 and 999,999 packets represents standard decimal notation (i.e. 1.5 pkts for 1,500 packets).
- **M pkts** for values from 1,000,000 up to (but not including) 1,000,000,000 packets.
- **G pkts** for values of 1,000,000,000 packets and greater.

Connected Clients and Devices

On selecting the ENET port, the **Connected Clients and Devices** section displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address. To filter the clients and devices connected to a specific network, select a network from the **Wired Network** drop-down list.

Network Assignment

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

1. Click the **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 Router details:
   a. Clicking on the device name of the AP configured as the primary Wi-Fi router..
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network Assignment** tab in the access point details page.
4. In the device port diagram, select a port to view the port details.

   The port configuration are displayed under:

   Identification–Displays port number, port name and connected state.

   Included Networks–Displays the tagged and untagged network mapped to the port. This is applicable only for AP22D and AP11D access points.

   Select the following options:

   - **Untagged Default Network**–This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
   - **Tagged 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 **Update** to finish mapping the network to the port.

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. 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 AP details:
   a. Clicking on the device name of the AP.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Connectivity**.
5. Specify a destination hostname or IP address to reach on the network in the **Network Destination** text box.
6. Click **Next**. The test begins to run on the AP and the test results are displayed on the screen.
7. Click **Close Connectivity Test** to complete the test.

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

Table 24: *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>

Router Details

The Router Details page provides details of the selected Wi-Fi router, which includes the Router name, IP address, MAC address, serial number, radio, ports, and model type. This page also provides a summary of the wireless radios including the number of clients that are currently connected. Instant On currently supports AP11D or AP22D devices to operate as a primary Wi-Fi router in the network.

The router details are displayed under the following categories:

- Overview
- Radios
- Ports
- IP Assignment
- Network Assignment
- Network Tools

Overview

The Router Details > **Overview** page comprises of the following sections:

- Identification
- Connectivity
- 802.1X Authentication
- Hardware
- Restart Device
- Replace Device
- Device Options

To view the details of the AP, follow these steps:

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 AP details:
   a. Clicking on the AP name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

Identification

The **Identification** section provides the basic details of the selected AP, which includes the AP name, status, and health.

The **Overview** > **Identification** section displays the following details:

- **Name**–Denotes the device name specified by the administrator or the Serial Number of the device. The maximum number of characters supported is 32.

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

- **Health**–Displays the health status of the device:
  - Good–Indicates that the health of the device is good.
  - Fair–Indicates the health of the device is fair.
  - Poor–Indicates the health of the device is poor.
- **State**–Denotes if the device is Online, Offline, Synchronizing, Rebooting, and Updating.
- **Online Since**–Denotes the time duration for which the device has been online.
- **Locator Light**–Used to locate your device when there are many devices in the site. Slide the **Locator Light** toggle switch to right ( ) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.
- **View in topology**–Used to view the device in the topology view. To view the topology view, click the link.

Hardware

The hardware section displays the following details:

- **Model**–The model number of the device.
- **MAC Address**–The MAC address of the device.
- **Serial Number (S/N)**–The Serial number of the device.
- **Part Number**–The part number assigned to the device.
- **Software**–The Instant On software version.

Connectivity

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

1. Click the **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 AP 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 dropdown list.
3. Under **Overview** > **Connectivity**, you can view the following information:
   - **Automatic(default)** – The IP address for the AP is assigned by the DHCP server.
   - **Static** – Assign a static IP address for the AP and configure the following parameters:
     a. **IP Address**–Enter a Static IP address.
     b. **Subnet Mask**–Enter the subnet mask.
     c. **Default Gateway**–Enter the IP address of the Default Gateway.
     d. **Primary DNS Server**–The IP address of the primary DNS server.
     e. **Secondary DNS Server**–The IP address of the secondary DNS server.
4. Click **Update**.

802.1X Authentication

Allows you to select the RADIUS profile for the Router.
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.

Restart Device

Instant On allows you to restart the device (AP, Gateway or Switch) if you suspect any problem with it.

To restart your device, follow these steps:

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 select and restart the device:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Restart** from the dropdown list.
3. Under **Overview** > **Restart Device**, click the **Restart** button.
4. Click **Restart Device** in the popup window that appears on the screen.

Replace Device

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

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

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

1. Click the **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. Select the offline AP you want to replace from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Replace** from the dropdown list.
3. Under **Overview** > **Replace Device**, click the **Replace** button.
4. Unplug the AP you want to replace and plug in your new AP to the network. When your device's lights are alternating between green and amber, click **Next**.
5. Enter the serial number located on your new Instant On AP and click **Discover**.
6. Once your AP is detected, select **Replace Device**.
7. Click **Finish** when your new AP is added to your network.

Device Options

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

Follow these steps to modify the status of the access point 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 AP 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 dropdown list.
3. Under **Overview** > **Device Options** > **Lights**, select one of the following options:
   a. **Normal**–Use this option to turn on the status and radio lights. This option is selected by default.
   b. **Quiet**–Use this option to turn off the status and radio lights. When this option is selected, the device lights are turned off during normal operation.
4. Click **Update**.

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 IP address directly from the device's page for both online and offline devices.

Follow these steps to reserve reserving an IP address from the device list:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click , or click **Inventory** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation**.

   To remove it, select **Remove IP Address Reservation**.

Follow these steps to reserve reserving an IP address from the device details:

1. Select the device from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the device IP address directly from the details, select **Remove**.

IP Reservation is only supported when Instant On functions as the DHCP server on the network, which occurs only when a Secure Gateway configured as a Wi-Fi Router is present at the site.

Radios

The **Radios** tab provides an option to override 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.

Important Considerations 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 dropdown for AP32 to include 5 GHz to re-establish the mesh link.
- 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.
- The 6 GHz radio spectrum is currently available only on AP32 access points.
- 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. In the **Radios** page, click the **Use Specific Channels and Power** checkbox for **2.4 GHz Radio**, **5 GHz Radio**, and **6 GHz Radio** respectively to view the device specific radio settings.
2. Under the respective **2.4 GHz Radio** and **5 GHz Radio** sections, select the **Specific Configurations** checkbox for each of the radios, to modify their channel and power values.
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.
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 channel width of 160 MHz is supported only on AP25 access points and on the 6 GHz radio channel for AP32 access points.

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:

Table 25: *Transmit Power Level and Threshold Values*

Transmit Power Level	Threshold for 2.4 GHz Radio	Threshold for 5 GHz Radio	Threshold for 6 GHz Radio
Low	6 dBm	15 dBm	15 dBm
	9 dBm	18 dBm	18 dBm
	12 dBm		21 dBm

Transmit Power Level	Threshold for 2.4 GHz Radio	Threshold for 5 GHz Radio	Threshold for 6 GHz Radio
Medium	15 dBm	21 dBm	24 dBm
	18 dBm		
High	21 dBm	24 dBm	27 dBm
	24 dBm	27 dBm	30 dBm
	27 dBm		
Very high	30 dBm	30 dBm	33 dBm
Max	This is the default setting.	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.

7. Click **Update** to save the changes.

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** section allows you to assign an Instant On AP to the wireless networks configured on site.

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

1. Click the **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 AP details:
   a. Clicking on the AP name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Under **Radios** > **Network Assignment** , click the checkbox next to a network name to assign the AP to that network.

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

Ports

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

1. Click the **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 Router details:
   a. Clicking on the device name of the AP configured as the primary Wi-Fi router.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Under the **Ports** tab, select any of the ports to view the following details:
   - Port number – The physical port number of the router.
   - Port status – The speed of the trunk is displayed if the port is the member of a trunk.
   - Upstream and Downstream throughput – The upstream and downstream throughput of the trunk is displayed when the port is the member of a trunk.

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

The **Ports** section for unconnected ports consists of the following settings:

- Name of the port in read and write mode.
- **Enabled** – Select the **Enabled** checkbox to enable the port.

Authentication

The Authentication option is available only when **Use Port Profile** is disabled. By default, **802.1X Authentication** is set to **No Authentication (default)**. To select **Port-based** authentication, RADIUS profile must be assigned to the access point under **Overview** > **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.

Power Management

Power Management options allow you to configure PoE supply to devices connected to the port. Select the checkbox to enable power management. After enabling, click on the View power schedule link to view the **Power Schedule Assignment**.

Under **Power Allocation**, select the following:

- **No Power over Ethernet**–Disables PoE for devices connected to the port assigned with the port profile.
- **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 26: *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

Connected Clients and Devices

On selecting a specific port of an AP11D or AP22D router, the **Connected Clients and Devices** section displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address. To filter the clients and devices connected to a specific network, select a network from the drop-down list.

Network Assignment

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. 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 Router details:
   a. Clicking on the device name of the AP configured as the primary Wi-Fi router..
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Assignment** tab in the router details page.
4. In the device port diagram, select a port to view the port details.

   The port configuration are displayed under:

   Identification–Displays port number, port name and connected state.

   Included Networks–Displays the tagged and untagged network mapped to the port.

Select the following options:

- **Untagged Default Network**–This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged 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 **Update** to finish mapping the network to the port.

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 router, follow these steps:

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 router details:
   a. Clicking on the router name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Connectivity**.
5. Under **Set Network Destination**, enter the hostname or IP address of the device to which the source device should connect.
6. Click **Next**. The Network tests will be executed and displayed for the router.

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

Table 27: *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>

Connectivity Rating	Roundtrip Time	Test Results Format
		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>

Switch Details

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

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

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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

The switch details are displayed under the following categories:

- Overview
- Ports
- Network Assignment
- Link Aggregation
- Network Tools
- Routes

Overview

The **Overview** tab of the switch details page contains the following sections:

- Identification
- Hardware
- Uplink
- Uplink
- Power over Ethernet (PoE)
- Restart Device
- Remove Device
- Replace Device

- Switch to Local Management
- Advanced Options

To view the details of the switch, follow these steps:

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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

Identification

The **Identification** section provides the basic details of the selected switch, which includes the switch name, status, and health.

The **Overview** > **Identification** section displays the following details:

- **Name**–Denotes the device name specified by the administrator or the Serial Number of the device. The maximum number of characters supported is 32.

  To reset the device name to its default name, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.
- **Health**–Displays the health status of the device:
  - Good–Indicates that the health of the device is good.
  - Fair–Indicates the health of the device is fair.
  - Poor–Indicates the health of the device is poor.
- **State**–Denotes if the device is Online, Offline, Synchronizing, Rebooting, and Updating.
- **Online Since**–Denotes the time duration for which the device has been online.
- **Locator Light**–Used to locate your device when there are many devices in the site. Slide the **Locator Light** toggle switch to right ( ) to turn on the locator light in the device. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.
- **View in topology**–Used to view the device in the topology view. To view the topology view, click the link.

Hardware

The hardware section displays the following details:

- **Model**–The model number of the device.
- **MAC Address**–The MAC address of the device.
- **Serial Number (S/N)**–The Serial number of the device.
- **Part Number**–The part number assigned to the device.
- **Software**–The Instant On software version.

Uplink

The uplink section displays the following information:

- **Device**– The name of the uplink device. You can click on the link to view the device details page.
- **Uplink Device IP Address**–The IP address of the uplink device.

Connectivity

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

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

- **Automatic (default)** – The Instant On switch will inherit the IP address assigned by the DHCP in the network.
- **Static** –Specify a static IP address for the Instant On switch by entering the following network parameters:
  - **IP Address**–Enter the IP address for the switch.
  - **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 DNS server.
  - **Secondary DNS Server**–Enter the IP address of the DNS server.

Power over Ethernet (PoE)

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

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

802.1X Authentication

Allows you to select the RADIUS profile for the device.

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.

Click **View Details**, to view and edit an existing RADIUS profile.

Restart Device

Instant On allows you to restart the device (AP, Gateway or Switch) if you suspect any problem with it.

To restart your device, follow these steps:

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 select and restart the device:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Restart** from the dropdown list.
3. Under **Overview** > **Restart Device**, click the **Restart** button.
4. Click **Restart Device** in the popup window that appears on the screen.

Remove Device

Follow these steps to remove an Instant On device (AP or Switch) which is still online:

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. Select the device you want to remove from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Remove** from the dropdown list.
3. Under **Overview** > **Remove Device**, click the **Remove** button.
4. Click **Remove Device** in the popup window that appears on the screen.

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. 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. Select the offline switch you want to replace from the device inventory by one of the following methods:
   a. Clicking on the device name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **Replace** from the dropdown list.
3. Under **Overview** > **Replace Device**, click **Replace**.
4. Unplug the switch you want to replace and plug in your new switch to the network. When your device's lights are alternating between green and amber, click **Next**.
5. Enter the serial number located on your new Instant On switch and click **Discover**.
6. Once your switch is detected, select **Replace Device**.
7. Click **Finish** when your new switch is added to your network.

Switch to Local Management

The **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.

Follow these steps to enable Local Management for Switches:

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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Under **Overview** > **Local Management**, click **Switch**.
4. Click **Local Management** in the popup window. The switch is removed from the site and restarted in the local management mode.

For more information, see Local Management for Switches.

Device Options

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 Options

The following selections are available under advanced options:

- Allow Routing Between Networks
- Allow Jumbo Frames

Routing

Configure routing on the Instant On switch. Routing is disabled by default. This feature is currently available only for Instant On 1930 Series and 1960 Series switches. To configure routing for the switch perform the following steps:

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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. To enable routing on a switch or stack, under **Overview** > **Device Options** > **Advanced Options**, select the **Allow routing between networks** checkbox. To disable routing, deselect the checkbox.
4. When **Allow routing between networks** is selected, ● icon is displayed in the device details page under **Routes**, next to networks that can be routed. If the ● icon is not visible, it implies that routing is turned off for the network. Hover the cursor to the end of row, click the ••• button, and select **Enable Routing**.
5. To configure routing for a network, under **Routes**, hover the cursor to the end of the row, click the ••• button, and select **Change IP addressing** from the drop-down list:
   a. 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** – Select a subnet mask from the drop-down list.
   b. Click the **Change IP addressing** 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.
- For a 1960 Series stack, the routing is defined at the stack level. If the conductor switch goes offline, then the backup switch takes over the routing service for the stack.

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. Under **Overview** > **Advanced Options**, select the **Allow Jumbo frames** checkbox.
2. Click **Update**.

   The Instant On switch reboots automatically to apply the changes.

Once the setting is enabled on a 1960 Series switch 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.

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 IP address directly from the device's page for both online and offline devices.

Follow these steps to reserve reserving an IP address from the device list:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click , or click **Inventory** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation**.

   To remove it, select **Remove IP Address Reservation**.

Follow these steps to reserve reserving an IP address from the device details:

1. Select the device from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the device IP address directly from the details, select **Remove**.

NOTE

IP Reservation is only supported when Instant On functions as the DHCP server on the network, which occurs only when a Secure Gateway configured as a Wi-Fi Router is present at the site.

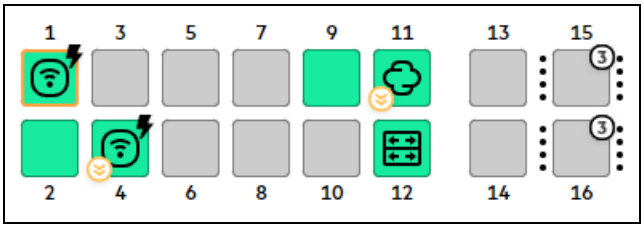
Ports

The ports are visually represented on the page in the same manner as the actual physical ports on the device. Each port is numbered according to the port number on the switch and displays its current status. Select a port to open the port configuration.

Viewing Port Details

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 28: *Port Icons*

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

Identification

Under **Identification**, when a port is selected the following options are displayed:

- Name of the port in read and write mode.
- **Enabled** –Select the checkbox to enable the port. To disable the port, unselect the checkbox. 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.
- **State**–State of the port.
- **Use Port Profile**–Allows you to assign a port profile to the selected port.
- **Port Profile**–On enabling **Use Port Profile**, the **Port Profile** field is displayed.

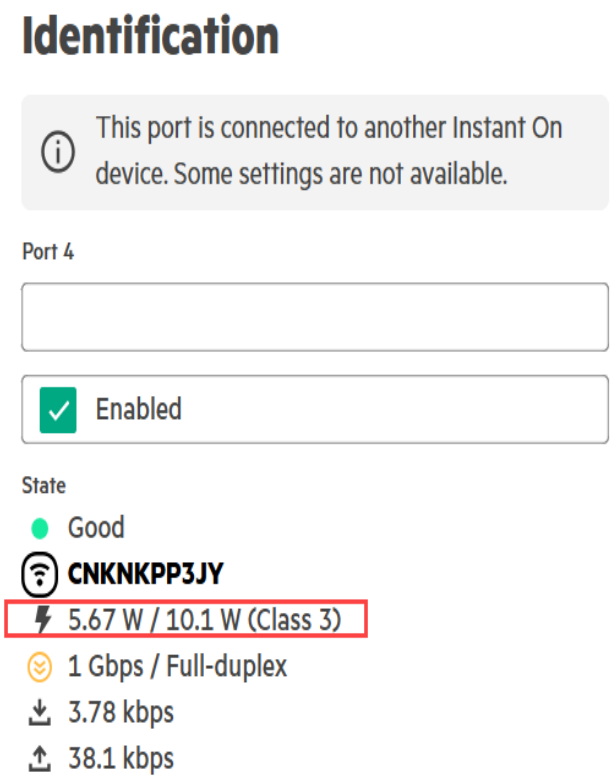
  From the **Port Profile** drop-down list, select either an existing port profile or create a new port profile.
  For more information on creating a port profile, see Creating a Port Profile.
  After a port profile assigning, **View Port Profile** is displayed. On clicking the **View Port Profile**, opens the port profile detail panel on the left.
  Click **View Details**, to navigate to the port profile configuration page.

If a port profile is assigned, then **Security**, **Authentication, Power Management** sections are not displayed. These parameters are configured in the port profile.

PoE Specification

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

Figure 7 *PoE Specification*



Security

The security section consists of the following options:

- **Untrusted Port Protections (DHCP and ARP)**–Enable this option when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. This setting is enabled by default. For more information, see Security.
- **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 (BPDU Guard)**–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. This option is disabled by default. 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 **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 Access

Under **Ports** > **Port Access**, select the **Specific Clients** checkbox to allow the port to connect to specific clients.

Connected Clients and Devices

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

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

1. Click the **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 switch 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 **Ports** > **Port Access**, select the **Specific Clients** checkbox.
4. Under **Allowed Clients and Devices**, click **Add**.
5. Click the **Search** button and connect the clients and devices to the port to be discovered.
6. Once the search is complete, select the checkbox next to the clients and devices you want to add to the Allowed list and click the **Add Clients and Devices** button.
7. Click **Update**.

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

Clients and Devices Connected to this Port

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

Power Management

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

- **Power 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 29: *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

- **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.**

- **Power schedule** – Select this checkbox to either enable or disable power schedule on the port. If enabled, the PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **View power schedule**. For more information on configuring **Power Schedule**, see Power Management.

Port Options

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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Port Usage

Port Usage option displays the total accumulated data over the past 24-hour period. The data volume is displayed in **bytes**.
The configurations displayed under **Power Management** are:

- **Downloaded**–displays the total accumulated download data over the previous 24-hour period.
- **Uploaded**–displays the total accumulated upload data over the previous 24-hour period.

Port Usage option includes the total number of packets processed during the 24-hour period.

- **pkts** for values less than 1,000,000 packets. Values between 1,000 and 999,999 packets represents standard decimal notation (i.e. 1.5 pkts for 1,500 packets).
- **M pkts** for values from 1,000,000 up to (but not including) 1,000,000,000 packets.
- **G pkts** for values of 1,000,000,000 packets and greater.

Connected Clients and Devices

On selecting the port, the **Connected Clients and Devices** section displays the list of clients and devices connected to the port. By default, the clients and devices for **All Networks** applicable to the port are displayed. The clients and infrastructure devices directly connected to the port are displayed as a link to the client details page. The indirectly connected clients are displayed by their MAC address. To filter the clients and devices connected to a specific network, select a network from the **Wired Network** drop-down list.

Network Assignment

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.

Identification

Under **Identification**, when a port is selected the following options are displayed:

- Name of the port in read and write mode
- **State**–State of the port.

Included networks

Select the following options:

- **Untagged Default Network**–This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged 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.

Link Aggregation

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

Table 30: *Switch Ports Aggregation*

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

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

1. Click the **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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Link Aggregation** tab.
4. Click **Create**.
5. Under **Identification**, configure the following:
   - **Name**–Provide a custom name for the Link aggregation in the text field.
   - **Enabled**–Select the checkbox to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. Unselect the checkbox to disable the LACP ports.
   - **Port Members**–Select the ports to add as members of the link aggregation. The list of selected port members is displayed.

     To assign a port profile, enable the **Use Port Profile** option. From the **Port Profile** drop-down list, select an existing port profile or create a new one.
     For more information on creating a port profile, see Creating a Port Profile.
     Once a port profile is assigning, the **View Port Profile** is displayed. When you click the **View Port Profile**, he port profile details panel opens on the left.

     To modify the configuration, click **View Details** to navigate to the port profile configuration page.

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

6. Under **Link Aggregation**, you must select either **Static (default)** or **LACP** as the aggregation type.
7. This is an option settings. Under **Security** > **Port Security**, select **DHCP and ARP Port Protections (Untrusted Port)** or **Port Isolation (Protected Port)**.
8. Under **Security** > **Spanning Tree Protections**, you must select one option from the list of Spanning Tree Protection options. The list of options 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.
9. Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.
10. Click **Create**.

Identification

The **Identification** section displays the following information:

- **Name**–Provide a custom name for the Link aggregation in the text field.
- **Enabled**–Select the checkbox to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. select the checkbox to disable the LACP ports.
- **Port Members**–Displays the list of ports that are currently members of the link aggregation. When you select a port that is not part of the existing link aggregation, a new link aggregation must be created. Each device port can belong to only one link aggregation at a time.

  To assign a port profile, enable the **Use Port Profile** option. From the **Port Profile** drop-down list, select an existing port profile or create a new one.
  For more information on creating a port profile, see Creating a Port Profile.
  Once a port profile is assigning, the **View Port Profile** is displayed. When you click the **View Port Profile**, he port profile details panel opens on the left.

  To modify the configuration, click **View Details** to navigate to the port profile configuration page.

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

Link Aggregation

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

In **Security** > **Port Security** section consists of the following options:

- **DHCP and ARP Port Protections (Untrusted Port)**–Enable this option when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. This setting is enabled by default. For more information, see Security.
- **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.

In **Security** > **Spanning Tree Protections**, select an option listed under **Spanning Tree Protections** 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 **Spanning Tree Protections** section consists 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.

Port Access

Under **Ports** > **Port Access**, select the **Specific Clients** checkbox to allow the port to connect to specific clients.

During discovery, port restrictions on the link aggregation are temporarily disabled to enable new clients and devices to connect.

To add clients, complete the following steps:

1. Select the **Specific Clients** checkbox.
   Allowed Clients and Devices option is displayed.
2. Click **Add**.
   The **Select Clients and Devices to Allow**, window is displayed.
3. Click **Search**, to detect new devices.
4. Select the devices, and click **Add Clients and Devices**.

Port Options

Port Options 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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Clients and Devices

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

Transceiver Details

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

The following transceiver details are displayed under the Ports tab:

Table 31: *Transceiver Details*

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 is offline but a transceiver is detected, the transceiver information will still be displayed.
- Instant On supported transceivers are recommended for optimal performance. Please refer to the Instant On product datasheets for supported transceiver list and 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.

Delete Link Aggregation

To delete the link aggregation, complete the following steps:

1. Click **Delete**.
2. In the **Delete Link Aggregation** pop-up, confirm the delete operation.

Routes

To configure routing for a network, under **Routes**, hover the cursor to the end of the row, click the ••• button, and select **Change IP addressing** from the drop-down list:

1. 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** – Select a subnet mask from the drop-down list.
2. Click the **Change IP addressing** 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.
- For a 1960 Series stack, the routing is defined at the stack level. If the conductor switch goes offline, then the backup switch takes over the routing service for the stack.

To enable routing for a network, under **Routes**, hover the cursor to the end of the row, click the ••• button, and select **Enable Routing** from the drop-down list:

Power Usage

The **Power Usage** page 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.

- 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.

To search for a device, under **Search Powered Clients and Devices** search bar, enter the name, and select the device from the drop-down list.

A **View 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** client details table the following details:

Table 32: *Power Usage client details*

Column Label	Description
Name	This column displays the name of the powered clients and devices.
Type	This column displays the type of devices.
Port	This column indicates the port numbers.
Priority	This column specifies the priority level associated with powered client and device.
Power Usage	This column indicates power used by the device.
Maximum Power	This column shows the maximum power available to the device.

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

Network Tools

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

Port Mirroring

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

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

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

1. Click the **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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click **Start** next to **Start Port Monitoring**.
5. Under **Select Mirroring Source > Stack Member**, select a stack member.
6. Under **Source**, select one of the following:
   a. **Ports**–Select the port(s) to be used as the source port(s).
   b. **Network**–Select one of the available networks from the drop-down list.
7. Click **Next**.
8. Based on your selection above, you will need to select the **Source Ports** or **Source Networks** from which the traffic should be mirrored.
9. Select one of the following as the **Source** and click **Next**:
   a. Transmit and receive
   b. Transmit
   c. Receive
10. 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
11. Click **Start mirroring** to initiate the mirroring of the packets sent from the source to the destination. To stop the mirroring, click **Stop mirroring** at anytime

Test Connectivity

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. 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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Connectivity**.
5. In the **Set Network Destination** page, enter the hostname or IP address of the device to which the source device should connect.
6. Click **Next**. The Network tests will be executed and displayed for the device.

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

Table 33: *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. 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 switch name.
   b. Hover the cursor on the switch name, to the right-hand corner of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Cable**.
5. In **Select Port to Test** page, select the port on which you want to run the cable test.
6. Click **Next**. Initiates the cable test for the selected port.

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

Table 34: *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.

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 are connected in a ring topology and follow the instructions provided in Sign Out. The discovery protocol should be able to detect the Instant On 1960 switch stack.
2. In the **Add new devices** page, select the stack from the list of discovered devices in the network.
3. Click **Finish**.

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

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

Create a New Stack–After Initial Setup

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

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 1960 switch details and create a stack:
   a. Clicking on the switch name of the standalone Instant On 1960 Series switch on which the stack is to be created.
   b. Hover the cursor to the end of the row of the standalone 1960 switch, click the ••• button, and select **Create Stack** from the dropdown list.
3. Under **Overview** > **Create Stack**, click the **Create** button.
4. Select the Instant On 1960 Series switches that should be added as part of the stack.
5. If you have selected multiple devices, then under **Role** select the device that will be assigned as the role backup.
6. Click **Finish**.

   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. 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 stack details:
   a. Clicking on the switch name of the standalone Instant On 1960 Series switch on which the stack is to be created.
   b. Hover the cursor to the end of the row of the standalone 1960 switch stack , click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Stack Members** tab. Ensure that the Instant On 1960 switch to be added in the stack is listed in the device inventory as a standalone 1960 Series switch.
4. Click **Add Members**.
5. In the Add Devices window, select the Instant On 1960 Series switch you wish to add to the stack and then click **Add**.

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

Stack Details

The **Stack Details** page provides details of the selected stack comprising of at least two Instant On 1960 Series switches. Options are provided to add or remove an Instant On 1960 Series switch from the stack, and also to re-assign the role assigned to each switch in the stack. The **Stack** page displays every device in the stack sorted by their role, namely, Conductor, Backup, and Member. Each Instant On 1960 switch is recognized by its current acting role, followed by the custom name set by the user. If a switch in the stack has

not been assigned a custom name, then its serial number will be used instead. The roles will appear in the screen based on the number of Instant On 1960 switches in the stack.

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

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 stack details:
   a. Clicking on the stack name.
   b. Hover the cursor to the end of the row of the switch stack, click the ••• button, and select **View Details** from the dropdown list.

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

- Overview
- Stack Members
- Ports
- Network Assignment
- Link Aggregation
- Network Tools
- Routes

Overview

The Overview tab of the Stack Details page consists of the following sections:

- Identification
- 802.1X Authentication
- Uplink
- Restart Stack
- Unstack
- Advanced Options

Identification

The **Identification** section provides the basic details of the selected switch stack, which includes the switch stack name, status, and health. To view the details of the switch, follow these steps:

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 stack details:
   a. Clicking on the stack name.
   b. Hover the cursor to the end of the row of the switch stack, click the ••• button, and select **View Details** from the dropdown list.

   The **Overview** > **Identification** section displays the following details:
   - **Name**–Denotes the device name specified by the administrator or the Serial Number of the device. The maximum number of characters supported is 32.

To reset the switch stack name to its default name, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom device name is assigned.

- **Health**–Displays the health status of the stack:
  - Good–Indicates that the health of the stack is good.
  - Fair–Indicates the health of the stack is fair.
  - Poor–Indicates the health of the stack is poor.
- **State**–Denotes if the device is Online, Offline, Synchronizing, Rebooting, and Updating.
- **Online Since**–Denotes the time duration for which the device has been online.

3. The **Locator Light** setting is used to locate your device when there are many devices in the site. Slide the **Locator Light** toggle switch to right ( ) to turn on the locator light in the all the devices in the stack. The locator light will be active for 30 minutes after you turn on the toggle switch. The light is turned off by default.
4. To view the device in the topology view, click the **View in topology** link.

802.1X Authentication

Allows you to select the RADIUS profile for the device.

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.

Click **View Details**, to view and edit an existing RADIUS profile.

Uplink

The uplink section displays the following information:

- **Device**– The name of the uplink device. You can click on the link to view the device details page.
- **Uplink Device IP Address**–The IP address of the uplink device.

Restart Stack

To restart the stack, follow these steps:

1. Under **Overview** > **Restart Stack**, click the **Restart** button.
2. Click **Restart Stack** in the popup window.

Unstack

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

1. Under **Overview** > **Unstack**, click **Unstack**. A popup appears on the screen requiring confirmation.
2. Click **Unstack**.

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

Advanced Options

The following selections are available under advanced options:

- Allow Routing Between Networks
- Allow Jumbo Frames

Routing

Configure routing on the Instant On switch. Routing is disabled by default. This feature is currently available only for Instant On 1930 Series and 1960 Series switches. To configure routing for the switch perform the following steps:

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 switch name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the dropdown list.
3. To enable routing on a switch or stack, under **Overview** > **Device Options** > **Advanced Options**, select the **Allow routing between networks** checkbox. To disable routing, deselect the checkbox.
4. When **Allow routing between networks** is selected, ● icon is displayed in the device details page under **Routes**, next to networks that can be routed. If the ● icon is not visible, it implies that routing is turned off for the network. Hover the cursor to the end of row, click the ••• button, and select **Enable Routing**.
5. To configure routing for a network, under **Routes**, hover the cursor to the end of the row, click the ••• button, and select **Change IP addressing** from the drop-down list:
   a. 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** – Select a subnet mask from the drop-down list.
   b. Click the **Change IP addressing** 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.
- For a 1960 Series stack, the routing is defined at the stack level. If the conductor switch goes offline, then the backup switch takes over the routing service for the stack.

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. Under **Overview** > **Advanced Options**, select the **Allow Jumbo frames** checkbox.
2. Click **Update**.

   The Instant On switch reboots automatically to apply the changes.

NOTE

Once the setting is enabled on a 1960 Series switch 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.

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 IP address directly from the device's page for both online and offline devices.

Follow these steps to reserve reserving an IP address from the device list:

1. Click the **Devices** ( ) tile on the Instant On web application home page or click , or click **Inventory** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation**.

   To remove it, select **Remove IP Address Reservation**.

Follow these steps to reserve reserving an IP address from the device details:

1. Select the device from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the device IP address directly from the details, select **Remove**.

NOTE

IP Reservation is only supported when Instant On functions as the DHCP server on the network, which occurs only when a Secure Gateway configured as a Wi-Fi Router is present at the site.

Stack Members

The **Stack Members** tab displays the list of Instant On 1960 Series switches that are connected in the stack. The following details are displayed:

Table 35: *Stack Details*

Category	Description
Device	Displays the name of the Instant On device set by the administrator.
Health	Displays the health status of the Instant On devices connected at the site: ■ Good – Indicates that the health score is good. ■ Fair – Indicates the health score is fair. ■ Poor – Indicates the health score is poor.
State	Denotes the state of the Instant On device, such as Online, Offline, Restarting, Updating, or Synchronizing.
State Duration	Denotes the amount of time the device has been connected to the current state.
Type	Denotes the type of Instant On device - AP, switch, or stack.
Model	Displays the model type of the Instant On device.
MAC Address	Displays the MAC address of the Instant On device.

Category	Description
IP Address	Displays the IP address currently used by the Instant On device.
Role	Denotes the role assigned to the Instant On 1960 switch in the stack. ■ **Conductor**–The Conductor is the Instant On 1960 Series switch on which the stack is created. ■ **Backup**–Denotes the secondary Instant On 1960 Series switch which is configured in the stack. The Backup switch takes over the operations when the Conductor switch is offline. ■ **Member**–Denotes the third or fourth Instant On 1960 Series switch which is part of the stack.
Clients	Denotes the number of clients connected to the Instant On device.

Identification

The **Stack Members** > **Identification** section provides the basic details of the selected switch, which includes the switch name, status, and health. For more information, see Identification.

Connectivity

The **Stack Members** > **Connectivity** section allows you to configure the IP assignment for the Instant On switch. For more information, see Switch Details.

Hardware

The **Stack Members** > **Hardware** section displays the details pertaining to the switch hardware connected as a member in the stack. For more information, see Switch Details.

Power over Ethernet

The **Stack Members** > **Power over Ethernet** section displays the local network IP of the Instant On 1960 Series switches in the stack.

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

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

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

Restart Member

To restart a member of the switch stack, follow these steps:

1. Under **Stack Members**, follow one of these steps:
   a. Clicking on the switch name of the standalone Instant On 1960 Series switch on which the member should be restarted.
   b. Hover the cursor to the end of the row of the standalone 1960 switch device, click the ••• button, and select **Restart** from the drop-down list. You can also select **View Details** and click **Restart** next to the **Restart Member**.
2. Click **Restart Member** in the popup window that appears on the screen.

Unstack Member

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

1. Under **Stack Members**, follow one of these steps:
   a. Clicking on the switch name of the Instant On 1960 Series member switch.
   b. Hover the cursor to the end of the row of the 1960 switch stack member, click the ••• button, and select **Unstack** from the drop-down list. You can also select **View Details** and click **Unstack** next to the **Unstack**.

   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.
2. Click **Unstack** from the **Unstack Member** popup window.

   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.

Change Roles

The **Change Roles** button provides an option to change the roles assigned to each Instant On 1960 Series switch in the stack.

Follow these steps to change the role of the switches in the stack:

1. In the **Stack Members** screen, click the **Change Roles** button.
2. Select a switch from each of the following dropdown lists to set the role:
   a. Conductor
   b. Backup
   c. Member
3. Click **Change Roles**.

Ports

The ports are visually represented on the page in the same manner as the actual physical ports on the device. Each port is numbered according to the port number on the switch and displays its current status. Select a port to open the port configuration. When a port is selected the following options are displayed:

- Name of the port. The default name of the port is port <selected port ID number>.
- **Enabled**–Select the checkbox to enable the port. To disable the port, unselect the check-box.
- **Status**–Status of the port.
- **Use Port Profile**–Allows you to assign a port profile to the selected port.
- **Port Profile**–On enabling **Use Port Profile**, the **Port Profile** field is displayed.

  From the Port Profile drop-down list, select either an existing port profile or create a new port profile.
  For more information on creating a port profile, see Creating a Port Profile.
  After a port profile assigning, **View Port Profile** is displayed. On clicking the **View Port Profile**, opens the port profile detail panel on the left.
  Click **View Details**, to navigate to the port profile configuration page.

NOTE

If a port profile is assigned, then the **Security**, **Authentication, Power Management** sections are not displayed. These parameters are configured in the port profile.

NOTE

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

Security

The security section consists of the following options:

- **Untrusted Port Protections (DHCP and ARP)**–Enable this option when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. This setting is enabled by default. For more information, see Security.
- **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** 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:

NOTE

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.

Included networks

Select the following options:

- **Untagged Default Network**—This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged 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 Access

Under **Ports** > **Port Access**, select the **Specific Clients** checkbox to allow the port to connect to specific clients.

Port Options

Port Options 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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Port Usage

Port Usage option displays the total accumulated data over the past 24-hour period. The data volume is displayed in **bytes**.

The configurations displayed under **Power Management** are:

- **Downloaded**–displays the total accumulated download data over the previous 24-hour period.
- **Uploaded**–displays the total accumulated upload data over the previous 24-hour period.

Port Usage option includes the total number of packets processed during the 24-hour period.

- **pkts** for values less than 1,000,000 packets. Values between 1,000 and 999,999 packets represents standard decimal notation (i.e. 1.5 pkts for 1,500 packets).
- **M pkts** for values from 1,000,000 up to (but not including) 1,000,000,000 packets.
- **G pkts** for values of 1,0

Clients and Devices

- **Specific Clients**–This checkbox appears under **Ports** > **Port Access** and allows you to lock the port and stop new devices from joining the port. When this checkbox is not selected, the port is locked, and all clients connected to the port are allow-listed and granted access to the port while new clients are blocked. Select the checkbox to unlock the port and allow new devices to connect. This option is unavailable on ports in which Instant On devices are connected. This option is displayed when clients and devices are connected to the port.

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.

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

Power Management

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

- **Power Allocation**–Select either one of the following options to configure a power supply policy for the port:
  - **Usage(default)** – The power allocated to the port is based on usage and is unrestricted.
  - **Class** – The power allocated to the port is based on the PoE standard of the device. The power class of devices are categorized as follows:

Table 36: *Power Class of Devices*

Class	Maximum Power from PSE
Class 0	15.4 Watts
Class 1	4 Watts

Class	Maximum Power from PSE
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.

- **Power Schedule**–Select this checkbox to enable power schedule on the port. The PoE supply to the port is determined by the power schedule defined. To change the power schedule, click on **View power schedule**. For more information on configuring **Power Schedule**, see Power Management.

Network Assignment

The **Network Assignment** tab displays the current mapping of the switch ports to a specific VLAN ID. You can also select a member of the stack from the **Stack Member** drop-down and assign a specific VLAN ID for its switch ports. 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.

Included networks

Select the following options:

- **Untagged Default Network**–This is the default setting. The port receives and sends traffic from the default network without using a VLAN tag. To custom map the port to an untagged VLAN, click the **Untagged Network** drop-down list and select a network from the list. Only one untagged network can be assigned to a port at a given time.
- **Tagged 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.

Link Aggregation

The **Link Aggregation** tab for a stack provides options to configure link aggregation groups for each device in the stack. Link aggregation configuration depends on the number of ports available on the switch. Instant On currently supports switches with the following number of ports:

Table 37: *Switch Ports Aggregation*

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

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

1. Click the **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 stack details:
   a. Clicking on the stack name.
   b. Hover the cursor to the end of the row of the switch stack, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Link Aggregation** tab.
4. Under **Stack Member**, click the drop-down and select one of the 1960 Series switches added in the stack.
5. Click **Create**.
6. Under **Identification**, configure the following:
   - **Name**–Provide a custom name for the Link aggregation in the text field.
   - **Enabled**–Select the checkbox to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. Unselect the checkbox to disable the LACP ports.
   - **Port Members**–Select the ports to add as members of the link aggregation. The list of selected port members is displayed.

     To assign a port profile, enable the **Use Port Profile** option. From the **Port Profile** drop-down list, select an existing port profile or create a new one.
     For more information on creating a port profile, see Creating a Port Profile.
     Once a port profile is assigning, the **View Port Profile** is displayed. When you click the **View Port Profile**, he port profile details panel opens on the left.

     To modify the configuration, click **View Details** to navigate to the port profile configuration page.

NOTE

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

7. Under **Link Aggregation**, you must select either **Static (default)** or **LACP** as the aggregation type.

8. This is an option settings. Under **Security** > **Port Security**, select **DHCP and ARP Port Protections (Untrusted Port)** or **Port Isolation (Protected Port)**.
9. Under **Security** > **Spanning Tree Protections**, you must select one option from the list of Spanning Tree Protection options. The list of options are:
   - **No spanning tree protections (default)**
   - **Block spanning tree protocol (BPDU guard)**
10. Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.
11. Click **Create**.

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

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

Identification

The **Identification** section displays the following information:

- **Name**–Provide a custom name for the Link aggregation in the text field.
- **Enabled**–Select the checkbox to enable the LACP ports. It indicates that the port members of the link aggregation are available for devices to connect. select the checkbox to disable the LACP ports.
- **Port Members**–Displays the list of ports that are currently members of the link aggregation. When you select a port that is not part of the existing link aggregation, a new link aggregation must be created. Each device port can belong to only one link aggregation at a time.

  To assign a port profile, enable the **Use Port Profile** option. From the **Port Profile** drop-down list, select an existing port profile or create a new one.
  For more information on creating a port profile, see Creating a Port Profile.
  Once a port profile is assigning, the **View Port Profile** is displayed. When you click the **View Port Profile**, he port profile details panel opens on the left.

  To modify the configuration, click **View Details** to navigate to the port profile configuration page.

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

Link Aggregation

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

The security section consists of the following options:

- **Untrusted Port Protections (DHCP and ARP)**–Enable this option when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network. This setting is enabled by default. For more information, see Security.
- **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.

In **Security** > **Spanning Tree Protections**, select an option listed under **Spanning Tree Protections** 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 **Spanning Tree Protections** section consists of the following options:

- **No spanning tree protections (default)**–Disables spanning tree protection. This option is selected as the default value.
- **Block spanning tree protocol (BPDU guard)**–Stops the incoming and outgoing BPDUs received on the port.

Port Access

Under **Ports** > **Port Access**, select the **Specific Clients** checkbox to allow the port to connect to specific clients.

During discovery, port restrictions on the link aggregation are temporarily disabled to enable new clients and devices to connect.

To add clients, complete the following steps:

1. Select the **Specific Clients** checkbox.
   Allowed Clients and Devices option is displayed.
2. Click **Add**.
   The **Select Clients and Devices to Allow**, window is displayed.
3. Click **Search**, to detect new devices.
4. Select the devices, and click **Add Clients and Devices**.

Port Options

Port Options 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).

Under **Port Options** > **Advanced Options**, select the **Limit Broadcast and Multicast Storms** checkbox to limit excessive broadcast and multicast traffic.

Clients and Devices

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

Delete Link Aggregation

To delete the link aggregation, complete the following steps:

1. Click **Delete**.
2. In the **Delete Link Aggregation** pop-up, confirm the delete operation.

Network Tools

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

Start Port Mirroring

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

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

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

1. Click the **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 stack details:
   a. Clicking on the stack name.
   b. Hover the cursor to the end of the row of the switch stack, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click **Start** next to **Start Port Monitoring**.
5. Under **Select Mirroring Source > Stack Member**, select a stack member.
6. Under **Source**, select one of the following:
   a. **Ports**–Select the port(s) to be used as the source port(s).
   b. **Network**–Select one of the available networks from the drop-down list.
7. Click **Next**.
8. Based on your selection above, you will need to select the **Source Ports** or **Source Networks** from which the traffic should be mirrored.
9. Select one of the following as the **Source** and click **Next**:
   a. Transmit and receive
   b. Transmit
   c. Receive

10. 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
11. Click **Start mirroring** to initiate the mirroring of the packets sent from the source to the destination.

    To stop the mirroring, click **Stop mirroring** at anytime

Test Connectivity

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

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

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 stack details:
    a. Clicking on the stack name.
    b. Hover the cursor to the end of the row of the switch stack , click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Connectivity**.
5. In the **Select Source Member** page, click on the radio button next to an Instant On switch stack member from the list to run the connectivity test.

    Only active devices of a site can be selected in this field.
6. Click **Next**.
7. In the **Set Network Destination** page, enter the hostname or IP address of the device to which the source device should connect.
8. Click **Next**. The Network tests will be executed and displayed for every device in the stack.

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

Table 38: *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>

Connectivity Rating	Roundtrip Time	Test Results Format
		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 followed by a switch 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. 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 switch name.
   b. Hover the cursor on the switch name, to the right-hand corner of the row, click the ••• button, and select **View Details** from the dropdown list.
3. Click the **Network Tools** tab.
4. Click the **Test** button, next to **Test Cable**.
5. In the **Select Source Member** page, select a stack member on which you want to run the cable test.
6. Click **Next**.
7. In **Select Port to Test** page, select the port on which you want to run the cable test.
8. Click **Next**. Initiates the cable test for the selected port.

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

Table 39: *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.

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 Modifying an 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.

Chapter 10
Networks

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

When a gateway is present in the topology, the Networks tile is split into two distinct sections, LAN and WAN. The LAN regroups wired and wireless networks on the LAN side while the WAN section lists the interfaces used to connect to the Internet. You can also create a VPN network which allows clients to establish remote connections through a VPN tunnel.

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

- LAN
- WAN
- WAN Redundancy
- Guest Portal

To view the **Networks > Overview** or **LAN** page, click the **Networks** tile on the Instant On home page, or click **Networks** from the navigation pane on the left:

When a security gateway is deployed at the site, then the **Overview** tab is renamed to the **LAN** tab.

Table 40: *Network Information*

	Description
Network	Identifies the Instant On network used to connect computers, tablets, or phones together. The network name is also used as the Wi-Fi identifier.
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 inactive.
State	Shows the status of the network, whether Active or Inactive.
Type	Indicates the type of network. The networks can be Wired, Wireless, or VPN.
Usage	Indicates the type of network traffic or user group, such as Employee, Guest, Voice, or Remote.
VLAN (Wired Network)	Wired Networks: Shows the VLAN ID that was assigned for the network. Wireless Network: Shows the network name of the network. VPN network: No value is displayed.
IP Subnet	Displays the IP Subnet value only when a Wi-Fi router or Gateway is present at the site.

	Description
Clients	Displays the number of clients currently connected to the network. For more information on each individual client, see Managing Clients
24-hour Usage	Displays the volume of data, in bytes, transferred in the network during the last 24-hour period.

Hover the cursor over a network, click the ••• button and select one of the following options:

- **View Details**–Allows you to view the details of the network.
- **Deactivate**–Deactivates the network.
- **Delete**–Deletes the network.

Refer to the following topics to create a wireless, wired, VPN network, or WAN connection:

- Configuring a Wired Network
- Configuring a Wireless Network
- Configuring a VPN Network
- Creating a Secondary WAN

Creating a Network

To create a network, perform the following steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, click **Create Network**.
3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the network.
   b. **Network Type**–Select **Wired**, **Wireless**, or **VPN** option. The wireless option appears only when your site has both wired and wireless networks. The VPN option appears only when a secure gateway is deployed at a site. A site supports a maximum of 1 VPN network.
   c. Click **Next**.

Refer to the following topics to create a wireless, wired or VPN network:

- Configuring a Wired Network
- Configuring a Wireless Network
- Configuring a VPN Network

Configuring a Wired Network

The wired network is suitable for users whose network infrastructure includes if Instant On switches and, optionally, a secure gateway.

During site creation, wired network is created based on the devices discovered . If a switch is discovered, a default wired network is automatically created. The default network has a management VLAN whose value is read-only. The default wired network that was created during initial setup cannot be deleted unless you choose

to delete the site entirely from your account. Once the initial setup is complete, you can use the following procedure to create up to a maximum of 22 wired networks for a site.

The following procedure creates a wired network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, click **Create Network**.
3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the wired network.
   b. **Network Type**–Select the **Wired** option. The wired option appears only when your site has both wired and wireless networks.
   c. Click **Next**.
4. Under **Network Usage**, select **Employee (default)** option.
5. Under **Properties** > **VLAN**, enter a new VLAN ID.
6. Under **Properties** > **Network Options**, enable the **IGMP Snooping** checkbox. 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. Disable this setting when experiencing problems with multicast applications. Select this checkbox to reduce traffic to registered multicast groups in the network.

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

7. Under **Security** > **Network Security**, enable the **DHCP and ARP Attack Protections** checkbox. Enable this setting when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network.

DHCP and ARP Attach Protections does not apply to the Instant On 1830 switch series.

8. Click **Create Network**.

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.

To create a Guest Wired Network, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, click **Create Network**.
3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the wired network.
   b. **Network Type**–Select the **Wired** option. The wired option appears only when your site has both wired and wireless networks.
   c. Click **Next**.
4. Under **Network Usage**, select the **Guest** option.
5. Under **Properties** > **VLAN**, enter a new VLAN ID.
6. Under **Properties** > **Network Options**, enable the **IGMP Snooping** checkbox. 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. Disable this setting when experiencing problems with multicast applications. Select this checkbox to reduce traffic to registered multicast groups in the network.

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

7. Under **Network Properties** > **Network Usage**, select **Guest**, to indicate that the network is for guest users.
8. Under **Security** > **Network Security**, enable the **DHCP and ARP Attack Protections** checkbox. Enable this setting when untrusted devices are connected to the port. This setting in combination with Network Security configuration is used to prevent DHCP and ARP attacks on the wired network.

DHCP and ARP Attach Protections does not apply to the Instant On 1830 switch series.

9. Click **Create Network**.

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, select **Voice** under **Network Usage**.

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.

Configuring a Wireless Network

The wireless network allows users to configure both employee and guest networks.

Employee Network

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

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

To configure an employee network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.

2. Under **Networks** > **Overview**, click **Create Network**.
3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the employee network. This will also be broadcast as the SSID for the WLAN network.
   b. **Network Type**–Select the **Wireless** option. The wireless option appears only when your site has both wired and wireless networks.
   c. Click **Next**.
4. Under **Network Properties** > **Network Usage**, select **Employee**, to indicate that the network is for an enterprise.
5. Under **Network Password (PSK)**, enter a password of your choice in the **Network password** text box. This enables you to secure the network using a shared password (PSK).

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. 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.
7. On selecting **WPA2 Personal** or **WPA2 + WPA3 Personal Network** options, displays the **Network Password (PSK)** section. Under **Network Password (PSK)** > **Password**, you must set a password.
8. On selecting **WPA2 Enterprise** or **WPA2 + WPA3 Enterprise** options, displays the **Authentication** section. Under **Authentication** > **RADIUS Profile** drop-down list you must select either an existing RADIUS profile or create a new RADIUS profile.

   For more information on creating a radius profile, see Creating a RADIUS Profile.
9. On assigning a RADIUS profile, **View RADIUS Profile** is displayed.
10. Click **View RADIUS Profile**, opens the RADIUS profile detail's panel on the left.
11. Click **Next.**
12. Under **IP Assignment,** select either **Specific to This Network (default)** or **Same as a Local Network**.
    - For **Same as a Local Network (default)**, select a network from the **Wired Network** drop-down list.
    - For **Specific to This Network** enter the Base IP Address and select a subnet mask from the **Subnet Mask** drop-down list.
13. Click **Create Network**, to finish creating the Employee Network.

Guest Network

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

To create a Guest Network, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, click **Create Network**.

3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the guest network. This will also be broadcast as the SSID for the WLAN network.
   b. **Network Type**–Select the **Wireless** option. The wireless option appears only when your site has both wired and wireless networks.
   c. Click **Next**.
4. Under **Network Properties** > **Network Usage**, select **Guest**, to indicate that the network is for guest users.
5. Under **Security > Network 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 Configuring a Wireless Network.
   - **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, click the **Guest portal** checkbox under **Network Options**.
7. Click **Next.**
8. Under **IP Assignment**, select either **Specific to This Network (default)** or **Same as a Local Network**.
   - For **Specific to This Network (default)** enter the Base IP Address and select a subnet mask from the **Subnet Mask** drop-down list.
   - For **Same as a Local Network**, select a network from the **Wired Network** drop-down list.
9. Click **Create Network**, to finish creating the Guest Network.

Configuring a 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.

To create a VPN network, follow these steps:

1. Click the **LAN** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **LAN**, click **Create Network**.

3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the VPN network.
   b. **Network Type**–Select the **VPN** option.
   c. Click **Next**.
4. Under **Network Properties** > **Listening Port**, 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**.

5. Click **Next**.
6. Under **IP Assignment** > **Network Address**, enter the IP 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. Click **Next**.
8. Under **Tunneled Destinations** > **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. You must select at least one network from the **Selected Networks** list.
9. Click **Create Network**.

   Once completed, the VPN network is created, and the corresponding policy is automatically generated to allow access to the selected destinations.

Modifying an Employee Network

To modify an employee network, perform the following steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the employee network from the list of **Networks**.

The following section provides details of the **Overview** tab.

Identification

The **Overview > Identification** setting allows you to change the name and status of the network. To modify the network name and status, perform the following steps:

1. Enter a new name under **Name** to change the employee network name.
2. Select the **Enabled** checkbox to activate the network. To disable the network, deselect the checkbox.

The **Identification** setting also displays the **Health, State**, and **Network Usage** details of the network.

Security

The **Security** setting allows you to configure **Network Security** and **Network Options.** To configure the security setting, perform the following steps:

1. 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.
2. On selecting **WPA2 Personal** or **WPA2 + WPA3 Personal Network** options, displays the **Network Password (PSK)** section. Under **Network Password (PSK)** > **Password**, you must set a password.
3. On selecting **WPA2 Enterprise** or **WPA2 + WPA3 Enterprise** options, displays the **Authentication** section. Under **Authentication** > **RADIUS Profile** drop-down list you must select either an existing RADIUS profile or create a new RADIUS profile.

   For more information on creating a radius profile, see Creating a RADIUS Profile.
4. On assigning a RADIUS profile, **View RADIUS Profile** is displayed.
5. Click **View RADIUS Profile**, opens the RADIUS profile detail's panel on the left.

Deactivate Network

If you choose to make the network inactive temporarily and prevent clients from connecting to it, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, follow one of the following methods:
   a. Clicking on the network name. The Network details page is displayed. Under **Security** > **Network Options**, you have the option to hide the SSID for the network, by clicking the **Hidden Network** checkbox. To activate the network once again, unselect the **Hidden Network** checkbox.
   b. Hover the cursor over the network you want to deactivate temporarily, click the ••• button, and select **Deactivate** from the drop-down list. To activate the network once again, follow the same procedure and select **Activate** from the drop-down list.

The Management Network cannot be deactivated.

Delete Network

Follow these steps to delete a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.

2. Under **Networks** > **Overview**, use one of the following methods to view the network details:
   a. Click the Network name and follow Step 3.
   b. Hover the cursor over the network you want to delete, click the ••• button, and select **Delete** from the drop-down list.
3. Click the **Delete** button, next to **Delete Network**.
4. Click **Delete Network** from the popup window.

IP Assignment

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:

- **Same as a 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 **Wired 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.
  On enabling the **Specific to this network** option, you can configure the **Automatic IP Address Assignment** section.

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 IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
2. Click **Update**.

Network Assignment

The **Network Assignment** page allows you to configure the radio settings for the wireless network and also to allow or deny a wireless network on a specific device (access point only).

Radio

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

To configure the radio frequency, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network Assignment** tab.
4. Under **Radio**, select the radio frequency. The available frequencies are:
   - **2.4 GHz**–The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
   - **5 GHz**–The AP will broadcast the wireless network only on the 5 GHz radio frequency.
   - **6 GHz**–The AP will broadcast the wireless network only on the 6 GHz radio frequency.

WPA3 or OWE (Enhanced Open for Guest Networks) security is required for the wireless network to operate in the 6 GHz radio frequency.

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** checkbox. By default, 802.11b rates are disabled for all the networks. To enable this option, select the checkbox. This allows 2.4 GHz clients that are far away to connect to the network by enabling lower data rates.

Enabling this option might slow down the network performance.

Access Point

This section displays the list of access points that are deployed at the site.

Under **Access Point** > **Devices**, select the checkboxes next to all the access points that can broadcast the network and allow client connections to the wireless network.

Schedule

The **Networks** > **Schedule** page displays the details of the scheduled policy applied on the network, with a link to the applied policy. If a policy is not applied, you can click on the **View policies** link to see the list of available policies.

For more information on network schedules and application access restrictions, see Policies.

Access Control

The **Access Control** tab allows you to configure network access restrictions.

Network Access

The **Access Control** section in the Instant On web application allows you to configure network access restrictions for wired or wireless clients based on IP destination addresses.

The following procedure configures network access restrictions on a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Access Control** tab.
4. Under **Network Access** > **Access Restrictions**, select the **Network Destinations** checkbox.
5. Under **Allowed Destinations**, select one of the following:
   a. **Internet**–Select this checkbox to allow the clients to access the internet. This setting is always enabled by default on bridged networks.
   b. **Same Network**–Select this checkbox to allow clients to receive an IP address on the same subnet as the assigned network. This option is available only on networks that use a primary Wi-Fi router as a gateway where the Internet option is not a mandatory setting in **Network Destinations**.
   c. **Specific IP Address**–Select this checkbox to allow the client to access specific resources using an IP address.
      i. Under **Allowed Destination IP Addresses**, click **Add**.
      ii. In the **Add Allowed IP Address** popup window, enter a destination IP address to allow on the selected network.
      iii. Click **Add IP Address**.
6. Click **Update**.

Specific 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. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network that you want to delete, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Access Control** tab.
4. Under **Network Access** > **Access Restrictions**, select the **Specific Clients** checkbox.
5. Under **Allowed Clients**, click **Add**.
6. Click **Search**. The Instant On devices begin scanning for nearby clients that are available to connect to the network.

7. 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.

8. Click **Update**.

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.

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.

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.

Multicast Optimizations

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

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

To configure multicast optimization, follow these steps:

1. Under **Wireless Options** > **Quality of Service**, select the **Multicast Optimizations** checkbox.
2. Click **Update**.

Multiple Clients Optimizations

This setting is available only when the Wi-Fi 6 toggle switch is enabled. This feature improves the channel efficiency when multiple Wi-Fi 6 clients are connected by enabling OFDMA. This setting is disabled by default on the network, select the **Multiple Client Optimization (OFDMA)** checkbox under **Wi-Fi Options** to enable this feature.

Modifying a Guest Network

To modify a guest network, perform the following steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the guest network from the list of **Networks**.

The following section provides details of the **Overview** tab.

Identification

The **Overview > Identification** setting allows you to change the name and status of the network. To modify the network name and status, perform the following steps:

1. Enter a new name under **Name** to change the guest network name.
2. Select the **Enabled** checkbox to activate the network. To disable the network, deselect the checkbox.

The **Identification** setting also displays the **Health, State**, and **Network Usage** details of the network.

Security

The **Security** setting allows you to configure **Network Security** and **Network Options.** To configure the security setting, perform the following steps:

1. Under **Security > Network 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.
2. Under **Security > Network Options**, click the **Guest portal** checkbox.
3. Click **Update**. The changes are saved and a **View guest portal** link is generated.
4. Click the **View guest portal** link. You will be redirected to the **Networks** > **Guest Portal** screen.

Wi-Fi Enhanced Open (OWE)

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

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

1. Ensure that the **Security** type for the Guest network is set to **Open**.
2. Select the **Wi-Fi Enhanced Open** radio button to enable the feature.
3. Click **Save**.

Deactivate Network

If you choose to make the network inactive temporarily and prevent clients from connecting to it, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, follow one of the following methods:
   a. Clicking on the network name. The Network details page is displayed. Under **Security** > **Network Options**, you have the option to hide the SSID for the network, by clicking the **Hidden Network** checkbox. To activate the network once again, unselect the **Hidden Network** checkbox.
   b. Hover the cursor over the network you want to deactivate temporarily, click the ••• button, and select **Deactivate** from the drop-down list. To activate the network once again, follow the same procedure and select **Activate** from the drop-down list.

The Management Network cannot be deactivated.

Delete Network

Follow these steps to delete a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, use one of the following methods to view the network details:
   a. Click the Network name and follow Step 3.
   b. Hover the cursor over the network you want to delete, click the ••• button, and select **Delete** from the drop-down list.
3. Click the **Delete** button, next to **Delete Network**.
4. Click **Delete Network** from the popup window.

Configuring Guest Portal

Guest portal can be accessed using a web browser. 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 web application, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select one of the active Guest Network connections.
3. Under **Security** > **Network Options**, click the **Guest portal** checkbox.
4. Click **Update**. The changes are saved and a **View guest portal** link is generated.
5. Click the **View guest portal** link. You will be redirected to the **Networks** > **Guest Portal** screen.
6. Under **Type**, select one of the following options:
   - **Internal**
   - **External**

7. Based on your selection, enter values in the required fields. For more information, see:
   a. Configuring Internal Captive Portal
   b. Configuring External Captive Portal
8. Click **Apply changes**.

Configuring Captive Portal

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

- Configuring Internal Captive Portal
- Configuring External Captive Portal

Configuring Internal Captive Portal

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

Table 41: *Internal Captive Portal Configuration*

Parameter	Description
Page Content	■ **Logo / Image**–Click the image icon to browse and upload an image from your device. ■ Ensure that you upload the image only in the png, jpg, gif, or bmp formats. ■ **Background Color**–Click the box to view the color palette and choose a color for the background of the internal captive portal page.
Welcome Message	Design the welcome message by updating the following fields: ■ **Welcome Text**–Enter the text for the welcome message. Example: Welcome to Guest Network. ■ **Font Color**–Click the box to view the color palette and choose a color for the font. ■ **Font Family**–Choose a font type from the drop-down list. ■ **Font Size**–Drag the slider to set the size of the font.
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 Color**–Click the box to view the color palette and choose a color for the font. ■ **Font Family**–Choose a font type from the drop-down list. ■ **Font Size**–Drag the slider to set the size of the font. ■ **Terms and Conditions Text**–Enter or paste your terms and conditions in the text box. ■ **Agreement Text**–Enter a comment in the text box. For example: **I agree to the terms and conditions**. ◦ **Font Color**–Click the box to view the color palette and choose a color for the font. ◦ **Font Family**–Choose a font type from the drop-down list.
Accept Button	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

Table 41: *Internal Captive Portal Configuration*

Parameter	Description
	clicking the accept button. ■ **Background Color**–Tap the box to view the color palette and choose a color for the background. ■ **Font Color**–Click the box to view the color palette and choose a color for the font. ■ **Font Family**–Choose a font type from the drop-down list. ■ **Border Radius**–Drag the slider to set the border radius of the accept button.

Configuring External Captive Portal

You can configure an external captive portal for your guest network by configuring RADIUS authentication and accounting parameters.

Customizing the Captive Portal Page

To customize the external captive portal, follow these steps:

1. Enter the **Portal URL** for the External Captive Portal page.
2. Specify a **Redirect URL** if you want to redirect the users to another URL.
3. Under **Authentication**, select 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 acknowledgment**–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.

4. Configure the following external captive portal parameters, based on your selection in Step 3.
   In the **RADIUS Profile** drop-down list you must select either 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**, displays the RADIUS profile configuration page.

Table 42: *External Captive Portal Configuration Parameters*

Parameter	Description
Require RADIUS-Message-Authenticator	Select this checkbox to enable the AP to discreetly discard packets from the RADIUS servers that do not have the Message Authenticator. This parameter is available only for User authentication (default) option.
RADIUS Accounting	Select the RADIUS accounting checkbox, 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. This parameter is available only for User authentication (default) option.
Primary RADIUS Server	Configure a primary RADIUS server for authentication by updating the following fields:

Table 42: *External Captive Portal Configuration Parameters*

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

Table 42: *External Captive Portal Configuration Parameters*

Parameter	Description
	▪ **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 Assignment**–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. This parameter is available only for User authentication (default) option.
Allowed Destinations	Bypasses the guest portal and uses one or more of the following Social Network destinations, as selected by the user. ▪ Facebook ▪ X ▪ LinkedIn ▪ Weibo ▪ WeChat This parameter is available for both User authentication (default) and Guest portal acknowledgment options.
Allowed Domains	Allows access to social network domains. Click **Add** and enter a new **Domain Name** in the **Add Allowed Domain** popup window. This allows unrestricted access to additional domains. This parameter is available for both User authentication (default) and Guest portal acknowledgment options.

5. Click **Update**.

IP Assignment

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:

- **Same as a 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 **Wired 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.

On enabling the **Specific to this network** option, you can configure the **Automatic IP Address Assignment** section.

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 IP address of the primary DNS server.
     - **Secondary DNS Server**–Enter the IP address of the secondary DNS server.
2. Click **Update**.

Network Assignment

The **Network Assignment** page allows you to configure the radio settings for the wireless network and also to allow or deny a wireless network on a specific device (access point only).

Radio

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

To configure the radio frequency, follow these steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network Assignment** tab.
4. Under **Radio**, select the radio frequency. The available frequencies are:
   - **2.4 GHz**–The AP will broadcast the wireless network only on the 2.4 GHz radio frequency.
   - **5 GHz**–The AP will broadcast the wireless network only on the 5 GHz radio frequency.

- **6 GHz**–The AP will broadcast the wireless network only on the 6 GHz radio frequency.

WPA3 or OWE (Enhanced Open for Guest Networks) security is required for the wireless network to operate in the 6 GHz radio frequency.

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** checkbox. By default, 802.11b rates are disabled for all the networks. To enable this option, select the checkbox. This allows 2.4 GHz clients that are far away to connect to the network by enabling lower data rates.

Enabling this option might slow down the network performance.

Access Point

This section displays the list of access points that are deployed at the site.

Under **Access Point** > **Devices**, select the checkboxes next to all the access points that can broadcast the network and allow client connections to the wireless network.

Access Control

The **Access Control** tab allows you to configure network access restrictions.

Network Access

The **Access Control** section in the Instant On web application allows you to configure network access restrictions for wired or wireless clients based on IP destination addresses.

The following procedure configures network access restrictions on a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Access Control** tab.
4. Under **Network Access** > **Access Restrictions**, select the **Network Destinations** checkbox.
5. Under **Allowed Destinations**, select one of the following:
   a. **Internet**–Select this checkbox to allow the clients to access the internet. This setting is always enabled by default on bridged networks.
   b. **Same Network**–Select this checkbox to allow clients to receive an IP address on the same subnet as the assigned network. This option is available only on networks that use a primary Wi-Fi router as a gateway where the Internet option is not a mandatory setting in **Network Destinations**.
   c. **Specific IP Address**–Select this checkbox to allow the client to access specific resources using an IP address.
      i. Under **Allowed Destination IP Addresses**, click **Add**.
      ii. In the **Add Allowed IP Address** popup window, enter a destination IP address to allow on the

selected network.

iii. Click **Add IP Address**.

6. Click **Update**.

Specific 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. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network that you want to delete, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Access Control** tab.
4. Under **Network Access** > **Access Restrictions**, select the **Specific Clients** checkbox.
5. Under **Allowed Clients**, click **Add**.
6. Click **Search**. The Instant On devices begin scanning for nearby clients that are available to connect to the network.
7. 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.

8. Click **Update**.

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

Schedule

The **Networks** > **Schedule** page displays the details of the scheduled policy applied on the network, with a link to the applied policy. If a policy is not applied, you can click on the **View policies** link to see the list of available policies.

For more information on network schedules and application access restrictions, see Policies.

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

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.

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.

Multicast Optimizations

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

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

To configure multicast optimization, follow these steps:

1. Under **Wireless Options** > **Quality of Service**, select the **Multicast Optimizations** checkbox.
2. Click **Update**.

Multiple Clients Optimizations

This setting is available only when the Wi-Fi 6 toggle switch is enabled. This feature improves the channel efficiency when multiple Wi-Fi 6 clients are connected by enabling OFDMA. This setting is disabled by default on the network, select the **Multiple Client Optimization (OFDMA)** checkbox under **Wi-Fi Options** to enable this feature.

Modifying a Wired Network

To modify a wired, perform the following steps:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the wired network from the list of **Networks**.

The following section provides details of the **Overview** tab.

Identification

The **Overview > Identification** setting allows you to change the name and status of the network. To modify the network name and status, perform the following steps:

1. Enter a new name under **Name** to change the main network name.
2. Select the **Enabled** checkbox to activate the network. To disable the network, deselect the checkbox.

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

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

The **Identification** setting also displays the **Health, State**, and **Network Usage** details of the network.

Important Points to Note:

- Deactivating the wired network means that no wired network station will be able to connect. The network will be shut down at the port level and would not be able to pass traffic anymore. The network is removed from all the wired ports.

- Deactivating a wired-network that has one or more associated wireless-network(s) displays a dialog box indicating that all the wireless networks and associated clients will be disconnected from the network. Click **Deactivate** to continue this operation.
- Re-activating a wireless-network on a wired-network that was previously deactivated displays a dialog box indicating that the associated wired-network will also be activated. Click **Activate** to continue this operation.
- Re-activating a wired-network that has one or more associated wireless-networks, activates the associated-wireless networks as well. Click **Activate** to continue this operation.

Properties

The Properties setting allows you to configure the VLAN and network options. To modify these settings, perform the following steps:

1. Enter a new **VLAN** to change the VLAN ID.
2. Under **Network Options**, select the following options:
   a. **IGMP snooping**–Use this checkbox to enable or disable IGMP Snooping.
   b. **Guest Portal**–Use this checkbox to configure a guest portal for guest users.

Security

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

DHCP Snooping

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

ARP Attack Protection

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

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

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, click **Create Network**.
3. Under **Network Identification**, configure the following:
   a. **Name**–Enter a name for the employee network. This will also be broadcast as the SSID for the WLAN network.
   b. **Network Type**–Select the **Wired** option. The wireless option appears only when your site has both wired and wireless networks.
   c. Click **Next**.
4. Under **Network Properties** > **VLAN**, enter a new VLAN ID.
5. Under **Network Properties > Security**, enable the **DHCP and ARP Attack Protections** checkbox.

6. 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.
7. Click **Update** to save the configurations.

Delete Network

Follow these steps to delete a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Under **Networks** > **Overview**, use one of the following methods to view the network details:
   a. Click the Network name and follow Step 3.
   b. Hover the cursor over the network you want to delete, click the ••• button, and select **Delete** from the drop-down list.
3. Click the **Delete** button, next to **Delete Network**.
4. Click **Delete Network** from the popup window.

Energy Efficient Ethernet

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

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

IP Assignment Reservation

The **IP assignment** configuration in the Instant On web application allows you to configure internal or external DHCP and NAT for clients on employee networks or guest networks. 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 Client and Reserving an IP Address for a Device.

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 clients 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**.

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.

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.

Clients with MAC randomization enabled are not supported by IP reservation, as the feature requires a fixed MAC address to reserve an IP.

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**.

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.

Follow these steps to configure IP address reservation:

1. Click the **IP Assignment** tab.
2. Under **IP Address Reservation**, click **Add**. The list of clients connected to the site are displayed along with their IP addresses.
3. Click on the client or device to reserve its DHCP IP address. The device and its IP address will be added to the **IP address reservations** list.

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

4. Click **Add**.

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.

Network Assignment

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. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the wired network name.
   b. Hover the cursor over the wired network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Network assignment** tab.
4. Under Network Assignment, select an Instant On Router or Switch from the **Devices** drop-down list, and click on one of the following options, to assign the network VLAN in bulk to all the ports:
   - **Remove All**–Removes the VLAN from all the ports.
   - **Tag All**–Assigns and tags the VLAN of a particular wired network to all the ports of the selected Instant On device.
   - **Untag All**–Assigns and untags the VLAN of a particular network to all the ports of the selected Instant On device.

NOTE

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 displayed with a **T** (tagged), or **U** (untagged) decorator subsequently every time you click on a particular port.

5. Click **Update**.

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.

Access Control

The **Access Control** section in the Instant On web application allows you to configure network access restrictions for wired or wireless clients based on IP destination addresses.

The following procedure configures network access restrictions on a network:

1. Click the **Networks** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.

2. In the **Networks** > **Overview** screen, select one of the following methods to view the network details:
   a. Clicking on the network name.
   b. Hover the cursor over the network, click the ••• button, and select **View Details** from the drop-down list.
3. Click the **Access Control** tab.
4. Under **Network Access** > **Access Restrictions**, select the **Network Destinations** checkbox.
5. Under **Allowed Destinations**, select one of the following:
   a. **Internet**–Select this checkbox to allow the clients to access the internet. This setting is always enabled by default on bridged networks.
   b. **Same Network**–Select this checkbox to allow clients to receive an IP address on the same subnet as the assigned network. This option is available only on networks that use a primary Wi-Fi router as a gateway where the Internet option is not a mandatory setting in **Network Destinations**.
   c. **Specific IP Address**–Select this checkbox to allow the client to access specific resources using an IP address.
      i. Under **Allowed Destination IP Addresses**, click **Add**.
      ii. In the **Add Allowed IP Address** popup window, enter a destination IP address to allow on the selected network.
      iii. Click **Add IP Address**.
6. Click **Update**.

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.

Modifying a VPN Network

To modify a VPN network, follow these steps:

1. Click the **LAN** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the VPN network from the list of **Networks**.

The VPN Network details page contains the following sections:

Identification

The **Identification** setting allows you to change the network name and enable or disable the VPN network. To modify these settings, perform the following steps:

1. Enter a new name under **Name** to change the VPN network name.
2. Select the **Enabled** checkbox to activate the network. To disable the network, deselect the checkbox.

The **Identification** setting also displays the **Health, State**, and **Network Usage** details of the network. For VPN networks, the **Network Usage** is displayed as Remote.

Properties

The **Properties** sections displays the following information:

- **Site hostname**–The site host name is automatically assigned by the system and displayed in a read-only format. It is unique to each site and registered under the system domain. This host name is used during client setup to securely connect to the gateway and access the VPN network.
- **Listening Port**–The listening port is displayed. The default port is 51820. You can update the value if needed.

Public Key

The **Public Key** section displays the cryptographic key associated with the VPN network.

You can perform the following actions:

- To copy the displayed public key to the clipboard, click the **Copy** button.
- To generate a new key, click the **Regenerate** button.

The Private key is auto-generated and not displayed on this page. Also, private keys are not stored on Instant On servers.

After changing any configuration on the VPN Network details page, click **Update** to save, or **Cancel** to discard them.

Delete Network

To delete the VPN network, click the **Delete** button next to **Delete Network**. Deleting the network disconnects all clients using the network,

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.

IP Assignment

The **IP Assignment** page displays the IP address allocation parameters for the VPN network.

To view the IP assignment details, follow these steps:

1. Click the **LAN** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the VPN network from the list of **Networks**.
3. Click the **IP Assignment** tab to view the following details:
   - **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.
   - **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** page 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.

The **Client Configurations** table displays the following information:

Table 43: *Client Configuration Details*

Field	Description
Client Configuration	Name of the client.
State	Indicates the current operation status of the client.
IP Address	Displays the IP address of the client. This field is auto-generated.

Hover the cursor over a client configuration, click the ••• button and select one of the following options:

- **View Details**–Allows you to view the details of the client configuration.
- **Enable**–Enables the client VPN configuration. This option is displayed when the client configuration is disabled.
- **Disable**–Disables the client VPN configuration. This option is displayed when the client configuration is enabled.
- **Delete**–Deletes the client configuration. Deleting the configuration will disconnect the client from the network.

Creating a Client Configuration

To create a client configuration, follow these steps:

1. Click the **LAN** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. Select the VPN network from the list of **Networks** for which you want to configure clients.

3. Click the **Client Configurations** tab, and click **Create Client Configuration**.
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 **Next**.
6. Under **Cryptographic Client Identity** > **Key Pairs Generation**, 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 enter the public key in the **Public Key (Base64)** field. The public key must be a valid Base64 -encoded string consisting of 44 characters.
7. Click **Create Client Configuration**.
   A pop-up window 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–Click the **Copy** button to copy the WireGuard configuration to the clipboard.
   - Download–Click the **Download** button to download the WireGuard configuration file.
8. Click **OK**.

Client Configuration Details

The Client Configuration details page contains the following sections:

- Identification
- Client Configuration Details
- Public Key
- Client Configuration

To view the details of the client configuration, follow these steps:

1. Click the **LAN** ( ) tile on the Instant On web application home page or click **Networks** > **LAN** from the navigation pane on the left.
2. Select the VPN network from the list of networks.
3. Click the **VPN Network** > **Client Configurations** tab.
4. Use one of the following methods to view the Client Configuration details:
   a. Clicking on the client name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

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.
- **Enabled**–Indicates whether the client configuration is enabled or not. Use the checkbox 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** button to generate a new WireGuard client configuration.

Delete Client

To delete a client, click the **Delete** button next to **Delete Client**. Deleting the client configuration will disconnect the client from 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 44: *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 degraded performance.
Poor	The WAN health score is poor. The connection is experiencing significant issues.

	Description
None	The WAN connection is in unknown state.

Table 45: *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**.

To view the **WAN** page, click the **WAN** tile on the Instant On home page, or click **Networks** > **WAN** page from the navigation pane on the left:

Table 46: *WAN Information*

	Description
Network	Displays the name of the network. 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.
State	Shows the status of the network, whether Online or Offline.
Type	Indicates the connection type.
Priority	Indicates the primary or secondary role of the WAN connection.
IP Assignment	Specifies how the IP address is assigned to the WAN connection.
IP Address	Specifies the IP address assigned to the WAN connection
Uplink VLAN	Specifies the VLAN ID associated with the network.

Hover the cursor over a network, click the ••• button and select one of the following options:

- **View Details**–Allows you to view the details of the network.
- **Delete**–Deletes the network. You cannot delete the primary WAN connection.

Overview

The **Overview** tab of the WAN details page contains the following sections:

- Identification
- Connection
- Connectivity
- Uplink

To view the details of the WAN connection, follow these steps:

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

Identification

The **Identification** section provides the basic details of the selected WAN connection, which includes the WAN connection name, health, and status.

The **Overview** > **Identification** section displays the following details:

- **Name**–Denotes the WAN connection name. By default, the name of the primary WAN connection is displayed as Internet.
- **Health**–Displays the health status of the WAN connection:
  - 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 inactive.
- **State**–Denotes if the network is Online or Offline.

Connection

The **Overview** > **Connection** section displays the following details:

- **Priority**– Indicates the primary or secondary role of the WAN connection.
- **Connection Type**–Denotes 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.

Connectivity

Configure the IP assignment for the WAN Connection. You can configure either one of the following options:

- **Automatic (default)** – The Instant On switch will inherit the IP address assigned by the DHCP in the network.
- **Static** –Specify a static IP address for the Instant On switch by entering the following network parameters:
  - **IP Address**–Enter the IP address for the switch.
  - **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 DNS server.
  - **Secondary DNS Server**–Enter the IP address of the 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.

Uplink

The **Overview** > **Uplink** section displays the Uplink VLAN for the network routing.

Delete Network

The **Overview** > **Delete Network** section provides the option to delete the network. You cannot delete the primary WAN connection.

Network Assignment

The **Network Assignment** page facilitates the assignment of WAN and LAN networks to Instant On devices at the site.

The primary WAN network is connected to the primary WAN port. The primary ports are:

- Port 4 on SG1004 gateway
- Port 5 on SG2505P gateway

You can assign 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.

All the ports on an Instant On secure gateway can be configured at the same time and assigned to a particular VLAN network. The **Network Assignment** page provides a global view of the WAN network. 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.

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

1. Click the **WAN** tile on the Instant On web application home page, or click **Networks** from the navigation pane on the left.
2. In the **WAN** > **Network Assignment** page, select one of the following methods to view the network details:
   a. Clicking on the WAN connection name.
   b. Hover the cursor over the WAN, click the ••• button, and select **View Details** from the drop-down list.

3. Click the **Network assignment** tab.
4. Modify the status of each port by clicking on it. The status of the port is displayed with a **T** (tagged), or **U** (untagged) decorator subsequently every time you click on a particular port.
5. Click **Update**.

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. Click the **WAN** tile on the Instant On home page, or navigate to the **Networks** > **WAN** page from the navigation pane on the left.
2. Click **Create Network**.
3. Under **Identify the Network**, configure the following:
   a. **Name**–Enter a name for the WAN connection.
   b. **Priority**–By default, the priority value is set to **Secondary**.
   c. Click **Next**.
4. Under **Set Connectivity**, 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.
   - **Uplink VLAN**–Assign an Uplink VLAN for network routing. The value must be between 1 and 4092.
5. Click **Next**.

6. Under **Assign Network**, select an available port to assign the WAN connection and select whether the port is tagged or untagged.
   - 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.
7. Click **Create Network**. The secondary WAN is created and displayed in the **WAN** table.

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. Click the **WAN** tile on the Instant On home page, or navigate to the **Networks**> **WAN Redundancy** page from the navigation pane on the left.
2. 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.

Chapter 11
Applications

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 smart phones. 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.

- 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 categorization and filtering is not guaranteed.
- The availability of different categories is based on the availability of wired-only, wireless-only, or wired and wireless clients in the site.

Applications Overview

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

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

Table 47: *Application Information*

Parameter	Description
Category	Shows the name of the application category.
24-hour Usage	Shows the total usage for a given application category, in bytes.
24-hour Usage %	Shows the total usage for a given application category, in percentage (%).

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

Table 48: *Application Categories and their Classification*

Application Category	Icon	Instant On Classification
Wired–Traffic from client devices physically connected to the network through an Ethernet switch port. **NOTE:** This category is not present for Wireless-only sites or for sites with a		▪ Wired client traffic

Application Category	Icon	Instant On Classification
Gateway.		
Web–General web infrastructure and internet services, including web browsing, computer and internet information, online advertising, dynamically generated content, proxies, and related web technologies		▪ Computer and Internet Info ▪ Computer and Internet Security ▪ Dynamically Generated Content ▪ Parked Domains ▪ Speed test ▪ Web ▪ Web Advertisement
Utilities–Infrastructure and support services used to enable application delivery and network operations, including authentication, file and cloud storage, content delivery, databases, hosting, peer-to-peer, and remote access technologies.		▪ Compression ▪ Content Delivery Networks ▪ File Management ▪ File Server ▪ File Transfer ▪ Internet Portals ▪ Middleware ▪ Peer to Peer ▪ Personal Storage ▪ Terminal ▪ Thin Client ▪ Web Hosting
Productivity–Work-oriented applications and services that support business operations and efficiency, including enterprise tools, cloud services, collaboration platforms, security software, search, translation, and reference resources.		▪ Antivirus ▪ Application Service ▪ Cloud-Based Services ▪ Database ▪ ERP ▪ Enterprise ▪ Map Service ▪ Microsoft Office ▪ Printer ▪ Reference and Research ▪ Search Engines ▪ Security Service ▪ Shareware and Freeware ▪ Telephony ▪ Translation ▪ Web Search Engines
Streaming–Audio and video streaming services and high-bandwidth media platforms, including music, movies, live broadcasts, and on-demand multimedia content.		▪ Audio/Video ▪ Music ▪ Multimedia Streaming

Application Category	Icon	Instant On Classification
Business and economy–Business-related websites, services, and applications, including financial services, banking, payments, insurance, real estate, legal services, stock markets, enterprise commerce, and economic information.		▪ Business and Economy ▪ Cryptocurrency ▪ Financial Services ▪ Individual Stock Advice and Tools ▪ Job Search ▪ Legal ▪ Payment Service ▪ Real Estate
Uncategorized–Traffic and services that do not clearly fit into a defined category but may still be necessary for normal network operation. **NOTE:** This category is not visible when no unidentified traffic is detected.		▪ Dead Sites ▪ Unidentified Applications
Instant messaging and email–Messaging, email, and communication platforms that enable real-time or asynchronous user interaction, including instant messaging, web-based email, video and audio conferencing, and Internet communication services		▪ Disposable Email Accounts ▪ Email ▪ Instant Messaging ▪ Internet Communications ▪ Multimedia Conferencing ▪ Video Chat ▪ Web based email
Shopping–E-commerce platforms and market places that support buying, selling, auctions, classified listings, pay-to-surfservices, and online retail transactions.		▪ Auctions ▪ Classified Ads ▪ Pay to Surf ▪ Shopping ▪ Web E-Commerce
Social network–Social networking platforms and online communities that enable users to connect, share content, participate in discussions, and build relationships around personal or professional interests.		▪ Blogging ▪ dating ▪ Forum ▪ Personal sites and Blogs ▪ Social Networking ▪ Social Networks
Lifestyle–Sites that cover beauty and fashion trends, dining, entertainment and arts, maps and navigation, religion, society and travel.		▪ Entertainment ▪ Leisure ▪ Travel ▪ Location ▪ Fashion
Adult content–Content intended for mature audiences, including pornography, gambling, illegal drugs, nudity, violence, and other adult or potentially harmful themes.		▪ Abused Drugs ▪ Adult and Pornography ▪ Gambling ▪ Illegal ▪ Low-THC Cannabis Products

Application Category	Icon	Instant On Classification
		▪ Marijuana ▪ Nudity ▪ Self Harm ▪ Sex Education ▪ Swimsuits & Intimate Apparel
Education–Educational institutions, online learning platforms, training services, and academic resources, including schools, universities, professional certifications, and e-learning tools.		▪ Education ▪ Educational Institutions ▪ Training and Tools
Explicit content–Sensitive or potentially disturbing content not suitable for general audiences, such as weapons, cults, cheating and plagiarism, alcohol and tobacco, and graphic or shocking material.		▪ Abortion ▪ Alcohol and Tobacco ▪ Cheating ▪ Cult and Occult ▪ Gross ▪ Hate and Racism ▪ Questionable ▪ Violence ▪ Weapons
Gaming–Online and offline gaming platforms, multi player game services, downloadable games, gaming communities, and related content or tools.		▪ Games ▪ Online Gaming
Government and politics–Government agencies and public sector services at local, regional, and national levels, as well as military organizations, political content, advocacy, public policy, and civic information		▪ Government ▪ Military ▪ Philosophy and Political Advocacy
Kids and family–Websites and applications designed specifically for children and families, including educational, entertainment, and age-appropriate interactive content.		▪ Children and Teenagers Content
Malicious and risky–Known malicious or high-risk content and tools that may compromise security or privacy, including malware, phishing, bot nets, hacking tools, spyware, adware, proxy avoidance, and spam infrastructure.		▪ Bot Nets ▪ Hacking ▪ Keyloggers and Monitoring ▪ Malware Sites ▪ Phishing and Other Frauds ▪ Proxy Avoidance and Anonymizers ▪ Spam URLs ▪ Spyware and Adware
News and media–News outlets and media services providing current events, journalism, weather, magazines, newspapers, radio, and other informational or editorial content.		▪ News Portal ▪ News and Media

Application Category	Icon	Instant On Classification
Sports and recreation–Sports-related content and recreational activities, including live scores, sports news, teams, events, hobbies, outdoor activities, and leisure pursuits.		▪ Hunting and Fishing ▪ Recreation and Hobbies ▪ Sports
Creative Content–Creative media platforms and tools, including image and video libraries, digital art, design resources, and generative Artificial Intelligence systems used to create text, images, audio, video, or code.		▪ Artificial Intelligence ▪ Generative AI ▪ Image and Video Search
Networking Protocol–Core networking and transport protocols required for network communication and operation, including routing, tunneling, IP services, authentication protocols, DNS, and network management protocols		▪ Authentication ▪ Behavioral ▪ Cert. Authority (SSL/TLS) ▪ DNS Over HTTPS ▪ Encrypted ▪ Network Management ▪ Network Service ▪ Routing ▪ Standard ▪ Tunneling

Application Category Details

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

1. Click the **Applications** tile on the Instant On home page, or click Application from the left navigation menu. The **Applications** page opens.
2. Under **Application** > **Overview**, use one of these methods to view the details of the application category:
   a. Clicking on the application category name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
3. The page displays the following information:
   a. **Most Used Websites and Applications**–Displays the Network Usage and Client Usage data for that application category.
   b. **Network Usage**–Denotes the data transferred on the network specific to the selected web category, during the last 24 hours.
   c. **Application Category Control**–Displays the list of policies that are currently applied to the application category. Click on the policy name to view the policy configuration and make modifications as required. For more information on managing access to Application Categories, see Policies.
   d. **Legend**–Includes the color codes to each different network. The color codes in the legend are used to display the donut chart.
   e. **Client Usage**–Displays the data usage of top five clients specific to the selected web category.

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.

Application Visibility and Control Settings

This page allows you to configure application visibility and control settings for the network.

Application details are required for application policies to operate. If no details are available, then you cannot configure application visibility and control settings.

To configure application visibility and control settings on the network, follow these steps:

1. Click **Applications** ( ) tile on the Instant On home page, or click on Applications in the left navigation menu.
2. Click **Visibility and Control**.
3. 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 Summary Only**–Provides only an overview of uploaded and downloaded data of all the networks for the last 24 hours in the Applications page. Choose this option for better network performance. Selecting this option hides the Applications tab in the web application.

Application Usage Summary

The application usage summary for the last 24 hours is displayed in the **Overview** section when **Application Summary Only** is selected under **Visibility and Control**.

The following information is displayed in the usage summary:

- **Transferred**–Displays the total amount of data transferred in the network for the last 24 hours.
- **Downloaded**–Displays the total amount of data downloaded in the network for the last 24 hours.
- **Uploaded**–Displays the total amount of data uploaded in the network for the last 24 hours.

Chapter 12
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 Clients List

The **Overview** section displays the list of all active clients in the site. The list of connected clients includes wired, wireless, and infrastructure clients connected to a network in the site. Detailed information about a connected client can be viewed in the Client Details page by clicking on a particular client name in the list. You can also on click on any of the client rows to view the client information in the side panel.

Table 49: *Client details*

Column Label	Description
Client	Name of the client. Click on the client name from the list to view the **Client Details page**. The Client Details page lists detailed information about 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.
State Duration	Denotes the amount of time that 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.
Network	Denotes the network to which the client is connected.
Type	Denotes if the connected client is a wired, wireless, or VPN client.
MAC Address	MAC address of the client. This field is not applicable for the VPN client.
IP Address	IP address of the client.

Column Label	Description
Device	The network device to which the client is connected.
Interface	Denotes the device interface to which the client is connected. The Wireless client will display the radio (2.4 GHz, 5 GHz, or 6 GHz) to which it is connected.
24-hour Usage	Indicates the data usage by the client for the last 24 hours.

Blocking a Wireless Client

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

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

1. Click the **Clients** ( ) tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Overview** tab to view the list of connected clients.
3. Hover the cursor over a wireless client. A ••• button is displayed at the end of the row.
4. Click the ••• button and select **Block** from the drop-down list. The client is immediately blocked and moved to the **Blocked** list.

Adding a Client to Watchlist

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

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

1. Hover the cursor over a wired or wireless client. A ••• button is displayed at the end of the row.
2. Click the ••• button and select **Add to Watchlist**. The client is added to the **Watchlisted** ( ) list.

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

1. Hover the cursor over a wired or wireless client. A ••• button is displayed at the end of the row.
2. Click the ••• button and select **Remove from Watchlist**. The client is removed from the **Watchlisted** ( ) list.

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.

Multi-select Mode is enabled when you select an item from the **Action** drop-down list. Once enabled,you can choose multiple client rows simultaneously to perform bulk actions such as **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.

Refer to the following topics for more information on blocked and watchlisted clients:

- Blocked Clients
- Watchlisted Clients
- Classification Tags

Blocked Clients

The **Blocked** tab lists the details of wireless clients that are barred from joining networks in the site. You can block up to 256 clients. Clients blocked in a site can be unblocked from this page. The **Blocked** tab displays the following information:

Table 50: *Blocked client details*

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

Unblocking a Blocked Client

Follow these steps to unblock a blocked wireless client:

1. Click on the **Clients** ( ) tile in the Instant On homepage of the web application. The **Clients** page is displayed.
2. Click the **Blocked** tab to view the list of blocked clients.
3. Hover the cursor over a blocked client. A ••• button is displayed at the end of the row.
4. Click the ••• button and select **Allow**. The client is unblocked and is displayed under the **Overview** tab with the rest of the connected clients.

NOTE

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.

Watchlisted Clients

The client watchlist feature allows you to monitor the status of the wired, wireless clients , 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.

If a client is in the Watchlisted list and is offline, the **Connectivity** label on the client details page changes to **Last Connectivity**, and the client details are available only from the **Watchlisted** table.

NOTE

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

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

1. Hover the cursor over a wired or wireless client. A ••• button is displayed at the end of the row.
2. Click the ••• button and select **Remove from Watchlist**. The client is removed from the **Watchlisted** ( ) list.

The following table describes the parameters of the Watchlisted Clients table.

Table 51: *Client details*

Column Label	Description
Client	Name of the client. Click on the client name from the list to view the **Client Details page**. The Client Details page lists detailed information about 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.
State Duration	Denotes the amount of time that 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.
Network	Denotes the network to which the client is connected.
Type	Denotes if the connected client is a wired client ( ), a wireless client ( ), or VPN client ().
MAC Address	MAC address of the client. **NOTE:** There is no MAC address available for a VPN client.
IP Address	IP address of the client.
Device	The network device to which the client is connected.
Interface	Denotes the device interface to which the client is connected. The Wireless client will display the radio (2.4 GHz, 5 GHz, or 6 GHz) to which it is connected. **NOTE:** There is no Interface information available for a VPN client.
24-hour Usage	Indicates the data usage by the client for the last 24 hours.

Viewing Wireless Client Details

The Wireless Client details page provides detailed information about clients in your network. The Client details page is accessed from the **Overview** tab.

Wireless clients include laptops, personal computers, tablets, mobile phones, etc. that connect to the Instant On network through wireless.

To view the wireless client details page for a specific client, follow these steps:

1. Click the **Clients** tile on the Instant On home page. The **Clients** page is displayed.
2. Click the **Overview** tab to view the list of connected clients to your site.
3. Click on a client name from the list to view the **Client Details** page for that device.

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

- Identification
- Hardware
- Connectivity
- Connection
- Client Usage

Table 52: *Wireless Client Details*

Column Label	Description
Identification	
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 valid characters in the client name. To reset the client name to its default name, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom client name is assigned.
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.
Classification	Denotes the category of the client device. The client devices can be classified by category, family, and OS. For example, a client can be classified as a computer, smart device, or VoIP, and its family can be Windows, Linux, or Apple Mac.
Hardware	
MAC Address	MAC address of the client.
Connectivity	
IP Address	IP address of the client.
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.
Radio Frequency	Displays the radio frequency (2.4 GHz or 5 GHz) to which it is connected.
Protocol	The Wi-Fi standard of the client connection. The Wi-Fi standard mapping is displayed as follows: ■ **Wi-Fi 5**– 802.11ac standard. ■ **Wi-Fi 4**– 802.11n standard.

Column Label	Description
	The Wi-Fi standard will not be displayed for legacy Wi-Fi clients using 802.11b or 802.11g standards.
Security	Displays the security standard used by the wireless client to connect to the network.
Signal Strength	Indicates the client signal quality.
Download Data Rate	Displays the most recently recorded download speed.
Upload Data Rate Upload	Displays the most recently recorded upload speed.
Receive Data Rate	Displays the rate (in Mbps) at which the data was received for the client.
Transmit Data Rate	Displays the rate (in Mbps) at which the data was transmitted for the client.
Client Usage (For Last 24 hours)	
Application Category	This section displays the data usage by the client, for various application categories. The categories that are visited by the client is also represented by a donut chart. This is displayed only for wireless clients.
Downloaded	Displays the total amount of data (in MB), downloaded in the network throughout the day.
Uploaded	Displays the total amount of data (in MB), uploaded in the network throughout the day.
Downloading at	The download throughput of the device in the last 30 seconds, in bytes per second.
Uploading at	The upload throughput of the device in the last 30 seconds, in bytes per second.

Block Client

You can also block the wireless client from the Client details page. Click the **Block** button next to **Block Client**. The client is immediately blocked and moved to the **Blocked** list.

Watchlist Client

You can also add the wireless client to the watchlist. Click the **Add** button next to **Add Client to Watchlist**. The client is added o the **Watchlisted** list.

To remove a client from the watchlist, click **Remove** next to **Remove Client from Watchlist**.

Classification Tags

This component displays all classification tags applied to the client. You can select or unselect tags within the tag chip. Click the **Change** button next to **Classification Tags**. The **Change Classification** page is displayed.

The search bar filters the global tag library, and selecting a tag instantly adds it to the list. To delete the classification tag, click **X**.

Client Classification option under **Actions** allows you to update classification tags for multiple clients simultaneously by selecting them directly from the **Clients** page.

NOTE

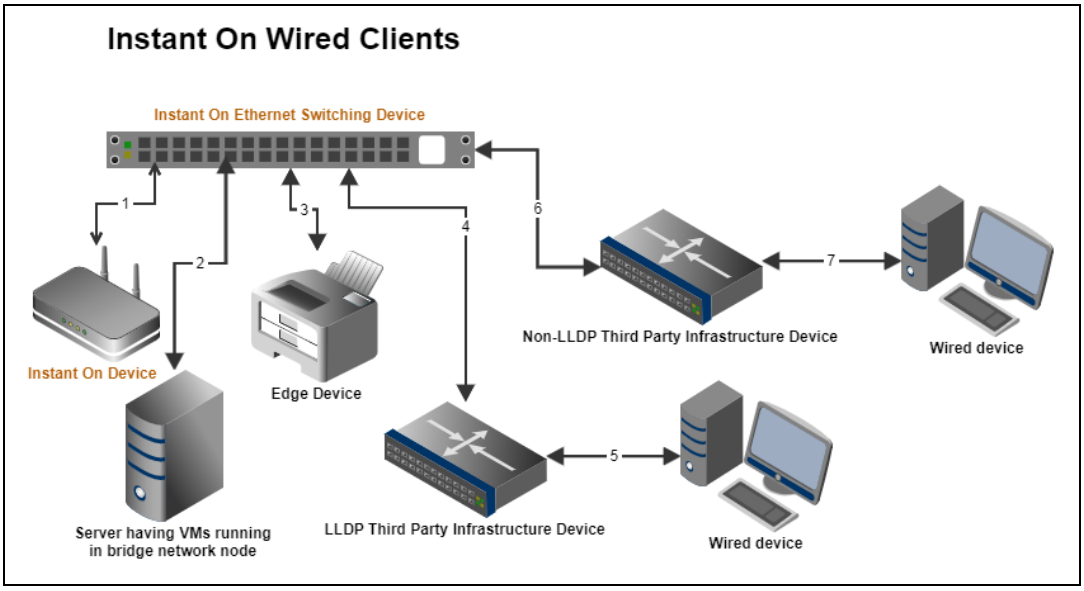
- When two or more clients are selected, the section **Assign classification tags to the [N] selected clients** is displayed.
- When a single client is selected, the process shall follow the same flow as when accessing the tag through **Client Details** > **Classification Tags**.

Viewing Wired Client Details

The Wired Client details page provides detailed information about clients in your network. The Client details page is accessed from the **Overview** tab.

A wired client is defined as a client connected to an Instant On device that supports Ethernet switching. Wired clients are printers, server, switches, and infrastructure devices connected to the wired network. Wired clients are further classified into infrastructure clients. Infrastructure clients are switches and other network devices through which other wired clients are connected to the network.Wired clients are categorized based on the following scenarios:

Figure 8 *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

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

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

1. Click the **Clients** ( ) tile on the Instant On home page. The **Clients** page is displayed.
2. Click the **Overview** tab to view the list of connected clients.
3. Click the client name of the wired client from the list of connected clients.

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

- Identification
- Hardware
- Connectivity
- Connection
- Port Usage

Table 53: *Wired Client Details*

Column Label	Description
Identification	
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, click the reset icon and then click **Update** to save the change. The reset icon is displayed only when a custom client name is assigned.
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.
Classification	Denotes the category of the client device. The client devices can be classified by category, family, and OS. For example, a client can be classified as a computer, smart device, or VoIP, and its family can be Windows, Linux, or Apple Mac.
Hardware	
MAC Address	MAC address of the client.
Connectivity	

Column Label	Description
IP Address	IP address of the client.
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	Displays the port to which the client is connected.
Speed / Duplex	Displays the speed of the port and indicates whether the client is connected in a full duplex or half duplex mode.
Port Usage	
Port Usage	Displays the total amount of data uploaded and downloaded in a pie chart.
Downloading at	The download throughput of the device in the last 30 seconds, in bytes per second.
Uploading at	The upload throughput of the device in the last 30 seconds, in bytes per second.

Classification Tags

This component displays all classification tags applied to the client. Click the **Change** button next to **Classification Tags**. The **Change Classification** page is displayed.

The search bar filters the global tag library, and selecting a tag instantly adds it to the list. To delete the classification tag, click **X**.

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**.

PoE Power Cycle

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

1. Click the **Clients** ( ) tile on the Instant On home page. The **Clients** page is displayed.
2. In the **Connected clients** list, hover the cursor over the wired client. A power cycle () button is displayed at the end of the row.
3. Click the () button to power cycle the wired client. The port will then be sequentially powered off and then be powered on. The **Duration** column displays a message that the client is being power cycled.

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. From the **Actions** drop-down list, select **Power Cycle** to enter **Multi-select Mode**.
3. Select the checkbox for each wired PoE client you want to power-cycle, then select **Confirm**. Each selected client's port is powered off and then back on in sequence, with the Duration column showing the progress of the power cycle.

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.

Watchlist Client

You can also add the wireless client to the watchlist. Click the **Add** button next to **Add Client to Watchlist**. The client is added o the **Watchlisted** list.

To remove a client from the watchlist, click **Remove** next to **Remove Client from Watchlist**.

You can also block the wired client from the Client details page. Click the **Add** button next to **Add Client to Watchlist**. The client is added o the **Watchlisted** list.

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. Click the **Clients** ( ) tile on the Instant On home page, or click **Clients** from the navigation pane on the left.
2. Hover the cursor to the end of the row, click the ••• button, and select **Add IP Address Reservation** from the options. The client's current IP address is reserved by default, adjust it if needed, then select **Confirm**.
3. To remove an existing reservation, open the same menu and select **Remove IP Address Reservation**.

The following procedure reserve or remove a client's IP address directly from the Clients details:

1. Select the client from the list.
2. Under **Add IP Address Reservation**, click Add.
3. To remove the client's IP address directly from the Clients details, select **Remove**.

IP Reservation supports clients with a fixed MAC address, so clients using MAC randomization are not eligible. The option is also unavailable if DHCP is disabled on the network. Each network supports up to 128 IP Reservations, which can be added or removed either from the **Clients** page or from the **IP Assignment** tab (**Networks** > **IP Assignment**).

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.

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 Client Details

The VPN Client details page provides detailed information about clients connected to the VPN network. The Client details page is accessed from the **Overview** tab.

You cannot block or watchlist the VPN client.

VPN clients include laptops, personal computers, tablets, mobile phones, etc. that connect to the Instant On network through VPN.

To view the VPN client details page for a specific client, follow these steps:

1. Click the **Clients** tile on the Instant On home page. The **Clients** page is displayed.
2. Click the **Overview** tab to view the list of connected clients to your site.
3. Click on a VPN client name from the list to view the **Client Details** page for that device.

Table 54: *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.
Connectivity	
IP Address	The IP address of the client.

Column Label	Description
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.

Classification Tags

The **Classification Tags** tab provides a complete record of every classification tag that has accessed the site. The **Classification Tags** tab displays the following information:

Table 55: *Classification Tags client details*

Column Label	Description
Classification Tag	This column does not display a list of all possible or existing classification tags. Only those recorded as active will be displayed on the Site.
Clients	This column indicates the number of clients on record that had accessed the site with the assigned tag.

Client Classification option under **Actions** allows you to update classification tags for multiple clients simultaneously by selecting them directly from the **Clients** page.

- 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**.

The **Classification Tag Details** page shall provide a dedicated view for reviewing a specific classification tag. You can rename the tag. It will also include: **N Clients** (Number of clients who visited the Site with this tag)

Chapter 13
Security

The **Security** page serves as a centralized location for configuring and monitoring threat-related security and Internet firewall settings.

NOTE

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 are enabled by default.

NOTE

The option to add exceptions is available to Admin or Operator roles.

The **Security** page provides visibility and control over the following threat-related functions:

- Threats
- Threat Exceptions
- Threat Management
- Internet firewall

NOTE

The **Security** page is displayed only on sites containing security gateways. It is accessible only to users with administrative privileges.

Threats

The **Security** > **Threats** section displays the list of threats detected on the site. 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 change the default action taken.

The **Threats** table displays the following information:

Table 56: *Threats Details*

Field	Description
Threat	Name of the Threat identifier.
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.

Field	Description
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, 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. ■ Undefined–The system could not determine the threat's severity.
Source	Denotes the source host or origin of the threat.
Destination	Denotes the destination host of the threat.

Threat Actions

To add an allow or block exception, follow these steps:

1. Click the **Threats** tile on the Instant On web application home page, or Click **Security** from the navigation pane on the left.
2. Under **Security** > **Threats**, hover the cursor 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.
   - **View Exception**–Displays the threat exception.

Threat Exceptions

The **Threat Exceptions** page lists all the exception made to a threat to override the default action taken by the threat management.

Table 57: *Threats 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, 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.

Field	Description
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.

You can click on any of the threats to view more details about any specific threat in the Threat side panel.

Removing the Threat Exceptions

To remove the threat from the exceptions list, follow these steps:

1. Click the **Threats** tile on the Instant On web application home page, or Click **Security** from the navigation pane on the left.
2. Under **Security** > **Threat Exception**, hover the cursor to the end of the row of a network policy, click the ••• button, and select **Remove Exception**.

Threat Management

The Threat Management tab allows you to enable or disable the Threat detection and prevention. It 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, follow these steps:

1. Click the **Threats** tile on the Instant On web application home page, or Click **Security** from the navigation pane on the left.
2. Under **Security** > **Threat Management**, select one of the following options:
   - **Threat Detection and Prevention (default)**–Activates the threat management. This option is enabled by default. When enabled, all incoming and outgoing traffic routed through 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.

Firewall

The Firewall page 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 configure one or more policies for the firewall, click the **View policies**. You will be redirected to the Policies page.

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 or an Application Layer Gateway (ALG) protocol is enabled or disabled, it applies only to new sessions .Existing sessions continue without any changes. To ensure that all connections follow the latest configuration, you must restart the firewall.

To restart the firewall, click the **Restart Firewall** button. Restarting the firewall terminates all active sessions and ensures that all new sessions operate according to the policy applied to the secure gateway. This action may temporarily affect network services and client connections.

Chapter 14
Managing Your Account

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

To navigate to the **User Account Management** page, click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.

Identification

The Identification section displays the primary administrator email account used to manage the operations for the site.

Changing Account Password

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

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Profile** > **Change Password**, click the **Change** button.
3. In the **Change Password** window, enter the following details:
   a. **Current Password**–Enter the current password for the administrator account.
   b. **New Password**–Enter the new password for the administrator account.
4. Click **Change Password** to save your changes.

Two-Step Verification

The **User Account Management** > **Profile** page allows administrators to add Two-Step Verification (TSV) on their own account. TSV 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-Step Verification. If you do not have an authenticator app installed on your device, download one for your corresponding operating system.

Enabling Two-Step Verification

To set up Two-Step Verification for your administrator account, follow these steps:

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Profile** > **Enable Two-Step Verification**, click the **Enable** button.
3. Under **Confirm Password**, enter your **Current Password**, and click **Next**.

4. Under **Set Up Alternative Email**, enter a valid alternate email address in the **Alternative Email** and **Confirm Alternative Email** text boxes respectively. The alternative email address is required to sign in if you face any issues using the authenticator app.
5. Click **Next**.
6. Under **Set Up Authenticator**, copy the key provided below and manually enter it in the authenticator app, or scan the QR code using the authenticator app.
7. Enter the code in the **Verification Code** text box.
8. Click the **Enable Two-Step Verification** button, to save the changes.

Once two-step verification is activated on the administrator account, you are required to enter the one-time password generated by the authenticator app, each time you login to the Instant On web application.

Disabling Two-Step Verification

This setting is available only for administrator accounts on which two-step verification is currently enabled. Use this setting to disable additional sign-in security and only request a valid password. To disable two-step verification for your administrator account, follow these steps:

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Profile** > **Disable Two-Step Verification**, click the **Disable** button.
3. Under **Confirm Password**, enter your **Current Password**.
4. Click **Disable Two-Step Verification**. A message is displayed on the screen that two-step verification is disabled on the administrator account. Additionally, an email notification is sent to the user informing about the change in setting.

Changing the Recovery Email Address

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

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

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Profile** > **Change Alternative Email**, click the **Change** button.
3. Enter the **New alternative email** address.
4. **Confirm new alternative email** by re-entering the new email address.
5. Under **Confirm Password**, enter your **Current Password**, and click **Next**.
6. Click **Change alternative email** to apply the changes. A message is displayed on the screen that the alternative email address is changed. Additionally, an email notification is sent to the user informing about the change in setting.

Preferences

The **Preferences** section provides the options to customize the design settings based on the following fields:

- **Language**–Indicates the language preference for the interface, notifications, and other communications (SSO). By default the entry for this field is auto-detected. The administrator of the account can modify the

language to one of the following supported languages:

- German
- English
- Spanish
- French
- Italian
- Japanese
- Korean
- Portuguese
- Simplified Chinese
- Traditional Chinese

- **Theme**–Indicates the color theme preference for the application interface. The following options are available for selection:
  - System
  - Light
  - Dark

Communications

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

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Communications**, select the **Receive personalized communications about Instant On and select partner products, services, offers, and events according to** HPE Privacy Statement checkbox, to receive notifications on our **Product Updates and Offers**.

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

3. Click **Update**. A message is displayed on the screen confirming the success of the update.

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

Delete Account

The **Delete Account** screen allows you to delete an Instant On administrator account and revoke access to any associated products and services.

- The administrator account will be deleted with all its associated data.
- If the deleted account was being used as the primary administrator account, all sites that belonged to the account will be deleted, and all devices will be factory reset.
- Sites with multiple administrator accounts will not be deleted if one of the accounts is deleted.

The following procedure allows you to delete an Instant On administrator account:

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Under **Profile** > **Delete Account**, click the **Delete** button.
3. Under **Confirm Deletion**, copy the code displayed on the screen and enter it in the **Confirmation Code** text box.
4. Click **Delete Account** to permanently delete all account data and remove access to associated sites, devices, and services.

Notifications

Notifications are push 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.

Notifications in web application are displayed as an alert ( ) in the page header. If no action is taken on the alert, the notification remains in the alert and can still be viewed at anytime until it is cleared. All alerts triggered on the site can be viewed by clicking on **Show all alerts** in the **Site Health** tile.

Enabling or Disabling Alert Notifications

To enable notifications for alerts, follow these steps:

1. Click the account icon (the alphabet icon) displayed on the header and select **Account Details** from the drop-down menu. The **User Account Management** page is displayed.
2. Click the **Notifications** tab.
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 each alert category, use the checkboxes to enable or disable the alerts you want to be notified about as mobile or email notifications. You will receive notifications on your mobile device or email when the selected alert is triggered in the site. For more information on viewing and managing alerts, see:

- Viewing and Managing Alerts using the Web Application

By default, the **Mobile** notifications are enabled for all five 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
- Software
- Watchlisted Client

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

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.

Chapter 15
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:

- Manual policy creation—You manually define the required parameters to configure the policy. Manual policy creation is available on all site topologies. For more information, see Manual Policy Creation. For more information, see Manual Policy Creation.
- AI-Assisted policy creation—Policies are created using prompts in an interactive, text-based format. 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.

Instant On provides both Manual policy creation and AI-Assisted policy creation methods on every site. The policy capabilities available to you depend on the devices present in the site.

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 includes the following rules:
   - All LAN ports are granted access to the internet by default.
   - Communication 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 Networks documentation.

Overview

The **Policies** > **Overview** section displays the list of policies created for the site, in order of their highest to lowest priority. The policy details are categorized under the following fields:

Table 58: *Policy Details*

Field	Description
Priority	Denotes the order in which the policies are to be executed. The policy list is displayed in decreasing order of its priority, number 1 being the highest.
Policy	Denotes the set of rules created to govern the applications usage and networks schedule.
Action	Denotes the action to be performed by the policy: - **Enable**–Makes an entity type available.

Field	Description
	■ **Disable**–Makes an entity type unavailable. ■ **Allow**–Allows an entity type. ■ **Block**–Blocks an entity type. ■ **Restrict**–Restricts an entity type. Available on gateway and switch-only sites; on switch-only sites the destination is limited to a specific IP address or subnet. ■ **Forward**–Forward an entity type. This action is available only for gateway sites.
Rule	Defines the action that needs to be carried out by the policy. A rule determines the action on a policy that must be performed and on which entity.
Schedule	Denotes the time and duration for which the policy needs to take effect on the entity.
State	Denotes the current state of the policy.
Type	Denotes the policy type. The available types are Network activation and Application Access.

The following table explains about the supported combination of the valid action and entity types.

Table 59: *Combinations of policies actions and entity types*

Action	Entity Type	Schedule Support	Firewall Support	Wireless Networks Support	Devices Support	Clients Support	Application Categories Support
Enable	Wireless network	Yes (mandatory)	No	Yes	No	No	No
Disable	Wireless network	Yes (mandatory)	No	Yes	No	No	No
Allow	Application	No	Yes	Yes	No	No	Yes
Block	Application	No	Yes	Yes	No	No	Yes

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. Under **Policies** > **Overview**, click the **Reorder** button.
2. Use the ^ and v icons displayed under the **Schedule** field, to reorder the priorities for the policies.
3. Click **Update**.

Deleting a Policy

1. Click the **Policies** tile on the Instant On web application home page, or click **Policies** from the navigation pane on the left.
2. Under **Policies** > **Overview**, hover the cursor over the network you want to delete, click the ••• button,

and select **Delete** from the drop-down list.

3. Click **Delete Policy** from the popup window.

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 inputs.

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 during specific times.
- Client Policy–Control which destinations 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-Assisted Policy Creation

- Policies cannot be edited using the AI-assistance. To edit an existing policy, hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.
- 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. Navigate to **Policies** > **Overview**.
2. Click the **Create as Conversation** button.

   The **Create Policies** page 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.

4. Click **Submit**.

   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. The optional settings available while creating AI-assisted policy are:
   - Click the Start Over icon to delete the current conversation and begin again.
   - Click the Delete icon to delete the proposed policy.
   - Click the Edit icon to manually edit to the suggested policy. After editing the policy, click **Edit Policy** to save the change and return to the **Create Policy** page.
8. Click **Accept** to confirm.

   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 rule actions, sources, and destinations 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. Under **Policies** > **Overview**, click the **Create Policy** button.
2. The **Set Rule and Conditions** page is displayed.
3. Under **Rule**, 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 active.
      - **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.
4. Click **Next**.

   The **Set Policy Applicability** page is displayed.
5. Under **Set Policy Applicability**, configure the following settings:
   - **Identification**, enter a name for the policy, and enable or disable the policy using the checkbox.
   - Set the **Priority** for the policy.
     - Under **Position**, select either **Lower** or **higher**.
     - Under **Policy**, select a policy from the drop-down list.
   - Under **Schedule**, select one of the following options:
     - **Always Active**–Click this option to make the wireless network always available for users to connect.

- **Create Schedule**–Click this option to create a schedule during which the network should become available for users to connect. Follow the instructions provided in Schedules.
- Existing Schedules–Select an existing schedule.

6. Click **Finish**.

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. Under **Policies** > **Overview**, click the **Create Policy** button.
2. Under **Actions**, select **Applications**.
3. Click **Next**.

   The **Set Rule and Conditions** page is displayed.
4. Under **Rule**, configure the following settings.
   a. **Action**–Select one of the following actions for the rule:
      i. **Allow**–Allows traffic matching the specified application categories and wireless networks pass.
      ii. **Deny**–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. **To Access** or **From Accessing**–Select the application categories from the **Applications** drop-down list, for which the action needs to be applied. For the current list of application categories, see Applications.
5. Click **Next**.

   The **Set Policy Applicability** page is displayed.
6. Under **Set Policy Applicability** > **Identification**, enter a name for the policy.
   a. Set the **Priority** for the policy.
      i. Under **Position**, select either **Lower** or **higher**.
      ii. Under **Policy**, select a policy from the drop-down list.
7. Click **Finish**.

Instant On supports manual policy creation for sites with a secure gateway for the following categories:

Creating a Manual Policy

Instant On supports the manual policy creation process for sites, serving as a simplified alternative for users.

On a switch-only site, the **Forward** action and **Clients** source are not available, and destinations are limited to a specific IP subnet or IP address. The **IP Sources** and **Networks**(wired) sources remain available

The following procedure describes how to create a policy:

1. Under **Policies** > **Overview**, click the **Create Policy** button.
2. The **Set Rule and Conditions** page is displayed.
3. Configure the following settings.
   a. **Action**–Select one of the following actions for the rule:
      - **Allow**–Allows a network available for users.
      - **Block**–Blocks a network available for users.
      - **Restrict**–Restricts a network available for users.
      - **Forward**–Forwards a network available for users.
      - **Enable**–Makes a network available for users to connect when the provided schedule is active.
      - **Disable**–Makes a network unavailable when the provided schedule is disabled.
   b. Under **Source**, select one of the following:
      - **Clients**–Select **Clients** to access the options for **All Clients** or **Selected Client**s.
      - **IP Sources**–Select **IP Sources** to access the options for **IP Subnets** or **IP Addresses**.
      - **Networks**–Select **Networks** to access the options for **All Networks** or **Selected Networks**.
4. Click **Next**.

   The **Create Policy** page is displayed.
5. Under **Create Policy**, configure the following settings:
   - **Allow**, enter a name for the policy.
   - **Source**, enter the source for the policy.
   - **To Access**, enter the destination for the policy from the drop-down list.
6. Click **Next**.

   The **Set Policy Applicability** page is displayed.
7. Under **Set Policy Applicability** > **Identification**, enter a name for the policy.
   a. Set the **Priority** for the policy.
      i. Under **Position**, select either **Lower** or **higher**.
      ii. Under **Policy**, select a policy from the drop-down list.
8. Click **Finish**.

Instant On provides support for all networks as destinations.

Updating a Policy

Instant On allows you to update an existing policy.

To update policies created using AI assistance, the available configurable parameters depend on the category and type of policy.

Updating a Site Policy

The site policy is available only for sites with a gateway.

To update a site policy, follow these steps:

1. Under **Policies** > **Overview**, hover the cursor to the end of the row of a network policy, click the ••• button, and select **View Details** from the drop-down list.

2. Under **Identification** > **Name**, update the name of the policy.
3. Enable or disable the policy using the checkbox.
4. Under **Rule** > **Action**, it is set to **Forward**. The value is non-editable.
5. Under **Rule** > **WAN source**, update the type remote source. One option must be selected as the remote source.
   - **Internet**–Internet is the default option selected as the remote source.
   - **IP Subnet**–On selecting **IP Subnet**, you must assign at least one source IP address.

     To add an IP subnet, click **Add** and enter the Base IP address and subnet mask in the **Add IP Subnet** pop-up window.

     To remove an IP Address, hover the cursor to the end of the row, click the ••• button, and select **Remove**.
   - **IP Address**–On selecting **IP Address**, you must assign at least one source IP address.

     To add an IP address, click **Add** and enter the source IP address in the **Add IP Address** pop-up window.

     To remove an IP Address, hover the cursor to the end of the row, click the ••• button, and select **Remove**.
6. Under **Rule** > **Protocol**, You must select a protocol. The available protocols are **TCP**, **UDP**, or **TCP and UDP**.
7. Under **Rule** > **Port**, update the port number on the gateway that is connected to WAN.
8. Under **To** > **LAN IP Address**, update the destination LAN IP Address.
9. Under **To** > **LAN Port**, update the destination port number.
10. (Optionally) Click **Delete**, to permanently delete a policy.
11. Click **Update** to save the changes.

Updating a Client Policy

The client policy is available only for sites with a gateway.

To update a client policy, follow these steps:

1. Under **Policies** > **Overview**, hover the cursor to the end of the row of a network policy, click the ••• button, and select **View Details** from the drop-down list.
2. Under **Identification** > **Name**, enter the name of the policy you are modifying.
3. Enable or disable the policy using the checkbox.
4. Under **Rule** > **Action**, select either **Allow**, **Block** or **Restrict** from the drop-down list.
5. Under **Rule** > **Clients**, select one of the following:
   - **All Clients**–Select **All Clients**, to apply the rule to all the clients deployed to the site.
   - **Specific Clients**–Select **Specific Clients**, to apply the rule to specific clients deployed to a site. You must select at least one client.

     To add a client, click **Add**. Select a client from the **Client** drop-down list in the **Add Specific Clients pop-up** window and click **Add Client**. To remove a client, hover the cursor to the end of the row, click the ••• button, and select **Remove**.

6. Under **To Access** or **From Accessing** > **Selected Destinations**, select all the required options:
   - **Domains**–On selecting **Domains**, you must add at least one domain.

     To add a domain, click **Add** in the **Destination Domains** section**.** Enter the domain name and click **Add Domain**.

     To remove a domain, hover the cursor to the end of the row, click the ••• button, and select **Remove**.
   - **IP Addresses**–On selecting **IP Addresses**, you must add at least one IP address.

     To add a destination IP address, click **Add** in the **Destination IP Address** section. Enter the **IP address** and click **Add IP Address**.

     To remove an IP Address, hover the cursor to the end of the row, click the ••• button, and select **Remove**.
   - **IP Addresses Range**–On selecting **IP Addresses Range**, you must add at least one IP address range.

     To add a destination IP address range, click **Add** in the **Destination IP Address Ranges** section. Enter the **Start IP address** and **End IP Address** and click **Add IP Address Range**.

     To remove an IP address range, hover the cursor to the end of the row, click the ••• button, and select **Remove**.
7. Under **Schedule**, select one of the following options:
   a. **Always Active**–Click this option to make the wireless network always available for users to connect.
   b. Existing Schedules–Select an existing schedule.
8. (Optionally) Click **Delete**, to permanently delete a policy.
9. Click **Update** to save the changes.

Updating a Network Policy

To update a network activation policy, follow these steps:

1. Under **Policies** > **Overview**, hover the cursor to the end of the row of a network policy, click the ••• button, and select **View Details** from the drop-down list.
2. Under **Identification** > **Name**, enter the name of the policy you are modifying.
3. Enable or disable the policy using the checkbox.
4. Under **Rule** > **Action**, select either **Activate** or **Deactivate** from the drop-down list.
5. Under **Rule** > **Networks**, select all the networks on the list for which the rule needs to be applied.
   - **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.
6. Under **Schedule**, select one of the following options:
   a. **Always Active**–Click this option to make the wireless network always available for users to connect.
   b. Existing Schedules–Select one of the existing schedule.
7. (Optionally) Click **Delete**, to permanently delete a policy.
8. Click **Update** to save the changes.

To update a network firewall policy, follow these steps:

1. Under **Policies** > **Overview**, hover the cursor to the end of the row of a network policy, click the ••• button, and select **View Details** from the drop-down list.
2. Under **Identification** > **Name**, enter the name of the policy you are modifying.
3. Enable or disable the policy using the checkbox.
4. Under **Rule** > **Action**, it is set to either **Allow**, **Block** or **Restrict**.
5. Under **Rule** > **Network**, select the network.
6. Under **To Access** or **From Accessing** > **Selected Destinations**, select all the required options:
   - Internet–The action is applied to the internet.
   - Domains–The action is applied to a domain. You must select at least one domain.
   - IP Subnet–The action is applied to the IP subnet. You must select at least one IP Subnets.
   - IP Address–The action is applied to the IP Address. You must select at least one IP Address.
7. (Optionally) Click **Delete**, to permanently delete a policy.
8. Click **Update** to save the changes.

Updating an Application Policy

To update an application policy, follow these steps:

1. Under **Policies** > **Overview**, hover the cursor to the end of the row of an application policy, click the ••• button, and select **View Details** from the drop-down list.
2. Under **Identification** > **Name**, enter the name of the policy you are modifying.
3. Under **Rule** > **Action**, select either **Allow** or **Block** from the drop-down list.
4. U Under **Rule** > **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.
5. Under **To Access** or **From Accessing** > **Applications**, select the categories for which the action needs to be applied.
6. (Optionally) Click **Delete**, to permanently delete a policy.
7. Click **Update** to save the changes.

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** page lists all the schedules that have been created to be included in the policies for the site.

The following fields are displayed:

Table 60: *Schedule Details*

Field	Description
Schedule	Displays the name given to the schedule.
State	Denotes the activity status of the schedule.

Field	Description
Active Days	Denotes the days of the week during which the schedule will be operational.
Active Hours	Denotes the hours of the day, during which the schedule will be operational.

Creating a Schedule

Follow these steps to create a new schedule:

1. In the **Policies** > **Schedules** page, click **Create Schedule**.
2. Under **Set Daily Schedule** > **Identification**, enter a name for the schedule you are creating.
3. 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 the days for which you need to configure a schedule. under **Active Days**.
      - 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.
4. Click **Create Schedule**.
5. To modify an existing schedule, go to **Policies > Schedules** and follow these steps:
   a. Click the Schedule Name.
   b. Hover the cursor to the end of the row, click the ••• button, and select **View Details** from the drop-down list.

Updating a Schedule

Instant On allows you to enable or disable a network for users at a particular time of the day. You can update an existing schedule by following these steps:

1. Under **Policies** > **Schedules** page, hover the cursor to the end of a row, click the ••• button, and select **View Details** from the drop-down list.
2. Under **Identification > Name**, enter a name for the schedule you are modifying.
3. Under **Network Access Schedule**, select one of the following values for **Type**:
   - **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.
   - **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:
       a. After selecting **Variable**, click on the day of the week for which you need to configure a schedule.
       b. 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.
4. Optionally, to permanently delete a schedule, click **Delete**.
5. Click **Update** to save the changes.

Chapter 16
Profiles

The **Profiles** page 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.

To access the **Profiles** page, select **Profiles** from the left navigation pane. The profile page consists of the following components:

- **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.

  For more information, see Ports Profile Page.
- **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.

  For more information, see RADIUS Profile Page.

Ports Profile Page

On the **Ports** profile page, the port profile table lists all configured port profiles. The table displays the following information:

Table 61: *Port Profile Table*

Column	Description
Profile	Name of the port profile.
(VLAN) Untagged Networks	VLAN ID and the name of the untagged network associated with the port profile.
Tagged Networks	Total count of tagged networks configured for the profile.
802.1X Authentication	802.1X authentication method configured for the port profile, such as No authentication, Client-based or Port-based.
Power over Ethernet	Operational state of Power over Ethernet (PoE) for the port profile. Displays information relate to the configured schedule.
References	Total number of physical ports currently using the port profile.

Hover the cursor over a policy, click the ••• button, and select one of the following options:

- **View Details**– Displays detailed information about the port profile configuration.
- **Duplicate**– Creates a copy of the existing port profile.
- **Delete**–Deletes the port profile. It is required to confirm the deletion in the **Confirm Profile Deletion** pop-up window.

Viewing the Port Profile Details

To view the Port Profile details page, use one of the following:

- Hover the cursor over a profile, click the ••• button, and select **View Details**.
- Click on the port profile name.
- Click anywhere on the port profile column, opens the port profile detail's panel on the right, then click **View Details**.

Exporting the Port Profile Table

The administrators can export the port profile table in a .csv format.

To export the port profile table, complete the following steps.

1. On the port profile page, click on the **Actions** drop-down menu.
2. Click **Export**.
3. The table is exported as a .csv file.

   The downloaded file includes details such as **Profile**, **(VLAN) Untagged Networks**, **Tagged Networks**, **802.1X Authentication**, **Power over Ethernet**, and **References**.

Deleting a Profile

1. Click the **Profiles** from the navigation pane on the left on the Instant On web application home page.
2. Under **Profiles** table, hover the cursor over the profile you want to delete, click the ••• button, and select **Delete** from the drop-down list.
3. In the **Confirm Profile Deletion** pop-up window, click **Delete Profile**.

Duplicating a Port Profile

To duplicate a port profile, complete the following steps:

1. Click the **Profiles** from the navigation pane on the left on the Instant On web application home page.
2. In the port profile table, hover the cursor over a profile, click the ••• button.
3. Click **Duplicate**.
4. On the **Identify the Profile** page, enter a name for the duplicate profile.
5. Click **Next**.
6. In the **Port Assignment** page, select the devices and is associated port to assign the port profile.
7. Click **Duplicate Port Profile**.

   The newly created port profile is displayed in the port profile table.

Creating a Port Profile

To create a Port Profile, complete the following steps:

1. On the Instant On web application home page, select **Profiles** from the left navigation pane. By default, the Port Profile table is displayed.
2. Under **Profiles** > **Ports**, click **Create Port Profile**.
3. Under **Identify the Profile** page, configure the following:
   - **Name**–Enter a name for the port profile.
   - **Port Options**–The **Speed/Duplex** option displays the link speed and how the port handles the traffic in both directions (Half or Full-Duplex). In the **Advanced Options** section, additional port-level configurations are available.

     The **Limit broadcast and Multicast Storms** configuration is an optional setting, and is enabled by default. Use the checkbox to enable or disable the **Limit broadcast and Multicast Storms** configuration. This configuration does not apply to the gateways.
4. Click **Next**.

   The **Port Security and Authentication** page is displayed.
5. This is an optional setting. Under **Port Security and Authentication** > **Security** > **Port 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** > **Security** > **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 do 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** > **802.1X 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. Click **Next**.

   The **Power Management** page is displayed. The **Power Management** page allows you to configure the Power over Ethernet (PoE) functionality and related power settings for ports that power other devices.

9. Under the **Power Management** > **Power Allocation**, select the PoE option.

   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 the **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 the **Power Management** > **Power Management Options** > **Power Schedule**, use the checkbox to either enable or disable the 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.

    For more information on configuring Power Schedule, see Power Management.

13. Click **Next**.

    The **Network Assignment** page is displayed.

14. In the **Network Assignment** page, 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. Click **Next**.

    The **Port Assignment** page is displayed.
16. Under the **Port Assignment** > **Device** drop-down list, select a device.

    The port associated with the selected 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. Click on the device drop-down list to select a device. A check mark appears on the top-right corner of the selected port 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. Click **Create Port Profile**.

    The new port profile is displayed in the port profile table.

Port Profile Details

The port profile displayed under the following categories:

Overview

Network Assignment

Port Assignment

Overview

The **Overview** tab of the port profile details page contains the following sections:

- **Identification**–Displays the name assigned to the port profile by the administrator.
- **Security** > **Port Security**–Displays the security configuration applied to the port profile.

  The different types of **Port Security** options are:
    - **Untrusted Port Protections (DHCP and ARP)**–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**–Not applicable to gateways and access points. This section displays the **Spanning Tree Protections** (STP) configuration applied to the port profile.

- **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** > **802.1X 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 62: *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	Maximum Power from PSE
Class 5	45 Watts
Class 6	60 Watts

- **Power Management** > **Port Priority**–Assigns a priority level to the ports. 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.

Power Mode is applicable only to the Instant On1840 and 1940 Switch Series

- **Power Management** > **Power Management Options**–This is an optional settings. Select the **Power Schedule** checkbox 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.
- **Port Options**–The **Speed/Duplex** option displays the link speed and how the port handles the traffic in both directions (Half or Full-Duplex). Allows you to modify the **Advanced Options**, such as enabling or disabling **Limit Broadcast and Multicast Storms**.
- **Delete Port Profile**–Allows you to permanently delete the port profile.

  To delete the port profile, follow these steps:

  a. Click **Delete**.

  b. In the **Confirm Profile Deletion** pop-up window, click **Delete Profile**.

After changing any configuration in the **Overview** page of the port profile, click **Update** to save the changes, or **Cancel** to discard changes.

Network Assignment

The **Network Assignment** tab of the port profile details page contains the following sections:

- **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 from the list. 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.

After changing any configuration in the **Network Assignment** page of the port profile, click **Update** to save, or click **Cancel** to discard changes.

Port Assignment

The **Port Assignment** tab of the port profile details page contains the following sections:

- **Device**

  Displays the list of devices supporting port profiles in the site. On selecting a device from the device drop-down list, displays its port assignment diagram.

  You can assign the port profile to multiple devices and ports. You can only select device ports if the parameters configured for the port profile are supported on selected device port. If the port profile is assigned to a device port, a check mark is displayed on the top-right corner of the port.

  To assign the port profile to all the available device port, click on **Assign to All**.

  To unassign the port profile for all the device ports, click on **Remove All**.

- **Selected Ports**

  Displays the list of device ports to which the port profile is assigned.

After changing any configuration in the **Port Assignment** page, click **Update** to save the changes, or click **Cancel** to discard changes.

RADIUS Profile Page

In the **RADIUS** profile page, the RADIUS profile table lists down all the RADIUS profiles configured. The table displays the following information:

Table 63: *RADIUS Profile Table*

Column	Description
Profile	Name of the RADIUS profile.
Primary Server	IP address or name of the primary RADIUS server.
Secondary Server	IP address or name of the secondary RADIUS server.

Table 63: *RADIUS Profile Table*

Column	Description
Accounting	Displays information if accounting is enabled or disabled for the RADIUS.
References	Total number of networks currently using the RADIUS profile.

Hover the cursor over a policy, click the ••• button, and select one of the following options:

- **View Details**– Displays detailed information about the port profile configuration.
- **Delete**–Deletes the port profile. It is required to confirm the deletion in the **Confirm Profile Deletion** pop-up window.

Viewing the RADIUS Profile Details

To view the RADIUS Profile details page, complete the following steps:

1. On the Instant On application home page, select **Profile** from the left-hand navigation pane.
   By default, the port profile table page is displayed.
2. Click **RADIUS**.
3. Use one of the following methods to view the port profile details:
   - Hover the cursor over a profile, click the ••• button, and select **View Details**.
   - Click on the port profile name.
   - Click anywhere on the port profile column, opens the RADIUS profile detail's panel on the right, then click **View Details**.

Exporting the RADIUS Profile Table

The administrators can export the port profile table in a .csv format.

To export the port profile table, complete the following steps.

1. On the port profile page, click on the **Actions** drop-down menu.
2. Click **Export**.
3. The table is exported as a .csv file.
   The downloaded file includes details such as **Profile**, **Primary Server**, **Secondary Server**, **Accounting** and **References**.

Deleting a RADIUS Profile

1. Click the **Profiles** from the navigation pane on the left on the Instant On web application home page.
2. Click **RADIUS**.
3. Under **Profiles** table, hover the cursor over the profile you want to delete, click the ••• button, and select **Delete** from the drop-down list.
4. In the **Delete Profile** pop-up window, click **Delete Profile**.

Creating a RADIUS Profile

To create a RADIUS Profile, complete the following steps:

1. On the Instant On web application home page, select **Profiles** from the left navigation pane.

   By default, the port profile table is displayed.
2. Click **RADIUS** from the left navigation pane.

   The **RADIUS** profile table is displayed.
3. Under **Profiles** > **RADIUS**, click **Create RADIUS Profile**.

   The **Identify the Profile** page is displayed.
4. In the **Name** text field, assign a name for the RADIUS profile.
5. Click **NEXT**.

   The **Set Authentication Servers** page is displayed.
6. This is an optional setting. Under the **Security** > **RADIUS Security** section, use the checkbox to enable or disable **Require RADIUS Message-Authenticator** option.
7. This is an optional setting. Under **Authentication Servers** > **RADIUS Options**, use the checkbox 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. Click **Next**.

    The **Set Network Access Attributes** page 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. Click **Create RADIUS Profile**.

    The new RADIUS profile is displayed in the RADIUS Profile table.

RADIUS Profile Details

The RADIUS profile configurations displayed under the following categories:

Overview

Network Assignment

Device Assignment

Overview

The **Overview** tab of the **RADIUS** profile details page contains the following sections:

- **Identification**— Displays the name assigned to the RADIUS profile by the administrator.
- **Security**—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**—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 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.

- **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 request. 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 connections that are applied to a network device. 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**.
- **Delete Profile**–Allows you to permanently delete the RADIUS profile.

  To delete the RADIUS profile, follow these steps:
  1. Click **Delete**.
  2. In the **Delete Profile** pop-up window, click **Delete Profile**.

After changing any configuration in the **Overview** page of the RADIUS profile, click **Update** to save the changes, or click **Cancel** to discard changes.

Network Assignment

The **Network Assignment** tab displays the network assignment configuration for the RADIUS profile.

The **Network Assignment** tab includes:

- **RADIUS Profile**–The **RADIUS Profile** drop-down list allows you to select a network referencing this RADIUS profile.
- **Identification**–The Identification section includes:
  - **Name**–Displays the network name that is selected from the list of networks referencing this RADIUS profile. On clicking over the network name, displays the network details page. For more information, see Networks.
  - **Health**– Displays the current network health status.
    - Good–Indicates that the health of the stack is good.
    - Fair–Indicates that the health of the stack is fair.
    - Poor–Indicates that the health of the stack is 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. On clicking the RADIUS profile name, opens the RADIUS Profile **Overview** page.

  For more information, see Overview.

After changing any configuration in the **Network Assignment** page of the RADIUS profile, click **Update** to save the changes, or click **Cancel** to discard changes.

Device Assignment

The **Device Assignment** tab of the RADIUS profile details page contains the following sections:

- **Device–**Displays the list of devices associated with the RADIUS profile. Use the device drop-down to select a device.
- **Identification**

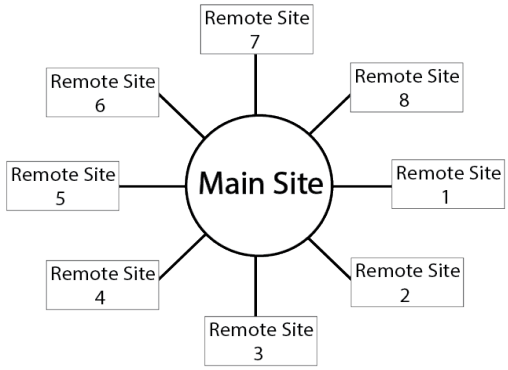
  On selecting a device from the drop-down list, the following information is displayed:
  - **Name**–Displays the name of the device referencing the RADIUS profile.
  - **Health**– Displays the device health status, such as **Good**, **Fair,** and **Poor**.
  - **State**–Displays whether the device is **Online** or **Offline**.
  - **Online Since**–Displays the date and time when the device entered the online state.
- **802.1X Authentication**

  Displays the name of the RADIUS profile associated with 802.1X Authentication for the selected device.

Chapter 17
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 displays the list of domains configured.

The details of the domains in the **Domains** page are listed under the following categories:

Table 64: *Domain Table*

Category	Description
Domain	Displays the name of the domain.
Health	Displays the health status of the domain: ■ Good–Indicates that the health of the tunnel between the remote and the main site is good. ■ Fair–Indicates the health of the tunnel between the remote and the main site is fair. ■ Poor–Indicates the health of the tunnel between the remote and the main site is poor.
Health Score	Displays the health percentage of the domain. The health score is calculated based on the operational status of VPN connections between the sites and 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%.

Table 64: *Domain Table*

Category	Description
Alerts	Displays the number of alerts triggered by the system when an unusual activity is observed in the domain. Types of Alerts and its Severities: ■ Major– The alerts classified as major are considered as the most severe by the system and prompt the user to take an immediate action. ■ Minor–The alerts are classified as minor when a degradation in performance is observed, but without any downtime. ■ Informational–The information alert indicates that a change has occurred in the domain, but there are no interruptions.
Sites	Displays the total number of sites in the domain, including the main site and all connected sites.

Hover the cursor over a domain, click the ••• button and select one of the following options:

- **View Details**–Allows you to view the details of the domain.
- **Delete**–The delete operation will permanently delete the current domain and all associated data. To delete a domain, you must enter the 6-digit numeric code displayed on the page.

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 **Managed Sites** page is displayed.
2. Click the List View icon ( ) on the top-right corner of the page to view the sites **Overview** page.
3. Click **Domains** tab in the sites list view, to view the domains page.
4. Click **Create Domain** button.

   The **Identify the Domain** page is displayed.
5. In **Identify the Domain** page, enter a name for the domain.

   The name of the domain must not exceed 64 characters.
6. In the **Main Site** drop-down, select a main site to which other remote 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.
7. Click **Next.**
8. 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.

9. Click **Next.**

10. In the **Specify Network Access** page, expand the network list and select the wired networks to allow access between the **Connected site** and the **Main site** networks.

NOTE

VLANs with the same IP subnet cannot be selected as the wired network between the connected site and the main site.

11. Click **Create Domain**.

Overview

To view the domain details page, complete following the steps:

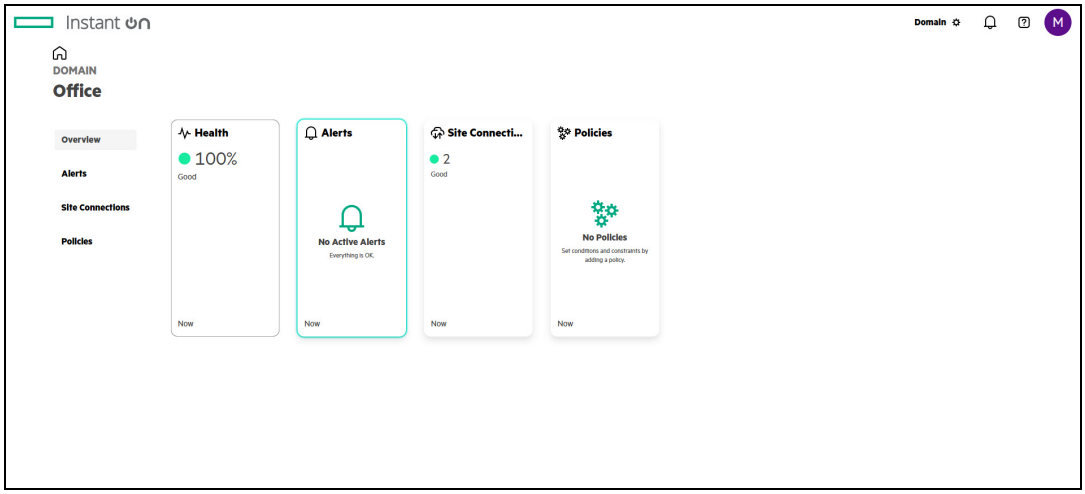
1. Login to your Instant On account using your administrator credentials. The **Managed Sites** page is displayed.
2. Click the List View icon ( ) on the top-right corner of the screen to view the sites **Overview** page.
3. Click **Domains** tab in the sites list view.

NOTE

To navigate back to the **Managed Sites** page, you must go back to the sites **Overview** page and click the Card View icon ( ) on the top-right corner of the screen.

4. Use one of the following methods to view the domain's details:
   a. Clicking on the domain name.
   b. Hover the cursor to the end of the row of the domain you want to view, click the ••• button, and select **View Details** from the drop-down list.

Figure 9 *Domain Dashboard*



The domain details page comprises of the following components:

Content	Description
Instant On logo	Displays the Instant On logo and functions as a button to return to the Instant On home page.

Content	Description
Domain Management()	Clicking this icon takes you to the **Domain management** page. For more information, see Domain Management.
Alerts ( )	Displays the alerts that are triggered by the system when an unusual activity is observed in the domain. See Alerts for more information.
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 between the sites and valid communication-enabling policies.
Alerts	Displays the list of alerts generated at the domain. See Alerts for more information.
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 a health counter for all the connected sites. See Site Connections for more information.
Policies	Displays the number of active and total policies configured for the domain. See Policies for more information.

Domain Management

Click the domain management icon () at the top-right corner of the UI screen. The **Domain Management** page displays the following user settings that can be modified in the Instant On application:

- Identification
- Delete Domain

Identification

The **Identification** page allows you to modify the domain name.

Delete Domain

Deleting a domain shall permanently delete the current domain and all associated data. To delete a domain, you must enter the 6-digit numeric code displayed on the page.

Alerts

Alerts are triggered by the system when an unusual activity is observed with the domain.

To view the **Alerts** page, click the **Alerts** ( ) tile on the domain details page or from the navigation pane on the left.

The **Overview** tab in the Alerts page displays the list of alerts under the following:

Category	Description
Alert	Displays the short summary of the alert generated.
Severity	Displays the severity of the alert generated.
Source	Displays site name for which the alert is generated.

Category	Description
State	Displays if the alert is active or cleared.
Raised	Displays the time at which the alert was received.
Cleared	Displays the time at which the alert was cleared.

The different types of alerts are classified as follows:

Table 65: *Types of Alerts and its Severities*

Alert Type (Severity)	Icon	Description
Major		The alerts classified as major are considered as the most severe by the system and prompt the user to take an immediate action.
Minor		The alerts are classified as minor when a degradation in performance is observed, but without any downtime. .
Informational		The information alert indicates a change has occurred in the domain, but there are no interruptions.

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 **Alerts (** **)** tile on the site home page will display a **No Active Alerts** message.

The search bar allows your to use the search functionality to view a specific alert.

The table below shows the list of possible alerts:

Table 66: *List of Alerts*

Name	Severity	Condition	Description
Domain offline	Major	All tunnels are down (main site)	All connections to the domain are down (main site).
Connection to domain offline	Minor	Tunnel down (connected site)	The connection to the domain is down (connected site). Minor at first, becomes major after 5 min.
WAN offline	Minor	WAN connection is offline	A WAN connection is offline.

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

Alert Details

You can view the additional details for an alert. Click on any alert in the table to view the details in the right side panel. The right panel displays the following information:

- Severity
- Source
- Date and time the alert was raised
- Date and time the alert was cleared
- Time duration
- Symptoms
- Probable causes
- Recommended Actions

Exporting the Alerts Table

The administrators can export the alerts table in a .csv format.

To export the alerts table, complete the following steps.

1. Click on the **Actions** drop-down.
2. Click **Export**.
3. Specify the location to save the export file and assign a name to the export file.
4. Click **Save**.

   The alerts table is successfully exported. The downloaded .csv file contains alerts information such as severity, source, state, alerts generated time, and alert clear time.

Site Connections

The **Site Connections** > **Overview** page displays information about all sites that are connected to the main site for the specific domain.

The table includes the following information:

Category	Description
Site	Name of the site that are connected to the main site to create a domain
Health	Displays the health status of the site: ■ Good–Indicates that the health of the device is good. ■ Fair–Indicates the health of the device is fair. ■ Poor–Indicates the health of the device is poor.
Connection State	The connection status of the site.
Connection State Duration	Displays the time duration the site is in a connected to the domain without any interruption.
WAN IP Address	Displays the WAN IP Address of the site. It is a valid IPv4 address assigned by an Internet Service Provider through DHCP.
Public Address	Displays the Public IP Address of the site. The Public IP Address of a site is its external IP address that is visible on the internet. It is the IP Address reachable from the Internet, assigned by the Internet Service Provider.
24-hour Usage	Total amount of data used during the last 24 hours.

Removing a Connected Site

To remove a site from the domain, hover the cursor over a site, click the ••• button and select **Remove Site**.

Exporting the Site Connections Table

The administrators can export the alerts table in a .csv format.

To export the alerts table, complete the following steps.

1. Click on the **Actions** drop-down.
2. Click **Export**.
3. Specify the location to save the export file and assign a name to the export file.
4. Click **Save**.
5. The site connection table is successfully exported. The downloaded .csv file contains information such as site name, health, connection state, connection state duration, WAN IP address, public IP Address and 24-hour usage for all remote sites that are connected to the main site in the selected domain.

Adding Sites

To add a site from the **Site Connections** page, complete the following steps:

1. Click **Add Site**.
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. Click **Next**.
4. In the **Specify Network Access** page, expand the network list and select the wired networks to allow access between the **Connected site** and the **Main site** networks.
5. Click **Add Site**.

Main Site

The **Site Connections** > **Main Site** page displays information about the main site such as:

- **Identification**–Name of the main site.
- **Connectivity**–Connection details such as WAN IP address, subnet mask and public IP Address.

Policies

The **Policies** page 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 **View Details** allows you to view the domain policy and update the domain policy. To view the domain policy details, you can do the following:

- Click on the policy name.
- Hover the cursor over a domain policy, click the ••• button and **View Details**.

To view the **Policies** page, click the **Policies** () tile on the domain details page or from the navigation pane on the left.

Domain Policy Details

The domain policy details page allows the administrators to view the policy details and manage or update the **Network Access** policy.

The domain policy details are displayed under the following categories:

- Identification
- Rule
- Connected Site
- Main Site

Identification

The **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. Click on the **Name** text box to update the name for the domain 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.

The **LAN Network Types** section displays the policy rule applies to which network categories–**Wireless**, **Wired**, and **VPN**. which includes the following:

- **Wireless Networks**–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 Networks**–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 Networks**–When **VPN Networks** is **ON**, the **VPN Network** name is displayed below the **VPN Networks** label.

Connected Site

The **Connected Site** displays the remote site connected to the main site. The **Wired Networks** displays all the available remote site's wired network connections. To enable a wired connection to connect to the main site, selecting the checkbox adjacent to the specific wired network.

Main Site

The **Main Site** displays the name of the main site and the selected wired networks that connect to the remote site. To enable a wired connection, to connect to the remote site select the checkbox adjacent to the specific wired network.

After updating the domain policy, select one of the options:

- **Update**–To save the configuration changes.
- **Cancel**–To cancel the configuration changes done for the domain policy.