

Aruba Central



a Hewlett Packard
Enterprise company

User Guide

Copyright Information

© Copyright 2020 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

| | |
|--|-----------|
| Contents | 3 |
| About this Guide | 24 |
| Intended Audience | 24 |
| Related Documents | 24 |
| Conventions | 24 |
| Contacting Support | 25 |
| What is Aruba Central? | 26 |
| Key Features | 26 |
| Supported Web Browsers | 27 |
| Operational Modes and Interfaces | 27 |
| Standard Enterprise Mode | 27 |
| Managed Service Provider Mode | 28 |
| Supported Devices | 29 |
| Supported Instant APs | 29 |
| Supported Switch Platforms | 32 |
| Supported Aruba Gateways | 33 |
| Getting Started with Aruba Central | 35 |
| Key Terms and Concepts | 35 |
| Workflow Summary | 36 |
| Creating an Aruba Central Account | 37 |
| Zones and Sign Up URLs | 37 |
| Signing up for an Aruba Central Account | 37 |
| Accessing Aruba Central Portal | 41 |
| Login URLs | 41 |
| Logging in to Aruba Central | 41 |
| Changing Your Password | 42 |
| Logging Out of Aruba Central | 42 |
| Accessing Aruba Central Mobile Application | 42 |
| About the Network Operations User Interface | 42 |
| Workflow to Navigate the Network Operations User Interface | 43 |
| About the Standard Enterprise Mode User Interface | 44 |
| Launching the Network Operations App | 45 |
| Parts of the Network Operations App User Interface | 45 |
| Search Bar | 46 |
| Help Icon | 47 |

| | |
|--|-----------|
| Account Home Icon | 47 |
| User Icon | 47 |
| Filter | 48 |
| Time Range Filter | 48 |
| Left Navigation Pane | 48 |
| Launching the Global Dashboard | 48 |
| Manage | 48 |
| Analyze | 49 |
| Maintain | 49 |
| Launching the Network Operations App for MSP | 50 |
| Parts of the Network Operations App for MSP | 50 |
| Search Bar | 51 |
| Help Icon | 52 |
| Account Home Icon | 52 |
| User Icon | 52 |
| Filter | 53 |
| Time Range Filter | 53 |
| Left Navigation Pane | 53 |
| Launching the MSP Global Dashboard | 53 |
| Manage | 54 |
| Analyze | 54 |
| Maintain | 54 |
| Launching the MSP Group Dashboard | 54 |
| Manage | 55 |
| Starting Your Free Trial | 55 |
| Get Started with the Free Trial | 56 |
| Using the Initial Setup Wizard | 57 |
| Using the Device Inventory Page | 57 |
| Setting up Your Aruba Central Instance | 59 |
| Getting Started with Aruba Central | 60 |
| In the Initial Setup Wizard | 61 |
| From the Device Inventory Page | 62 |
| Manually Adding Devices | 62 |
| Email Notifications for Software Upgrades | 65 |
| Enabling Email Notifications | 66 |
| Search Bar | 66 |
| | 69 |
| Account Home | 70 |
| Apps | 70 |

| | |
|---|----|
| Network Operations | 70 |
| ClearPass Device Insight | 71 |
| Global Settings | 71 |
| Managing Your Device Inventory | 71 |
| Viewing Devices | 72 |
| Adding Devices to Inventory | 72 |
| Onboarding Devices | 72 |
| Adding Devices (Evaluation Account) | 73 |
| Using the Initial Setup Wizard | 73 |
| Using the Device Inventory Page | 73 |
| Adding Devices (Paid Subscription) | 73 |
| In the Initial Setup Wizard | 73 |
| From the Device Inventory Page | 73 |
| Manually Adding Devices | 74 |
| Adding Devices Using MAC address and Serial Number | 74 |
| Adding Devices Using Activate Account | 75 |
| Adding Devices Using Cloud Activation Key | 75 |
| Key Management | 76 |
| Evaluation Subscription Key | 76 |
| Upgrading to a Paid Account | 77 |
| Paid Subscription Key | 77 |
| Adding a Subscription Key | 77 |
| Viewing Subscription Key Details | 78 |
| Managing Subscriptions | 78 |
| Assigning Subscriptions | 79 |
| Assigning Device Subscriptions | 79 |
| Enabling Automatic Assignment of Subscriptions | 79 |
| Manually Assigning Subscriptions | 80 |
| Assigning Network Service Subscriptions | 80 |
| Assigning Gateway Subscriptions | 81 |
| Gateway Subscriptions | 81 |
| Assigning Subscriptions to Gateways | 81 |
| Virtual Gateway Subscriptions | 81 |
| Removing Subscriptions from Devices | 82 |
| Removing a Device Subscription from a Device | 82 |
| Removing a Network Service Subscription from a Device | 82 |
| Understanding Device Subscription Expiration Dates | 83 |
| Acknowledging Subscription Expiry Notifications | 83 |
| Acknowledging Notifications through Email | 83 |
| Acknowledging Notifications in the UI | 83 |

| | |
|---|----|
| Renewing Subscriptions | 83 |
| Managing Sites | 84 |
| Creating a Site | 84 |
| Adding Multiple Sites in Bulk | 85 |
| Assigning a Device to a Site | 85 |
| Converting Existing Labels to Sites | 85 |
| Editing a Site | 86 |
| Deleting a Site | 86 |
| Managing Labels | 86 |
| Creating a Label | 87 |
| Assigning a Label to a Device | 87 |
| Detaching a Device from a Label | 88 |
| Editing a Label | 88 |
| Deleting a Label | 88 |
| Groups for Device Configuration and Management | 88 |
| Group Operations | 89 |
| Group Configuration Modes | 89 |
| Default Groups and Unprovisioned Devices | 90 |
| Best Practices and Recommendations | 90 |
| Working with Groups | 90 |
| Managing Groups | 91 |
| Creating a Group | 91 |
| Assigning Devices to Groups | 92 |
| Viewing Groups and Associated Devices | 92 |
| Creating a New Group by Importing Configuration from a Device | 93 |
| Cloning a Group | 93 |
| Moving Devices between Groups | 93 |
| Configuring Device Groups | 93 |
| Configuring Groups in MSP Mode | 93 |
| Deleting a Group | 94 |
| Moving an IAP Between Groups | 94 |
| Provisioning Devices Using UI-based Workflows | 94 |
| Provisioning Instant APs using UI-based Configuration Method | 94 |
| Provisioning Switches Using UI-based Configuration Method | 96 |
| Provisioning Aruba Gateways Using UI-based Configuration Method | 96 |
| Provisioning Devices Using Configuration Templates | 98 |
| Creating a Group with Template-Based Configuration Method | 98 |
| Provisioning Devices Using Configuration Templates and Variable Definitions | 99 |
| Editing a Template | 99 |
| Managing Variable Files | 99 |

| | |
|---|-----|
| Downloading a Sample Variables File | 99 |
| Modifying a Variable File | 100 |
| Uploading a Variable File | 103 |
| Modifying Variables | 104 |
| Backing Up and Restoring Configuration Templates | 104 |
| Important Points to Note | 104 |
| Creating a Configuration Backup | 105 |
| Viewing Contents of a Backed Up Configuration | 105 |
| Restoring a Backed Up Configuration | 106 |
| Managing Backups | 106 |
| Backing Up and Restoring Templates and Variables Using APIs | 107 |
| Viewing Configuration Status | 107 |
| Accessing the Configuration Audit Page | 107 |
| Applying Configuration Changes | 108 |
| Auto Commit Workflow | 108 |
| Manual Commit Workflow | 108 |
| Viewing Configuration Overrides and Errors | 109 |
| Viewing Configuration Status for Devices at the Group Level (Template Configuration Mode) | 110 |
| Viewing Configuration Status for a Device (Template Configuration Mode) | 110 |
| Viewing Configuration Status for Devices at the Group Level (UI-based Configuration Mode) | 111 |
| Viewing Configuration Status for a Device (UI-based Configuration Mode) | 111 |
| Backing up and Restoring Configuration Templates | 111 |
| Connecting Devices to Aruba Central | 112 |
| Domain names for Aruba Central Portal Access | 112 |
| Domain Names for Device Communication with Aruba Central | 113 |
| Domain Names for Device Communication with Aruba Activate | 113 |
| Cloud Guest Server Domains for Guest Access Service | 114 |
| Domain Names for OpenFlow | 114 |
| Other Domain Names | 115 |
| Connecting Instant APs to Aruba Central | 116 |
| Connecting Aruba Switches to Aruba Central | 116 |
| Connecting SD-WAN Gateways to Aruba Central | 116 |
| Certificates | 118 |
| Uploading Certificates | 118 |
| Managing Certificates on Instant APs Configured Using Templates | 119 |
| Managing Software Upgrades | 119 |
| Viewing Firmware Details | 119 |
| Upgrading a Device | 121 |
| Setting Firmware Compliance | 122 |
| Using Troubleshooting Tools | 122 |

| | |
|---|-----|
| Troubleshooting Network Issues | 123 |
| Troubleshooting AP Connectivity Issues | 124 |
| Troubleshooting Switch Connectivity Issues | 126 |
| Troubleshooting Gateway Connectivity Issues | 127 |
| Viewing the Device Output | 128 |
| Troubleshooting Device Issues | 128 |
| Viewing the Device Output | 129 |
| Advanced Device Troubleshooting | 130 |
| Troubleshooting Access Points | 130 |
| Troubleshooting Switches | 131 |
| Troubleshooting Gateways | 131 |
| Filtering Commands | 132 |
| Viewing the Device Output | 132 |
| Viewing Audit Trails in the Account Home Page | 133 |
| Viewing Audit Trails in the Standard Enterprise Mode | 134 |
| Classification of Audit Trails | 134 |
| Removing Devices | 135 |
| Removing a Device from the Device Inventory Page | 135 |
| Users and Roles | 135 |
| Configuring System Users | 136 |
| Adding a System User | 136 |
| Resend Email Invite | 137 |
| Viewing User Details | 138 |
| Editing a User | 138 |
| Deleting a User | 138 |
| Viewing Audit Trail Logs for Users | 138 |
| Configuring User Roles | 139 |
| Predefined User Roles | 139 |
| Custom Roles | 140 |
| Adding a Custom Role | 140 |
| Module Permissions | 141 |
| Viewing User Role Details | 142 |
| Editing a User Role | 142 |
| Deleting a User Role | 142 |
| Two-Factor Authentication | 142 |
| Installing the Google Authenticator App | 143 |
| Enabling Two-factor Authentication for User Accounts | 143 |
| Two-factor Authentication for Aruba Central Web Application | 143 |
| Two-factor Authentication for the Aruba Central Mobile App | 144 |
| Registering a New Mobile Device | 144 |

| | |
|--|------------|
| Support Access | 144 |
| Enabling Support Access | 144 |
| Disabling Support Access | 144 |
| Monitoring Your Network | 145 |
| Overview | 145 |
| APs | 145 |
| Navigation and Granularity | 146 |
| Access Points Table | 146 |
| AP Details Page View | 148 |
| Filters | 148 |
| AP Details Panel | 148 |
| Left Pane in AP Details Page | 149 |
| APs—Overview Tab | 150 |
| Device | 150 |
| Network | 150 |
| Radios | 150 |
| Data Path | 151 |
| Health Status | 151 |
| APs—AI Insights | 151 |
| Excessive AP Channel Changes | 152 |
| Clients with Low SNR Uplink Connections | 152 |
| AP with High Memory Utilization | 152 |
| AP with High 2.4 GHz Airtime Utilization | 152 |
| AP with High 5 GHz Airtime Utilization | 153 |
| Frequent AP Transmit Power Changes | 153 |
| AP with Missing Telemetry | 153 |
| AP with High CPU Utilization | 153 |
| Excessive AP Reboots | 154 |
| MAC Authentication Failures | 154 |
| 4-way Handshake (EAPOL Key) Failures | 154 |
| 802.1x Authentication Failures | 154 |
| High DHCP Failures | 154 |
| APs—Usage Tab | 155 |
| APs—Spectrum Tab | 155 |
| Channel Utilization and Quality | 156 |
| Non-WiFi Interferers List | 157 |
| Spectrum Scan Feature | 158 |
| APs—Clients Tab | 158 |
| APs—RF Tab | 158 |

| | |
|--|-----|
| Channel Utilization | 158 |
| Noise Floor | 158 |
| Frames | 159 |
| Channel Quality | 159 |
| RF Neighbors | 159 |
| APs—Tunnels Tab | 159 |
| VPNC | 159 |
| Gateway | 160 |
| APs—Location Tab | 160 |
| APs—Alerts & Events Tab | 160 |
| APs—Actions | 160 |
| Live Instant AP Monitoring | 161 |
| Enabling and Disabling Live Monitoring | 161 |
| AP Details in Go Live Mode | 161 |
| Renaming an AP | 162 |
| Deleting an Offline AP | 162 |
| Monitoring Switches and Switch Stacks | 162 |
| Switch Details | 164 |
| Switches—Overview Tab | 164 |
| Switch | 164 |
| Network | 165 |
| Ports | 165 |
| Hardware | 166 |
| Uplink | 166 |
| Usage | 167 |
| Stack Members | 167 |
| Switches—Ports Tab | 168 |
| Port Status | 168 |
| Faceplate | 168 |
| Ports | 168 |
| Viewing Port-Level Information | 168 |
| Switches—PoE Tab | 169 |
| PoE Status | 169 |
| Faceplate | 169 |
| Ports PoE | 169 |
| PoE Consumption | 170 |
| Viewing PoE Port-Level Information | 170 |
| Switches—VLANs Tab | 171 |
| VLANs | 171 |
| Faceplate | 172 |

| | |
|---|-----|
| Switches—Routing Tab | 172 |
| Routing | 173 |
| Switches—Hardware Tab | 173 |
| Hardware | 173 |
| Power Supplies | 174 |
| Fans | 174 |
| CPU | 174 |
| Memory | 174 |
| Temperature | 174 |
| Switches—Connected Tab | 174 |
| Client Devices | 174 |
| Neighbour Devices | 175 |
| Switches—Actions | 175 |
| Deleting an Offline Switch | 175 |
| Assigning Uplink Ports | 176 |
| Gateways | 176 |
| Page Views | 176 |
| Gateway Details Page | 177 |
| Gateways—Overview Tab | 179 |
| Gateway—WAN Tab | 181 |
| Gateways—LAN Tab | 187 |
| Gateways—Tunnels Tab | 192 |
| Gateways—Routing Tab | 194 |
| Gateways—Path Steering Tab | 206 |
| Application Visibility | 208 |
| Gateways—Sessions Tab | 209 |
| Deleting an Offline Gateway | 211 |
| WIDS Events | 212 |
| Overview | 212 |
| Viewing Intrusion Details Page | 212 |
| Intrusion Detection System Events Configuration | 212 |
| Monitoring WIDS Events | 212 |
| Intrusion Detection | 212 |
| Generating Alerts for Security Events | 213 |
| Generating Reports for Security Events | 214 |
| Network Health Dashboard | 214 |
| Overview | 215 |
| Summary | 216 |
| Site Health Dashboard | 217 |
| Wi-Fi Connectivity | 219 |

| | |
|---|-----|
| Connectivity Summary Bar | 219 |
| Connection Experience | 220 |
| AI Insights | 220 |
| Connection Problems | 221 |
| Connection Events | 222 |
| AI Insights | 223 |
| AI Insights Categories | 223 |
| 802.1X Authentication Failures | 224 |
| 4-way Handshake (EAPOL Key) Failures | 225 |
| AP with Missing Telemetry | 225 |
| AP Transmit Power Recommendation | 225 |
| AP with High 2.4 GHz Airtime Utilization | 225 |
| AP with High 5 GHz Airtime Utilization | 226 |
| AP with High Memory Utilization | 226 |
| Clients with Excessive 2.4 GHz Dwell Time | 226 |
| Excessive AP Channel Changes | 226 |
| Excessive AP Reboots | 227 |
| Frequent AP Transmit Power Changes | 227 |
| Clients with Low SNR Uplink Connections | 227 |
| AP with High CPU Utilization | 227 |
| High DHCP Failures | 228 |
| MAC Authentication Failures | 228 |
| Sites—AI Insights | 228 |
| 802.1X Authentication Failures | 229 |
| 4-way Handshake (EAPOL Key) Failures | 229 |
| AP with Missing Telemetry | 229 |
| AP with High 2.4 GHz Airtime Utilization | 230 |
| AP with High 5 GHz Airtime Utilization | 230 |
| AP with High Memory Utilization | 230 |
| Clients with Excessive 2.4 GHz Dwell Time | 231 |
| Excessive AP Channel Changes | 231 |
| Excessive AP Reboots | 231 |
| Frequent AP Transmit Power Changes | 231 |
| Clients with Low SNR Uplink Connections | 232 |
| AP with High CPU Utilization | 232 |
| High DHCP Failures | 232 |
| MAC Authentication Failures | 232 |
| All Clients | 233 |
| Client Overview | 236 |
| Wireless Client Overview | 237 |

| | |
|--|-----|
| Viewing Clients Connected to Wireless Networks | 237 |
| Wireless Client Summary | 237 |
| Wireless Client Summary | 237 |
| Wireless Client Details | 238 |
| Wireless Client Sessions | 243 |
| Applications | 244 |
| Live Events | 244 |
| Events | 245 |
| Tools | 245 |
| Live Client Monitoring | 245 |
| Disconnecting a Wireless Client from an AP | 246 |
| Live Events | 246 |
| Troubleshooting a Client | 246 |
| Live Events Details | 247 |
| Wired Client Overview | 247 |
| Viewing Clients Connected to Wired Networks | 247 |
| Wired Client Summary | 247 |
| Wired Client Summary | 247 |
| Wired Client Details | 248 |
| Wired Client Sessions | 249 |
| Applications | 250 |
| Events | 251 |
| Tools | 251 |
| Application Visibility | 251 |
| Visibility Dashboard | 252 |
| Applications | 252 |
| Websites | 252 |
| Blocked Traffic | 253 |
| VisualRF | 254 |
| VisualRF Dashboard | 254 |
| Viewing Network Information | 255 |
| Customizing the Floor Plan View | 255 |
| Viewing Campus, Sites, Buildings, and Floors | 255 |
| Viewing AP Overlay Information | 257 |
| Viewing Client Devices | 258 |
| Planning and Provisioning Devices | 258 |
| Creating a Campus | 258 |
| Creating a Building | 258 |
| Creating a Floor Plan | 259 |
| Importing a Floor Plan | 260 |

| | |
|--|------------|
| Modifying Floor Plan Properties | 260 |
| Adding Devices to the Floor Plan | 261 |
| Printing a Bill of Materials Report | 261 |
| VisualRF APIs | 261 |
| Topology | 262 |
| Before You Begin | 262 |
| Viewing the Topology Map | 262 |
| Grouping VPN Concentrators | 263 |
| Example of a Topology Map: | 263 |
| Details and Filter Pane | 263 |
| Alerts & Events | 265 |
| Viewing the Alerts Summary | 265 |
| Viewing the Events Summary | 266 |
| Advanced Event Filtering | 266 |
| Configuring Alerts | 267 |
| User Alerts | 268 |
| Switch Alerts | 268 |
| Gateway Alerts | 270 |
| Access Point Alerts | 271 |
| Connectivity Alerts | 272 |
| WAN Health Alerts | 272 |
| Audit Alerts | 273 |
| Site Alerts | 274 |
| Viewing Enabled Alerts | 274 |
| Reports | 275 |
| Report Categories | 275 |
| Creating a Report | 281 |
| Editing a Report | 282 |
| Viewing a Report | 283 |
| Downloading a Report | 283 |
| Deleting a Report | 283 |
| Deleting Multiple Reports | 284 |
| Viewing Audit Trails in the Standard Enterprise Mode | 284 |
| Classification of Audit Trails | 285 |
| Instant APs | 286 |
| Supported Deployment Modes | 286 |
| Configuration and Management | 286 |
| Provisioning Instant APs | 287 |
| Deploying a Wireless Network Using Instant APs | 287 |

| | |
|--|-----|
| Setting Country Code | 288 |
| Country Code Configuration in Aruba Central from UI | 288 |
| Setting Country Code at Group Level | 288 |
| Setting Country Code at Device Level | 289 |
| Country Code Configuration at Group Level from API | 289 |
| Configuring Device Parameters | 290 |
| Configuring External Antenna | 293 |
| EIRP and Antenna Gain | 293 |
| Configuring Antenna Gain | 294 |
| Adding an Instant AP | 294 |
| Deleting an Instant AP from the Network | 294 |
| Configuring System Parameters for an AP | 294 |
| Configuring VLAN Name and VLAN ID | 298 |
| Points to remember | 299 |
| Configuring Dual 5 GHz Radio Bands on an Instant AP | 299 |
| Configuring Network Profiles on Instant APs | 300 |
| Configuring Wireless Network Profiles on Instant APs | 300 |
| Creating a Wireless Network Profile | 301 |
| Configuring VLAN Settings for Wireless Network | 305 |
| Configuring Security Settings for Wireless Network | 306 |
| Configuring ACLs for User Access to a Wireless Network | 311 |
| Viewing Wireless SSIDs Summary Table | 312 |
| Management Frames Protection | 312 |
| Enabling Management Frames Protection Feature for Wireless Networks in Aruba Central | 312 |
| Client Isolation | 312 |
| Enabling Client Isolation Feature for Wireless Networks in Aruba Central | 312 |
| Configuring Wireless Networks on Guest Users on Instant APs | 313 |
| Splash Page Profiles | 313 |
| Configuring Access Points Ports Networks on Guest Users on Instant APs | 319 |
| Splash Page Profiles | 320 |
| Configuring Network Port Profile AssignmentDownloadable User Roles | 326 |
| ClearPass Policy Manager Certificate Validation for Downloadable User Roles (DUR) | 327 |
| Enabling Downloadable User Roles Feature for Wireless Networks in Aruba Central | 327 |
| Enabling Downloadable User Roles Feature for Wired Networks in Aruba Central | 328 |
| Configuring Wired Port Profiles on Instant APs | 328 |
| Configuring General Network Profile Settings | 329 |
| Configuring VLAN Settings | 329 |
| Configuring Security Settings | 330 |
| Configuring Access Settings | 331 |
| Configuring Network Port Profile Assignment | 332 |

| | |
|--|-----|
| Viewing Wired Port Profile Summary Table | 332 |
| Editing a WLAN Profile | 332 |
| Editing a Access Points Ports Profile | 333 |
| Deleting a Network Profile | 333 |
| Aruba Mesh Network and Mesh Instant AP | 333 |
| Mesh Network Overview | 333 |
| Mesh Instant APs | 334 |
| Instant AP as Mesh Portal | 334 |
| Instant AP as Mesh Point | 334 |
| Automatic Mesh Role Assignment | 334 |
| Mesh Role Detection during System Boot-Up | 334 |
| Mesh Role Detection during System Running Time | 335 |
| Setting up Instant Mesh Network | 335 |
| Configuring Wired Bridging on Ethernet 0 for Mesh Point | 335 |
| Mesh Cluster Function | 336 |
| Configuring Time-Based Services for Wireless Network Profiles | 336 |
| Before You Begin | 336 |
| Creating a Time Range Profile | 336 |
| Configuring ARM and RF Parameters on Instant APs | 338 |
| ARM Overview | 338 |
| Configuring ARM Features | 339 |
| Configuring Radio Parameters | 342 |
| Configuring IDS Parameters on APs | 343 |
| Rogue APs | 344 |
| Configuring Wireless Intrusion Detection and Protection Policies | 344 |
| Detection | 344 |
| Protection | 346 |
| Firewall Settings | 347 |
| Configuring Authentication and Security Profiles on Instant APs | 347 |
| Supported Authentication Methods | 347 |
| Support for Multiple PSK in WLAN SSID | 352 |
| Points to Remember | 352 |
| WPA3 Encryption | 353 |
| WPA3-Enterprise | 353 |
| Configuring WPA3 for Enterprise Security for Wireless Network | 354 |
| Configuring WPA3 for Personal Security | 354 |
| Authentication Servers for Instant APs | 354 |
| External RADIUS Server | 354 |
| RADIUS Server Authentication with VSA | 355 |
| Internal RADIUS Server | 355 |

| | |
|--|-----|
| Authentication Termination on Instant AP | 355 |
| Dynamic Load Balancing between Authentication Servers | 356 |
| Configuring External Authentication Servers for APs | 356 |
| Configuring Users Accounts for the Instant AP Management Interface | 359 |
| Configuring Guest and Employee User Profiles on Instant APs | 360 |
| Configuring Roles and Policies on Instant APs for User Access Control | 361 |
| ACL Rules | 361 |
| Configuring Network Address Translation Rules | 362 |
| Configuring Network Service ACLs | 362 |
| Configuring User Roles for AP Clients | 364 |
| Configuring Role Derivation Rules for AP Clients | 365 |
| Configuring Firewall Parameters for Wireless Network Protection | 367 |
| Configuring Firewall Parameters for Inbound Traffic | 367 |
| Configuring ACLs for Deep Packet Inspection | 370 |
| Configuring ACLs on APs for Website Content Classification | 372 |
| Configuring Custom Redirection URLs for Instant AP Clients | 373 |
| Creating a List of Error Page URLs | 373 |
| Configuring ACL Rules to Redirect Users to a Specific URL | 374 |
| Configuring Firewall Parameters for Inbound Traffic | 374 |
| Enabling ALG Protocols on Instant APs | 377 |
| Blacklisting Instant AP Clients | 377 |
| Configuring Instant APs for VPN Services | 378 |
| Instant AP VPN Overview | 378 |
| Supported VPN Protocols | 379 |
| Configuring Instant APs for VPN Tunnel Creation | 379 |
| Configuring IPsec VPN Tunnel | 380 |
| Configuring Automatic GRE VPN Tunnel | 381 |
| Configuring a GRE VPN Tunnel | 381 |
| Configuring an L2TPv3 VPN Tunnel | 382 |
| Configuring Routing Profiles for Instant AP VPN | 383 |
| Configuring DHCP Pools and Client IP Assignment Modes on Instant APs | 384 |
| Configuring DHCP Scopes on Instant APs | 384 |
| Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients | 390 |
| Configuring Services | 391 |
| Configuring AirGroup Services | 391 |
| AirGroup Features | 392 |
| AirGroup Services | 392 |
| Configuring an Instant AP for RTLS Support | 394 |
| Configuring an Instant AP for ALE Support | 395 |
| ALE with Aruba Central | 395 |

| | |
|---|------------|
| Enabling ALE support on an Instant AP | 395 |
| Managing BLE Beacons | 395 |
| Support for BLE Asset Tracking | 396 |
| Configuring OpenDNS Credentials on Instant APs | 396 |
| Configuring CALEA Server Support on Instant APs | 397 |
| Configuring Instant APs for Palo Alto Networks Firewall Integration | 398 |
| Configuring an Instant AP for Network Integration | 398 |
| Configuring XML API Interface | 399 |
| Application Visibility and Deep Packet Inspection | 399 |
| Enabling Application Visibility Service on APs | 400 |
| Configuring Uplink Interfaces on Instant APs | 400 |
| Uplink Interfaces | 400 |
| Uplink Preferences and Switching | 404 |
| Enforcing Uplinks | 404 |
| Setting an Uplink Priority | 405 |
| Enabling Uplink Pre-emption | 405 |
| Switching Uplinks based on the Internet Availability | 405 |
| Configuring Preferred Uplink on AP-318 and 370 Series APs | 406 |
| Configuring Enterprise Domains | 406 |
| Configuring SNMP Parameters | 407 |
| Configuring Community String for SNMP | 408 |
| Configuring SNMP Traps | 408 |
| Configuring Syslog and TFTP Servers for Logging Events | 409 |
| Configuring Syslog Server on Instant APs | 409 |
| Configuring TFTP Dump Server Instant APs | 410 |
| Resetting an AP | 411 |
| Rebooting APs | 411 |
| Mapping Instant AP Certificates | 412 |
| Configuring HTTP Proxy on Instant AP | 413 |
| Configuring APs Using Templates | 413 |
| Sample Template | 415 |
| Password Management in Configuration Templates for AP | 417 |
| Aruba Switches | 419 |
| Supported Switch Platforms | 419 |
| Getting Started with Aruba Switch Deployments | 421 |
| Provisioning Workflow | 421 |
| Provisioning a Factory Default Switch | 421 |
| Provisioning a Pre-configured or Locally-Managed Switch | 421 |
| Group Assignment | 421 |

| | |
|---|-----|
| Configuration and Management | 422 |
| Switch Monitoring | 422 |
| Troubleshooting and Diagnostics | 423 |
| Provisioning Factory Default Switches | 423 |
| Step 1: Onboard the Switch to Aruba Central | 423 |
| Step 2: Assign the Switch to a Group | 423 |
| Step 3: Connect the Switch to Aruba Central | 424 |
| Step 4: Provision the Switch to a Group | 424 |
| Step 5: Verify the configuration Status | 426 |
| Provisioning Pre-Configured Switches | 426 |
| Workflow 1—Pre-Provisioning a Switch | 427 |
| Step 1: Onboard the Switch to Aruba Central | 427 |
| Step 2: Assign the Switch to a Group | 428 |
| Step 3: Enable Aruba Central Management Service on the Switch | 428 |
| Step 4: Provision the Switch to a Group | 428 |
| Step 5: Verify the configuration Status | 430 |
| Workflow 2—Provisioning a Switch On-Demand | 430 |
| Step 1: Enable Aruba Central Management Service on the Switch | 431 |
| Step 2: Add the Switch to Aruba Central | 431 |
| Step 3: Assign a Subscription | 431 |
| Step 4: Provision the Switch to a Group | 431 |
| Step 5: Verify the configuration Status | 433 |
| Managing Password in Configuration Templates | 433 |
| Password for Switches | 433 |
| Password for APs | 433 |
| Setting Password using Variables | 433 |
| Configuring Aruba Switches | 434 |
| CA Certificate Installation using API and Templates | 434 |
| Using Configuration Templates for Switch Management | 435 |
| Creating a Group for Template-Based Configuration | 435 |
| Creating a Configuration Template | 435 |
| Important Points to Note | 436 |
| Best Practices | 437 |
| Configuring or Viewing Switch Properties in UI Groups | 437 |
| Configuring or Viewing the Switch Properties | 439 |
| Configuring Switch Ports on Aruba Switches | 440 |
| Configuring PoE Settings on Aruba Switch Ports | 441 |
| Configuring VLANs on Switches | 442 |
| Adding VLAN Details | 443 |
| Editing the VLAN Details | 444 |

| | |
|---|------------|
| Deleting VLAN Details | 444 |
| Configuring DHCP Relay Settings | 444 |
| Configuring Trunk Groups on Aruba Switches in UI Groups | 445 |
| Adding Trunk Groups on Switches | 445 |
| Editing Trunk Groups on Switches | 446 |
| Deleting Trunk Groups on Switches | 446 |
| Enabling Spanning Tree Protocol on Aruba Switches in UI Groups | 446 |
| Configuring Loop Protection on Aruba Switch Ports | 447 |
| Configuring Port Rate Limit on Aruba Switches in UI Groups | 448 |
| Configuring CDP | 449 |
| Configuring Access Policies on Aruba Switches | 449 |
| Configuring SNMP on Aruba Switches | 450 |
| Configuring community settings | 450 |
| Configuring trap settings | 451 |
| Configuring DHCP Pools on Aruba Switches | 451 |
| Configuring DHCP Snooping | 453 |
| Enabling DHCP Snooping on a Switch | 453 |
| Adding Authorized DHCP Servers for a Switch | 453 |
| Deleting Authorized DHCP Servers for a Switch | 453 |
| Enabling DHCP Snooping for a VLAN | 453 |
| Configuring IGMP | 454 |
| Configuring Time Synchronization | 454 |
| Predefined DST Rules | 456 |
| Configuring Routing on Aruba Switches | 456 |
| Configuring System Parameters for a Switch | 457 |
| Configuring Administrator Credentials for Mobility Access Switch | 457 |
| Configuring Administrator and Operator Credentials for Other Aruba Switches | 457 |
| Configuring a Name Server | 458 |
| Aruba Switch Stack | 459 |
| Provisioning Switch Stacks in Aruba Central | 459 |
| Assigning Labels and Sites | 460 |
| Configuring Switch Stacks | 460 |
| Monitoring Switch Stacks | 460 |
| Viewing Switch Stacks in Site Topology | 460 |
| Configuring Switch Stacks using Template Groups | 460 |
| Configuring Switch Stacks using UI Groups | 461 |
| Onboarding commander and members to Aruba Central | 461 |
| Recommended deployment workflow | 462 |
| Creating a switch stack | 462 |
| Editing a Stack | 463 |

| | |
|---|------------|
| Removing a stack | 463 |
| Adding a stack member | 463 |
| Editing a stack member | 464 |
| Removing a stack member | 464 |
| Aruba SD-Branch Solution | 466 |
| Why SD-WAN? | 466 |
| Key Features and Benefits | 466 |
| How It Works | 467 |
| What are the Solution Requirements? | 469 |
| How Do I Get Started? | 470 |
| API Gateway | 471 |
| API Gateway and NB APIs | 471 |
| Accessing API Gateway | 472 |
| Domain URLs | 473 |
| Viewing Swagger Interface | 473 |
| List of Supported APIs | 474 |
| Creating Application and Token | 475 |
| Using OAuth 2.0 for Authentication | 476 |
| Access and Refresh Tokens | 477 |
| Obtaining Access Token | 477 |
| Accessing APIs | 477 |
| Viewing and Revoking Tokens | 478 |
| Adding a New Token | 479 |
| Obtaining Token Using Offline Token Mechanism | 479 |
| Obtaining Token Using OAuth Grant Mechanism | 480 |
| Step 1: Authenticating a User and Creating a User Session | 480 |
| Example | 480 |
| Step 2: [Optional] Generating Client Credentials | 481 |
| Example | 481 |
| Step 3: Generating Authorization Code | 482 |
| Example | 482 |
| Step 4: Exchanging Auth Code for a Token | 483 |
| Example | 484 |
| Step 5: Refreshing a Token | 484 |
| Example | 485 |
| Step 6: Deleting a Token | 486 |
| Example | 486 |
| Viewing Usage Statistics | 486 |
| Webhooks | 487 |

| | |
|--|------------|
| Creating and Updating Webhooks Through the UI | 488 |
| Refreshing Webhooks Token Through the UI | 489 |
| Creating and Updating Webhooks Through the API Gateway | 489 |
| List of Webhooks APIs | 490 |
| Sample Webhooks Payload Format for Alerts | 491 |
| Access Point Alerts—Sample JSON | 491 |
| Switch Alerts—Sample JSON | 499 |
| Gateway Alerts—Sample JSON | 504 |
| Miscellaneous Alerts—Sample JSON | 511 |
| Guest Access | 513 |
| Guest Access Dashboard | 513 |
| Creating Apps for Social Login | 514 |
| Creating a Facebook App | 514 |
| Creating a Google App | 515 |
| Creating a Twitter App | 516 |
| Creating a LinkedIn App | 516 |
| Configuring a Guest Access Splash Page Profile | 516 |
| Adding a Guest Access Splash Page Profile | 517 |
| Customizing a Splash Page Design | 520 |
| Localizing a Guest Portal | 521 |
| Previewing and Modifying a Splash Page Profile | 524 |
| Associating a Splash Page Profile to an SSID | 524 |
| Configuring Visitor Accounts | 525 |
| Adding a visitor | 525 |
| Deleting Visitors | 526 |
| Downloading Visitor Account Details | 527 |
| Presence Analytics | 528 |
| Enabling Presence Analytics Service | 528 |
| Using Presence Analytics | 528 |
| Activity Dashboard | 528 |
| Setting RSSI Threshold and Dwell Time | 534 |
| Unified Communications | 535 |
| Heuristics Classification | 535 |
| Enabling Unified Communications | 535 |
| Enabling Call Prioritization | 536 |
| Editing Protocol | 536 |
| Unified Communications Dashboard | 536 |
| Installation Management | 539 |
| Installation Management and Monitoring | 539 |

| | |
|--|------------|
| Installation Management Workflow | 540 |
| Installer Workflow | 540 |
| Managing Site Deployments | 541 |
| Creating a Site | 542 |
| Assigning Groups to a Site | 542 |
| Adding an Installer and Assigning Sites for Installation | 542 |
| Downloading the Installer Mobile App | 543 |
| Registering as an Aruba Installer | 543 |
| Installing Devices on a Site | 543 |
| Monitoring and Troubleshooting Installation Issues | 544 |
| Glossary of Terms | 545 |

This user guide describes the features supported by Aruba Central and provides detailed instructions to set up and configure devices such as Instant APs, Aruba Switches, and Aruba SD-WAN Gateways.

Intended Audience

This guide is intended for system administrators who configure and monitor their networks using Aruba Central.

Related Documents

In addition to this document, the Aruba Central product documentation includes the following documents:

- *Aruba Central Help Center*
- *Aruba Central Getting Started Guide*
- *Aruba Central Managed Service Provider User Guide*
- *Aruba Central SD Branch Solution Guide*

Conventions

The following conventions are used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

| Type Style | Description |
|----------------|--|
| <i>Italics</i> | This style is used to emphasize important terms and to mark the titles of books. |
| System items | This fixed-width font depicts the following: <ul style="list-style-type: none">■ Sample screen output■ System prompts |

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Contacting Support

Table 2: *Contact Information*

| | |
|---|---|
| Main Site | arubanetworks.com |
| Support Site | support.arubanetworks.com |
| Airheads Social Forums and Knowledge Base | community.arubanetworks.com |
| North American Telephone | 1-800-943-4526 (Toll Free) 1-408-754-1200 |
| International Telephone | arubanetworks.com/support-services/contact-support/ |
| Software Licensing Site | lms.arubanetworks.com |
| End-of-life Information | arubanetworks.com/support-services/end-of-life/ |
| Security Incident Response Team | Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com |

Aruba Central offers unified network management, AI-based analytics, and IoT device security for wired, wireless, and SD-WAN networks. All of these capabilities are combined into one easy-to-use platform, which includes the following apps:

- **Network Operations**—Provides unified network management by consolidating wired, wireless, and SD-WAN deployment and management tasks, real-time diagnostics, and live monitoring, for simple and fast problem resolution.
- **ClearPass Device Insight**—Provides a single pane of glass for device visibility employing automated device discovery, machine learning (ML) based fingerprinting and identification. For more information, see [Aruba ClearPass Device Insight Information Center](#).

Key Features

Aruba Central offers the following key features and benefits:

- Streamlined configuration and deployment of devices—Leverages the ZTP capability of Aruba devices to bring up your network in no time. Aruba Central supports group configuration of devices, which allows you to provision and manage multiple devices with similar configuration requirements with less administrative overhead.
- Integrated wired, WAN, and wireless Infrastructure management—Offers a centralized management interface for managing wireless, WAN, and wired networks in distributed environments, and thus help organizations save time and improve efficiency.
- Advanced analytics and assurance—With continuous monitoring, AI-based analytics provide real-time visibility and insight into what's happening in the Wi-Fi network. The insights utilize machine learning that leverage a growing pool of network data and deep domain experience.
- Secure cloud-based platform—Offers a secure cloud platform with HTTPS connection and certificate based authentication.
- Interface for Managed Service Providers—Offers an additional interface for MSPs to provision and manage their respective tenant accounts. Using the MSP mode, service provider organizations can administer network infrastructure for multiple organizations in a single interface.
- SD-Branch Management—Offers a simplified solution for managing and monitoring SD Branch devices such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches. It also provides detailed dashboards showing WAN health and pictorial depictions of the branch setup. The Aruba SD-Branch solution extends the SD-WAN concepts to all elements in a branch setup to deliver a full-stack solution for managing WLAN, LAN and WAN connections. The SD-Branch solution provides a common cloud-management model that simplifies deployment, configuration, and management of all components of a branch setup. The solution leverages the ZTP and cloud management capabilities of Aruba devices to integrate management and infrastructure for WAN, WLAN, and LAN and provide a holistic solution from access network to edge with end-to-end security. It also addresses all communications in distributed deployments, from micro branches to medium or large branches. For more information, see the [Aruba SD-Branch Solution](#).
- Health and usage monitoring—Provides a comprehensive view of your network, device status and health, and application usage. You can monitor, identify, and address issues by using data-driven dashboards, alerts, reports, and troubleshooting workflows. Aruba Central also utilizes the DPI feature of the devices to monitor, analyze and block traffic based on application categories, application type, web categories and

website reputation. Using this data, you can prioritize business critical applications, limit the use of inappropriate content, and enforce access policies on a per user, device or location basis.

- Guest Access—Allows you to manage access for your visitors with a secure guest Wi-Fi experience. You can create guest sponsor roles and social logins for your guest networks. You can also design your guest landing page with custom logos, color, and banner text.
- Presence Analytics—Offers a value added service for Instant AP based networks to get an insight into user presence and loyalty. The Presence Analytics dashboard allows you to view the presence of users at a specific site and the frequency of user visits at a given location or site. Using this data, you can make business decisions to improve customer engagement.

Supported Web Browsers



To view the Aruba Central UI, ensure that JavaScript is enabled on the web browser.

Table 3: *Browser Compatibility Matrix*

| Browser Versions | Operating System |
|-------------------------------------|--------------------|
| Google Chrome 39.0.2171.65 or later | Windows and Mac OS |
| Mozilla Firefox 34.0.5 or later | Windows and Mac OS |
| Internet Explorer 10 or later | Windows |
| Safari 7 or later | Mac OS |

Operational Modes and Interfaces

Aruba offers the following variants of the Aruba Central web interface:

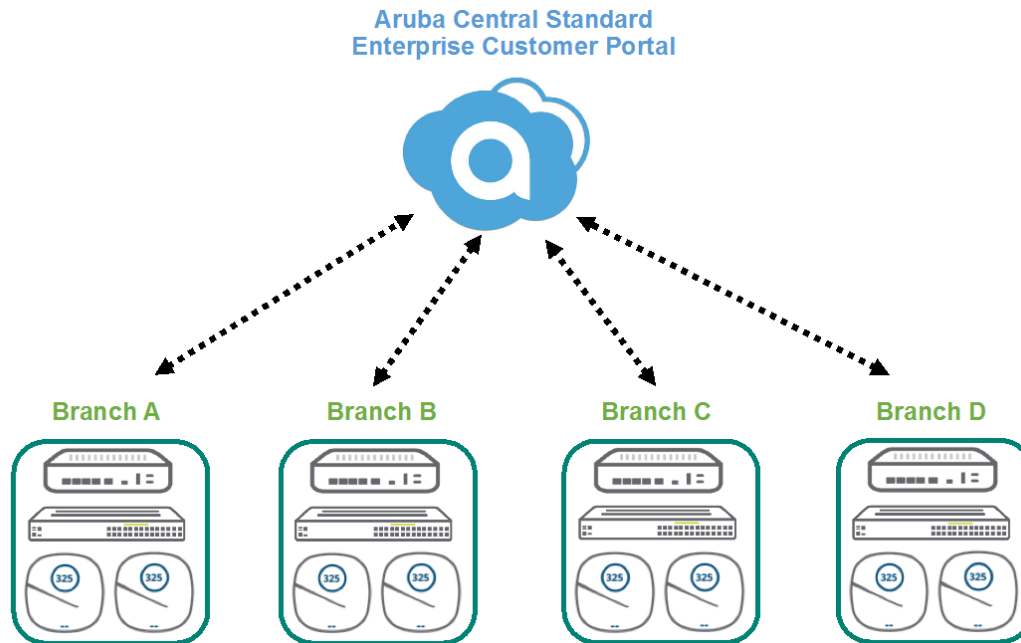
- [Standard Enterprise Mode](#)
- [Managed Service Provider Mode](#)

Standard Enterprise Mode

The Standard Enterprise interface is intended for users who manage their respective accounts end-to-end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision devices and subscriptions to manage their respective accounts.

The following figure illustrates a typical Standard Enterprise mode deployment.

Figure 1 *Standard Enterprise Mode*

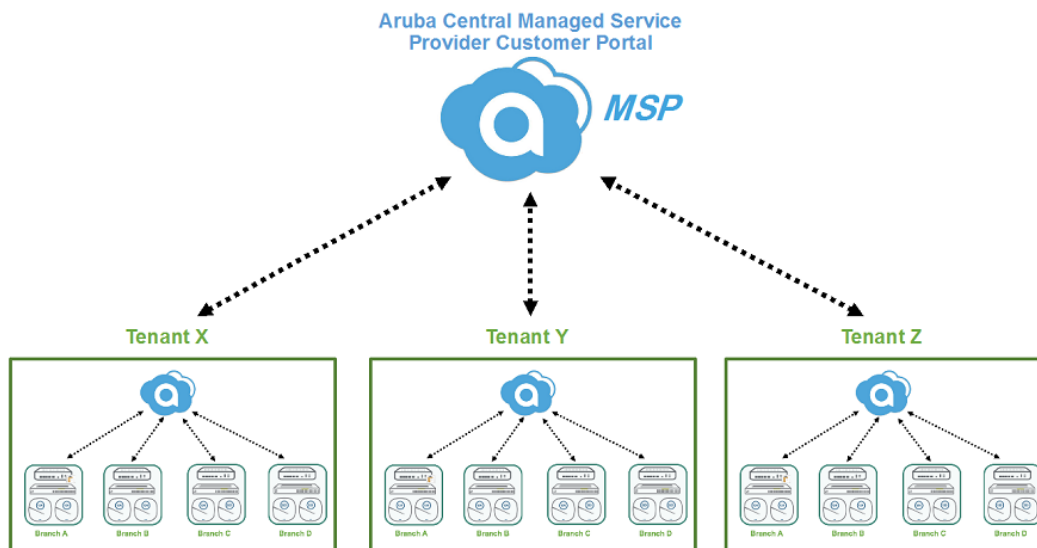


Managed Service Provider Mode

Aruba Central offers the MSP mode for managed service providers who need to manage multiple customer networks. The MSP administrators can provision tenant accounts, allocate devices, assign licenses, and monitor tenant accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. Tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

The following figure illustrates a typical MSP mode deployment.

Figure 2 *Managed Service Provider Mode*



Supported Devices

This section provides the following information:

- [Supported Instant APs](#)
- [Supported Switch Platforms](#)
- [Supported Aruba Gateways](#)

Supported Instant APs

The following section discusses the supported Instant APs:

Supported Indoor APs

Aruba Central supports the following indoor APs:

- AP-555
- AP-535
- AP-534
- AP-515
- AP-514
- AP-505H
- AP-505
- AP-504
- AP-345
- AP-344
- AP-318
- AP-303
- AP-303P
- AP-303H
- AP-203H
- AP-203R/AP-203RP
- IAP-304/305
- IAP-207
- IAP-334/335
- IAP-314/315
- IAP-324/325
- IAP-228
- IAP-205H
- IAP-103
- IAP-114/115
- IAP-204
- IAP-205
- IAP-214/215
- IAP-224/225

- RAP-3WNP
- RAP-108/109
- RAP-155/155P
- IAP-134/135
- IAP-104
- IAP-105
- IAP-92/93

Supported Outdoor APs

Aruba Central supports the following outdoor APs:

- AP-577EX
- AP-577
- AP-575EX
- AP-575
- AP-574
- AP-518
- AP-387
- AP-377EX
- AP-377
- AP-375EX
- AP-375
- AP-374
- AP-367
- AP-365
- IAP-277
- IAP-274/275
- IAP-175

Supported Instant AP Firmware Versions

The current release of Aruba Central supports only the following Instant AP firmware versions:

- 8.7.0.0
- 8.6.0.4
- 8.6.0.3
- 8.6.0.2
- 8.5.0.9
- 8.5.0.8
- 8.5.0.7
- 8.5.0.6
- 8.5.0.5
- 8.4.0.6
- 8.3.0.12

- 8.3.0.11
- 6.5.4.17
- 6.5.4.16
- 6.5.4.15
- 6.5.1.5-4.3.1.9
- 6.4.4.8-4.2.4.16

IAP-103, RAP-108, RAP-109, IAP-114, IAP-115, IAP-204, IAP-205, and IAP-205H Instant APs are no longer supported from Aruba Instant 8.3.0.0 onwards.



By default, AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends that you not upgrade these access points to 8.5.0.0 or 8.5.0.1 firmware versions as the upgrade process changes the uplink port from Eth1 to Eth0 port thereby making the devices unreachable.

APs Supporting Power Draw

The following APs support Power Draw:

- AP-577EX
- AP-577
- AP-575EX
- AP-575
- AP-574
- AP-518
- AP-515
- AP-514
- AP-505H
- AP-505
- AP-504
- AP-387
- AP-377
- AP-375
- AP-374
- AP-345
- AP-344
- IAP-335
- IAP-334
- AP-318
- IAP-314
- IAP-305
- IAP-304
- AP-303H



For more information about Aruba's End-of-life policy and the timelines for hardware and software products at the end of their lives, see: <https://www.arubanetworks.com/support-services/end-of-life/>.

Data sheets and technical specifications for the supported AP platforms are available at:
<https://www.arubanetworks.com/products/networking/access-points/>.

Supported Switch Platforms



To manage your Aruba switches using Aruba Central, ensure that the switch software is upgraded to 16.05.0007 or a later version. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 4: *Supported Aruba Switch Series, Software Versions, and Switch Stacking*

| Switch Platform | Supported Software Versions | Recommended Software Versions | Switch Stacking Support | Supported Stack Type (Frontplane (VSF) / Backplane (BPS)) |
|---------------------------|-----------------------------|-------------------------------|---|---|
| Aruba 2530 Switch Series | YA/YB.16.05.0008 or later | YA/YB.16.10.0003 | N/A | N/A |
| Aruba 2540 Switch Series | YC.16.03.0004 or later | YC.16.10.0003 | N/A | N/A |
| Aruba 2920 Switch Series | WB.16.03.0004 or later | WB.16.10.0003 | Yes Switch Software Dependency: WB.16.04.0008 or later | BPS |
| Aruba 2930F Switch Series | WC.16.03.0004 or later | WC.16.10.0003 | Yes Switch Software Dependency: WC.16.07.0002 | VSF |
| Aruba 2930M Switch Series | WC.16.04.0008 or later | WC.16.10.0003 | Yes Switch Software Dependency: WC.16.06.0006 | BPS |
| Aruba 3810 Switch Series | KB.16.03.0004 or later | KB.16.10.0003 | Yes Switch Software Dependency: KB.16.07.0002 | BPS |
| Aruba 5400R Switch Series | KB.16.04.0008 or later | KB.16.10.0003 | Yes Switch Software Dependency: KB.16.06.0008 | VSF |



Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins.

Table 5: *Supported Aruba Mobility Access Switch Series and Software Versions*

| Mobility Access Switch Series | Supported Software Versions |
|--|---|
| <ul style="list-style-type: none"> ■ S1500-12P ■ S1500-24P ■ S2500-24P ■ S3500-24T | ArubaOS 7.3.2.6 ArubaOS 7.4.0.3 ArubaOS 7.4.0.4 ArubaOS 7.4.0.5 ArubaOS 7.4.0.6 |

Data sheets and technical specifications for the supported switch platforms are available at:
<https://www.arubanetworks.com/products/networking/switches/>

Supported Aruba Gateways

The Aruba SD-WAN Gateway portfolio includes Aruba Gateways that function as Branch Gateways and VPN Concentrators.

The following tables list the Aruba Gateway platforms and the ArubaOS software versions supported in Aruba Central:

Table 6: *Supported Aruba Branch Gateways*

| Platform | Minimum Supported Software Version | Latest Software Version | Recommended Software Version |
|----------------------------|------------------------------------|-------------------------|------------------------------|
| Aruba 7210, 7220, and 7240 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 |
| Aruba 9012 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 |
| Aruba 9004 | ArubaOS 8.5.0.0-1.0.7.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.5.0.0-1.0.7.1 |
| Aruba 7005 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7008 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7010 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7024 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7030 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |

Table 7: *Supported Aruba VPN Concentrators*

| Platform | Minimum Supported Software Version | Latest Software Version | Recommended Software Version |
|--------------|------------------------------------|-------------------------|------------------------------|
| Aruba 7220 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.5.1 |
| Aruba 7240 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7240XM | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7210 | ArubaOS 8.1.0.0-1.0.0.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.1 |
| Aruba 7280 | ArubaOS 8.1.0.0-1.0.6.0 | ArubaOS 8.5.0.0-2.0.0.0 | ArubaOS 8.4.0.0-1.0.6.4 |

Data sheets and technical specifications for the supported Gateways are available at:
<https://www.arubanetworks.com/products/networking/gateways-and-controllers/>

Thank you for choosing Aruba Central as your network management solution!

Before you get started with Aruba Central, we recommend that you review the [Key capabilities of Aruba Central](#) and the [list of Aruba devices supported in Aruba Central](#).

Key Terms and Concepts

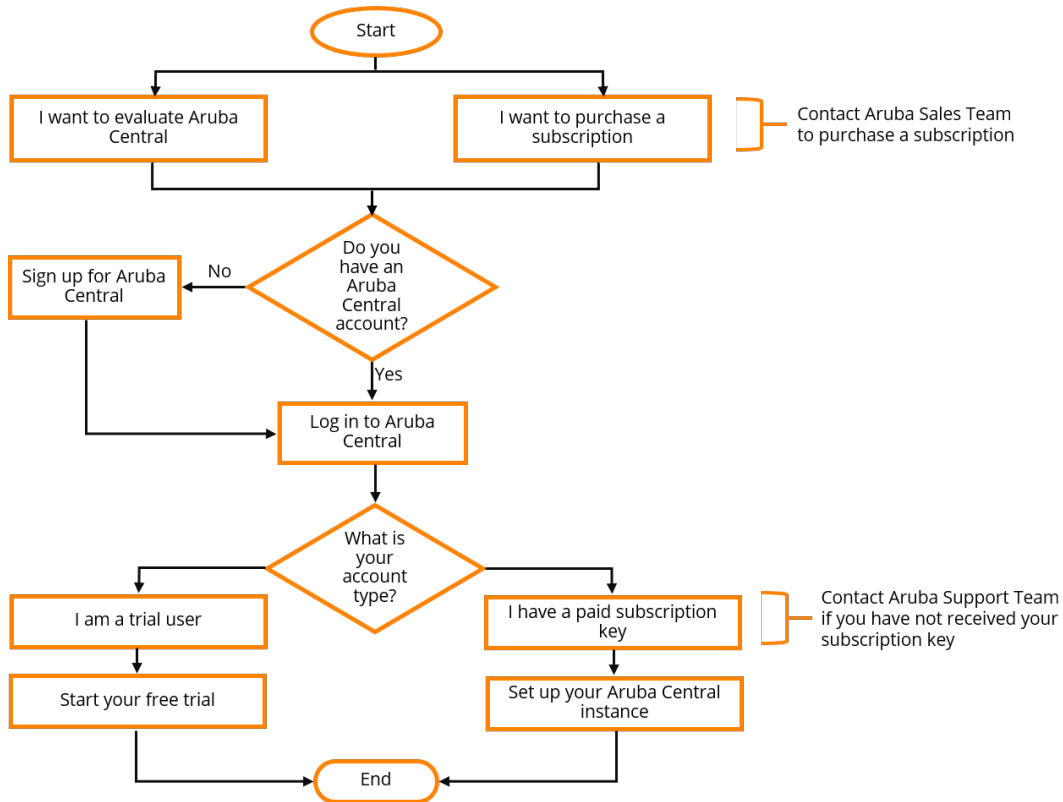
Take a few minutes to familiarize yourself with the key terms and concepts used in the help topics.

| | |
|--------------------------------------|---|
| Cluster Zone | Refers to an Aruba Central deployment area within a specific region. In other words, cluster zones are regional grouping of one or more container instances on which Aruba Central is deployed. Cluster zones allow your deployments to restrict customer data to a specific region and plan timezone-specific maintenance windows. Each cluster zone has separate URLs for signing up for Aruba Central, accessing Aruba Central portal, and for allowing devices to communicate with Aruba Central. To view the zone in Aruba Central UI, click the User Settings menu at the bottom of the left navigation pane. |
| Enterprise Mode | Refers to the Aruba Central solution deployment mode in which the customers provision, manage, and maintain their networks end-to-end for their respective organizations or businesses. |
| Managed Services Mode | Refers to the Aruba Central deployment mode in which the service providers, resellers, administrators, and retailers to centrally manage and monitor multiple tenant or end-customer accounts from a single management interface. |
| Subscription | Refers to the license granted to a customer for using a product or service. |
| Evaluation Account | Refers to the Aruba Central account created for evaluating Aruba Central solution and its services. |
| Paid Subscriber | Refers to the customers who have purchased a subscription to obtain access to Aruba Central and its services. |
| Subscription Key | Refers to the license key. A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS. |
| Customer ID Subscriber ID | Refers to the identity number of your Aruba Central account. To view your subscriber ID, click the User Settings menu at the bottom of the left navigation pane in the Aruba Central UI. |
| Zero Touch Provisioning | Refers to one of the following: <ul style="list-style-type: none"> ■ Zero Touch Provisioning of Aruba Central accounts— When you purchase a subscription key and add this subscription key in Aruba Central, Aruba Central queries the Aruba Activate database to retrieve the devices mapped to your purchase order and add these devices to the inventory. This process is referred to as zero touch provisioning in Aruba Central. ■ Zero Touch Provisioning of Devices—Most Aruba devices support self-provisioning; that is, when you connect a device to a provisioning network, it can automatically download provisioning parameters from the Activate server and connect to their management entity. |
| Onboarding | Refers to the process of importing devices to Aruba Central's device inventory, activating subscriptions, and making devices available for management from Aruba Central. |

| | |
|---------------------|---|
| Device Sync | Refers to the process of synchronizing devices from the Activate database. The device sync operation allows Aruba Central to retrieve devices from Activate and automatically add these devices to the device inventory in Aruba Central. |
| Provisioning | Refers to the process of setting up a device for deploying networks as per the configuration requirements of your organization. |
| Group | Refers to the device configuration container in Aruba Central. You can combine devices with common configuration requirements into a single group and apply the same configuration to all the devices in that group. |
| Site | Refers to the physical locations where devices are installed. Organizing devices per sites allows you to filter your dashboard view per site. |
| Label | Refers to the tags used for logically grouping devices based on various parameters such as ownership, specific areas within a site, departments, and so on. |

Workflow Summary

The following illustration summarizes the steps required for getting started with Aruba Central:



Navigate through the following topics to know more about the onboarding and provisioning procedures:

- [Creating an Aruba Central Account on page 37](#)
- [Accessing Aruba Central Portal on page 41](#)
- [Starting Your Free Trial on page 55](#)
- [Setting up Your Aruba Central Instance on page 59](#)

Creating an Aruba Central Account

To start using Aruba Central, you need to register and create an Aruba Central account. Both evaluating and paid subscribers require an account to start using Aruba Central.

Zones and Sign Up URLs

Aruba Central instances are available on multiple regional clusters. These regional clusters are referred to as zones. When you register for an Aruba Central account, Aruba creates an account for you in the zone that is mapped to the country you selected during registration.

If you access the Sign Up URL from the www.arubanetworks.com website, you are automatically redirected to the sign up URL. To create an Aruba Central account in the zone that is mapped to your country, use the following zone-specific sign up URLs.

Table 8: *Sign Up URLs & Apps*

| Regional Cluster | Sign Up URL | Available Apps |
|------------------|--|---|
| US-1 | https://portal.central.arubanetworks.com/signup | Network Operations |
| US-2 | https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/ | <ul style="list-style-type: none">■ Network Operations■ ClearPass Device Insight |
| Canada-1 | https://portal-ca.central.arubanetworks.com/signup | Network Operations |
| China-1 | https://portal.central.arubanetworks.com.cn/signup | Network Operations |
| EU-1 | https://portal-eu.central.arubanetworks.com/signup | <ul style="list-style-type: none">■ Network Operations■ ClearPass Device Insight |
| APAC-1 | https://portal-apac.central.arubanetworks.com/signup | Network Operations |
| APAC-EAST1 | https://portal-apaceast.central.arubanetworks.com/signup | Network Operations |
| APAC-SOUTH1 | https://portal-apacsouth.central.arubanetworks.com/signup | Network Operations |

Signing up for an Aruba Central Account

To sign up for an Aruba Central account:

1. Go to <http://www.arubanetworks.com/products/sme/eval/>.
2. Click **SIGN UP NOW**. The **Registration** page opens.
3. Select the language.
4. Enter your email address. Based on the email address you entered, the Registration page guides you to the subsequent steps:

Table 9: Registration Workflow

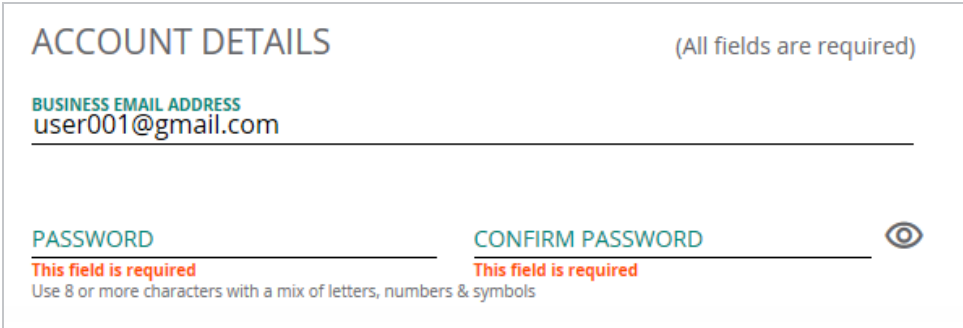
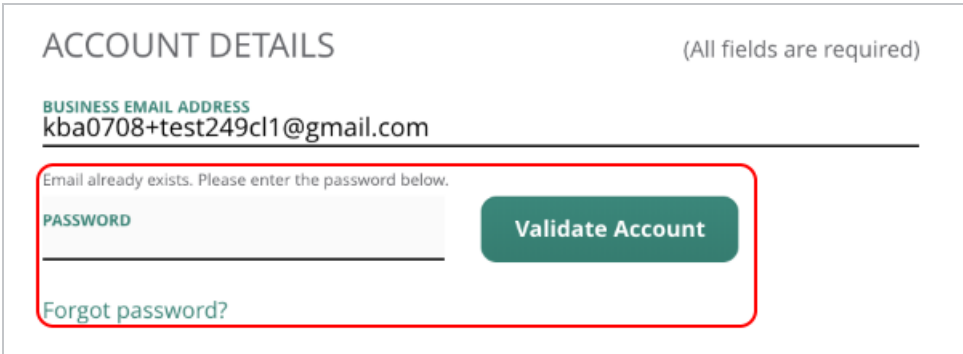
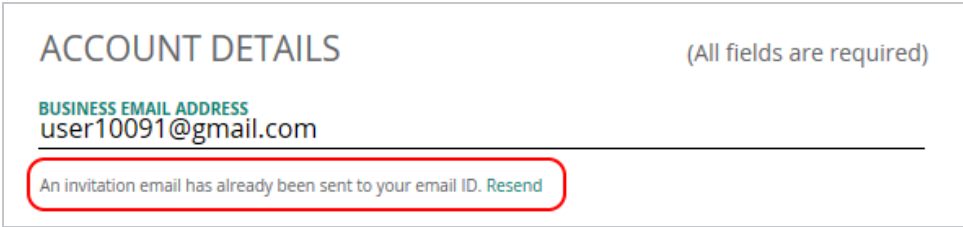
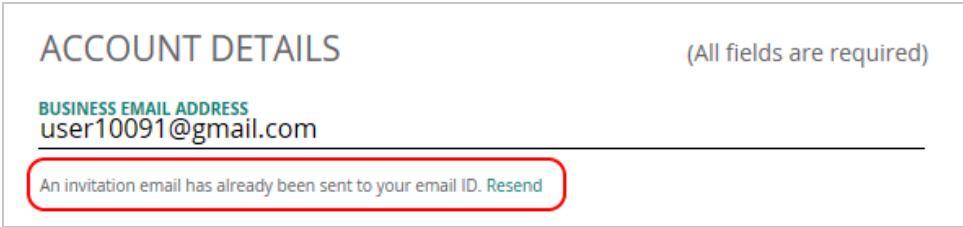
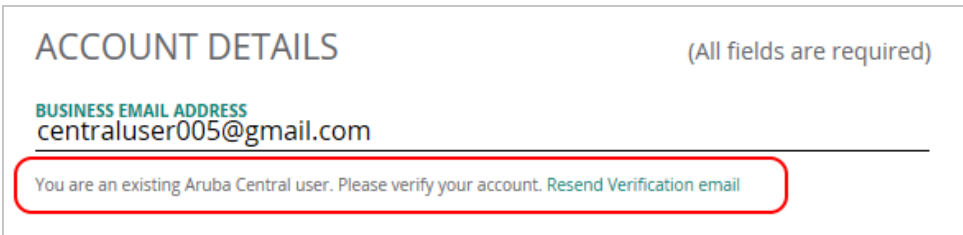
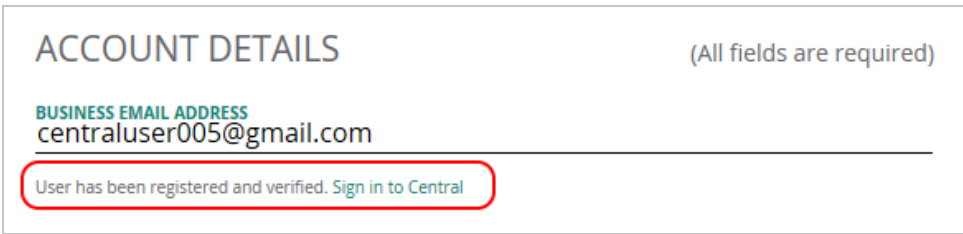

| If... | Then... |
|---|---|
| If you are a new user: | <p>The Registration page prompts you to create a password. To continue with the registration, enter a password in the Password and Confirm Password fields.</p>  |
| If you are an existing Aruba customer, but you do not have an Aruba Central account: | <p>The Registration page displays the following message: Email already exists. Please enter the password below. To continue with registration, validate your account:</p> <ol style="list-style-type: none"> 1. Enter the password. 2. Click Validate Account. <p>NOTE: If you do not remember the password, click Forgot Password to reset the password.</p>  |
| If your email account is already registered with Aruba, but you do not have an Aruba Central account: | <p>The Registration page displays the following message: An invitation email has already been sent to your email ID. Resend. To continue with the registration:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the Sign Up page to sign in to Aruba Central.  |
| If you are invited to join as a user in an existing Aruba Central customer account: | <p>The Registration page displays the following message: An invitation email has already been sent to your email ID. Resend. To continue with the registration:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend. A registration invitation will be sent your account. 3. Click the registration link. The user account is validated. 4. Complete the registration on the Sign Up page to sign in to Aruba Central.  |

Table 9: Registration Workflow

| If... | Then... |
|---|---|
| If you are a registered user of Aruba Central and have not verified your email yet: | <p>The Registration page displays the following message: You are an existing Aruba Central user. Please verify your account. Resend Verification email. To continue:</p> <ol style="list-style-type: none"> 1. Go to your email box and check if you have received the email invitation. 2. If you have not received the email invitation, go to the Registration page and click Resend Verification email. A registration invitation will be sent your account. 3. Click the account activation link. 4. After the email verification is completed successfully, click Log in to access Aruba Central.  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the label '(All fields are required)'. Below it, the 'BUSINESS EMAIL ADDRESS' field contains 'centraluser005@gmail.com'. A red-bordered box highlights a message: 'You are an existing Aruba Central user. Please verify your account. Resend Verification email'.</p> |
| If you are already a registered user of Aruba Central and have verified your email: | <p>The Registration page displays the following message: User has been registered and verified. Sign in to Central. Click Sign in to Central to skip the registration process and access the Aruba Central portal.</p>  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the label '(All fields are required)'. Below it, the 'BUSINESS EMAIL ADDRESS' field contains 'centraluser005@gmail.com'. A red-bordered box highlights a message: 'User has been registered and verified. Sign in to Central'.</p> |
| If your email address is in the arubanetworks.com or hpe.com domain: | <p>The Single Sign-On option is enabled. You can use your respective Aruba or HP Enterprise credentials to log in to your Aruba Central account after the registration.</p>  <p>The screenshot shows the 'ACCOUNT DETAILS' section with the label '(All fields are required)'. Below it, the 'BUSINESS EMAIL ADDRESS' field contains 'user1@hpe.com'. A red-bordered box highlights a message: 'Single sign-on enabled'.</p> |

5. To continue with registration, enter your first name, last name, company name, address, country, state, ZIP code, and phone details.
6. Specify if you are an Aruba partner.
7. Ensure that you select an appropriate zone. The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central

server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers.

The screenshot shows a registration form with the following fields and options:

- ADDRESS:** Market Square, Outer Ring Road (with an "ADD LINE" button).
- CITY:** Bangalore (selected from a dropdown menu).
- STATE:** Karnataka (selected from a dropdown menu).
- ZIP CODE:** 560103.
- PHONE NUMBER:** +91 9240598432.
- Are you an Aruba Partner?:** Yes (radio button), No (selected radio button).
- SERVER DETAILS:** (All fields are required). The dropdown menu shows "APAC-SOUTH1" as the selected server.
- Privacy Notice:** Data collected by Dashboard, including some limited personal data, will be transferred and stored on servers in the zone you select on this page.

A callout box points to the "APAC-SOUTH1" selection with the text: "Based on the location you specify, the Aruba Central server is pre-selected."

8. From the **Interested Apps** section, select the app(s) that you want to pre-provision. You must select at least one app to continue:

- **Network Operations**
- **ClearPass Device Insight**

INTERESTED APPS

The "Interested Apps" section displays two app cards:

- Network Operations:** Represented by a green gear icon and a checked checkbox.
- ClearPass Device Insight:** Represented by a red padlock icon and an unchecked checkbox.

See [Table 8](#) for the app(s) available in the zone in which you are signing up.



If you are interested in evaluating the Aruba Central MSP solution, select only the **Network Operations** app.

9. Select the **I agree to the Terms and Conditions** check box.

10. Set a preferred mode of communication for receiving notifications about Aruba products and services.

11. Optionally, to read about the the privacy statement, click the **HPE Privacy Statement** link. To opt out of marketing communication, you can either click the unsubscribe link available at the bottom of the email or click the link as shown in the following figure:

For more information on how HPE manages, uses and protects your information please refer to [HPE Privacy Statement](#). You can always withdraw or modify your consent to receive marketing communication from HPE. This can be done by using the opt-out and preference mechanism at the bottom of our email marketing communication or by following this [link](#).

12. Click **Sign Up**. Your new account is created in the zone you selected and an email invitation is sent to your email address for account activation.
13. Access your email account and click the **Activate Your Account** link. After you verify your email, you can [log in](#) to Aruba Central.

Accessing Aruba Central Portal

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central.

If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created.

Login URLs

When you try to access Aruba Central portal, you are redirected to the Aruba Central URL that is mapped to your cluster zone.

Table 10: Cluster Zone— Portal URLs

| Regional Cluster | Sign Up URL |
|------------------|--|
| US-1 | https://portal.central.arubanetworks.com/signup |
| US-2 | https://portal-prod2.central.arubanetworks.com/signup OR https://signup.central.arubanetworks.com/ |
| Canada-1 | https://portal-ca.central.arubanetworks.com/signup |
| China-1 | https://portal.central.arubanetworks.com.cn/signup |
| EU-1 | https://portal-eu.central.arubanetworks.com/signup |
| APAC-1 | https://portal-apac.central.arubanetworks.com/signup |
| APAC-EAST1 | https://portal-apaceast.central.arubanetworks.com/signup |
| APAC-SOUTH1 | https://portal-apacsouth.central.arubanetworks.com/signup |

Logging in to Aruba Central

To log in to Aruba Central:

1. Access the Aruba Central login URL for your zone.
2. Notice that the zone is automatically selected based on your geographical location.
3. Enter the email address and click **Continue**.
4. Log in using your credentials.



If your user credentials are stored in your organization's Identity Management server and SAML SSO authentication is enabled for your IdP on Aruba Central, complete the SSO authentication workflow.

5. Enter the password.



If you have forgotten password, you can click the **Forgot Password** and reset your password. The Forgot Password link resets only your Aruba Central account; hence, it is not available to SSO users.


6. If you have forgotten your password,

7. Click **Continue**. The **Initial Setup** wizard opens.

- If you have a paid subscription, click **Get Started** and set up your account.
- If you are a trial user, click **Evaluate Now** and [start your trial](#).

Changing Your Password

To change your Aruba Central account:


1. In the Aruba Central UI, click the user icon () in the header pane.
2. Click **Change Password**.
3. Enter a new password.
4. Log in to Aruba Central using the new password.



The **Change Password** menu option is not available for federated users who sign in to Aruba Central using their SSO credentials.

Logging Out of Aruba Central

To log out of Aruba Central:

1. In the Aruba Central UI, click the user icon () in the header pane.
2. Click **Logout**.

Accessing Aruba Central Mobile Application

Aruba Central mobile application lets you manage, monitor, and optimize your Central account. You can log in to your Aruba Central account using your credentials from the mobile application. To download the Aruba Central application, visit the App Store on iOS devices running iOS 9.0 or later and Google Play Store on Android devices running android 5.0 Lollipop or later.

About the Network Operations User Interface

The **Network Operations** app is one of the apps in Aruba Central that helps to manage, monitor, and analyze your network.

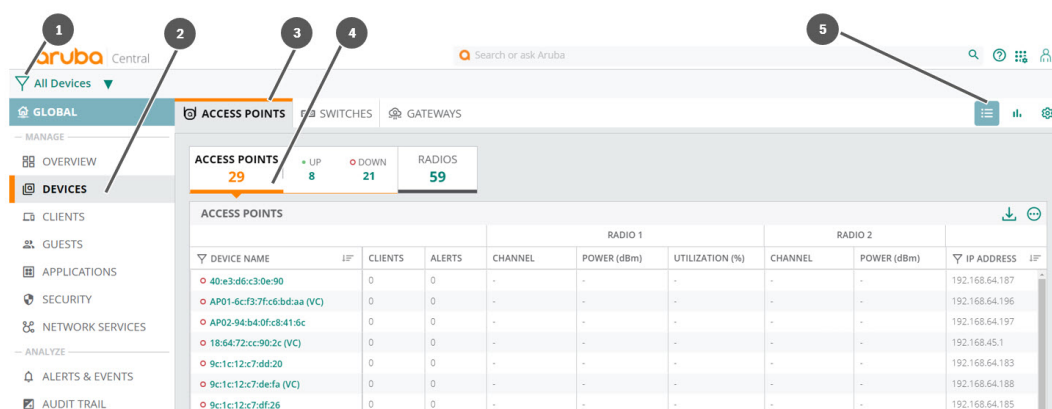
Aruba offers the following variants of the **Network Operations** app user interface:

- **Standard Enterprise mode**— This mode is intended for customers who manage their respective accounts end-to-end. In the Standard Enterprise mode, the customers have complete access to their accounts. They can also provision and manage their respective accounts.
- **Managed Service Provider (MSP) mode**— This mode is for managed service providers who need to manage multiple customer networks. With MSP mode enabled, the MSP administrators can provision customer accounts, allocate devices, assign licenses, and monitor customer accounts and their networks. The administrators can also drill down to a specific tenant account and perform administration and configuration tasks. The tenants can access only their respective accounts, and only those features and application services to which they have subscribed.

Workflow to Navigate the Network Operations User Interface

The following image shows the navigation elements on the **Network Operations** app:

Figure 3 Navigation Elements of the Network Operations App





| Callout Number | Description |
|----------------|---|
| 1 | Filter to select a group, device, label, site, or all devices. |
| 2 | Menu item under left navigation contextual menu. Menu is dependent on the filter selection. |
| 3 | First-level tab on dashboard. |
| 4 | Second-level tab on dashboard. |
| 5 | Summary, List, or Configuration view for dashboard. |

The **Network Operations** app uses a filter to set the view to one of the following dashboards:

- Global dashboard— When the filter is set to **All Devices** (for standard modes) or **All Groups** (for managed service modes).
- Gateway dashboard— When the filter is set to a Gateway.
- Switch dashboard— When the filter is set to a Switch.
- Virtual Controller dashboard— When the filter is set to a controller.
- Group dashboard— When the filter is set to a group.
- Label dashboard— When the filter is set to a label.
- Site dashboard— When the filter is set to a site.

The menu for the left navigation pane for the dashboard changes dependent on the type of dashboard displayed. In this sense, the left navigation pane functions as a contextual menu. Selecting any item on the left navigation pane displays a dashboard. The dashboard can have one or all of the following views:

- Summary view— Click the  summary icon to display the summary dashboard. The summary dashboard displays a number of charts. Use the time range filter to change the time-lines for the charts.
- List view— Click the  list icon to display the tables for the selected dashboard. For example, the dashboard in list view under **Manage > Devices > Access Points** displays a list of online and offline APs.


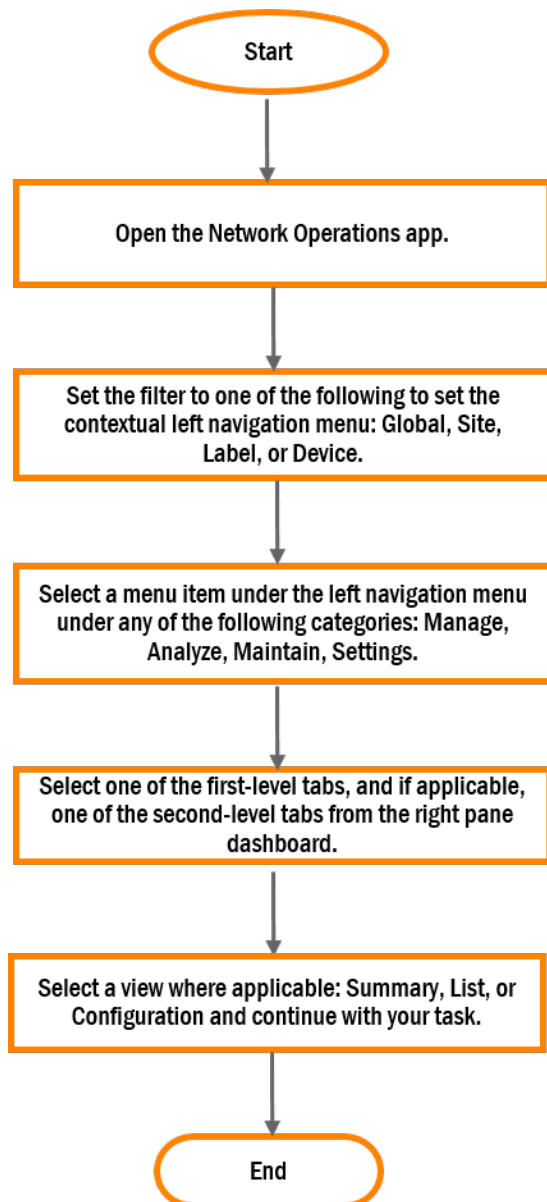
- Configuration view— Click the  configuration icon to enable the configuration options for a specific dashboard. For example, the Global dashboard in configuration view under **Analyze > Alerts & Events** enables you to configure alerts.

Figure 4 *Navigation Workflow for Network Operations App*



Related Topics:

- [About the Standard Enterprise Mode User Interface](#)
- [Launching the Network Operations App for MSP on page 50](#)

About the Standard Enterprise Mode User Interface

This section discusses the user interface for the Standard Enterprise mode for the **Network Operations** app.

Launching the Network Operations App

If the **Network Operations** app is the only app provisioned, the **Network Operations** app is displayed at each user login. If there are a number of apps provisioned such as **Network Operations**, **ClearPass**, **Device Insight**, and so on, the **Account Home** page is displayed at each user login. From the **Account Home** page, you can manage network inventory, subscriptions, and user access.

In the event of multiple apps provisioned, complete the following procedure to launch the **Network Operations** app:

1. Log in to the **Account Home** page.
The **Account Home** page displays the apps and **Global Settings**
For more information, see [Accessing Aruba Central Portal](#).
2. Click **Launch** on the **Network Operations** tile.
The **Network Operations** app is launched.


Figure 5 Launching the **Network Operations** App

ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS


EVALUATION 1532 DAYS LEFT



Network Operations
Manage your wired, wireless, and WAN infrastructure

LAUNCH

EVALUATION 88 DAYS LEFT



ClearPass Device Insight
Discover and Profile devices connected to the network

LAUNCH

GLOBAL SETTINGS

USERS AND ROLES
Manage user access

KEY MANAGEMENT
Manage your subscription keys

DEVICE INVENTORY
View an inventory of all your devices

DATA COLLECTORS
Manage on premise data collectors

AUDIT TRAIL
View the audit trail logs

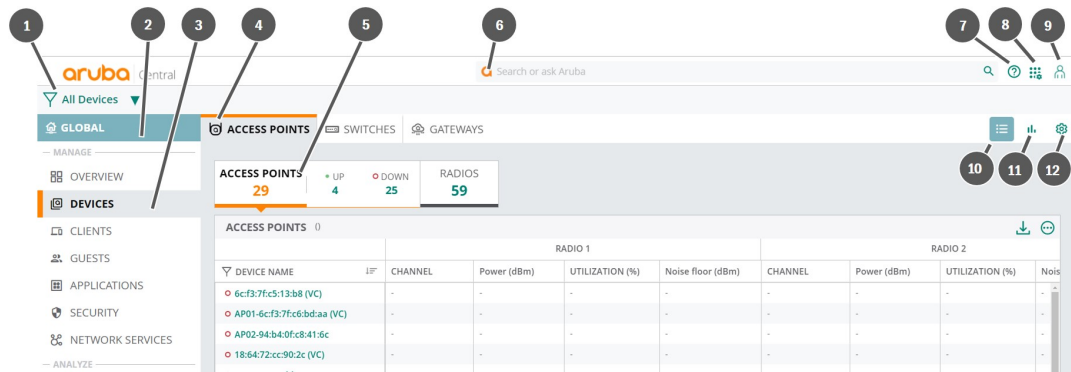
SINGLE SIGN ON
Create and manage SSO profiles

STREAMING API
Manage Streaming API and Webhook end points

Parts of the Network Operations App User Interface


After you launch the **Network Operations** app, the Standard Enterprise view is displayed.

Figure 6 Parts of the Network Operations App



| Callout Number | Description |
|----------------|--|
| 1 | Filter to select a group, device, label, site, or all devices. For more information, see Filter . |
| 2 | Dashboard based on filter selection. For more information, see Launching the Global Dashboard . |
| 3 | Menu item under left navigation contextual menu. Menu is dependent on the filter selection. For more information, see Manage , Analyze , and Maintain |
| 4 | First-level tab on dashboard. |
| 5 | Second-level tab on dashboard. |
| 6 | Search Bar. For more information, see Search Bar . |
| 7 | Help icon. For more information, see Help Icon . |
| 8 | Account Home icon For more information, see Account Home Icon . |
| 9 | User Settings icon. For more information, see User Icon . |
| 10 | List icon. For more information, see Launching the Global Dashboard . |
| 11 | Summary icon For more information, see Launching the Global Dashboard . |
| 12 | Configuration icon. For more information, see Launching the Global Dashboard . |

Search Bar


The search bar  enables users to look for help information.

Help Icon


The help icon  contains the following options:

- **Get help on this page**—Selecting this option changes the appearance of some of the text on the UI to green italics. On the UI, when you point to the text in green italics, a dialog box displays the help information for that text. To disable this option, click **Done**.
- **Tutorials**—Displays the Aruba Central product learning center.
- **Feedback**—Allows you to provide feedback on the Aruba Central. You can choose the rating from the range of 1 to 10, where 1 being extremely unlikely and 10 being extremely likely and type your comment into the box and click **Submit** to submit the feedback.
- **Documentation Center**—Directs you to the online help documentation.
- **Airheads Community**—Directs you to the Aruba support forum.
- **View / Update Case**—Enables you to view or edit an existing support ticket in the Aruba Support Portal at <https://asp.arubanetworks.com>. You must log in to this portal.
- **Open New Case**—Enables you to create a new support ticket in the Aruba Support Portal at <https://asp.arubanetworks.com>. You must log in to this portal.

Account Home Icon

The Account Home icon  enables you to go to the **Account Home** page and switch to another app if you have one subscribed. Most of the apps require service subscriptions to be enabled on the devices. Contact your administrator or the Aruba Central Support team to obtain access to an application service.


User Icon

The user icon  enables you to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:


- **Switch Customer**—Enables you to switch to another account. This is especially required during troubleshooting scenarios.
- **Change Password**—Enables you to change the password of the account.
- **User Settings**
 - **Time Zone**—Displays the zone, date, time, and time zone of the region.
 - **Language**—Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
 - **Idle Timeout**—Administrators can set a timeout value for inactive user sessions in the Idle Timeout field. The value is in minutes.
 - **Get system maintenance notifications**—Administrators can select the check box to receive system maintenance notification on their registered email ID. Email notifications are sent before any scheduled maintenance activity or unplanned outage.
 - **Get software update notifications**—Administrators can select the check box to receive software update notification on their registered email ID.
- **Enable MSP**—Enables MSP mode and switches the user interface to the MSP mode. This option changes to **Disable MSP** when the MSP mode is enabled. You can select **Disable MSP** to switch to the Standard Enterprise interface. The MSP mode can be disabled only if there is no tenant data. The option is grayed out if there are any active tenant accounts.
- **Terms of Service**—Displays the terms and conditions for using Aruba Central services.

- **Logout**—Enables you to log out of from your account.

Filter

The filter  enables you to select by group, individual devices, labels, and sites for performing specific configuration and monitoring tasks. If no filter is applied, by default the filter is set to **All Devices**.

Time Range Filter

The time range filter  enables you to set a time duration for showing monitoring and reports data. This time filter is not displayed when you view the configuration or device details. It is displayed only when you view monitoring data. You can set the filter to any of the following time ranges:

- 3 hours
- 1 day
- 1 week
- 1 month
- 3 months

Left Navigation Pane




The left navigation pane is a *contextual* menu that displays a number of configuration, monitoring, and troubleshooting options depending on the type of group, label, site or device you select from the filter.

Launching the Global Dashboard

In the **Network Operations** app, use the filter to select **All Devices**. The Global dashboard is displayed.

In the Global dashboard under the left navigation pane, you can see a number of menu items divided under the following categories: **Manage**, **Analyze**, and **Maintain**. If you set the filter to other options, some of these menu items under the parent categories are not listed as they are no longer applicable to the context.

Selecting each menu item in the left navigation pane displays a corresponding dashboard with tabs. Each tab may support all or some of the following functions:

- **Summary** —Click the summary icon to view a graphical representation of the data.
- **List** —Click the list icon to view a tabular representation of the data.
- **Configuration** —Click the configuration icon to enable configuration mode.

The next sections discuss the left navigation menu items in the Global dashboard.

Manage

The following menu items are included:

- **Devices**—Enables you to view a list of devices that are part of the network. In summary view, the dashboard displays a summary of bandwidth usage, client count, top devices in use, top 5 clients in the network, and a list of network profiles configured on the devices in the network. In configuration view, the dashboard enables you to configure the devices that are part of your Aruba Central setup.
- **Overview**—Enables you to view all devices across sites on a map. This tab also provides AI insights on each site. You can also import and view floor plans.
- **Clients**—Enables you to view the number of wired and wireless clients and a status of their connection in the network.
- **Guests**—Provides a dashboard to view information about cloud guests. Also enables you to create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors,

and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy.

- **Applications**—Displays a dashboard for applications that help you monitor the Aruba Central Setup. The **Visibility** dashboard displays metrics and graphs related to client traffic flow for different applications, websites, and blocked traffic. The Unified Communications application (**UCC**) actively monitors and provides visibility into Lync/Skype for Business traffic and allows you to prioritize sessions. **UCC** also leverages the functions of the Service Engine on the cloud platform and provides rich visual metrics for analytical purpose.
- **Security**—Displays a summary of the rogue devices and intrusion detected in the network. You can view a list of rogue devices, WIDS events, and interferences detected in the network.
- **Network Services**—Consists of SD-WAN overlay, virtual gateways, and cloud security tabs.

Analyze

The following menu items are included:

- **Alerts & Events**—Displays and configures a list of alerts and events. This page also enables you to acknowledge these alerts and events.
- **Live Events**—Starts live monitoring of the client. Live monitoring is supported only if the Instant AP is running 8.4.0.0 firmware version or a later version. Live monitoring stops after 15 minutes. At any point, you can click **Stop Live** to go back to the historical view.
- **Audit Trail**—Displays audit trail for the events pertaining to device allocation, configuration, user addition deletion, and firmware upgrade status.
- **Tools**—Network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. **Network Check** captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection. **Device check** aims to identify, diagnose, and debug issues for Aruba Switches. **Commands** enables you to perform network health check on devices at an advanced level using command categories. Read-only users can also perform advance checks.

Maintain

The following menu items are included:

- **Install Manager**—Enables you to manage and monitor device installations at specific physical locations or sites. **Install Manager** enables third-party installation operations managers to set up installer profiles and monitor device installations at the given sites.
- **Firmware**—Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. Also enables you to manage firmware compliance for all devices.
- **Reports**—Enables you to create, view, edit, and download various reports. You can configure the reports to run on demand or periodically. You must have read/write privileges or you must be an Admin user to be able to create reports.

Related Topics:

[Account Home](#)

[Managed Service Provider](#)

[Launching the Network Operations App for MSP](#)




This topic discusses the Network Operations app in MSP mode. To know more about the Account Home page, see the online Aruba Central documentation.

The MSP mode is intended for the managed service providers who manage multiple distinct tenant accounts. The MSP mode allows MSP customers to provision and manage tenant accounts, assign devices to tenant accounts, manage subscription keys and other functions such as configuring network profiles and viewing alerts.

Launching the Network Operations App for MSP

Aruba Central in MSP mode consists of the Network Operations app and the Account Home page.

After you create an Aruba Central account, the link to Aruba Central portal will be sent to your registered email address. You can use this link to log in to Aruba Central. If you are accessing the login URL from the www.arubanetworks.com website, ensure that you select the zone in which your account was created. The Network Operations app is displayed at each user login to Aruba Central.

From the Network Operations app, you can navigate to the Account Home page by clicking the Account Home icon .

From the Account Home page, you can navigate to the Network Operations app by clicking the Launch button for the Network Operations tile.

Figure 7 Launching the Network Operations App for MSP from Account Home


ACCOUNT HOME

Manage your Network Inventory, Subscriptions, and User Access. Use any of the following apps to make Aruba work better for you.

APPS

EVALUATION 1287 DAYS LEFT

MSP



Network Operations
Manage your wired, wireless, and WAN infrastructure

LAUNCH

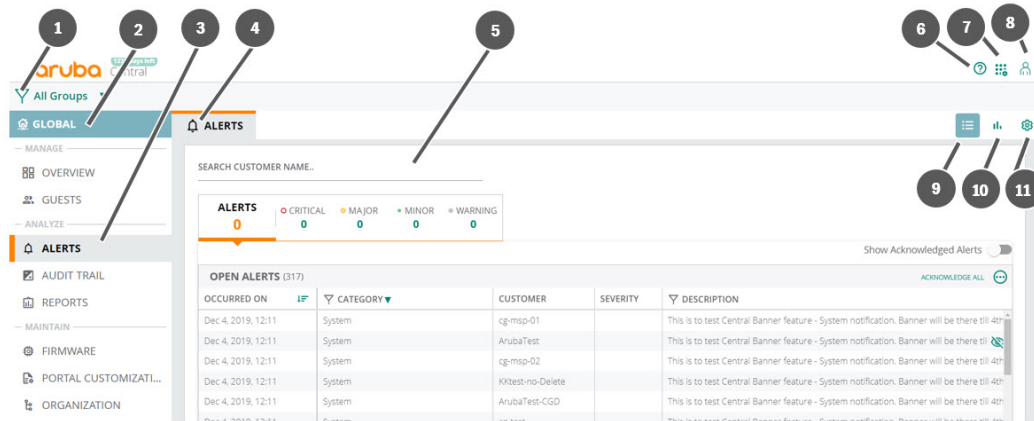
GLOBAL SETTINGS

| | | |
|--|--|---|
| USERS AND ROLES Manage user access | KEY MANAGEMENT Manage your subscription keys | DEVICE INVENTORY Manage the Devices in your Inventory |
| AUDIT TRAIL View audit-trail logs | SINGLE SIGN ON Create and manage SAML Profiles | API GATEWAY Access API Gateway and manage access tokens |

Parts of the Network Operations App for MSP

After you launch the **Network Operations** app, the MSP view opens.

Figure 8 Parts of the Aruba Central User Interface for MSP



| Callout Number | Description |
|----------------|---|
| 1 | Filter to select a group or all groups. For more information, see Filter . |
| 2 | Name of the dashboard, here it is set to Global as the filter is set to All Groups. |
| 3 | Menu item under left navigation contextual menu. Menu is dependent on the filter selection. |
| 4 | First-level tab on dashboard. The dashboard may also have second and third-level tabs dependent on the filter selection. |
| 5 | Dashboard for the selected menu item on left navigation pane. For more information, see Launching the MSP Global Dashboard . |
| 6 | Help icon. For more information, see Help Icon . |
| 7 | Account Home icon. For more information, see Search Bar . |
| 8 | User Settings icon. For more information, see User Icon . |
| 9 | List view. Click the list icon to view a tabular representation of the data. Only applicable for the global dashboard. |
| 10 | Summary view. Click the summary icon to view a graphical representation of the data. Only applicable for the global dashboard. |
| 11 | Configuration view. Click the configuration icon to enable configuration mode. |

Search Bar


The search bar  enables users to search help information.

Help Icon


The help icon  contains the following options:

- **Get help on this page**— Selecting this option changes the appearance of some of the text on the UI to green italics. On the UI, when you point to the text in green italics, a dialog box displays the help information for that text. To disable this option, click **Done**.
- **Tutorials**— Displays the Aruba Central product learning center.
- **Feedback**— Allows you to provide feedback on the Aruba Central. You can choose the rating from the range of 1 to 10, where 1 being extremely unlikely and 10 being extremely likely and type your comment into the box and click **Submit** to submit the feedback.
- **Documentation Center**— Directs you to the online help documentation.
- **Airheads Community**— Directs you to the Aruba support forum.
- **View / Update Case**— Enables you to view or edit an existing support ticket in the Aruba Support Portal at <https://asp.arubanetworks.com>. You must log in to this portal.
- **Open New Case**— Enables you to create a new support ticket in the Aruba Support Portal at <https://asp.arubanetworks.com>. You must log in to this portal.

Account Home Icon


The Account Home icon  enables you to go to the **Account Home** page.

User Icon


The user icon  enables you to view user account details such as account name, domain, customer ID, and zone details. It also includes the following options for managing your accounts:

- **Switch Customer**— Enables you to switch to another account. This is especially required during troubleshooting scenarios.
- **Change Password**— Enables you to change the password of the account.
- **User Settings**
 - **Time Zone**— Displays the zone, date, time, and time zone of the region.
 - **Language**— Administrators can set a language preference. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
 - **Idle Timeout**— Administrators can set a timeout value for inactive user sessions in the Idle Timeout field. The value is in minutes.
 - **Get system maintenance notification**— Administrators can select the check box to get system maintenance notification.
 - **Get software update notifications**— Administrators can select the check box to get software update notification.
- **Disable MSP**— Disables MSP mode and switches the user interface to the standard enterprise mode. This option changes to Enable MSP when the MSP mode is disabled. You can select **Enable MSP** to switch to the MSP mode. The MSP mode can be disabled only if there is no tenant data. The option is grayed out if there are any active tenant accounts.
- **Terms of Service**— Displays the terms and conditions for using Aruba Central services.
- **Logout**— Enables you to log out of from your account.

Filter

The filter  enables you to select by a group or **All Groups** for performing specific configuration and monitoring tasks. If no filter is applied, by default the filter is set to **All Groups**. When you set the filter to **All Groups**, the Global dashboard is displayed and when you set the filter to a group, the group dashboard is displayed.

Time Range Filter

The time range filter  enables you to set a time duration for showing monitoring and reports data. This time filter is not displayed when you view the configuration or device details. It is displayed only when you view monitoring data. You can set the filter to any of the following time ranges:

- 3 hours
- 1 day
- 1 week
- 1 month
- 3 months

Left Navigation Pane

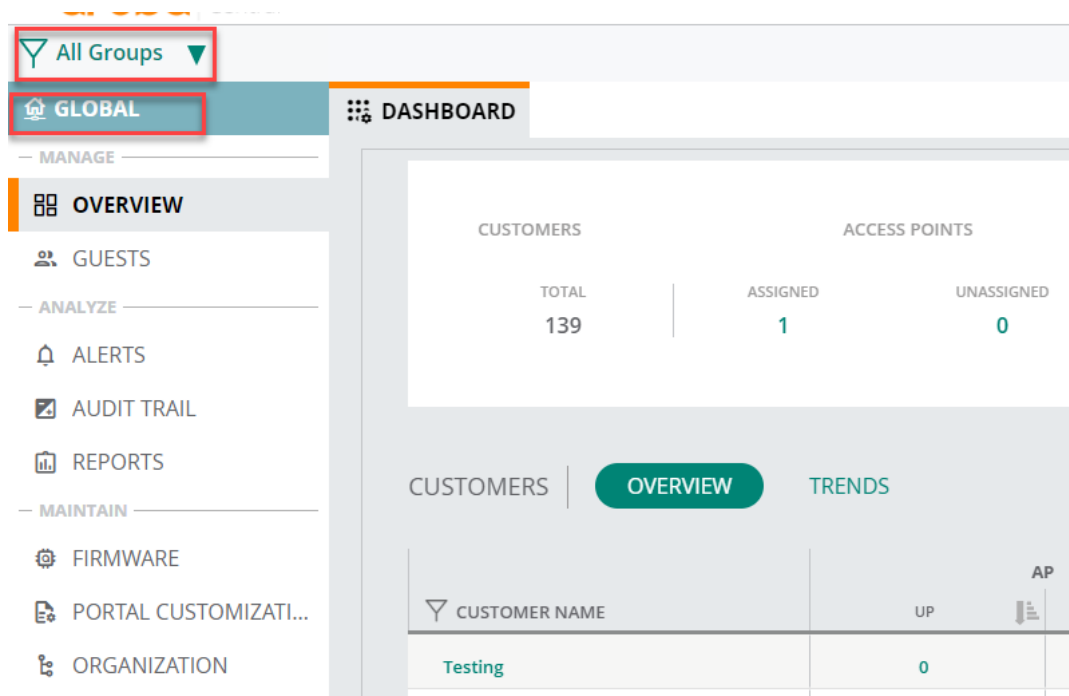
The left navigation pane is a *contextual* menu that displays a number of configuration, monitoring, and troubleshooting options depending on whether you select a group or **All Groups** from the filter.

Launching the MSP Global Dashboard




In the **Network Operations** app in MSP mode, use the filter to select **All Groups**. The Global dashboard is displayed.

In the Global dashboard under the left navigation pane, you can see a number of menu items divided under the following categories: **Manage**, **Analyze**, and **Maintain**.

Figure 9 Launching the Global Dashboard for MSP



Selecting each menu item in the left navigation pane displays a corresponding dashboard with tabs. Each tab may support all or some of the following functions:

- **Summary**  — Click the summary icon to view a graphical representation of the data. Only applicable for the global dashboard.
- **List**  — Click the list icon to view a tabular representation of the data. Only applicable for the global dashboard.
- **Configuration**  — Click the configuration icon to enable configuration mode.

The next sections discuss the left navigation menu items in the Global dashboard.

Manage

The following are included:

- **Overview**— Provides a summary of hardware and subscriptions owned by the MSP and the tenant accounts managed by the MSP. MSP administrators can perform tasks such as drilling down to a tenant account, editing an existing tenant account, and deleting a tenant account.
- **Guests**— Provides a dashboard to view information about cloud guests. Also enables you to create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy.

Analyze

The following are included:

- **Alerts**— Displays and configures a list of alerts. This page also enables you to acknowledge these alerts.
- **Audit Trail**— Displays audit trail for the events pertaining to device allocation, configuration, user addition deletion, and firmware upgrade status.
- **Reports**— Enables you to create, view, edit, and download various reports. You can configure the reports to run on demand or periodically. You must have read/write privileges or you must be an Admin user to be able to create reports.

Maintain

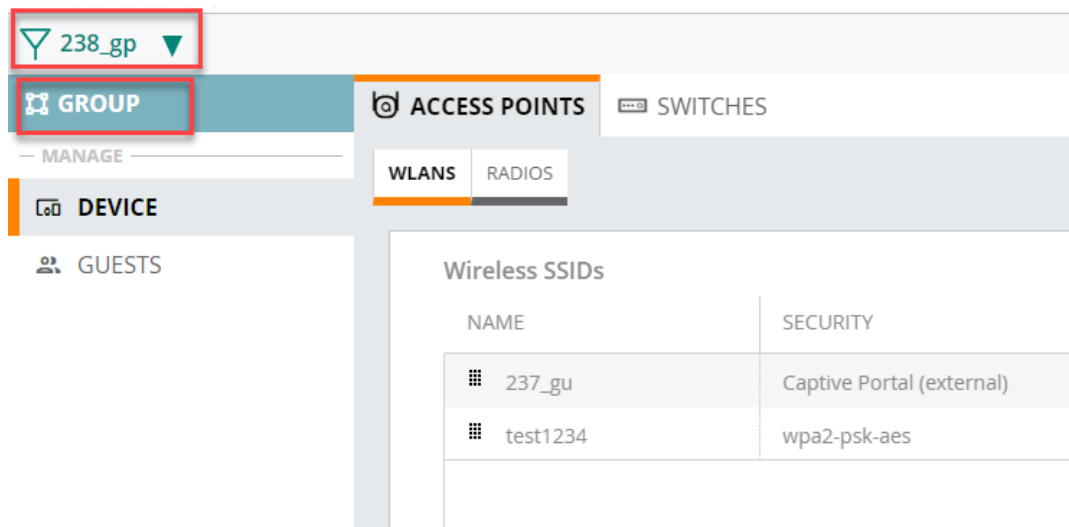
The following are included:

- **Firmware**— Provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device. Also enables you to manage firmware compliance for all devices.
- **Portal Customization**— Allows you to customize the look and feel of the user interface and the email notifications sent to the customers and users. For example, you can use your company logo in the user interface and company address in the email notifications sent to the customers or users.
- **Organization**— Enables you to create and manage groups under the **Groups** tab. Under the **Certificates** tab, you can view and add certificates.


Launching the MSP Group Dashboard

In the **Network Operations** app in MSP mode, use the filter to select a group. The group dashboard is displayed.

Figure 10 *Launching the Group Dashboard for MSP*



In the group dashboard under the left navigation pane, you can see the **Device** and **Guest** options under **Manage**.

Selecting an option in the left navigation pane displays a corresponding dashboard with tabs. Each tab supports the configuration icon  that enables the configuration mode. The next sections discuss the left navigation menu items in the group dashboard.

Manage

The following are included:

- **Device**—Enables you to configure APs and Switches for a specific group.
- **Guests**— Enables you to view and configure splash pages for guests.

Starting Your Free Trial

Aruba Central offers a 90-day evaluation subscription for customers who want to try the solution for managing their networks.

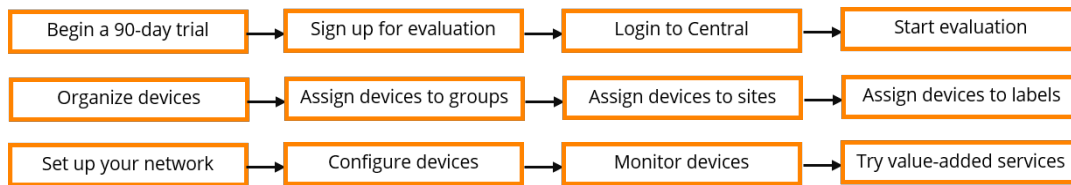
The evaluation subscription allows you to use the following functions:

Table 11: *Evaluation features*

| Application | Function |
|---------------------------------|---|
| Network Operations | <ul style="list-style-type: none"> ■ Device management <ul style="list-style-type: none"> ● Manage up to 10 Instant APs and/or switches ● Manage up to two SD-WAN Gateways ■ Monitoring—Monitor your devices, network and client status ■ Guest Access—Set up guest Wi-Fi on your custom portals ■ Presence Analytics—Analyze consumer presence data for your stores ■ Troubleshooting—Run diagnostic checks and troubleshoot device issues |
| ClearPass Device Insight | Discover, monitor, and automatically classify new and existing devices that connect to a network. |

Figure 11 shows the steps required for getting started with your free trial.

Figure 11 *Getting Started Workflow for Free Trial*



Get Started with the Free Trial

Complete the following steps to evaluate Aruba Central:

- [Step 1: Getting Started with the Initial Setup on page 56](#)
- [Step 2: Adding Devices on page 57](#)
- [Step 3: Organize Your Devices into Groups on page 57](#)
- [Step 4: Assigning Sites and Labels \(Optional\) on page 58](#)
- [Step 5: Configure Your Network on page 58](#)
- [Step 6: Monitor Your Network and Devices on page 58](#)
- [Step 7: Evaluate Value Added Services \(Optional\) on page 58](#)
- [Step 8: Cancel or Upgrade Your Subscription \(Optional\)](#)

Step 1: Getting Started with the Initial Setup

To get started with the trial:

1. [Register for evaluating Aruba Central.](#)
 2. [Log in to Aruba Central.](#)
- If you signed up to evaluate only the **Network Operations** app, the **Welcome to Aruba Central** page is displayed.
 - Click **Evaluate Now**. The **Get Started With Aruba Central** page guides you through the onboarding steps.
 - Click through the steps to set up your account and start using Aruba Central. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit Workflow**.



The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

- If you signed up to evaluate both **Network Operations** and **ClearPass Device Insight**, the **Network Operations** page is displayed.
For more information, see [ClearPass Device Insight Information Center](#).

Step 2: Adding Devices

To manage devices from Aruba Central, trial users must manually add the devices to Aruba Central's device inventory.

You can add up to 10 devices. The devices can be 10 Instant APs or 10 Switches, or a total of 10 Instant APs and switches.

Use one of the following methods to add devices to Aruba Central:

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number or MAC address of your devices.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
3. Click **Done**.
4. Review the devices in your inventory.

Using the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Add Devices**.
The **Add Devices** pop-up window is displayed.
3. Enter the serial number and the MAC address of each device.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
4. Click **Done**.
5. Review the devices in your inventory.

Step 3: Organize Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have Instant APs and Switches. Aruba Central allows you to manage configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to slave Instant AP in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Cloning an existing group allows you to create a base configuration for the devices and customize it as per your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.



A device can be part of only one group at any given time.

Groups in Aruba Central are mutually exclusive (independent) and do not follow a hierarchical model.

For more information on groups and group configuration workflows, see [Groups for Device Configuration and Management on page 88](#).

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use one of the following methods to assign your devices to groups.

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory**:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.

By default, the **Groups** page is displayed.

3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 4: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you can create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see [Managing Sites on page 84](#) and [Managing Labels on page 86](#).

Step 5: Configure Your Network

If you have added Instant APs as part of your evaluation, you can configure an employee and guest wireless network. If you have Switches or SD-WAN Gateways, configure wired access network or SD-WAN respectively.

Step 6: Monitor Your Network and Devices

Use [monitoring dashboards](#) to view the health of the device and network.

You can also [run reports](#), [configure alerts](#), and [view client details](#).

Step 7: Evaluate Value Added Services (Optional)

Enable Presence Analytics and Guest Access services on your Instant APs and review these services.

Step 8: Cancel or Upgrade Your Subscription (Optional)

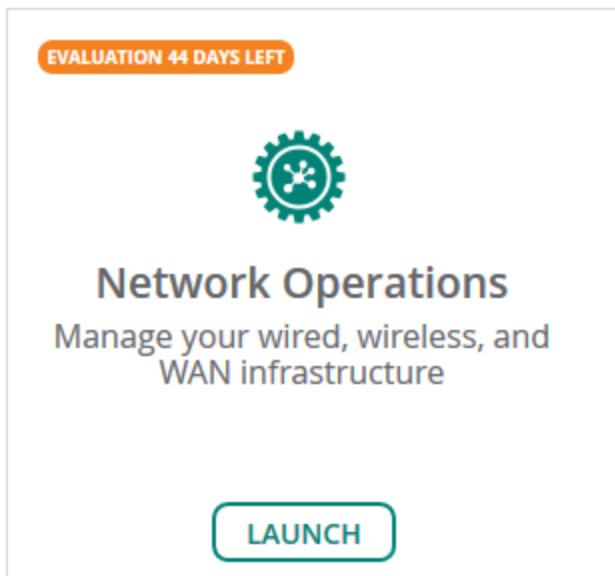
During the trial period or after you complete your trial, if you want to continue using Aruba Central for managing your devices, contact Aruba Customer Support to upgrade your subscription.

If you do not want to continue, contact Aruba support team to cancel your subscription or wait until the trial expires. When the trial period expires, your devices can no longer be managed from Aruba Central.

Upgrading to a Paid Account

If you have purchased a subscription, upgrade your account by completing the following steps:

1. On the respective app, click the link that shows the number of days left for the evaluation to expire:



The **Add a New Subscription** pop-up window opens.

2. Enter the new subscription key that you purchased from Aruba.
3. Click **Add Subscription**.

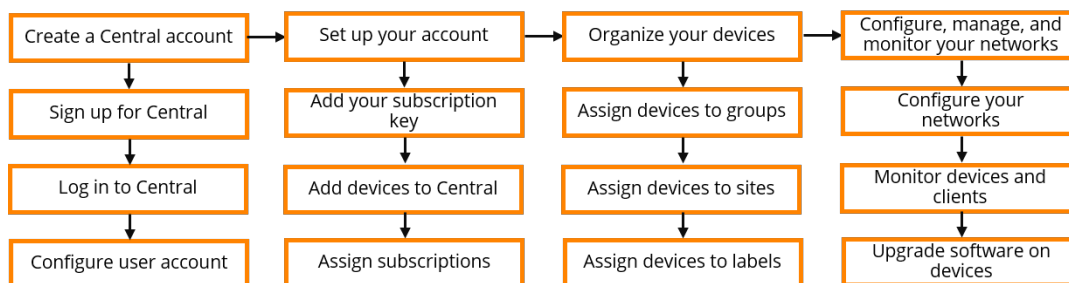
After you upgrade your account, you can add more devices and enable services, and continue using Aruba Central.

Setting up Your Aruba Central Instance

If you have purchased a subscription key to manage your devices and networks from Aruba Central, get started with steps described in this topic.

[Figure 12](#) illustrates the steps required for setting up your Aruba Central instance:

Figure 12 *Getting Started Workflow*



Getting Started with Aruba Central

Complete the following steps to start using Aruba Central for managing your devices and setting your networks.

- [Step 1: Getting Started on page 60](#)
- [Step 2: Adding a Subscription Key on page 60](#)
- [Step 3: Adding Devices on page 61](#)
- [Step 4: Assigning Subscriptions on page 63](#)
- [Step 5: Organize Your Devices into Groups on page 64](#)
- [Step 6: Assigning Sites and Labels \(Optional\) on page 65](#)
- [Step 7: Configuring Users on page 65](#)
- [Step 8: Configuring and Managing Networks on page 65](#)
- [Step 9: Monitoring Your Network and Devices on page 65](#)
- [Step 10: Upgrading Software Images on Devices on page 65](#)
- [Step 11: Running Diagnostic Checks and Troubleshooting Issues on page 65](#)

Step 1: Getting Started

To get started:

1. [Sign up](#) to create your Aruba Central account.
2. If you already have an Aruba Central account, [log in](#) to Aruba Central with your credentials. When you log in for the first time, the **Initial Setup** wizard opens and guides you through the onboarding workflow.
3. Click **Get Started**.
4. Click through the wizard to complete the onboarding workflow. If you want to exit the wizard and complete the onboarding steps on your own, click **Exit and go to Aruba Central**.



The Initial Setup wizard is displayed only when you log in to Aruba Central for the first time. The wizard is not available for Aruba Central users in the MSP mode.

Step 2: Adding a Subscription Key

At your first login, the **Initial Setup** wizard prompts you add your subscription key. To continue with the onboarding workflow, add your subscription key in the Add Subscription Key tab.

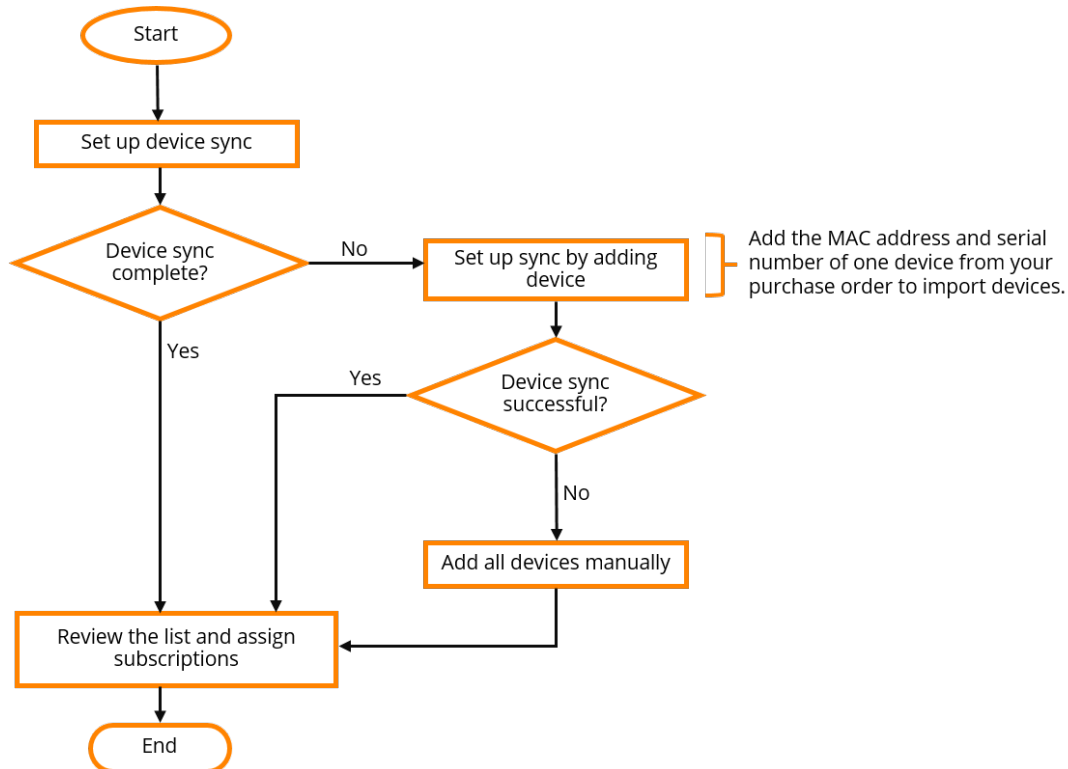
If you are not using the wizard, complete the following steps to add your subscription key.

To add a subscription key:

1. In the **Account Home** page, under **Global Settings**, click **Key Management**.
The **Key Management** page is displayed.
2. Enter your subscription key.
3. Click **Add Subscription**. The subscription key is added to Aruba Cloud Platform and the contents of the subscription key are displayed in the **Manage Keys** table.
4. Review the subscription details.

Step 3: Adding Devices

If you have a paid subscription, you can automatically import devices from the Activate database to the Aruba Central device inventory.



Setting up Device Sync for Automatic Device Addition

To set up device sync, use one of the following methods:

- [In the Initial Setup Wizard](#)
- [From the Device Inventory Page](#)

In the Initial Setup Wizard

1. Ensure that you have added a subscription key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of one device from your purchase order.

Most Aruba devices have the serial number and MAC address on the front or back of the hardware.

3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. Perform the following options:
 - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
 - **Contact support**—Contact Aruba Technical Support.

From the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.



Aruba Central imports only devices associated with your Central account from Activate.

2. Do one of the following:
 - Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
 - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
 - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home > Audit Trail** page.

3. Review the devices in your inventory.
4. Perform the following options:
 - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
 - **Contact support**—Contact Aruba Technical Support.

Manually Adding Devices

To add devices using MAC address and serial number, use one of the following methods:

- [In the Initial Setup Wizard](#)
- [From the Device Inventory Page](#)

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

1. In the **Add Devices** tab of the Initial Setup wizard.
2. Click **Add Device**.
3. Enter the serial number of MAC address of your device.
4. Click **Done**.
5. Review the list of devices.

From the Device Inventory Page

To add devices from the **Device Inventory** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Do one of the following:
 - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.

- If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home > Audit Trail** page.

3. Click **Done**.
4. Review the devices added to the inventory.



When you add the serial number and MAC address of one AP from a cluster or a switch stack member, Aruba Central imports all devices associated in the AP cluster and switch stack respectively.

For more information on adding devices, see [Onboarding Devices on page 72](#).

Step 4: Assigning Subscriptions

Aruba Central supports the following types of subscriptions:

- Device subscription—Allows you to manage and monitor your devices from Aruba Central. The device subscriptions can be assigned only to the devices managed by Aruba Central.
- Service subscription—Allows you to enable value added services on the APs managed from Aruba Central. For example, if you have APs, you can assign a service subscription for Guest Access.
- Gateway subscription—Allows you to manage and monitor SD-WAN Gateways from Aruba Central.

You can either enable automatic assignment of subscription or manually assign subscriptions to your devices. By default, the automatic subscription assignment is disabled.

Enabling Automatic Assignment of Subscriptions

Use one of the following options to enable automatic assignment of subscriptions:

In the Initial Setup Wizard

1. Verify that you have a valid subscription key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the **Assign Subscription** tab, turn on the **Auto Subscribe** toggle switch.

From the Subscription Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
2. Under **Device Subscriptions**, toggle the **Auto Subscribe** slider to ON. All the devices in your inventory are selected for automatic assignment of subscriptions. You can edit the list by clearing the existing selection and re-selecting devices.

Manually Assigning Subscriptions

In the Initial Setup Wizard

1. In the **Assign Subscription** tab, ensure that the **Auto Subscribe** toggle switch is turned off.
2. Select the devices in the list for which you want to manually assign subscriptions.
3. Click **Update Subscription**.

From the Subscription Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
2. On the **Subscription Assignment** page, ensure that the **Auto Subscribe** toggle is turned off.

3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

For more information on subscriptions and how to assign network service and SD-WAN Gateway subscriptions, see [Managing Subscriptions on page 78](#).

Step 5: Organize Your Devices into Groups

A group in Aruba Central functions as a configuration container for devices added in Aruba Central.

Why Should You Use Groups?

Groups allow you to create a logical subset of devices and simplify the configuration and device management tasks. Groups offer the following functions and benefits:

- Combining different types of devices under a group. For example, a group can have Instant APs and Switches. Aruba Central allows you to manage configuration of these devices in separate containers (wireless and wired management) within the same group. Any new device that is added to a group inherits the current configuration of the group.
- Assigning multiple devices to a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to slave Instant AP in their respective clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.
- Cloning an existing group allows you to create a base configuration for the devices and customize it as per your network requirements.

You can also use groups for filtering your monitoring dashboard content, generating reports, and managing software upgrades.



A device can be part of only one group at any given time.

Groups in Aruba Central are mutually exclusive (independent) and do not follow a hierarchical model.

For more information on groups and group configuration workflows, see [Groups for Device Configuration and Management on page 88](#).

Assigning Devices to Groups

After you successfully complete the onboarding workflow, the **Initial Setup** wizard prompts you to assign your devices to a group. You can click **Assign Group** and assign your devices to a group. You can also use one of the following methods to assign your devices to groups.

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory**:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 6: Assigning Sites and Labels (Optional)

A site in Aruba Central refers to a physical location where a set of devices are installed; for example, campus, branch, or venue. Aruba Central allows you to use sites as a primary navigation element. For example, if your devices are deployed in a campus, you could create a site called CampusA. You can also tag the devices within CampusA using labels. If your campus consists of multiple buildings, the devices deployed in the campus can be labeled as **Building1** or **Lobby**.

For more information on sites and labels and how to assign devices to sites and labels, see [Managing Sites on page 84](#) and [Managing Labels on page 86](#).

Step 7: Configuring Users

Add system users, assign user roles, and configure role based access control.

For more information, see [Configuring System Users on page 136](#).

Step 8: Configuring and Managing Networks

To start configuring your network setup:

1. [Connect your devices to Aruba Central](#).
2. Provision [Instant APs](#), [Switches](#), or [Gateways](#) to set up your WLAN, wired access and SD-WAN network.

Step 9: Monitoring Your Network and Devices

Use the [monitoring dashboards](#) to view the health of the device and network.

You can also [run reports](#), [configure alerts](#), and [view client details](#).

Step 10: Upgrading Software Images on Devices

View software images available for the devices provisioned in your account, run a compliance check for the recommended software version, and upgrade devices.

For more information and step-by-step instructions, see [Managing Software Upgrades on page 119](#).

Step 11: Running Diagnostic Checks and Troubleshooting Issues

Run diagnostic checks and troubleshooting commands to analyze network connectivity and latency issues and debug device issues if any. For more information and step-by-step instructions, see [Using Troubleshooting Tools](#).

Email Notifications for Software Upgrades

Aruba Central administrators would receive email notifications before any scheduled maintenance activity or unplanned outage. By default, email notifications are enabled. The email notification contains the following details:

- Start date and time.
- Estimated end date and time.
- Link to the **What's New** page where users can view the list of new features and enhancements included in the release.
- Impact of the outage.

Users can no longer check the status of Aruba Central using the following URLs:

- US—<http://status.central.arubanetworks.com>
- Canada—<http://ca-status.central.arubanetworks.com>

- APAC—<http://apac-status.central.arubanetworks.com>
- APAC East—<http://apaceast-status.central.arubanetworks.com>
- Europe—<http://eu-status.central.arubanetworks.com>

Enabling Email Notifications

By default, email notifications are enabled. However, if email notifications are disabled and you wish to enable system maintenance or software update email notifications, complete the following steps:

1. In the Aruba Central UI, click the user icon (👤) in the header pane.
2. Click **User Settings**.
3. In the **User Settings** pop-up window, do the following:
 - a. Select the **Get system maintenance notifications** check box to receive system maintenance notification on the registered email ID. Email notifications are sent before any scheduled maintenance activity or unplanned outage.
 - b. Select the **Get software update notifications** check box to receive software update notification on the registered email ID.
4. Click **Save**.

Figure 13 *Email Notifications*

USER SETTINGS

My Zone: US-2

Time Zone: Mar 10, 2020, 11:57:59 (+05:30)

Language: English

Idle Timeout: 30 min

Get system maintenance notifications: ☒

Get software update notifications: ☒

Cancel Save

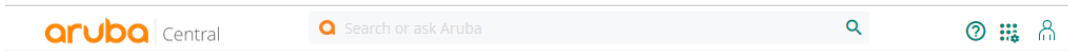
Search Bar

The search tool in the **Network Operations** app enables users to search for clients, devices, and infrastructure connected to the network. The tool also retrieves relevant documentation to help users efficiently operate their networks. From the search results, users can navigate to:

- Various pages in the **Network Operations** app such as configuration pages, client or device monitoring dashboards, or troubleshooting pages.
- Help page in the Aruba Central Help Center.

The search engine uses Natural Language Processing (NLP) to analyze queries and return relevant results. For example, the query, **Where do I configure a captive portal?** navigates the user to the **Guest Access** page where the user can accomplish this task.

Figure 14 *Search Bar*



Search Query Examples

This section describes few search query examples and shows how search results are displayed.

Example 1

In the following example, the search term, **20:4c**, returns clients or devices containing 20:4c in the MAC address. Hover over the result to view more details about the client or device. Click on the specific search result to navigate to the corresponding client details or device details page.

The screenshot shows a search interface with the query '20:4c' entered in the search bar. Below the search bar, it says 'We found the following results:'. The results are categorized into three sections: Clients, Access Points, and Gateways. In the Clients section, the first result is highlighted with a red box, showing details for MAC address 20:4c:03:43:e9:a0, including a table with columns for MAC, USERNAME, STATUS, and IP. The Access Points section shows one result for MAC 20:4c:03:18:d4:b0. The Gateways section shows three results for various MAC addresses. At the bottom, there is a 'Was this helpful?' feedback prompt.

Clients

| MAC | USERNAME | STATUS | IP |
|-------------------|----------|-----------|---------|
| 20:4c:03:43:e9:a0 | - | CONNECTED | 0.0.0.0 |

Access Points

Gateways

Example 2

In the following example, the search query, **Do my APs have any performance issues?**, returns relevant results for the query. From the list of results, click **View** to navigate to the **AI Insights** page or click **Read** to navigate to the **AI Insights** documentation.

The screenshot shows a search interface with the query 'Do my APs have any performance issues?' entered in the search bar. Below the search bar, it says 'We found the following results:'. The results are categorized into three sections: AI Insights, Network Health, and Advanced Device Troubleshooting. Each section has a 'VIEW' or 'READ' button. The AI Insights section is highlighted with a red box. At the bottom, there is a 'Was this helpful?' feedback prompt.

AI Insights

Please click 'View' to view further information about Global Insights.

AI Insights

AI Insights AI Insights The **AI Insights** tab in the Overview context menu displays information on AP performance issues such as, excessive channel changes, excessive reboots, airtime utilization, memory utilization at AP. The **AI Insights** information is available at the following contexts: Global (All Devices): Displays a consolidated report of **AI Insights** observed at the glob...

Network Health

AI Insights The number of **AI Insight** reports available for the site. The reports are organized by degree- High, Medium and Low depending on the number of events in the network. High Noise The number of APs with a high RF noise. Uplink Status Displays the Tunnel Status Displays the Explore Aruba Central Overview, the following pages are available: Summary Netwo...

Advanced Device Troubleshooting

To **perform** advanced troubleshooting on **APs**, the minimum software version required on Instant **APs** is 6.4.3.1-4.2.0.3. To **perform** advanced troubleshooting on **Mobility Access Switches**, the minimum version support is 7.4.0.6. Troubleshooting Switches To troubleshoot switches at an advanced level: 1. In the Commands tab, select the device type as Switch. 2. From t...

Following are few additional sample search queries:

- Troubleshoot client **aa:bb:cc:dd:ee:ff**. Enter the MAC address of the client.
- Do we have any authentication issues?

- How is the performance of my site?
- Show gateway *aa:bb:cc:dd:ee:ff* session table. Enter the MAC address of the device.
- Help me set up route orchestration.
- How does tunnel orchestration work?
- Configure or modify user roles.

Providing Feedback

Users can also provide feedback after the search results are displayed. Depending on how satisfied you are with the search results, click the thumbs-up or thumbs-down button. After you click one of these buttons, a text box appears in which you can enter comments.

Figure 15 *Feedback*

20:4c
 ✕

We found the following results:

Clients

MAC: 20:4c:03:43:e9:a0
● 20:4c:03:43:e9:a0

MAC: 20:4c:03:1a:01:6d
○ 20:4c:03:1a:01:6d

MAC: 20:4c:03:26:5e:2c
○ 20:4c:03:26:5e:2c

MAC: 20:4c:03:43:e6:e8
○ 20:4c:03:43:e6:e8

MAC: 20:4c:03:0a:be:d0
○ 20:4c:03:0a:be:d0

MAC: 20:4c:03:26:8d:bc
○ 20:4c:03:26:8d:bc

Access Points

MAC: 20:4c:03:18:d4:b0
○ AP3-20:4c:03:18:d4:b0

Gateways

MAC: 20:4c:03:0a:be:d0
○ Aruba7008_0A_BE_D0

MAC: 20:4c:03:40:0a:d0
● kkdesk-A9004_40_0...

MAC: 20:4c:03:81:eb:8a
● Aruba9004_81_EB_8A

MAC: 20:4c:03:30:00:9c

MAC: 20:4c:03:39:81:fc

MAC: 20:4c:03:39:76:b4

Was this helpful?
 👍
👎

Aruba Central is a cloud-native network operations and assurance solution for wired, wireless, and SD-WAN networks. Aruba Central unifies traditional management with AI-based network and user insights, and IoT device profiling in a single interface for simplified and secure management and control.

Apps

From the **Account Home** page, you can manage network inventory, subscriptions, and user access. You can provision or launch the following apps:

- **Network Operations**
- **ClearPass Device Insight**

The application(s) displayed in the **Apps** section of the page are dependent on the app(s) that you selected while signing up for Aruba Central.

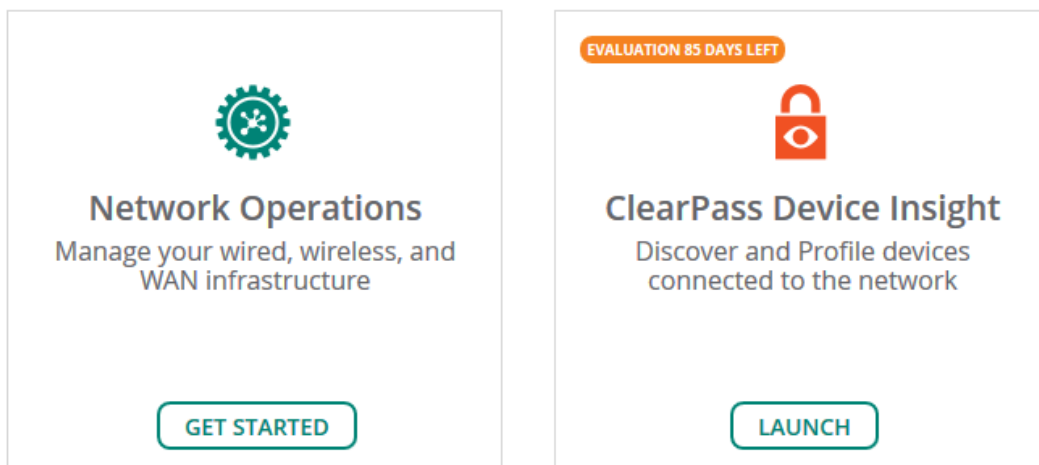
For more information, see [Creating an Aruba Central Account on page 37](#).

To provision an app, click **Get Started**. After the app is provisioned, click **Launch** to navigate to the corresponding application UI.

If the app provisioning fails, you can retry or contact Aruba Technical Support.

Figure 16 All Apps

APPS



Network Operations

Network Operations is a unified network operations, assurance and security platform that simplifies the deployment, management, and service assurance of wireless, wired and SD-WAN environments. Network Operations provides a cloud-based network management platform for managing your wireless, WAN, and wired networks with Aruba APs, Gateways, and Switches. Along with device and network management functions, the app also offers value-added services such as customized guest access, client presence, and service assurance analytics.

For more information, see [Aruba Central Help Center](#).

ClearPass Device Insight

ClearPass Device Insight enables network and security administrators to discover, monitor, and automatically classify new and existing devices that connect to a network. You can identify devices that include IoT devices, medical devices, printers, smart devices, laptops, VoIP phones, computers, gaming consoles, routers, servers, and switches.

For more information, see [Aruba ClearPass Device Insight Information Center](#).

Global Settings

In Aruba Central, most of the general administration tasks are grouped under **Global Settings**. The following table lists all the options and relevant app(s) to which the option is applicable:

Table 12: *Options & Apps*

| Option | App(s) |
|-------------------------|--|
| User and Roles | <ul style="list-style-type: none">■ Network Operations■ ClearPass Device Insight |
| Key Management | <ul style="list-style-type: none">■ Network Operations■ ClearPass Device Insight |
| Device Inventory | Network Operations |
| Subscription Assignment | Network Operations |
| Data Collectors | Data Collectors option appears only if the ClearPass Device Insight app is provisioned. |
| Audit Trail | Network Operations |
| Single Sign On | Network Operations |
| API Gateway | API Gateway option appears only if the Network Operations app is provisioned and if the API Gateway license is enabled. |
| Webhooks | Network Operations |

Managing Your Device Inventory

The devices purchased by the customers are automatically added the device inventory in their respective Aruba Central accounts. If the device you purchased does not show up in the inventory, you can manually add it.

Aruba Central allows you to add up to 32 devices manually by entering the valid MAC and serial number combination for each device.



Users having roles with **Modify** permission can add devices. Users having roles with **View Only** permission can only view the Device Inventory module.

Viewing Devices

The devices provisioned in your account are listed in the **Global Settings > Device Inventory** page.

The following table describes the contents of the **Device Inventory** page.

Table 13: *Device Details*

| Parameter | Description |
|----------------------|--|
| Serial Number | Serial number of the device. |
| MAC Address | MAC address of the device. |
| Type | Type of the device, for example Instant AP, switch, or gateway. |
| IP Address | IP address of the device. |
| Name | Name of the device. |
| Model | Hardware model of the device. |
| Part Number | Part number of the device. |
| Group | Name of the group to which the device is assigned. This column is displayed only for the Aruba Central Standard Enterprise mode users. |
| Subscription | Status of the subscription assignment |

Adding Devices to Inventory

For information on adding devices, see [Onboarding Devices](#).

Onboarding Devices

Aruba Central supports the following options for adding devices.

- If you are an evaluating user, you must manually add the serial number and MAC address of the devices that you want to manage from Aruba Central. For more information, see [Adding Devices \(Evaluation Account\) on page 73](#).
- If you are a paid subscriber, Aruba Central retrieves devices associated with your purchase order from Activate. Set up a sync to import devices from the Activate database, see [Adding Devices \(Paid Subscription\) on page 73](#).

This section includes the following topics:

- [Adding Devices \(Evaluation Account\)](#)
- [Adding Devices \(Paid Subscription\)](#)
- [Manually Adding Devices](#)

Adding Devices (Evaluation Account)

Use one of the following methods to add devices to Aruba Central:

Using the Initial Setup Wizard

1. In the **Add Devices** tab of the Initial Setup wizard, click **Add Device**.
2. Enter the serial number or MAC address of your devices.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
3. Click **Done**.
4. Review the devices in your inventory.

Using the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Add Devices**.
The **Add Devices** pop-up window is displayed.
3. Enter the serial number and the MAC address of each device.
You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.
4. Click **Done**.
5. Review the devices in your inventory.

Adding Devices (Paid Subscription)

If your devices are not added to your inventory, set up a device sync by adding one device from your purchase order.

To set up device sync, use one of the following methods:

- [In the Initial Setup Wizard](#)
- [From the Device Inventory Page](#)

In the Initial Setup Wizard

1. Ensure that you have added a subscription key and click **Next**.
2. In the **Add Devices** tab, enter the serial number and MAC address of one device from your purchase order.
Most Aruba devices have the serial number and MAC address on the front or back of the hardware.
3. Click **Add Device**. Aruba Central imports all other devices mapped to your purchase order.
4. Review the devices in your inventory.
5. Perform the following options:
 - **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
 - **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
 - **Contact support**—Contact Aruba Technical Support.

From the Device Inventory Page

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.



Aruba Central imports only devices associated with your Central account from Activate.

2. Do one of the following:

- Click **Sync Devices**. Enter the serial number and MAC address and click **Add Device**.
- Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
- If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home > Audit Trail** page.

3. Review the devices in your inventory.

4. Perform the following options:

- **Add Devices Manually**—Manually add devices by entering the MAC address and serial number of each device.
- **Add Via Mobile App**—Add devices from the Aruba Central mobile app. You can download the Aruba Central app from Apple App Store on iOS devices and Google Play Store on Android devices.
- **Contact support**—Contact Aruba Technical Support.

Manually Adding Devices

Aruba Central allows you to set up only manual sync of devices from Activate database using one of the following methods:

- [Adding Devices Using MAC address and Serial Number on page 74](#)
- [Adding Devices Using Activate Account on page 75](#)
- [Adding Devices Using Cloud Activation Key on page 75](#)



You can only set up only a manual sync for Aruba Central-managed folders such as the default, licensed, and non-licensed folders.

Adding Devices Using MAC address and Serial Number

You can find the serial number and MAC address of Aruba devices on the front or back of the hardware.

To add devices using MAC address and serial number, use one of the following methods:

- [In the Initial Setup Wizard](#)
- [From the Device Inventory Page](#)

In the Initial Setup Wizard

If you are using the Initial Setup wizard:

1. In the **Add Devices** tab of the Initial Setup wizard.
2. Click **Add Device**.
3. Enter the serial number of MAC address of your device.
4. Click **Done**.
5. Review the list of devices.

From the Device Inventory Page

To add devices from the **Device Inventory** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Do one of the following:
 - Click **Add Devices** to manually add devices by entering the MAC address and serial number of each device.
 - If you are a paid subscriber, you can add devices using a CSV file. Click **Import Via CSV** and select the CSV file. For a sample CSV file, click **Download sample CSV file**.



Manual addition of devices using a CSV file is restricted to 100 devices or to the number of available device management tokens. An error message is displayed if more than 100 devices are imported using the CSV file. You can view the status of the CSV upload in the **Account Home > Audit Trail** page.

3. Click **Done**.
4. Review the devices added to the inventory.



When you add the serial number and MAC address of one AP from a cluster or a switch stack member, Aruba Central imports all devices associated in the AP cluster and switch stack respectively.

Adding Devices Using Activate Account

Use this device addition method only when you want to migrate your inventory from Aruba AirWave or a standalone AP deployment to the Aruba Central management framework.



Use this option with caution as it imports all devices from your Activate account to the Aruba Central device inventory.

You can use this option only once. After the devices are added, Aruba Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.

To add devices from your Activate account:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Advanced** and select **Using Activate**.
3. Enter the username and password of your Activate account.
4. Click **Add**.
5. Review the devices added to the inventory.

Adding Devices Using Cloud Activation Key



When you import devices using the Cloud Activation Key, all your devices from the same purchase order are added to your Aruba Central inventory.

Before adding devices using cloud activation key, ensure that you have noted the cloud activation key and MAC address of the devices to add.

Locating Cloud Activation Key and MAC Address

To know the cloud activation key:

- For APs:
 1. Log in to the WebUI or CLI.
 - If using the WebUI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show about** command.
 2. Note the cloud activation key and MAC address.
- For Aruba Switches:
 1. Log in to the switch CLI.
 2. Execute the **show system | in Base** and **show system | in Serial** commands.
 3. Note the cloud activation key and MAC address in the command output.
- For Mobility Access Switches
 1. Log in to the Mobility Access Switch UI or CLI.
 - If using the UI, go to the **Maintenance > About**.
 - If using the CLI, execute the **show inventory | include HW** and **show version** commands.
 2. Note the cloud activation key and MAC address. The activation key is enabled only if the switch has access to the Internet.

Adding Devices Using Cloud Activation Key

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**.
The **Device Inventory** page is displayed.
2. Click **Advanced** and select **With Cloud Activation Key**. The **Cloud Activation Key** pop-up window opens.
3. Enter the cloud activation key and MAC address of the device.
4. Click **Add**.



If a device belongs to another customer account or is used by another service, Aruba Central displays it as a blocked device. As Aruba Central does not support managing and monitoring blocked devices, you may have to release the blocked devices before proceeding with the next steps.

Key Management

A subscription key is a 14-character alphanumeric string; for example, PQREWD6ADWERAS. Subscription keys allow your devices to be managed by Aruba Central. To use Aruba Central for managing, profiling, analyzing, and monitoring your devices, you must ensure that you have a valid subscription key. You must either have an evaluation subscription key or a paid subscription key. The evaluation subscription key is valid for 91 days.

Evaluation Subscription Key

The evaluation subscription key is enabled for trial users by default. It allows you to add up to a total of 10 devices. The evaluation subscription also allows you to enable services such as Presence Analytics and Guest Access on your devices.

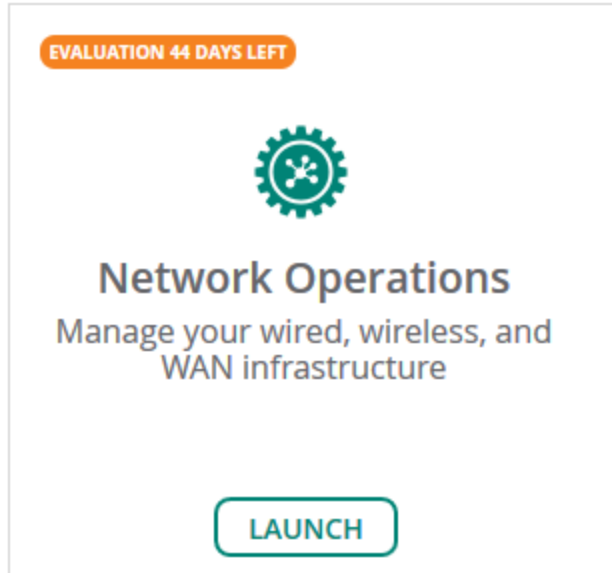
The **Account Home > Global Settings > Key Management** page displays the subscription expiration date. You will receive subscription expiry notifications through email on the 30th, 15th and 1 day before the

subscription expiry and on day 1 after the subscription expires. The number of days left for subscription expiry is also displayed in the respective app under the **Apps** section of the **Account Home** page.

Upgrading to a Paid Account

If you have purchased a subscription, upgrade your account by completing the following steps:

1. On the respective app, click the link that shows the number of days left for the evaluation to expire:



The **Add a New Subscription** pop-up window opens.

2. Enter the new subscription key that you purchased from Aruba.
3. Click **Add Subscription**.

After you upgrade your account, you can add more devices and enable services, and continue using Aruba Central.

Paid Subscription Key

If you have purchased a subscription key, you must ensure that your subscription key is added to Aruba Cloud Platform. If you are logging in for the first time, Aruba Cloud Platform prompts you to add your subscription key to activate your account. Ensure that you add the subscription key before onboarding devices to Aruba Cloud Platform.

The **Account Home > Global Settings > Key Management** page displays the subscription expiration date. You will receive subscription expiry notifications through email on the 90th, 60th, 30th, 15th, and 1 day before expiry and two notifications per day on the day 1 and day 2 after the subscription expiry.

When you upgrade or renew your subscription, or purchase another subscription key, you must add the key details in the **Account Home > Global Settings > Key Management** page to avail the benefits of the new subscription.

Adding a Subscription Key

To add a subscription key:

1. In the **Account Home** page, under **Global Settings**, click **Key Management**.
The **Key Management** page is displayed.
2. Enter your subscription key.

3. Click **Add Subscription**. The subscription key is added to Aruba Cloud Platform and the contents of the subscription key are displayed in the **Manage Keys** table.
4. Review the subscription details.

Viewing Subscription Key Details

To view subscription key details, in the **Account Home** page, under **Global Settings**, click **Key Management**.

The following table describes the contents of the **Manage Keys** table:

Table 14: *Subscription Key Details*

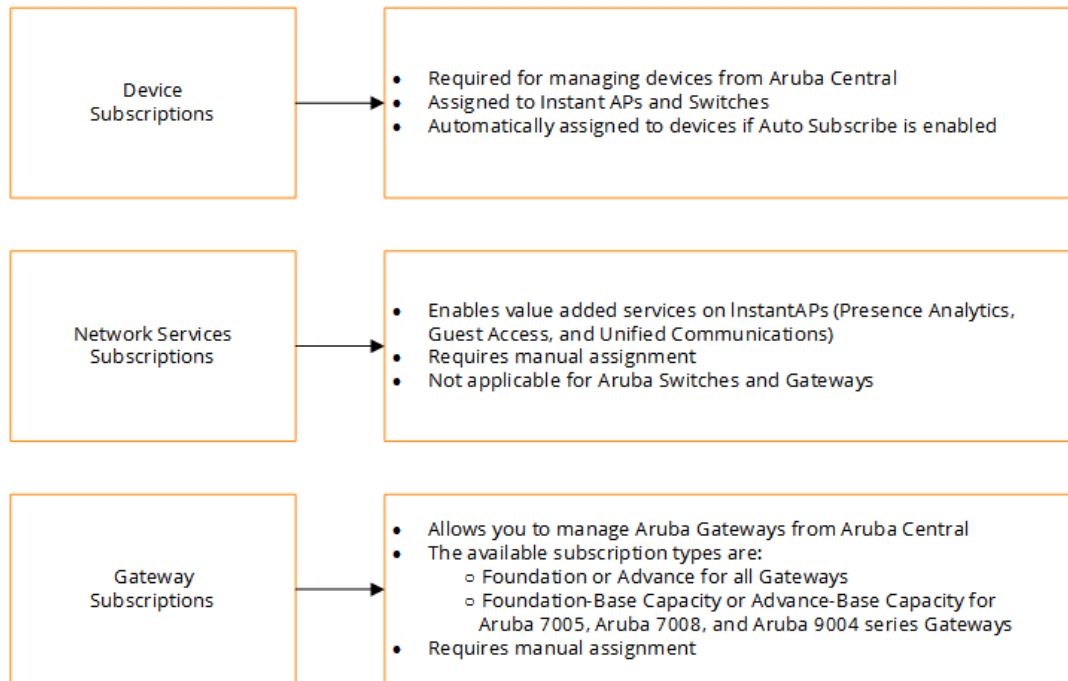
| Data Pane Item | Description |
|------------------------|--|
| Keys | Subscription key number. |
| Type | Type of the subscription. Aruba Central supports the following types of subscriptions: <ul style="list-style-type: none"> ■ Device subscriptions—The device subscription allows you to avail services such as device onboarding, configuration, management, monitoring, and reports. The device subscriptions can be assigned only to the devices managed by Aruba Central. ■ Service subscriptions—Aruba Central supports application services that you can run on the devices provisioned in your setup. For example, if you have Instant APs with 6.4.4.4-4.2.3.0 or later, you can assign a service subscription for Presence Analytics. ■ Gateway Subscriptions—Aruba Central supports a separate set of subscriptions for configuring and managing SD-WAN gateways. The Gateway subscriptions are marked as Foundation-<device>; for example, Foundation-70XX. ■ Virtual Gateways—Aruba Central supports a separate set of subscriptions for configuring and managing Virtual Gateways. The Virtual Gateway subscriptions are prefixed with a VGW-<bandwidth>; for example, VGW-500MB. |
| Expiration Date | Expiration date for the subscription key. |
| Quantity | Number of license tokens available for a subscription. Each Aruba Central subscription holds a specific number of tokens. For example, when a subscription is assigned to a device, Aruba Central binds the device with a token from the existing pool of subscriptions. |
| Status | Status of the subscription key. For example, if you are a trial user, Aruba Central displays the status of subscription key as Eval . |
| Apps | Name of the application. |

Managing Subscriptions

Aruba Central supports the following types of subscriptions:

- Device subscription—Allows you to manage and monitor your devices from Aruba Central. The device subscriptions can be assigned only to the devices managed by Aruba Central.
- Service subscription—Allows you to enable value added services on the APs managed from Aruba Central. For example, if you have APs, you can assign a service subscription for Guest Access.
- Gateway subscription—Allows you to manage and monitor SD-WAN Gateways from Aruba Central.

The following figure illustrates the supported subscription types and the assignment criteria:



Assigning Subscriptions

Read through the following sections to understand the subscription assignment procedures:

- [Assigning Device Subscriptions on page 79](#)
- [Assigning Subscriptions on page 79](#)
- [Assigning Gateway Subscriptions on page 81](#)

Assigning Device Subscriptions

You can either enable automatic assignment of subscriptions or manually assign subscriptions for the devices added in Aruba Central.

Enabling Automatic Assignment of Subscriptions

To enable automatic assignment of subscriptions, use one of the following methods:

In the Initial Setup Wizard

1. Verify that you have valid subscription key.
2. Ensure that you have successfully added your devices to the device inventory.
3. In the Assign Subscription tab, turn on the **Auto Subscribe** toggle switch.

From the Subscription Assignment Page

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Device Subscriptions**, toggle the **Auto Subscribe** slider to ON. All the devices in your inventory are selected for automatic assignment of subscriptions. You can edit the list by clearing the existing selection and re-selecting devices.



When a subscription assigned to a device expires or is canceled, Aruba Central checks for the available subscription tokens in your account and assigns the longest available subscription token to the device. If

your account does not have an adequate number of subscriptions, you may have to manually assign subscriptions to as many devices as possible. To view the subscription utilization details and the number of subscriptions available in your account, go to the **Account Home > Global Settings > Key Management** page.

To manually assign subscriptions, turn off the **Auto Subscribe** toggle.

Manually Assigning Subscriptions

To manually assign subscriptions to devices or override the current assignment:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Ensure that the **Auto Subscribe** toggle is turned off.
3. Select the devices to which you want to assign subscriptions.
4. Click **Update Subscription**.

Assigning Network Service Subscriptions

To assign a network service subscription, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Select the service subscription that you want to enable on a device. The available services are:
 - Cloud Guest
 - Presence Analytics
 - UCC

Clarity network service is deprecated. [Wi-Fi Connectivity](#) dashboard has replaced Clarity. The [Wi-Fi Connectivity](#) dashboard displays global connectivity details and insights. You do not require a separate service subscription to view the **Wi-Fi Connectivity** dashboard.



Although you can assign or unassign **Clarity** service subscription, **Clarity** does not monitor deployments or detect network performance issues.

3. Under **Network Service Subscriptions**, select the AP from the table on the right.
4. Drag and drop the device to the network service selected in the table on the left.

Important Note for MSP Users

Ensure that the device is assigned to a tenant before assigning a service subscription to it. When a device or network service subscription is assigned to a device that is not mapped to any specific tenant, the following error is displayed: **Please assign this device to a tenant before subscribing it. Tenant assignment can be performed in the Device Inventory page.**

Assigning Gateway Subscriptions

For Aruba Gateways to function as Aruba Gateways, you must onboard them to the Aruba Central's device inventory and ensure that a valid subscription is assigned to each Gateway. A valid subscription allows the Gateway to be managed by Aruba Central.

Gateway Subscriptions

Aruba Central supports the following types of subscriptions for Gateways:

- **Foundation**—This subscription can be assigned to all Gateways irrespective of the hardware model.
- **Foundation-Base capacity** —This subscription can be assigned to Aruba 7005, Aruba 7008, and Aruba 9004 Gateways. Gateway devices with the Foundation-Base capacity subscription can support up to 75 client devices per branch.

When the client capacity reaches the threshold:

- Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
- If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, Aruba Central sends an email notification with a list of Aruba Gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using Webhook.
- **Advance**—This subscription is available for all Aruba Gateways. It allows users to avail advanced features and services such as SaaS Express.
- **Advance-Base Capacity**—This subscription is available for Aruba 7005, Aruba 7008, and Aruba 9004 Gateways.

Assigning Subscriptions to Gateways

To assign subscription to a Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
The **Subscription Management** page is displayed.
2. Under **Gateway Subscriptions**, select the device to which you want to assign a subscription.
3. Expand the drop-down in the **Assignment** column for the selected device.
4. Select the subscription; for example, **Foundation**.
5. To assign subscription to multiple devices:
 - a. Select the devices in the table.
 - b. Click **Batch Assignment**.
 - c. Select the subscription to assign.

When a subscription assigned to a Gateway expires, Aruba Central automatically assigns a valid subscription from the same subscription category.

Virtual Gateway Subscriptions

Aruba Virtual Gateway is a virtual instance of headend gateway for SD-WAN. Aruba Central supports licenses based on the bandwidth capacity for Virtual Gateways.

All license assignments are undertaken by the Virtual Gateway orchestration app.

Aruba Central supports VGW licenses that cater to a variety of requirements. The options include one, three, or five year periods and the bandwidth options are 500 MBps, 2 GBps, and 4 Gbps capacity licenses.

The base SKUs available are: VGW-500M, VGW-2G, and VGW-4G. The availability of SKUs is also dependent on the installation consuming the license.

The account maintains a pool of VGW licenses, upon license expiry or if the license pool has no licenses left (all consumed) the license is unassigned from the account.

When deployed without valid or paid licenses, four evaluation (90 day) licenses of each base SKU is allocated to every customer account.

License consumption can be tracked in the **Key Management** or **Subscription Assignment** pages.

The list of licenses available against consumed licenses are also displayed during the deployment of a Virtual Gateway.

When the client capacity reaches the threshold:

- Aruba Central triggers the **Gateway base license capacity limit exceeded** alert.
- If the notification options for the **Gateway base license capacity limit exceeded** alert is configured, Aruba Central sends an email notification with a list Aruba Virtual Gateways that exceed the client capacity threshold. You can also configure alerts to trigger an incident using Webhook.

For a paid license email notifications are sent out in 30 day intervals starting on the 90th day before expiration and the last notification a day before the expiry of the license.



For an evaluation license email notifications are sent out on the 30th day before expiration and a day before the expiry of the license.

Evaluation licenses are auto-generated (four licenses of each SKU for 90 days) when the user deploys the first Virtual Gateway on Aruba Central.

When a subscription assigned to a Virtual Gateway expires, Aruba Central automatically assigns a valid subscription from the same subscription category. For more information on available SKUs, contact your Aruba Sales Specialist.

Removing Subscriptions from Devices

To remove the subscriptions from the devices, complete the following actions:

Removing a Device Subscription from a Device

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**. Ensure that the **Auto Subscribe** toggle is turned off. The devices that have the subscriptions assigned are selected and highlighted in green.
2. Clear the **Subscribed** check box for the device from which you want to unassign the subscription and click **Update Subscription**. The **Confirm Action** pop-up window with the **Do you want to modify the subscription for selected devices** message opens.
3. Click **Yes** to confirm. The subscription is unassigned and the **Subscribed** status for the device is marked as **No** in the devices table.

Removing a Network Service Subscription from a Device

To remove network service subscription from a device:

1. In the **Account Home** page, under **Global Settings**, click **Subscription Assignment**.
2. Under **Network Service Subscriptions**, select a subscription from the table on the left.
3. From the table on the right, select the devices from which you want to unassign the subscription.
4. Click **Batch Remove Subscriptions**. The subscription is unassigned from the selected devices.

Understanding Device Subscription Expiration Dates

In Aruba Central, each device expires individually. If you have multiple devices and if the expiration date varies, the device(s) are unsubscribed from Aruba Central according to the expiration date of the device(s). For example, if you have 100 devices and if 60 devices are expiring on March 31, 2020, and 40 devices are expiring on April 30, 2020, 60 devices are unsubscribed first, followed by 40 devices. As the subscription expiration date approaches, users receive expiry notifications. For more information about subscription expiry notifications, see [Acknowledging Subscription Expiry Notifications](#).

Acknowledging Subscription Expiry Notifications

In the **Account Home** page, under **Global Settings**, click **Key Management**. The **Key Management** page displays the expiration date for each subscription.

As the subscription expiration date approaches, users receive expiry notifications. The users with evaluation subscription receive subscription expiry notifications on the 30th, 15th and 1 day before the subscription expiry and on day 1 after the subscription expires.

The users with paid subscriptions receive subscription expiry notifications on the 90th, 60th, 30th, 15th, and 1 day before expiry and two notifications per day on the day 1 and day 2 after the subscription expiry.

Acknowledging Notifications through Email

If the user has multiple subscriptions, a consolidated email with the expiry notifications for all subscriptions is sent to the user. Users can acknowledge these notifications by clicking the **Acknowledge All** link in the email notification.

[Contact us](#) now to renew or purchase subscriptions [Acknowledge All](#)

Copyright © 2019 Aruba Networks, Inc. All rights reserved. [Privacy policy](#). 3333 Scott Blvd, Santa Clara, CA 95054



Acknowledging Notifications in the UI

If a subscription has already expired or is about to expire within 24 hours, a subscription expiry notification message is displayed in a pop-up window when the user logs in to Aruba Central.

To prevent Aruba Central from generating expiry notifications, click **Acknowledge**.

Renewing Subscriptions

To renew your subscription, contact your Aruba Central sales specialist.

Managing Sites

The **Sites** page allows you to create sites, view the list of sites configured in your setup, and assign devices to sites. The **Sites** page includes the following functions:

Table 15: *Sites Page*

| Name | Contents of the Table |
|--------------------------------|---|
| Convert Labels to Sites | Allows you to convert existing labels to sites. To convert labels, download the CSV file with the list of labels configured in your setup, add the site information, and upload the CSV file. For more information, see Creating a Site on page 84 . |
| Sites table | <p>Displays a list of sites configured. It provides the following information:</p> <ul style="list-style-type: none">■ Site Name—Name of the site.■ Address—Physical address of the site.■ Device Count—Number of devices assigned to a site. <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none">■ All Devices—Displays all the devices provisioned in Aruba Central.■ Unassigned—Displays the list of devices that are not assigned to any site. <p>You can also use the filter and sort icons on the Sites and Address columns to filter and sort sites respectively.</p> |
| New Site | Allows you to create a new site. |
| Bulk upload | Allows you to add sites in bulk from a CSV file. |
| Devices table | <p>Displays a list of devices provisioned. It provides the following information:</p> <ul style="list-style-type: none">■ Name—Name of the device■ Group—Group to which the device is assigned.■ Type—Type of the device. |

Creating a Site

To create a site, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. To add a new site, click **(+) New Site**. The **Create New Site** pop-up window opens.
6. In the **Create New Site** pop-up window, enter the following details:
 - a. **Site Name**—Name of the site. The site name can be a maximum of 32 single byte characters. Special characters are allowed.
 - b. **Street Address**—Address of the site.
 - c. **City**—City in which the site is located.
 - d. **Country**—Country in which the site is located.
 - e. **State/Province**—State or province in which the site is located.
 - f. **ZIP/Postal Code**—(Optional) ZIP or postal code of the site.
7. Click **Add**. The new site is added to the **Sites** table.

Adding Multiple Sites in Bulk

To import site information from a CSV file in bulk, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Click **(+) Bulk upload**. The **Bulk Upload** pop-up opens.
6. Download a sample file.
7. Fill the site information and save the CSV file in your local directory.



The CSV file for bulk upload of sites must include the mandatory information such as the name, address, city, state, and country details.

8. In the Aruba Central UI, click **Browse** and add the file from your local directory.
9. Click **Upload**. The sites from the CSV file are added to the site table.

Assigning a Device to a Site

To assign devices to a site, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select **Unassigned**. The list of devices that are not assigned to any site is displayed.
6. Select device(s) from the list of devices.
7. Drag and drop the devices to the site on the left. A pop-up window opens and prompts you to confirm the site assignment.
8. Click **Yes**.

Converting Existing Labels to Sites

To convert existing labels to sites, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Click **Convert Labels to Sites**. The **Confirm Conversion** pop-up window opens.
6. To download a CSV file with the list of labels configured in your setup, click **Download a File**. A CSV file with a list of all the labels in your setup is downloaded to your local directory.
7. Enter address, city, state, country, and ZIP code details for the labels that you want to convert to sites.



In the CSV file, you must enter the following details: address, city, state, and country.

8. Save the CSV file.

9. On the **Confirm Conversion** pop-up window, click **Browse** and select the CSV file with the list of labels to convert.
10. Click **Upload**.
11. Click **Convert**. The labels are converted to sites.

Points to Note

- If the conversion process fails for some labels, Aruba Central generates and opens an Excel file showing a list of labels that could not be converted to sites. Verify the reason for the errors, update the CSV file, and re-upload the file.
- Aruba Central does not allow conversion of sites to labels. If the existing labels are converted to sites, you cannot revert these sites to labels.
- When the existing labels are converted to sites, Aruba Central retains only the historical data for these labels. Aruba Central displays the historical data for these labels only in reports and on the monitoring dashboard.

Editing a Site

To modify site details, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select the site to edit and click the edit icon.
6. Modify the site information and click **Update**.

Deleting a Site

To delete a site, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Site(s)**.
5. Select the site to delete and click the delete icon.
6. Confirm deletion.

Managing Labels

The **Labels** page allows you to create labels, view a list of labels, and assign devices to labels. The page includes two tables. The table on the left lists the labels, whereas the table on the right lists the devices. These tables provide the following information:

Table 16: Labels

| Name | Contents of the Table |
|----------------|--|
| Labels | <p>Displays a list of labels configured. The table provides the following information:</p> <ul style="list-style-type: none"> ■ Name of the label ■ Number of devices assigned to a label <p>The table also includes the following sorting options to reset the table view on the right:</p> <ul style="list-style-type: none"> ■ All Devices—Displays all the devices provisioned in Aruba Central. ■ Unassigned—Displays the list of devices that are not assigned to any label. |
| Devices | <p>Displays a list of devices provisioned. The table provides the following information about the devices:</p> <ul style="list-style-type: none"> ■ Name—Name of the device ■ Group—Group to which the device is assigned ■ Type—Type of the device ■ Labels—Number of labels assigned to a device |

Creating a Label

To create a label, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. To add a new label, click **(+) Add Label**. The **Create New Label** pop-up window opens.
6. Enter a name for the label. The label name can be a maximum of 32 single byte characters. Special characters are allowed.
7. Click **Add**. The new label is added to the **All Labels** table.

Assigning a Label to a Device

To assign a label to a device, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Locate the label to which you want to assign a device.
6. In the table that lists the labels, you can perform one of the following actions:
 - Click **All Devices** to view all devices.
 - Click **Unassigned** to view all the devices that are not assigned to any labels.
7. Select **Unassigned**. The list of devices that are not assigned to any label is displayed.
8. Select device(s) from the list of devices.
9. Drag and drop the selected device(s) to a specific label. A pop-up window asking you to confirm the label assignment opens.
10. Click **Yes**.



Aruba Central allows you to assign up to five label tags per device.

Detaching a Device from a Label

To remove a label assigned to a device, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the device from the table on the right.
6. Click the delete icon.
7. To detach labels from the multiple devices at once, select the devices, and click **Batch Remove Labels**.
8. Confirm deletion.

Editing a Label

To edit a label, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the label to edit.
6. Click the edit icon.
7. Edit the label and click **Update**.

Deleting a Label

To delete one or several labels, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Click the **Sites and Labels** tab.
4. Set the toggle switch to **Labels**.
5. Select the label to delete.
6. Click the delete icon.
7. Confirm deletion.

Groups for Device Configuration and Management

Aruba Central simplifies the configuration workflow for managed devices by allowing administrators to combine a set of devices into groups. A group in Aruba Central is the primary configuration element that functions as a container for device management, monitoring, and maintenance. Groups enable administrators to manage devices efficiently by using either a UI-based configuration workflow or CLI-based configuration template.

Groups provide the following functions and benefits:

- Ability to provision multiple devices in a single group. For example, a group can consist of multiple Instant AP Virtual Controllers (VCs). These VCs can share common configuration settings and push the configuration updates to slave Instant APs in their respective Instant AP clusters. For example, you can apply a common security policy for the devices deployed in a specific geographical location.

- Ability to provision different types of devices in a group. For example, a group can consist of Instant APs, Gateways, and Switches.
- Ability to create a configuration base and add devices as necessary. When you assign a new device to a group, it inherits the configuration that is currently applied to the group.
- Ability to create a clone of an existing group. If you want to build a new group based on an existing group, you can create a clone of the group and customize it as per your network requirements.

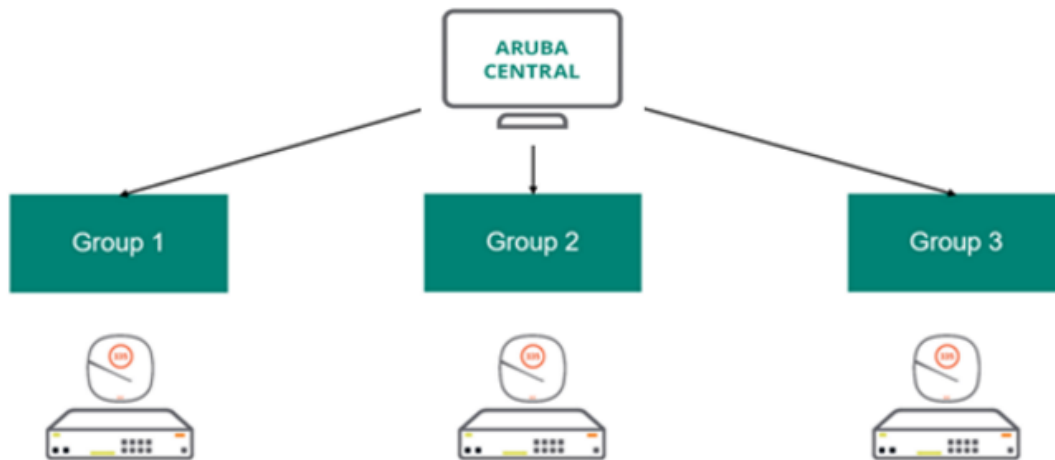


A device can be part of only one group at any given time.

Groups in Aruba Central are mutually exclusive (independent) and do not follow a hierarchical model.

The following figure illustrates a generic group deployment scenario in Aruba Central:

Figure 17 Group Deployment



Group Operations

The following list shows the most common tasks performed at a group level:

- Configuration—Add, modify, or delete configuration parameters for devices in a group
- User Management—Control user access to device groups and group operations based the type of user role
- Device Status and Health Monitoring—View device health and performance for devices in a specific group.
- Report Generation—Run reports per group.
- Alerts and Notifications—View and configure notification settings per group.
- Firmware Upgrades—Enforce firmware compliance across all devices in a group.

Group Configuration Modes

Aruba Central allows network administrators to manage device configuration using either UI workflows or configuration templates:

- UI-based configuration method—For device groups that use UI-based workflows, Aruba Central provides a set of UI menu options. You can use these UI menu options to configure devices in a group. You can also secure the UI-based device groups with a password and thus restrict user access.
- Template-based configuration method—For device groups that use a template-based workflow, Aruba Central allows you to manage devices using configuration templates. A device configuration template

includes a set of CLI commands and variable definitions that can be applied to all other devices deployed in a group.

If your site or store has different types of devices, such as the Instant APs, Switches, and Gateways, and you want to manage these devices using different configuration methods, that is, either using the UI or template-based workflows, you can create a single group and define a configuration method to use for each type of device. This allows you to use a single group for both UI and template based configuration and eliminates the need for creating separate groups for each configuration method.

For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG** prefix is added (**TG Group1**). You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

When you add Instant APs, Gateways, and switches to a group, Aruba Central groups these devices based on the configuration method you chose for the device type, and displays relevant workflows when you try to access the respective configuration menu.

For information on how to create a group, see [Managing Groups on page 91](#).

Default Groups and Unprovisioned Devices

The **default** group is a system-defined group to which Aruba Central assigns all new devices with factory default configuration. When a new device with factory default configuration connects to Aruba Central, it is automatically added to the **default** group.

If a device has customized configuration and connects to Aruba Central, Aruba Central marks the device as **Unprovisioned**. If you want to preserve the device configuration, you can create a new group and assign this device to the newly created group. If you want to overwrite the configuration, you can move the unprovisioned device to an existing group.



The unprovisioned state does not apply to Aruba Switches as only the factory-default switches can join Aruba Central. .

Best Practices and Recommendations

Use the following best practices and recommendations for deploying devices in groups:

- Determine the configuration method (UI or template-based) to use based on your deployment, configuration, and device management requirements.
- If there are multiple sites with similar characteristics—for example, with the same device management and configuration requirements—assign the devices deployed in these sites to a single group.
- Apply device-level or cluster-level configuration changes if necessary.
- Use groups cloning feature if you need to create a group with an existing group configuration settings.
- If the user access to a particular site must be restricted, create separate groups for each site.

Working with Groups

See the following topics for detailed information and step-by-step instructions on how to manage groups and provision devices assigned to a group:

- [Managing Groups](#)
- [Provisioning Devices Using UI-based Workflows](#)
- [Provisioning Devices Using Configuration Templates](#)

Managing Groups

The **Groups** page allows you to create, edit, or delete a group, view the list of groups provisioned in Aruba Central, and assign devices to groups.

This section describes the following topics:

- [Managing Groups on page 91](#)
- [Assigning Devices to Groups on page 92](#)
- [Creating a New Group by Importing Configuration from a Device on page 93](#)
- [Viewing Groups and Associated Devices on page 92](#)
- [Cloning a Group on page 93](#)
- [Moving Devices between Groups on page 93](#)
- [Configuring Device Groups on page 93](#)
- [Deleting a Group on page 94](#)

Creating a Group

Aruba Central allows you to manage configuration for different types of devices, such as Aruba Instant APs, Gateways, and switches in your inventory. These devices can be configured using either UI workflows or configuration templates. You can define your preferred configuration method when creating a group.

Aruba Central allows you to create a single group with different configuration methods defined for each device type. For example, you can create a group with the name **Group1** and within this group, you can enable template-based configuration method for switches and UI-based configuration method for Instant APs and Gateways. Aruba Central identifies both these groups under a single name (**Group1**). If a device type in the group is marked for template-based configuration method, the group name is prefixed with **TG**, (**TG Group1**). You can use **Group1** as the group ID for workflows such as user management, monitoring, reports, and audit trail.

After you assign devices to group and when you access configuration containers, Aruba Central automatically displays relevant configuration options based on the configuration method you defined for the device group.

To create a group:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Click (+) **New Group**. The **Create New Group** pop-up window opens.
4. Enter a name for the group. The group name can be a maximum of 32 single byte ASCII characters if you use the UI to create the names. However, if you are using an NB API, the character limit increases to 128. A group name supports all special characters excluding the ">" character. System-defined group names such as "default", "unprovisioned", and "global" are not allowed in group names.



By default, Aruba Central enables template-based configuration method for switches and UI-workflow-based configuration method for Instant AP and Gateway.

5. To enable template-based configuration method for all device categories:
 - For Instant APs or Gateways, select the **IAP and Gateway** check box.
 - For Switches, ensure that **Switch** check box is selected. The **Switch** check box is enabled by default.
6. To enable UI-based configuration method on all device categories:
 - a. For Instant APs and Gateways, ensure that the **IAP and Gateway** checkbox is cleared.

- b. For switches, clear the **Switch** checkbox.
7. Assign a password. This password enables administrative access to the device interface.
8. Click **Add Group**.



You can also create a group that uses different provisioning methods for switch, and IAP and Gateway device categories. For example, you can create a group with template-based provisioning method for switches and UI-based provisioning method for Instant APs and Gateways.

Assigning Devices to Groups

To assign a device to a group, in the **Account Home** page, under **Global Settings**, click **Device Inventory**:

1. Select the device that you want to assign to a group.
2. Click **Assign Group**. The **Assign Group** pop-up window opens.
3. Select the group to which you want to assign.
4. Click **Assign Device(s)**.

To assign a device to a group from the **Groups** page:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.

By default, the **Groups** page is displayed.

3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Viewing Groups and Associated Devices

To view the groups dashboard, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.

By default, the **Groups** page is displayed. The groups table on the left side of the page displays the following information:

- **Group Name**—Name of the group.
- **Devices**—Number of devices assigned to a group.
- **All Connected Devices**—Total number of devices provisioned in Aruba Central. The devices table on right side of the page shows all the devices provisioned in Aruba Central.
- **Unassigned Devices**—Total number of devices that are yet to be assigned. The devices table on the right shows the devices are not assigned any group.



The devices table is not available for MSP users as the devices are primarily assigned to tenant accounts. However, MSP administrators can drill down to a tenant account and view devices mapped to a group.

3. To view the devices assigned to a group, select the group from the table on the left. The devices table displays the following information:

- **Name**—Name of the device.
- **Location**—Physical location of the device.
- **Type**—Type of the device such as Instant AP or Switch.
- **Serial**—Serial number of the device.
- **MAC Address**—MAC address of the device.

Creating a New Group by Importing Configuration from a Device

To import configuration from an existing device to a new group, complete the following steps:

4. In the **Network Operations** app, filter **All Devices**.
5. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
6. Select the device from which you want to import the configuration.
7. Click **Import Configuration to New Group**. The **Import Configuration** pop-up window opens.
8. Enter a name for the group.
9. Configure a password for the group.
10. Click **Import Configuration**.

Cloning a Group

To clone a group, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. To create a clone of an existing group, select the group from the groups table and click **Clone Selected Group**.
4. Enter a name for the cloned group.
5. Click **Add Group**.

When you clone a group, Aruba Central also copies the configuration templates applied to the devices in the group.

Moving Devices between Groups

To move a device from one group to another group:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. From the devices table on the right, select the device that you want to move.
4. Drag and drop the device to the group to which you want to assign the device.
5. Click **Yes** when the system prompts you to confirm device movement.



MSP mode does not support moving devices across different groups.

Configuring Device Groups

For information on provisioning devices in groups, see the following topics:

- [Provisioning Devices Using UI-based Workflows on page 94](#)
- [Provisioning Devices Using Configuration Templates on page 98](#)

Configuring Groups in MSP Mode

For information on using groups in the MSP mode and instructions on how to assign devices to MSP tenants, see the [Aruba Central Managed Service Provider User Guide](#).

Deleting a Group



When you delete a group, Aruba Central removes all configuration, templates, and variable definitions associated with the group. Before deleting a group, ensure that there are no devices attached to the group.

To delete a group:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. From the list of groups, select the group that you want to delete.
4. Click the delete icon.
5. Confirm deletion.

Moving an IAP Between Groups

To move an IAP from one group to another group:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. From the groups table on the left, select the group from which you want to move the IAP.
4. From the devices table on the right, select the IAP that you want to move.
5. Drag and drop the IAP to the group that you want to assign the IAP to.
6. Click **Yes** when the system prompts you to confirm device movement.



MSP mode does not support moving devices across different groups.

Important Points to Note

- The IAP inherits the configuration of the group to which it is moved. However, only the system configuration is inherited and the **Per AP Settings** on the IAP are retained.
- If the IAP did not inherit the configuration of the new group, go to the **Configuration Audit** page of the IAP to check the configuration difference. For more information, see [Viewing Configuration Status](#).
- If firmware compliance is enabled on the new group and if the firmware version enforced by the group is different from the IAP firmware version, the firmware is upgraded and the IAP reboots.

Provisioning Devices Using UI-based Workflows

This section describes the important points to consider when assigning devices to UI groups:

- [Provisioning Instant APs using UI-based Configuration Method on page 94](#)
- [Provisioning Switches Using UI-based Configuration Method on page 96](#)
- [Provisioning Aruba Gateways Using UI-based Configuration Method on page 96](#)

Provisioning Instant APs using UI-based Configuration Method

An Instant AP device group may consist of any of the following:

- Instant AP Cluster—Consists of a master Instant AP and slave Instant APs in the same VLAN.

- VC—A virtual controller. VC provides an interface for entire cluster. The slave Instant APs and master Instant APs function together to provide a virtual interface.
- Master Instant AP and Slave Instant AP—In typical Instant AP deployment scenario, the first Instant AP that comes up is elected as the master Instant AP. All other Instant APs joining the cluster function as the slave Instant APs. When a master Instant AP is configured, the slave Instant APs download the configuration changes. The master Instant AP may change as necessary from one device to another without impacting network performance.

Aruba Central allows configuration operations at the following levels for a device group with Instant APs.

- **Per group configuration**—Aruba Central allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all VCs within a group can have common SSID settings.
- **Per VC Configuration**—Any changes that need to be applied at the Instant AP cluster level can be configured on a VC within a group. For example, VCs within a group can have different VLAN configuration for the SSIDs.
- **Per Device Configuration**—Although devices are assigned to a group, the users can maintain device-specific configuration such as radio, power, or uplink settings for an individual AP within a group.

When the APs that are not pre-provisioned to any group join Aruba Central, they are assigned to groups based on their current configuration.

Table 17: Instant AP Provisioning

| APs with Default Configuration | APs with Non-Default Configuration |
|--|--|
| <p>If an Instant AP with factory default configuration joins Aruba Central, it is automatically assigned to the default group or an existing group with similar configuration settings.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none"> ■ Manually assign them to an existing group. ■ Create a new group. | <p>If an Instant AP with non-default or custom configuration joins Aruba Central, it is automatically assigned to an unprovisioned group.</p> <p>The administrators can perform any of the following actions:</p> <ul style="list-style-type: none"> ■ Create a new group for the device and preserve device configuration. ■ Move the device to an existing group and override the device configuration. |

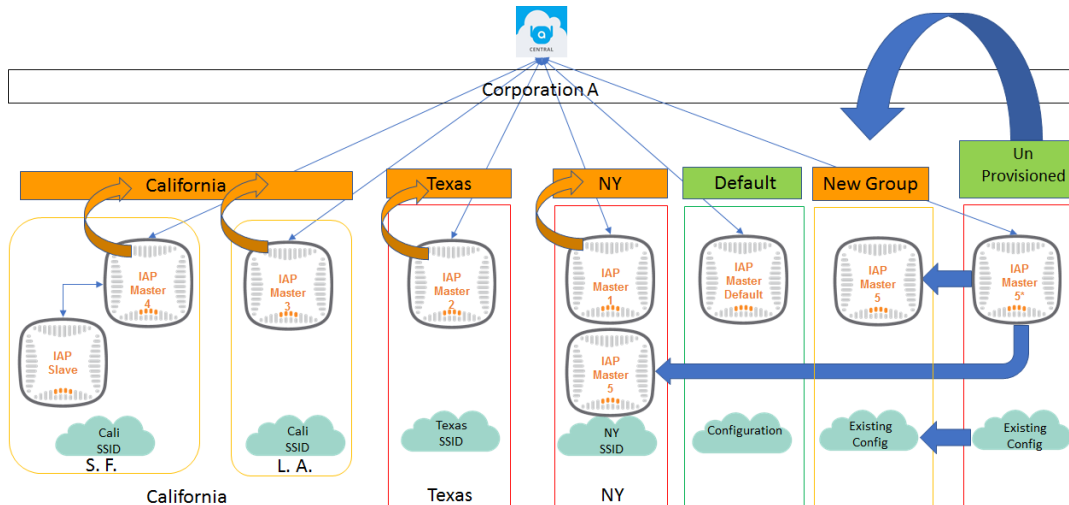


Ensure that the master Instant AP and slave Instant APs are assigned to the same group. You must convert the slave Instant AP to a standalone AP in order to move the slave Instant AP to another group independently.

In the following illustration, Instant APs from three different geographical locations are grouped under California, Texas, and New York states. Each state has unique SSIDs and can support devices from multiple locations in a state. As shown in [Figure 18](#), the California group has devices from different locations and has the same SSID, while devices in the other states/groups have different SSIDs.

When a device with the factory default configuration connects to Aruba Central, it is automatically assigned to the default group. If the device has custom configuration, it is marked as unprovisioned. If you want to preserve the custom configuration, create a new group for the device. If you want to overwrite the custom configuration, you can assign the device to an existing group.

Figure 18 *Instant AP provisioning*



For more information on how to configure Instant APs using UI-based configuration workflows, see [Deploying a Wireless Network Using Instant APs on page 287](#).

To view local overrides and configuration errors, select a template group and navigate to **Devices > Access Points > Settings > Configuration Audit** page.

Provisioning Switches Using UI-based Configuration Method

Aruba Central allows switches to join UI groups only if the switches are running factory default configuration. Aruba Central assigns switches with factory default configuration to the **default** group.



Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

The administrators can either move the switch to an existing group or create a new group.

Aruba Central allows the following configuration operations at the following levels for switches in a UI group:

- **Per group configuration**— Aruba Central allows you to maintain unique configuration settings for each group. However, these settings are applied to all devices within that group. For example, all switches within a group can have common VLAN settings.
- **Per Device Configuration**—Although the Switches inherit group configuration, the users can maintain device-specific configuration, for example, ports or DHCP pools.

For more information on how to configure switches using UI-based configuration workflows, see [Configuring or Viewing Switch Properties in UI Groups on page 437](#).

To view local overrides and configuration errors, select a template group and navigate to **Devices > Switches > Settings > Configuration Audit** page.

Provisioning Aruba Gateways Using UI-based Configuration Method

For SD-Branch deployments with Aruba Gateways, the following recommendations apply:

- Combine Branch Gateways of identical characteristics and configuration requirements under a single group.
- Create groups according to your branch requirements.
 - You can create separate groups for the small, medium, and large sized branches.

- You can also create separate groups for the branch sites in different geographical locations; for example, East Coast and West Coast branch sites. If these groups have similar characteristics with minor differences, you can create the first group and then clone it.
- You can use either a single group for all their devices or deploy devices in multiple groups. For example, you can deploy 7008 controllers and Aruba 2930F Switch Series with 24 ports in a single group for every branch.
- You can also deploy 7005 controller and Aruba 2930F Switch Series with 24 ports in one group and provision 7008 controller with Aruba 2930F Switch Series with 48 ports in another group.

Important Points to Note

- The groups in Aruba Central are not device-specific, however, Aruba recommends that you use the following guidelines for provisioning SD-WAN Gateways.
 - Assign Branch Gateways and VPN Concentrators to separate groups. Because the configuration requirements for Branch Gateways and VPN Concentrators are different, the Branch Gateways and VPN Concentrators must be assigned to different groups.
 - Ensure that the configuration group for SD-WAN Gateways consists of the same type of devices. For example, Branch Gateways assigned to a group must have the same number of ports.
- Before assigning SD-WAN Gateways to groups, you must set the device persona or role as Branch Gateway or VPN Concentrator.

Example

The following figures shows a few sample group deployment scenarios for Aruba Branch Gateways and VPN Concentrators:

Figure 19 *Branch Gateway Groups*

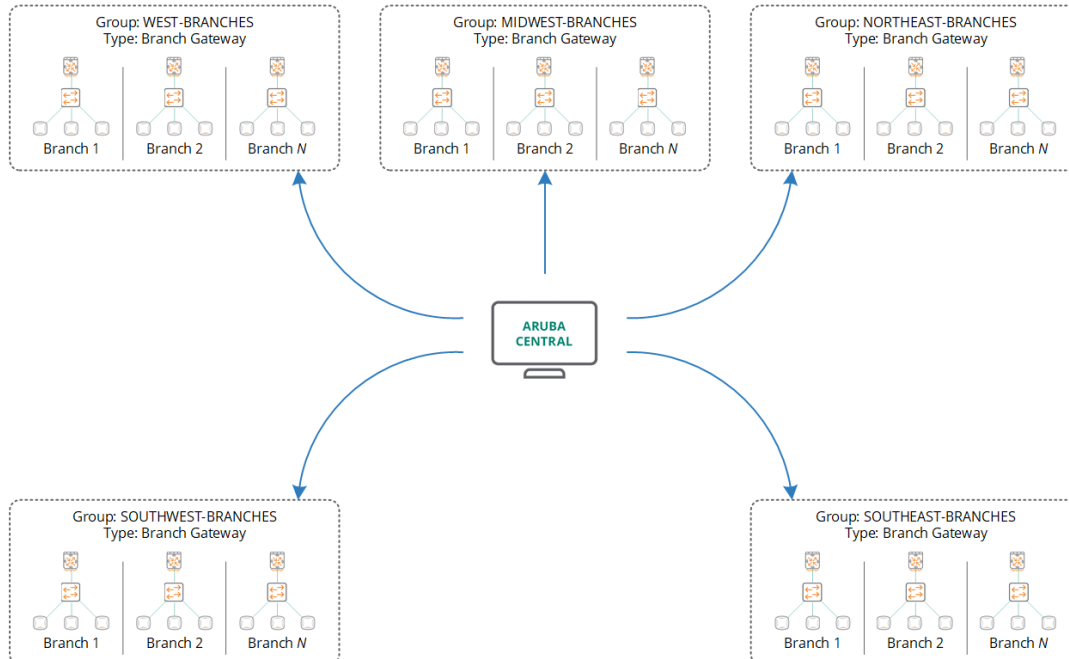
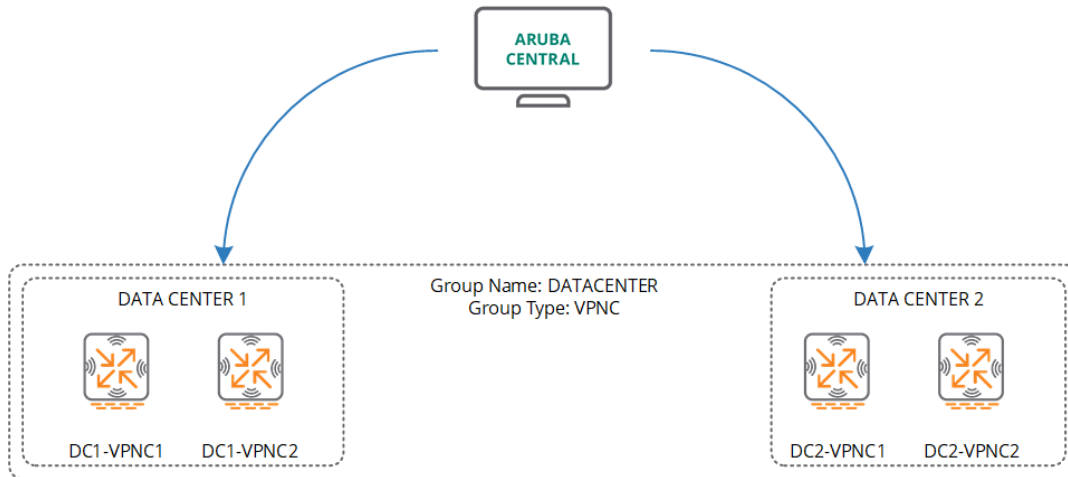


Figure 20 VPN Concentrator Groups



For more information on how to configure Aruba using UI-based configuration workflows, see the *SD-Branch Configuration* section in *Aruba Central Help Center*.

To view local overrides and configuration errors, select a template group and navigate to **Devices > Gateways > Settings > Configuration Audit** page.

Provisioning Devices Using Configuration Templates

Aruba Central allows you to provision devices using UI-based or template-based configuration method. If you have groups with template-based configuration enabled, you can create a template with a common set of CLI scripts, configuration commands, and variables. Using templates, you can apply CLI-based configuration parameters to multiple devices in a group.

If the template-based configuration method is enabled for a group, the UI configuration wizards for the devices in that group are disabled.

Creating a Group with Template-Based Configuration Method

To create a template group, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
By default, the **Groups** page is displayed.
3. Click **(+) New Group**.
The **Create New Group** pop-up window opens.
4. Enter the name of the group.
5. Select the device type for which you want to create a template group:
 - IAP and Gateway
 - Switch
6. Enter the password.
7. Click **Save**.



If the group is set as a template group, a configuration template is required for managing device configuration.

Provisioning Devices Using Configuration Templates and Variable Definitions

For information on configuration template, see the following topics:

- [Configuring APs Using Templates on page 413](#)
- [Using Configuration Templates for Switch Management on page 435](#)
- [Managing Variable Files on page 99](#)

Editing a Template

To edit or delete a template, select the template row and click the edit or delete icon, respectively.

Managing Variable Files

Aruba Central allows you to configure multiple devices in bulk using templates. However, in some cases, the configuration parameters may vary per device. To address this, Aruba Central identifies some customizable CLI parameters as variables and allows you to modify the definitions for these variables as per your requirements.

You can download a sample file with variables for a template group or for the devices deployed in a template group, update the variable definitions, upload the file with the customized definitions, and apply these configuration changes in bulk.


Important Points to Note

- Variables are associated to a device and not attached to a group. If you move a device between groups, variables persist with the device.
- Variables are displayed as part of the group to which the device belongs. After you upload the variables for a device, the association would stay in the system even if the device is moved to a UI group or template group.
- If the device is part of a UI group, variables are unused and not displayed in the UI. Aruba Central ignores the variables.
- If the device is moved to a template group, variables are displayed in the UI and used for configuration purposes.

Downloading a Sample Variables File

The sample variables file includes a set of sample variables that the users can customize. You can download the sample variables file in the JSON or CSV format.

To download a sample variables file:

1. In the **Network Operations** app, use the filter to select a group or device in which the template-based configuration mode is enabled.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the  icon.
4. Click **Variables**.
5. Select one of the following formats to download the sample variables file:
 - JSON—shows the file JSON format.
 - CSV—Shows the variables in different columns.
6. Click **Download Sample Variables File**. The sample variables file is saved to your local directory.

Modifying a Variable File

The CSV file includes the following columns for which the variable definitions are mandatory:

- **_sys_serial**—Serial number of the device.
- **_sys_lan_mac**—MAC address of the device.
- **modified**—Indicates the modification status of the device. The value for this column is set to N in the sample variables file. When you edit a variable definition, set the **modified** column to Y to allow Aruba Central to parse the modified definition.

Predefined Variables for Aruba Switches

The system defined variables in the sample variables files are indicated with **_sys** prefix.

[Table 18](#) lists the predefined variables for switches.

Table 18: *Predefined Variables Example*

| Variable Name | Description | Variable Value |
|----------------------------------|--|--|
| _sys_gateway | Populates gateway IP address. | 10.22.159.1 |
| _sys_hostname | Maintains unique host name. | HP-2920-48G-POEP |
| _sys_ip_address | Indicates the IP address of the device. | 10.22.159.201 |
| _sys_module_command | Populates module lines | module 1 type j9729a |
| _sys_netmask | Netmask of the device. | 255.255.255.0 |
| _sys_oobm_command | Represents Out of Band Management (OOBM) block. | oobm ip address dhcp-bootp exit |
| _sys_snmpv3_engineid | Populates engine ID. | 00:00:00:0b:00:00:5c:b9:01:22:4c:00 |
| _sys_stack_command | Represents stack block | stacking member 1 type "J9729A" mac-address 5cb901-224c00 exit |
| _sys_template_header | Represents the first two lines of the configuration file. Ensure that this variable is the first line in the template. | ; J9729A Configuration Editor; Created on release #WB.16.03.0003+ ; Ver #0f:3f.f3.b8.ee.34.79.3c.29.eb.9f.fc.f3.ff.37.ef:91 |
| _sys_use_dhcp | Indicates DHCP status (true or false) of VLAN 1 | 0 |
| _sys_vlan_1_untag_command | Indicates untagged ports of VLAN 1 | 1-28,A1-A2 |
| _sys_vlan_1_tag_command | Indicates tagged ports of VLAN 1 | 28-48 |



The `_sys_template_header_` and `_sys_snmpv3 engineid` are mandatory variables that must have the values populated, irrespective of their use in the template. If there is no value set for these variables, Aruba Central re-imports the values for these mandatory variables when it processes the running configuration of the device.

Predefined Variables for APs

For APs, the sample variables file includes the `_sys_allowed_ap` variable for which you can specify a value to allow new APs to join the Instant AP cluster.

Conditions

The following conditions apply to the variable files:

- The variable names must be on the left side of condition and its value must be defined on the right side. For example, `%if var=100%` is supported and `%if 100=var%` is not supported.
- The `<` or `<=` or `>` or `>=` operators should have only numeric integer value on the right side. The variables used in these 4 operations are compared as integer after flooring. For example, if any float value is set as `%if dpi_value > 2.8%`, it is converted as `%if dpi_value > 2` for comparison.
- The variable names should not include white space, and the `&` and `%` special characters. The variable names must match regular expression `[a-zA-Z0-9_]`. If the variables values with `%` are defined, ensure that the variable is surrounded by space. For example, `wlan ssid-profile %ssid_name%`.
- The first character of the variable name must be an alphabet. Numeric values are not accepted.
- The values defined for the variable must not include spaces. If quotes are required, they must be included as part of the variable value. For example, if the intended variable name is `wlan ssid-profile "emp ssid"`, then the recommended format for the syntax is `"wlan ssid-profile %ssid_name%"` and variable as `"ssid_name": "\emp ssid\""`.
- If the configuration text has the percentage sign `%` in it—for example, `"url "/portal/scope.cust-5001098/Splash%20Profile%201/capture"`—Aruba Central treats it as a variable when you save the template. To allow the use of percentage `%` as an escape character, use `\` in the variable definition as shown in the following example:

Template text

```
wlan external-captive-portal "Splash Profile 1_#guest#_"
server naw1.cloudquest.central.arubanetworks.com
port 443
url %url%
```

Variable

```
"url": "\"/portal/scope.cust-5001098/Splash%20Profile%201/capture\""
```

- Aruba Central supports adding multiple lines of variables in Instant AP configuration templates. If you want to add multiple lines of variables, you must add the `HAS_MULTILINE_VARIABLE` directive at the beginning of the template.

Example

```
#define HAS_MULTILINE_VARIABLE 1
%if allowed_aps%
%allowed_aps%
%endif%
```

Variable

```
"allowed_aps": "allowed-ap 24:de:c6:cb:76:4e\n allowed-ap ac:a3:1e:c5:db:d8\n allowed-ap 84:d4:7e:c4:8f:2c"
```



For Instant APs, you can configure a variable file with a set of values defined for a master AP in the network. When the variable file is uploaded, the configuration changes are applied to all Instant AP devices in the cluster.

Examples

The following example shows the contents of a variable file in the JSON format for Instant APs:

```
{
  "CK0036968": {
    "_sys_serial": "CK0036968",
    "ssid": "s1",
    "_sys_lan_mac": "ac:a3:1e:c5:db:7a",
    "vc_name": "test_config_CK0036968",
    "org": "Uber_org_test",
    "vc_dns_ip": "22.22.22.22",
    "zonename": "Uber_1",
    "uplinkvlan": "0",
    "swarmmode": "cluster",
    "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
    "hostname": "Uber_1"
  },
  "CJ0219729": {
    "_sys_serial": "CJ0219729",
    "ssid": "s1",
    "_sys_lan_mac": "ac:a3:1e:cb:04:92",
    "vc_name": "test_config_CK0036968",
    "org": "Uber_org_test",
    "vc_dns_ip": "22.22.22.22",
    "zonename": "Uber_1",
    "uplinkvlan": "0",
    "swarmmode": "cluster",
    "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
    "hostname": "Uber_2"
  },
  "CK0112486": {
    "_sys_serial": "CK0112486",
    "ssid": "s1",
    "_sys_lan_mac": "ac:a3:1e:c8:29:76",
    "vc_name": "test_config_CK0036968",
    "org": "Uber_org_test",
    "vc_dns_ip": "22.22.22.22",
    "zonename": "Uber_1",
    "uplinkvlan": "0",
    "swarmmode": "cluster",
    "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
    "hostname": "Uber_3"
  },
  "CT0779001": {
    "_sys_serial": "CT0779001",
    "ssid": "s1",
    "_sys_lan_mac": "84:d4:7e:c5:c6:b0",
    "vc_name": "test_config_CK0036968",
    "org": "Uber_org_test",
    "vc_dns_ip": "22.22.22.22",
    "zonename": "Uber_1",
    "uplinkvlan": "0",
    "swarmmode": "cluster",
    "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
    "hostname": "Uber_4"
  },
  "CM0640401": {
    "_sys_serial": "CM0640401",
    "ssid": "s1",
    "_sys_lan_mac": "84:d4:7e:c4:8f:2c",
    "vc_name": "test_config_CK0036968",
```



```

"org": "Uber_org_test",
"vc_dns_ip": "22.22.22.22",
"zonename": "Uber_1",
"uplinkvlan": "0",
"swarmmode": "cluster",
"md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
"hostname": "Uber_6"
},
"CK0037015": {
  "_sys_serial": "CK0037015",
  "ssid": "s1",
  "_sys_lan_mac": "ac:a3:1e:c5:db:d8",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
  "hostname": "Uber_7"
},
"CK0324517": {
  "_sys_serial": "CK0324517",
  "ssid": "s1",
  "_sys_lan_mac": "f0:5c:19:c0:71:24",
  "vc_name": "test_config_CK0036968",
  "org": "Uber_org_test",
  "vc_dns_ip": "22.22.22.22",
  "zonename": "Uber_1",
  "uplinkvlan": "0",
  "swarmmode": "cluster",
  "md5_checksum": "ed8a67a3d1be58261640ca53f8fd3bb8",
  "hostname": "Uber_8"
}
}

```


[Figure 21](#) shows a sample variables file in the CSV format:

Figure 21 Variables File in the CSV Format

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---------------------|--------------|---------------|-----------|-----------|---------------|-------------------|-----------|-----------|-----------|-----------|---------------------------------------|----------|-----------|-----------|-----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| 1 | _sys_serial | _sys_lan_mac | _sys_modified | _sys_gate | _sys_host | _sys_ip | _sys_mod | _sys_netn | _sys_cobr | _sys_inmi | _sys_stad | _sys_temj | _sys_use | _sys_vlan | _sys_vlan | att_gatew | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt | att_mgmt |
| 2 | 56620YW70:10:6f:9:N | 10.22.183 | Aruba-Sta | 10.22.183 | --- | 255.255.255.0 | 00:00:00:00:00:00 | stacking | ; | 0 | --- | 1/1-1/24-1 | TRUE | 10.22.181 | 181 | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | CN69HkW94:18:82:4:N | 10.22.182 | Aruba293 | 10.22.182 | --- | 255.255.255.0 | 00:00:00:00:00:00 | vsf | ; | 0 | --- | 1/1-1/22,1/24-1/28,2/1-2/23,2/25-2/28 | | | | | | | | | | | | | | |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | | | | | | | | | | | | | | |

Uploading a Variable File


To upload a variable file, complete the following steps:

1. Ensure that the **_sys_serial** and **_sys_lan_mac** variables are defined with the serial number and MAC address of the devices, respectively.
2. In the **Network Operations** app, use the filter to select a group or device in which the template-based configuration mode is enabled.
3. Under **Manage**, click **Devices > Switches**.
4. Click the  icon.
5. Click **Variables**.
6. Click **Upload Variables File** and select the variable file to upload.
7. Click **Open**. The content of the variable file is displayed in the **Variables** table.
8. To search for a variable, specify a search term and click **Search** icon.


9. To download variable file with device-specific definitions, click the download icon in the **Variables** table.

Modifying Variables

To modify variables without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, use the filter to select a group or device.
2. Under **Manage**, click **Devices** > **Switches**.
3. Click the  icon.
4. Click **Variables**.
5. Select a device and variable.
6. Modify the value and click **Add to Modifications**.
7. Click **Save**.

Alternatively, to modify a single variable without downloading a variable file, modifying the variable file, and uploading the customized variable file:

1. In the **Network Operations** app, use the filter to select a group or device.
2. Under **Manage**, click **Device** > **Switches**.
3. Click the  icon.
4. Hover over a desired variable and click **Edit**.
5. Modify the value and click **Save**.
6. Click **Save**.

Backing Up and Restoring Configuration Templates

Aruba Central allows you to create a backup of configuration templates and variables that you can restore in the event of a failure or loss of data. The **Configuration Backup and Restore** feature is available in the **Configuration Audit** page for devices deployed using template-based configuration method.

The **Configuration Backup and Restore** feature enables administrators to perform the following functions:

- Back up templates and variable files applied to the devices managed using the template-based configuration method.
- Restore an earlier known working combination of the configuration template and device variables in the event of a failure.

Important Points to Note

- The backup and restoration options are available for devices deployed using the template-based configuration method.
- When the backup or restore for a group is in progress, you cannot make configuration changes to that group.
- The restore operation restores the variables only for the devices that are currently provisioned or pre-provisioned to the group.
- The restore operation is terminated if the firmware version running on any one device in the group does not match the firmware version in the backed up file that is being restored. For example, if the configuration file was backed up when a switch was running 16.03.0003 and was later upgraded to 16.04.0003, the restore operation fails for the group.
- The restore operation deletes any templates applied to the group before the restore. It also deletes and replaces device variables with the backed up version that is being restored.

- The details pertaining to the actions carried out during the backup and restore operations are logged in the **Audit Trail** page.

Creating a Configuration Backup

To back up configuration templates and variables applied to devices:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **New Configuration Backup**. The **Create New Backup** pop-up box opens.
4. Enter a name for **Backup Name**.
5. Select **Do Not Delete** if you do not want the backed up file to be deleted by new backup after a threshold of 20 backups is exceeded.



You can create and maintain up to 20 backed up configuration files. If the number of backup files exceed 20, the old backed up configuration files are overwritten. However, if the backed up files are marked as **Do not Delete**, Aruba Central does not overwrite the backed up configuration files.

6. Click **OK**. The **Confirm Backup** pop-up window opens.
7. Read through the information. Select the check box to confirm that configuration changes to the group cannot be done when the backup is in progress.
8. Click **Proceed**. The backup for the group configuration is created.

Viewing Contents of a Backed Up Configuration

To view the contents of a backed up configuration:

1. Click the **Manage Backup** option.
2. Download the backup and untar the downloaded file. The following example shows the tree structure of a typical backup download.

```
<backup-name_timestamp>
├── templates
│   ├── <hppctemplate1.tpl>
│   ├── <iaptemplate1.tpl>
│   └── template_meta.json
└── variables
    ├── HPPC_variables_1.json
    ├── IAP_variables_1.json
    └── devices_meta.json
```

The variables are stored per device type, that is, Instant APs and Aruba Switches. For example, for all Instant APs, the variables are aggregated and stored together.



The aggregated file can include variables for up to 80 devices or up to 5 MB of variables data, based on whichever condition is met first. When the number of variables or the data size exceeds this limit, new aggregate files are created and added to the backup until all the variables in the selected group are backed up. The variable data limit applies only to the aggregated files. Aruba Central does not impose any limit on the number of devices or the device variables that can be backed up.

The following details are available for a backed up configuration snapshot:

- **Backups**—provides details of the number of available and allowed backup and allows you to perform the following actions:
 - Manage group configuration backups

- Create new configuration backups
- Modify backup delete protection
- **Last Backup**—provides details of the status and the timestamp of the last backup.
- **Last Restore**—provides details of the status and the timestamp of the last restore.

Restoring a Backed Up Configuration

To restore a backed up configuration snapshot:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **Restore Configuration Backup**. The **Restore from Backup** pop-up window opens.
4. Select the backup name that you want to restore from **Backup Name** drop-down list.
5. Select a required device type from the **Device Type** drop-down list.



Selecting a device type allows you to restore the backed up configuration by the specific device type, for example, Aruba IAP, Aruba Switch. By default, **All** is selected. When the device type is set to **All**, configuration restore does not follow any specific order.

6. Click **OK**. The **Confirm Configuration Restore** pop-up box opens.
7. Read the instructions. Then, select the check boxes to confirm your action for configuration restore.
8. Click **Proceed**. The selected backup configuration is restored.



Aruba recommends that the administrators take a backup of the current configuration of the group before the restore operation.

Managing Backups

To manage the backed up configuration files:

1. In the **Network Operations** app, use the filter to select a group that uses template-based configuration method.
2. Navigate to the **Configuration Audit** page. See [Viewing Configuration Status](#).
3. Under **Configuration Backup and Restore**, click **Manage Backup**. The **Last <#> Backups** pop-up window opens.
4. View the backup details such as date and time of backup, backup name, username, and the delete protection status for each configuration backup.
5. Click **Close**.
6. Click **Last Backup Log** to view the details of the latest backup. The **Last Backup Log** pop-up box displays the following details:
 - Group name
 - Backup name
 - Username that initiated the configuration backup
 - Details on whether templates and device variables are being saved, and completion of the configuration backup process.
7. To get the status of the last restore, click **Last Restore Log**. To get the error log for a restore error event, click **Last Restore Error Log**.

Backing Up and Restoring Templates and Variables Using APIs

Aruba Central supports the following NB APIs for the backup and restore feature:

- Create new configuration backup for group
[POST] /configuration/v1/groups/snapshot/{group}
- Create backups for multiple groups associated with a customer account
[POST]/configuration/v1/groups/snapshot/create_backups



Aruba Central creates a backup of configuration template and variables only for the groups included in the API request payload. You can use the include or exclude parameters to create backups for specific list of groups.

The following table describes the API response based on the inputs provided in the parameters:

Table 19: API Functionality for Backup Creation

| include_groups | exclude_groups | API Functionality |
|---------------------|---------------------|---|
| No groups specified | No groups specified | Raises an exception to either include or exclude groups. |
| group names | group names | Raises an exception to include or exclude groups. |
| [] | No groups specified | Raises an exception to provide valid values for the include groups parameter. |
| group names | No groups specified | Includes selected groups for the backup operation. |
| No groups specified | ALL_GROUPS | Creates a backup for all groups. |
| No groups specified | group names | Does not create backup for the excluded groups. |

- Restore a backed up version of the configuration template for all devices in a group:
[POST] /configuration/v1/groups/<group_name>/snapshots/<snapshot_name>/restore
The API restores a specific version of the backup snapshot for the group specified in the API request.
- Restore a backed up version of the configuration template by device type:
The **[POST]/configuration/v1/groups/{group}/snapshots/{snapshot}/restore** API provides you an option to restore the configuration by device type. By selecting a specific device type, you can control the order in which the configuration is restored by device type. This minimizes the impact of the configuration restore activity on the network.




Viewing Configuration Status

Aruba Central provides an audit dashboard for reviewing configuration changes for the devices provisioned in UI and template groups. The **Configuration Audit** menu option is available for APs, switches, and gateways.

Accessing the Configuration Audit Page

To access the **Configuration Audit** page:

- For Instant APs:
 - a. In the **Network Operations** app, use the filter to select a group or device.
 - b. Click **Devices**.

- c. Click the  icon.
- d. Click **Show Advanced**.
- e. Click **Configuration Audit**.
- For Aruba switches:
 - a. In the **Network Operations** app, use the filter to select a group or device.
 - b. Click **Devices**.
 - c. Click **Switches**.
 - d. Click the  icon.
 - e. Click **Configuration Audit**.
- For Aruba Gateways:
 - a. In the **Network Operations** app, use the filter to select a group or device.
 - b. Click **Devices**.
 - c. Click **Gateways**.
 - d. Click the  icon.
 - e. Click **Show Advanced**.
 - f. Click **Configuration Audit**.

Applying Configuration Changes

Aruba Central now supports a two-staged configuration commit workflow for Instant AP and switches.

The **Auto Commit State** section in the **Configuration Audit** page allows administrators to switch their preference for committing configuration changes to devices.

- When **Auto Commit State** is set to **ON**, the configuration changes are applied instantly to the device.
- When **Auto Commit State** is set to **OFF**, the administrators can build a candidate configuration, save it on cloud, review it, and then push the configuration changes to the managed devices for activation.



When a device is moved from one group to another, Aruba Central resets the **Auto Commit State** for the device. The device inherits the **Auto Commit State** settings of the group to which the device is moved.

Auto Commit Workflow

To enable Aruba Central to push configuration changes instantly, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or device.
2. Navigate to the **Configuration Audit** page.
3. Ensure that the **Auto Commit State** is set to **On**.
4. Based on configuration mode set for the device, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. Aruba Central automatically pushes the configuration changes to the devices.
5. View the failed or pending changes if any.

Manual Commit Workflow

To build configuration and review it before applying the changes to devices:

1. In the **Network Operations** app, use the filter to select a group or device.
2. Navigate to the **Configuration Audit** page.

3. Ensure that the **Auto Commit State** is set to **Off**.
4. Based on configuration mode set for the device, use either the UI workflows or a configuration template to complete the configuration workflow and save the changes. When you try to save the changes, Aruba Central displays the following message:

 Auto commit configuration is disabled for this device.
After saving all the changes, go to Config Audit page to commit changes to this device.

5. Click **Failed/PendingChanges**.
6. Click **Failed Push** and review the configuration.
7. Click **Close**.
8. If you want to push the configuration to devices, click **Commit Now**.



Aruba Central does not support the two-staged configuration commit workflow only for Aruba Gateways.

The tenant accounts in the MSP deployments do not inherit the **Auto Commit State** configured at the MSP level. The tenant account users can enable or disable **Auto Commit** state for the devices in their respective accounts.

Viewing Configuration Overrides and Errors

The **Configuration Audit** page allows you to view the configuration push errors, template synchronization errors, configuration sync, and device level configuration overrides. Some of notable status indicators available on page include:

- **Failed/Pending Changes**
 - **Failed Changes**—The devices managed by Aruba Central receive the configuration changes from Aruba Central. Occasionally, a managed device may fail to receive a configuration change from Aruba Central. The **Failed changes** tile allows you to view a list of the configuration push errors.
 - **Pending Changes**—With the Auto Commit feature is disabled, Aruba Central allows you to build your configuration changes, save it, and review it before committing the configuration changes. The **Failed/Pending Changes** tile displays the configuration that is not yet pushed to the devices.
- **Local Overrides**—In Aruba Central, devices are assigned to groups that serve as the primary configuration elements. Occasionally, based on the network provisioning requirements, the administrators may need to modify the configuration of a specific device in a group. As these modifications override the configuration settings that the device has inherited from the group, Aruba Central marks these changes as local overrides.
- **Configuration Conflicts**—For all connected devices in Aruba Central, when a new feature is introduced and applied to the device, one of two subsequent scenarios might ensue. The new feature might not cause any conflict with the existing configuration and no further action is required from the administrator. However, if the new feature causes a conflict with the existing configuration in the device, the feature is disabled automatically and no further configuration is pushed for that device. The **Configuration Audit** page displays a configuration conflict error. For each device under conflict, click the **Manage Configuration Conflict** link. In the subsequent **Configuration Conflict** page, enable the checkbox against each conflict and type REMOVE to remove the conflict. After you resolve all conflicts, you are able to push group configuration to the device.
- **Template Errors**—Devices deployed in the template group are provisioned using configuration templates. If there are errors in the templates or variable definitions, the configuration push to devices fails. Aruba Central records such failed instances as template errors and displays these errors on the **Configuration Audit** page.
- **Move Failures**—Aruba Central supports moving a device from one group to another. If the move operation fails, Aruba Central logs such instances as **Move Failures**.

Viewing Configuration Status for Devices at the Group Level (Template Configuration Mode)

On selecting a template group from the filter bar, the **Configuration Audit** page displays the options listed in [Table 20](#):

Table 20: *Configuration Audit Status for a Template Group*

| Data Pane Content | Description |
|---|---|
| Template Errors | Displays the number of template errors for the selected template group. Devices deployed in the template group are provisioned using configuration templates. If there are errors in the templates or variable definitions, the configuration push to the devices fails. Aruba Central records such failed instances as template errors and displays these errors on the Configuration Audit page. To view a complete list of errors, click View Template Errors . The Template Errors pop-up window allows you to view and resolve the template errors issues if any. |
| Failed/Pending Changes | Displays the number configuration sync errors for the selected template group. To view and resolve the configuration sync errors, click the Failed Config Difference link. |
| Configuration Backup and Restore | Allows you to create a backup of templates and variables applied to the devices in the template group. For more information, see Backing Up and Restoring Configuration Templates . |
| All Devices | The All Devices table provides the following device information for the selected group: <ul style="list-style-type: none">■ Name—The name of the device.■ Type—The type of the device.■ Auto Commit—Enabled or disabled status of the Auto Commit feature.■ Config Sync—Indicator showing configuration sync errors.■ Template Errors—Indicator showing configuration template errors for the devices deployed in template groups. |

Viewing Configuration Status for a Device (Template Configuration Mode)

On selecting a device that is provisioned in a template group, the **Configuration Audit** page displays the options listed in [Table 20](#):


Table 21: *Configuration Audit Status for Devices in Template Groups*

| Data Pane Content | Description |
|-------------------------------|--|
| Template Applied | Displays the template that is currently applied on the selected device. |
| Template Errors | Displays the number of template errors for the selected device. To view a complete list of errors, click View Template Errors . |
| Failed Changes | Displays configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the Failed/Pending Config Changes link. |
| Config Comparison Tool | Allows you to view the difference between the current configuration and the configuration that is yet to be pushed to the device (pending configuration). To view the current and pending configuration changes side by side, click View . |

Viewing Configuration Status for Devices at the Group Level (UI-based Configuration Mode)

On selecting a UI group, the **Configuration Audit** page displays the options listed in [Table 20](#).

Table 22: Configuration Audit Status for a UI Group

| Data Pane Content | Description |
|------------------------|--|
| Failed Changes | Displays the number of devices with configuration sync errors for the selected UI group. To view and resolve the configuration sync errors, click the Failed Config Difference link. |
| Local Overrides | Displays the number of devices with local overrides. To view a complete list of overrides, click the Manage Local Overrides link. The Local Overrides pop-up window opens. <ul style="list-style-type: none">■ To preserve the overrides, click Close.■ To remove the overrides, select the group name with local override, click Remove and click OK. |
| All Devices | <p>The All Devices table provides the following device information for the selected group:</p> <ul style="list-style-type: none">■ MAC Address—MAC address of the device.■ Name—The name of the device.■ IP Address—IP address of the device.■ Site—Name of the site to which the device is assigned.■ Type—The type of the device.■ Config Sync / Config Status—Indicator showing configuration sync errors.■ Local Override—Indicator showing configuration overrides for the devices deployed in UI groups. <p>NOTE: The MAC Address, IP Address, Config Status, Site, and Type columns are available only for groups in which Aruba Gateways are provisioned (Manage > Device > Gateways, click the settings  icon. The gateway configuration page is displayed. Navigate to Config Audit).</p> |

Viewing Configuration Status for a Device (UI-based Configuration Mode)

On selecting a device assigned to a UI group, the **Configuration Audit** page displays the options listed in [Table 20](#).

Table 23: Configuration Audit Status for a Device Assigned to a UI Group

| Data Pane Content | Description |
|------------------------|---|
| Failed Changes | Displays the number of devices with configuration sync errors for the selected device. To view and resolve the configuration sync errors, click the Failed Config Difference link. |
| Local Overrides | Displays the number of local overrides. To view a complete list of overrides, click the Manage Local Overrides link. The Local Overrides pop-up window opens. <ul style="list-style-type: none">■ To preserve the overrides, click Close.■ To remove the overrides, click Remove, and click OK. |

Backing up and Restoring Configuration Templates

Aruba Central allows you to back up configuration templates assigned to the devices deployed in a template group. The **Configuration Audit** pages for Instant AP, Switch, and Gateway configuration containers allow

you to create and manage backed up files and restore these files when required. For more information, see [Backing Up and Restoring Configuration Templates](#).

Connecting Devices to Aruba Central

Aruba devices support automatic provisioning, also known as ZTP. In other words, Aruba devices can download provisioning parameters from Aruba Activate and connect to their management entity once they are powered on and connected to the network.

Although most of the communication between devices on the remote site and Aruba Central server in the cloud is carried out through HTTPS (TCP 443), you may want to open the following ports for devices to communicate over network firewall.

This section includes the following topics:

- [Domain names for Aruba Central Portal Access on page 112](#)
- [Domain Names for Device Communication with Aruba Central on page 113](#)
- [Domain Names for Device Communication with Aruba Activate on page 113](#)
- [Cloud Guest Server Domains for Guest Access Service on page 114](#)
- [Domain Names for OpenFlow on page 114](#)
- [Other Domain Names on page 115](#)

Domain names for Aruba Central Portal Access

Table 24: *Domain Names and URLs for Aruba Central Portal Access*

| Region | Domain Name | Protocol |
|-------------|---|-----------------------|
| US-1 | portal.central.arubanetworks.com | HTTPS TCP port 443 |
| US-2 | portal-prod2.central.arubanetworks.com | HTTPS TCP port 443 |
| EU-1 | portal-eu.central.arubanetworks.com | HTTPS TCP port 443 |
| Canada-1 | portal-ca.central.arubanetworks.com | HTTPS TCP port 443 |
| China-1 | portal.central.arubanetworks.com.cn | HTTPS TCP port 443 |
| APAC-1 | portal-apac.central.arubanetworks.com | HTTPS TCP port 443 |
| APAC-EAST1 | portal-apaceast.central.arubanetworks.com | HTTPS TCP port 443 |
| APAC-SOUTH1 | portal-apacsouth.central.arubanetworks.com | HTTPS TCP port 443 |

Domain Names for Device Communication with Aruba Central

Table 25: Domain Names for Device Communication with Aruba Central

| Region | Aruba Central URL | URL for Device Connectivity | Protocol | FQDNs for SD-WAN Orchestrator Service |
|-------------|---|--|-----------------------|---|
| US-1 | app.central.arubanetworks.com | app1.central.arubanetworks.com | HTTPS TCP port 443 | app1-h2.central.arubanetworks.com |
| US-2 | app-prod2.central.arubanetworks.com | device-prod2.central.arubanetworks.com | HTTPS TCP port 443 | device-prod2-h2.central.arubanetworks.com |
| EU-1 | app2-eu.central.arubanetworks.com | device-eu.central.arubanetworks.com | HTTPS TCP port 443 | device-eu-h2.central.arubanetworks.com |
| Canada-1 | app-ca.central.arubanetworks.com | device-ca.central.arubanetworks.com | HTTPS TCP port 443 | device-ca-h2.central.arubanetworks.com |
| China-1 | app.central.arubanetworks.com.cn | device.central.arubanetworks.com.cn | HTTPS TCP port 443 | device-h2.central.arubanetworks.com.cn |
| APAC-1 | app2-ap.central.arubanetworks.com | app1-ap.central.arubanetworks.com | HTTPS TCP port 443 | app1-ap-h2.central.arubanetworks.com |
| APAC-EAST1 | app-apaceast.central.arubanetworks.com | device-apaceast.central.arubanetworks.com | HTTPS TCP port 443 | device-apaceast-h2.central.arubanetworks.com |
| APAC-SOUTH1 | app-apacsouth.central.arubanetworks.com | device-apacsouth.central.arubanetworks.com | HTTPS TCP port 443 | device-apacsouth-h2.central.arubanetworks.com |

Domain Names for Device Communication with Aruba Activate

Table 26: Domain Names for Device Communication with Aruba Activate

| Domain Name | Protocol |
|--------------------------|-----------------------|
| device.arubanetworks.com | HTTPS TCP port 443 |

Cloud Guest Server Domains for Guest Access Service

Table 27: *Domain Names for Cloud Guest Server Access*

| Region | Domain Name | Protocol |
|-------------|--|-------------------------------|
| US-1 | nae1.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | nae1-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| US-2 | naw2.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | naw2-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| EU-1 | euw1.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | euw1-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| Canada-1 | ca.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | ca-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| APAC-1 | ap1.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | ap1-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| APAC-EAST1 | apaceast.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | apaceast-elb.cloudguest.central.arubanetworks.com | TCP port 443 |
| APAC-SOUTH1 | apacsouth.cloudguest.central.arubanetworks.com | TCP port 2083 TCP port 443 |
| | apacsouth-elb.cloudguest.central.arubanetworks.com | TCP port 443 |

Domain Names for OpenFlow

Table 28: *Domain Names for OpenFlow*

| Region | Domain Name |
|----------|---|
| US-1 | https://app2-ofc.central.arubanetworks.com |
| US-2 | https://ofc-prod2.central.arubanetworks.com |
| EU-1 | https://app2-eu-ofc.central.arubanetworks.com |
| Canada-1 | https://ofc-ca.central.arubanetworks.com |
| China-1 | https://ofc.central.arubanetworks.com.cn |

| Region | Domain Name |
|-------------|---|
| APAC-1 | https://app2-ap-ofc.central.arubanetworks.com |
| APAC-EAST1 | https://ofc-apaceast.central.arubanetworks.com |
| APAC-SOUTH1 | https://ofc-apacsouth.central.arubanetworks.com |

Other Domain Names

Table 29: *Other Domain Names*

| Domain Name | Protocol | Description |
|--|-----------------------|---|
| sso.arubanetworks.com | TCP port 443 | Allows users to access their accounts on the internal server. |
| internal.central.arubanetworks.com internal2.central.arubanetworks.com | TCP port 443 | Allows users to access the Aruba Central Internal portal. |
| pool.ntp.org | UDP port 123 | Allows users to update the internal clock and configure time zone when a factory default device comes up. By default, the Aruba devices contact pool.ntp.org and use NTP to synchronize their system clocks. |
| activate.arubanetworks.com | TCP port 443 | Allows users to configure provisioning rules in Activate. |
| pqm.arubanetworks.com | ICMP or UDP port 4500 | Allows users to check the health of WAN uplinks configured on Branch Gateways. |
| images.arubanetworks.com | TCP port 80 | Allows users to access the server that hosts software images available for upgrading devices. |
| http://h30326.www3.hp.com | TCP port 80 | Allows users to access the Aruba switch software images. To view the URL for software updates, use the show activate software-update command. |
| d2vxf1j0rhr3p0.cloudfront.net | TCP port 80 | Allows users to access the CloudFront server for locating Instant AP software images. |
| rcs-m.central.arubanetworks.com (For all other regions) central-eu-rcs.central.arubanetworks.com (For Europe region) | TCP port 443 | Allows users to access a device console through SSH. |
| cloud.arubanetworks.com | TCP port 80 | Allows users to open the Aruba Central evaluation sign-up page. |
| aruba.brightcloud.com | TCP port 443 | Enables devices to access the Webroot Brightcloud server for application, application categories, and website content classification. |

| Domain Name | Protocol | Description |
|------------------------------------|--------------|--|
| bcap15-dualstack.brightcloud.com | TCP port 443 | Allows Aruba devices to look up the Webroot Brightcloud server for Website categories. |
| api-dualstack.bcti.brightcloud.com | TCP port 443 | Allows Aruba devices to access the IP Reputation and IP Geolocation service on the Webroot Brightcloud server. |
| database-dualstack.brightcloud.com | TCP port 443 | Allows Aruba devices to download the website classification database from the Webroot Brightcloud server. |



When configuring ACLs to allow traffic over a network firewall, use the domain names instead of the IP addresses.



For Branch Gateways to set up IPsec tunnel with the VPN concentrators, the UDP 4500 port must be open.

Connecting Instant APs to Aruba Central

To bring up Instant APs in Aruba Central:

1. Connect the Instant AP to a provisioning network.
2. Ensure that Instant AP is operational and is connected to the Internet.
3. Ensure that the Instant AP has a valid DNS server address either through DHCP or static IP configuration.
4. Ensure that NTP server is running and Instant AP system clock is configured.

Connecting Aruba Switches to Aruba Central

Note the following points about automatic provisioning of switches:

Pre-configured switches can now join Aruba Central. You can also import configuration from these switches to generate a template. For more information, see [Creating a Configuration Template](#).



If the switches ship with a version lower than the minimum supported firmware version, a factory reset may be required, so that the switch can initiate a connection to Aruba Central. For information, on the minimum firmware versions supported on the switches, see [Supported Switch Platforms on page 32](#).

During Zero Touch Provisioning, the Aruba switches can join Aruba Central only if they are running the factory default configuration, and have a valid IP address and DNS settings from a DHCP server.

The provisioning of the Aruba Mobility Access Switch fails when the provisioning process is interrupted during the initial booting and if the switch has a static IP address with no DNS server configured.

Connecting SD-WAN Gateways to Aruba Central

The Aruba Gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The Gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

Table 30: ArubaOS Hardware Platforms and Supported ZTP Ports

| ArubaOS Hardware Platform | Supported ZTP Ports |
|---------------------------|------------------------|
| Aruba 7005 Gateway | ALL ports except 0/0/1 |
| Aruba 7008 Gateway | ALL ports except 0/0/1 |
| Aruba 7010 Gateway | ALL ports except 0/0/1 |
| Aruba 7030 Gateway | ALL ports except 0/0/1 |
| Aruba 7024 Gateway | ALL ports except 0/0/1 |
| Aruba 7210 Gateway | ALL ports except 0/0/1 |
| Aruba 7220 Gateway | ALL ports except 0/0/1 |
| Aruba 7240 Gateway | ALL ports except 0/0/1 |
| Aruba 7280 Gateway | ALL ports except 0/0/1 |
| Aruba 9004 Gateway | ALL ports except 0/0/1 |
| Aruba 9012 Gateway | ALL ports except 0/0/1 |

To know the minimum software version required for the Gateways, see [Supported Aruba Gateways](#).

To automatically provision the Gateways:

1. Connect your Gateway to the provisioning network.
2. Wait for the device to obtain an IP address through DHCP. Gateways support multiple uplink ports. The first port to receive the DHCP IP connects to the Activate server and completes the provisioning procedure:
 - If the device has factory default configuration, it receives an IP address through DHCP, connects to Aruba Activate, and downloads the provisioning parameters. When a device identifies Aruba Central as its management entity, it automatically connects to Aruba Central.
3. Observe the LED indicators. Table 2 describes the LED behavior.

Table 31: LED Indicators

| LED Indicator | LCD Text | Description |
|-----------------------------------|-----------------|---|
| Solid Amber | Getting DHCP IP | Indicates that the uplink connection is UP, but DHCP IP is yet to be retrieved. |
| Blinking Amber | Activate Wait | Indicates that the device was able to reach the DHCP server and the connection to the Activate server is yet to be established. |
| Solid Green | Activate OK | Indicates that the device was able to retrieve provisioning parameters from the Activate server. |
| Alternating Solid Green and Amber | Activate Error | Indicates that the device was not able to retrieve provisioning parameters. |

After successfully connecting to Aruba Central, the Gateways download the configuration from Aruba Central and reload.



The Gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see *ArubaOS User Guide*.

Certificates

By default, Aruba Central includes a self-signed certificate that is available on the **Certificates** page. The default certificate is not signed by a root certificate authority (CA). For devices to validate and authorize Aruba Central, administrators must upload a valid certificate signed by a root CA.

Aruba devices use digital certificates for authenticating a client's access to user-centric network services. Most devices such as controllers and Instant APs include a server certificate by default for captive portal server authentication. However, Aruba recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted CA. Certificates can be stored locally on the devices and used for validating device or user identity during authentication.

Aruba Central-managed devices such as Instant AP and switches support the following root CA certificates:

| Instant APs | Switches |
|---|---|
| <ul style="list-style-type: none">■ AddTrust■ GeoTrust■ VeriSign■ Go Daddy | <ul style="list-style-type: none">■ Comodo■ GeoTrust |

Uploading Certificates

To upload certificates, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Select the **Certificates** tab.
The **Certificates** page opens.
4. Click the plus icon to add the certificate to the certificate store.
5. In the **Add Certificate** dialog box, do the following:
 - a. In the **Name** text box, specify the certificate name.
 - b. Select the type of certificate. You can select any one of the following certificates:
 - **CA**—Digital certificates issued by the CA.
 - **Server**—Server certificates required for communication between devices and authentication servers.
 - **CRL**—Certificate Revocation List that contains the serial numbers of certificates that have been revoked. This certificate is required for performing a certificate revocation check.
 - **OCSF Responder Cert**—OCSF responder certificates.
 - **OCSF Signer Cert**—OCSF Response Signing Certificate.OCSF certificates are required for OCSF server authentication.
 - c. From the **Format** drop-down list, select a certificate format; for example, PEM, DER, and PKCS12.
 - d. In the **Passphrase** text box, enter a passphrase.
 - e. In the **Retype Passphrase** text box, retype the passphrase for confirmation.



The **Passphrase** and **Retype Passphrase** text boxes are displayed only when you select **Server Certificate** from the **Type** drop-down list.

- f. In the **Certificate File** field, click **Browse** and select the certificate files.
- g. Click **Add**. The certificate is added to the Certificate Store.

Managing Certificates on Instant APs Configured Using Templates

Aruba Central supports uploading multiple certificates to Instant APs configured using templates. You can manage certificates either from the Aruba Central UI or through the API Gateway. For more information about APIs, see *API Documentation*.

To push certificates to Instant APs configured using templates:

1. Upload certificate(s) through one of the following methods:
 - **UI**—See [Uploading Certificates on page 118](#).
 - **API**—Use the **[POST] /configuration/v1/certificates** API.
2. Get the certificate name and MD5 checksum through one of the following methods:
 - **UI**—In the **Network Operations** app, filter **All Devices**. Under **Maintain**, click **Organization** and select the **Certificates** tab. The **Certificate Store** table displays these details.
 - **API**—Use the **[GET] /configuration/v1/certificates** API.
3. In the template, anywhere before the **per-ap settings** block, depending on your requirement, add one or more of the following commands:

```
ca-cert-checksum <ca_cert_checksum/ca_cert_name>
cp-cert-checksum <captive_portal_cert_checksum/captive_portal_cert_name>
radsec-ca-checksum <radsec_ca_checksum/radsec_ca_name>
radsec-cert-checksum <radsec_cert_checksum/radsec_cert_name>
server-cert-checksum <server_cert_checksum/server_cert_name>
```



You can either use the certificate name or the checksum value in the command. Or, you can set it as a variable and enter the variable value for the Instant AP. Aruba recommends using the certificate name.

Example 1

```
ca-cert-checksum my_default_cert
```

Example 2

```
ca-cert-checksum %ca_cert_name%
variable:
{
  "ca_cert_name": "my_default_cert"
}
```

Managing Software Upgrades

The **Firmware** page provides an overview of the latest supported version of firmware for the device, details of the device, and the option to upgrade the device.

This section includes the following topics:

- [Viewing Firmware Details](#)
- [Upgrading a Device](#)
- [Setting Firmware Compliance](#)

Viewing Firmware Details

To view the firmware details for devices provisioned in Aruba Central:

1. In the **Network Operations** app, use the filter to select a group or a device.

2. Under **Maintain**, click **Firmware**. The **Firmware** dashboard displays the following information:

Table 32: Firmware Maintenance

| Data Pane Item | Description |
|-----------------------------------|---|
| Search Filter | Allows you to define a filter criterion for searching devices based on the host name, MAC address, location, firmware version, and the current upgrade status of the device. |
| Filter by Upgrade Status | <p>Filters the device list based on any of the following firmware upgrade status:</p> <ul style="list-style-type: none"> ■ Show All ■ New Firmware Available ■ Scheduled ■ In progress ■ Failed ■ Firmware up to date ■ Upgrading ■ Scheduling in progress ■ Downloading Firmware ■ Upgrade successful, ready for reboot ■ Upgrade successful and rebooting AP ■ Upgrade in process ■ Firmware upgrade failed. Please try again ■ Rebooting ■ Live upgrade initiating ■ Live upgrade initiated <p>Show All is selected by default.</p> |
| Access Points | <p>Displays the following information:</p> <ul style="list-style-type: none"> ■ Name—Name of the AP. ■ APs—Number of APs associated to VC. ■ Firmware Version—The current firmware version running on the device. ■ Recommended Version—The version to which the device is recommended for the upgrade. ■ Upgrade Status—Status of the devices associated with the tenant account. This column displays either Newer firmware available or Firmware up to date. ■ Compliance Status—Status of the firmware compliance setting. The value displayed in this column is either Set, Not Set, Set<date and time>, or Compliance scheduled on. The Compliance scheduled on displays the date and time that is set in the Firmware Compliance Setting page. |
| Switch-MAS | <p>Displays the following details about Aruba switches managed through Aruba Central:</p> <ul style="list-style-type: none"> ■ Name—Host name of the switch. ■ MAC Address—MAC address of the switch. ■ Model—Hardware model of the switch. ■ Firmware Version—The current firmware version running on the switch. ■ Recommended Version—The version to which the device is recommended for the upgrade. ■ Upgrade Status—Status of the devices associated with the tenant account. This column displays either Newer firmware available or Firmware up to date. ■ Compliance Status—Status of the firmware compliance setting. The value displayed in this column is either Set, Not Set, Set<date and time>, or Compliance scheduled on. The Compliance scheduled on displays the date and time that is set in the Firmware Compliance Setting page. |
| Switch-Aruba | |
| Continue | Allows you to continue with firmware upgrade. |
| Manage Firmware Compliance | <p>Allows to set firmware compliance for devices within a group. Click Manage Firmware Compliance to view a list of supported firmware versions for each device in a group.</p> <p>To ensure firmware version compliance, complete the following steps in the Manage Firmware Compliance page:</p> |

Table 32: Firmware Maintenance

| Data Pane Item | Description |
|-----------------------|---|
| | <ul style="list-style-type: none"> ■ Groups—Select the group for which the compliance must be set. Select the specific group to set compliance at group level. ■ Firmware Version ■ Upgrade Type—Select the upgrade type, standard or sequential. ■ Auto Reboot—Select this check box to reboot Aruba Central automatically after the build is downloaded on the device. On reboot, the new build is installed on the device. ■ Select one of the following radio buttons to specify if the compliance must be carried out immediately or at a later date and time. <ul style="list-style-type: none"> ● Now— To set the compliance to be carried out immediately ● Later — To set at the later date and time ■ Save and Upgrade—Click this button to save the firmware compliance with the above settings. |
| Upgrade All | Allows you to simultaneously upgrade firmware for multiple devices. |
| Cancel Upgrade | Cancels a scheduled upgrade. |
| Cancel All | Cancels a scheduled upgrade for all devices. |

Upgrading a Device

To check for a new version on the image server in the cloud, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Maintain**, click **Firmware**.
3. To upgrade firmware for devices in a specific group, select a group from the group selection filter.
4. Select one or several devices to upgrade.
5. Click **Continue**. The **Upgrade <Device> Firmware** pop-up window opens.
6. Select a firmware version. You can either select a recommended version or manually choose a specific firmware version.



To obtain custom build details, contact Aruba Central Technical Support.

7. Select **Auto Reboot** if you want Aruba Central to automatically reboot after device upgrade.



The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switches, and Branch Gateways.

8. Specify if the upgrade must be carried out immediately or at a later date and time.
9. Click **Upgrade**. The device downloads the image from the server, saves it to flash, and reboots. Depending on the progress and success of the upgrade, one of the following messages is displayed:
 - Upgrading—While image upgrade is in progress.
 - Upgrade failed—When the upgrade fails.
10. If the upgrade fails, retry upgrading your device.



After upgrading a switch, click **Reboot**.

Setting Firmware Compliance

Aruba Central allows you to run a firmware compliance check and force firmware upgrade for devices in a group. To force a specific firmware version for all AP devices or Switches in a group, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Maintain**, click **Firmware**.
3. Verify the firmware upgrade status for the device.
4. Click **Manage Firmware Compliance** at the top right. The **Manage Firmware Compliance** window opens.
5. Select the groups, firmware version, upgrade type, and the time for upgrade.
6. Select **Auto Reboot** if you want Aruba Central to automatically reboot the device after a successful device upgrade.



The **Auto Reboot** option is available for Mobility Access Switches, Aruba Switches, and Branch Gateways.

7. Select one of the following as required:
 - Select **Now** to set the compliance to be carried out immediately.
 - Select **Later Date** to set the compliance at the later date and time.
8. Click **Save and Upgrade**. Aruba Central initiates a firmware upgrade operation only for the devices that support the selected firmware version. If any of selected devices do not support the firmware version selected for the upgrade, a list of unsupported devices is displayed.

Using Troubleshooting Tools

In the **Network Operations** app, use the filter to select a group or a device and then, select **Tools** menu option under **Analyze**. The **Tools** menu allows network administrators and users with troubleshooting permission to perform troubleshooting or diagnostics tests on devices and networks managed by Aruba Central. Users with admin role and custom roles that allow edit access to the troubleshooting module can troubleshoot network and device issues. For more information on user roles, see [Configuring User Roles on page 139](#).



The **Tools** menu option is not visible to users who do not have troubleshooting permission.

Aruba Central does not support performing diagnostic checks on offline devices.

The **Tools** page is divided into the following tabs:

- **Network Check**—Allows you to run diagnostic checks on networks and troubleshoot client connectivity issues. You must have admin privileges or read-write privileges to perform network checks.
- **Device Check**—Allows you to run diagnostic checks and troubleshoot switches. You must have admin privileges or read-write privileges to perform device checks.
- **Commands**—Allows you to perform network health check on devices at an advanced level using command categories. Read-only users can also perform advance checks.

You can also perform live troubleshooting by clicking **Open Live Events** at the top right corner of the **Tools** page. For information, see [Live Events on page 246](#).

This section includes the following topics:

- [Troubleshooting Network Issues on page 123](#)

- [Troubleshooting Device Issues on page 128](#)
- [Advanced Device Troubleshooting on page 130](#)

Troubleshooting Network Issues

Network check aims to identify, diagnose, and debug issues detected in an Aruba Central-managed network. The **Network Check** tab on the **Tools** page captures the troubleshooting utilities that are used to test a network entity and collect results based on your selection.

To perform a diagnostic check on the Aruba Central-managed network, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze**, click **Tools**. The **Tools** page opens.
3. Click the **Network Check** tab.
4. Select a device. You can run diagnostic checks on the following types of devices managed by Aruba Central:
 - [Access Points](#)
 - [Switches](#)
 - [Gateways](#)

[Table 33](#) lists the tests available for each device type:

Table 33: *Tests and Devices*

| Test | Access Point | Switch | Gateway |
|-------------------|--------------|-----------|-----------|
| Ping Test | Available | Available | Available |
| Traceroute | Available | Available | Available |
| HTTP Test | Available | NA | NA |
| HTTPS Test | Available | NA | NA |
| TCP Test | Available | NA | NA |
| Speed Test | Available | NA | NA |



Devices which are already running commands shall not execute newly added commands.

This section includes the following topics:

- [Troubleshooting AP Connectivity Issues](#)
- [Troubleshooting Switch Connectivity Issues](#)
- [Troubleshooting Gateway Connectivity Issues](#)

Troubleshooting AP Connectivity Issues

The following tests are available to diagnose issues pertaining to WLAN network connections:

Ping Test

Sends ICMP echo packets to the hostname or IP addresses of the selected devices to check for latency issues.

To perform a ping test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
7. Enter the count in the range as mentioned in the field. The count should be a number between 1 to 300.
8. Click **Run**. The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

HTTP Test

Sends packets to the HTTP URL and tries to establish a connection and exchange data. If the HTTP website returns a response, the issue could be isolated to the client device.

To perform an HTTP test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTP URL for which you want to perform the HTTP test, in the **URL** field. For example, `http://hostname` or `http://ipaddress`.

7. Enter the timeout value in seconds. The value should be between 1 to 10 seconds. The default timeout value is 1 second.
8. Click **Run**. The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTP test is supported only from version 8.3.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

HTTPS Test

Sends packets to the HTTPS URL and tries to establish a connection and exchange data. If the HTTPS website returns a response, the issue could be isolated to the client device. HTTPS is a performance test to identify the time taken to load a web page.

To perform an HTTPS URL test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **HTTPS Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter the HTTPS URL for which you want to perform the HTTPS test, in the **URL** field, For example, `https://URL` or `https://IPv4`.
7. Enter the timeout value in seconds. The value should be between 1 to 10 seconds. The default timeout value is 1 second.
8. Click **Run**. The test output is displayed in the **Device Output** section.

Important Points to Note

- HTTPS test is supported only from version 8.4.0.0 or above.
- The test supports only IPv4 address or domain name in the **URL** field.

TCP Test

Sends packets to the host, for example, FTP server, and tries to establish a connection and exchange data. If the FTP server returns a response, the issue could be isolated to the client device.

To perform a TCP test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **TCP Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. Enter a valid IPv4 address in the **Host** field. Hostname is not supported.
7. Enter the port number., in the **Port** field. The port number should be between 1 to 65535.
8. Enter the timeout value in seconds, in the **Timeout** field. The value should be between 1 to 10 seconds. The default timeout value is 5 seconds.
9. Click **Run**. The output is displayed in the **Device Output** section.

Important Point to Note

- TCP test is supported only from version 8.3.0.0 or above.

Speed Test

Performs a speed test to measure network speed and bandwidth. The speed test diagnostic tool is available only for Instant AP. To perform a speed test, you must provide the iPerf server address, protocol type, and speed test options such as bandwidth.

To execute a speed test on APs:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Access Point**.
4. From the **Test** drop-down list, select **Speed Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple APs.
6. In the **Host** field, enter a valid hostname.
7. From the **Protocol** drop-down list, select the protocol. The available options are **TCP** or **UDP**.
8. In the **Options** field, enter the option. For example, bandwidth.
9. Click **Run**. The test output is displayed in the **Device Output** section.



While performing troubleshooting on APs, a maximum of 20 APs are listed in the drop-down list. If there are more than 20 APs, use the **Search** option to search for an AP on which you would like to perform diagnostic checks.

Troubleshooting Switch Connectivity Issues

The following tests are available to diagnose issues pertaining to wired network connections:

Ping Test

Sends ICMP echo packets to the IP address of the selected switch to check for latency issues.

To perform a ping test on switches:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Switch**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple switches.



You can select Aruba Switch or Mobility Access Switch from the **Sources** drop-down list.

6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
7. In the **Repetitions** field, enter the repetition value. The value should be between 1 to 10000.
8. In the **Data Size** field, enter the data size. The value should be between 0 to 65471.



Mobility Access Switches do not support repetition and data size.

9. Click **Run**. The test output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on switches:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Switch**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple switches.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

Troubleshooting Gateway Connectivity Issues

The following tests are available to diagnose issues pertaining to WAN or SD-WAN network connections:

Ping Test

Sends ICMP echo packets to the IP addresses of the selected devices to check for latency issues.

To perform a ping test on Gateways:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.
3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Ping Test**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. From the **Destination Type** drop-down list, select one of the following:
 - **Hostname/IP Address**—Enter the hostname or IP address.
 - **Client**—Select a client.
 - **VPNC**—Select the VPN Concentrator.
7. In the **Packet Size** field, enter the packet size to capture and store the data packet to analyze network issues at a later stage. The range is from 10 to 2000 Bytes.
8. In the **Count** field, enter the count. The value should be between 1 to 100.
9. Click **Run**. The output is displayed in the **Device Output** section.

Traceroute

Tracks the packets routed from a network host.

To perform a traceroute test on Gateways:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Network Check**.

3. From the **Device Type** drop-down list, select **Gateway**.
4. From the **Test** drop-down list, select **Traceroute**.
5. From the **Sources** drop-down list, select source(s). You can select multiple Gateways.
6. Enter the hostname or IP address.
7. Click **Run**. The output is displayed in the **Device Output** section.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and target. It also shows the status of the tests as, in progress, complete, and the buffer time. If there are multiple devices, select the device for which you want to view the output.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Troubleshooting Device Issues

Device check aims to identify, diagnose, and debug issues on your device. The **Device Check** tab in the **Tools** page can be used to perform troubleshooting check for Aruba Switches only. When a troubleshooting operation is initiated, Aruba Central establishes a session with the Switch selected for the troubleshooting operation and displays the output in the **Device Output** section.

To perform a device check on a switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze**, click **Tools**. The **Tools** page opens.
3. Click the **Device Check** tab.



By default, the **Device Type** is set to **Switch** if a switch is configured in the data path, else a warning is displayed.

Multiple device selection is not allowed at this level.

Devices which are already running commands shall not execute newly added commands.

4. From the **Switch** drop-down list, select the switch.
5. Select one of the following tests to perform diagnostic checks on the selected switch:
 - **Cable Test**—Enables testing of the electrical connections in the switch cable. It checks whether the cabling is conformed to the cabling plans and is of expected quantity. It is useful for production and maintenance.



Cable Test is supported only from version 16.05.000 or above.

- **Interface Bounce**—Restarts the port interface and forces a client to re-initiate a DHCP request. This option is available only for Aruba Switches.
- **PoE Bounce**—Restarts the PoE port and the device that is either connected to the PoE port or powered by it. This option is available only for Aruba Switches.



If you select **Cable Test**, **PoE Bounce**, or **Interface Bounce**, you must enter the port number or the port number range as mentioned in the example text.

If you navigate to the **Tools** page from the **Clients** page, under **Device Check** the client context is already set and the port number is auto filled based on the client selected.

- **Chassis Locate**—Activates the Switch locator LED. The locator LED indicates the physical location where an Aruba Switch is currently installed.

Important Point to Note

- Interface Bounce, PoE Bounce, and Chassis Locate are supported above version 16.04.000.

6. Click **Run**. The output is displayed in the **Device Output** section.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

The output pane displays a list of devices on which the troubleshooting commands were executed, the test type, initial timestamp, source, and argument. It also shows the status of the tests as, in progress, complete, and the buffer time.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.
- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

Unlike the other tests, for Cable Test, the output is displayed in a tabular format, and you cannot download, email, or export the output.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Advanced Device Troubleshooting

Advanced device check aims to identify, diagnose, and debug issues on your device at an advanced level using commands. The **Commands** tab on the **Tools** page lists commands specific to a particular device to test the device entity and collect results based on your selection. When a troubleshooting operation is initiated, Aruba Central establishes a session with the devices selected for the troubleshooting operation and displays the output in the **Device Output** section.

To perform advanced troubleshooting on devices, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze**, click **Tools**. The **Tools** page opens.
3. Click the **Commands** tab.
4. Select a device. Network administrators can perform advanced troubleshooting on the following types of devices managed by Aruba Central:
 - [Access Points](#)
 - [Switches](#)
 - [Gateways](#)



Devices which are already running shall not execute newly added commands.

Troubleshooting Access Points

To troubleshoot APs at an advanced level:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Access Point**.
4. From the **Available Devices** drop-down list, select the AP. You can select multiple APs.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. (Optional) Enter the client MAC or IP address of the selected command and click **Apply**. If you do not want to apply any filter, click **Apply** without entering any value in the client MAC or IP address field.
8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
 - a. Click the **Repeat** check box.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.



To perform advanced troubleshooting on APs, the minimum software version required on Instant APs is 6.4.3.1-4.2.0.3.

To perform advanced troubleshooting on Mobility Access Switches, the minimum version support is 7.4.0.6.

Troubleshooting Switches

To troubleshoot switches at an advanced level:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Switch**.
4. From the **Available Devices** drop-down list, select the switch. You can select multiple switches.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. (Optional) Enter the client MAC or IP address of the selected command and click **Apply**. If you do not want to apply any filter, click **Apply** without entering any value in the client MAC or IP address field.
8. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
9. (Optional) To set a frequency for automatically executing the troubleshooting commands:
 - a. Click the **Repeat** check box.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
10. Click **Run**. The output is displayed in the **Device Output** section.

Troubleshooting Gateways

To troubleshoot Gateways at an advanced level:

1. In the **Network Operations** app, use the filter to select a group, device, label or site.
2. Under **Analyze > Tools**, click **Commands**.
3. In the **Commands** tab, select the device type as **Gateway**.
4. From the **Available Devices** drop-down list, select the Gateway. You can select multiple Gateways.
5. Select any command category and the **Commands** pane displays the associated commands.
6. Click **Add>** to add the selected commands to the **Selected Commands** pane.
7. (Optional) Select command(s) and click **<Remove** to remove selected command(s) or click **<Remove All** to clear the **Selected Commands** pane.
8. (Optional) To set a frequency for automatically executing the troubleshooting commands:
 - a. Click the **Repeat** check box.
 - b. Specify an interval for executing the troubleshooting commands. You can also specify how frequently the commands must be executed during a given interval.
 - c. Click **Reset** to modify the values in all the fields, and **Cancel All** for canceling all the repeats. Click the stop icon to stop a particular repeat.
9. Click **Run**. The output is displayed in the **Device Output** section.

Filtering Commands

In order to streamline the debug process and avoid huge data generation while troubleshooting, few commands enable Client MAC address, IP Address, and Port filtration. There are two types of filtration available:

- **Mandatory filters**— Commands marked with '*'

1. Based on your device perform the task till step 4.
2. Select the command marked with '*' and click **Add**.

The **Additional Filters** dialog box appears.

3. Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.

The parameters are generated based on the commands selected.

4. Click **Apply**.

In case of mandatory filter commands, if you do not enter the filtering parameters in the additional filters dialog box, the command does not get added to the selected command pane and you cannot perform the troubleshooting.

5. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

- **Optional filters**— Commands marked with '+'

1. Based on your device perform the task till step 4.
2. Select the command marked with '*' and click **Add**.

The **Additional Filters** dialog box appears.

3. Enter the parameters such as, Client MAC address, IP address, port number, port list, or policy name as required.

The parameters are generated based on the commands selected.

4. Click **Apply**.

In case of optional filter commands, if you do not enter the filtering parameters in the additional filters dialog box, the command still gets added to the selected command pane and you can perform your troubleshooting.

5. (Optional) Click **Edit All** to reset the filtration parameters for all the commands added in the selected command pane.

Viewing the Device Output

After you execute troubleshooting commands on the devices, Aruba Central displays the output in the **Device Output** section of the **Tools** page.

If there are multiple devices, select the device for which you want to view the output. It shows the status of the tests as, in progress, complete, and the buffer time.



Output history of device with buffer space issues shall be automatically cleared.

You can perform the following tasks from the **Device Output** section:

- Click **Clear** to clear the output. You can clear the output for a single device or for all devices. The **Clear** option is disabled for read-only users.
- Click the **Search** icon to search for text in the output.

- Click the **Email** icon and click **Send** to send the output as an email. You can also add email recipients in the **CC** field.
- Click the **Export** to export the command output as a zip file.
- Click the maximize icon to maximize the device output pane.

For more information on the output displayed for the CLI commands, see the following documents:

- *Aruba Instant CLI Reference Guide* for Instant AP CLI command output
- *HPE ArubaOS-Switch Management and Configuration Guide* for Aruba Switch CLI command output
- *ArubaOS 7.4.x CLI Reference Guide* for Mobility Access Switches CLI command output
- *ArubaOS CLI Reference Guide* for SD-WAN Gateway CLI command output

Viewing Audit Trails in the Account Home Page

The **Audit Trail** page in **Account Home** shows the logs for all the device management, configuration, and user management events triggered in Aruba Central and ClearPass Device Insight. You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username
- IP Address
- Category
- Description
- Target
- Source (Only in the MSP mode)

To view audit trail logs:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.
The **Audit Trail** page opens.
2. From the **Select App** drop-down list, select one of the following:
 - **All Apps**—Displays audit trail logs for all apps.
 - **Network Operations**—Displays audit trail logs for the **Network Operations** app.
 - **ClearPass Device Insight**—Displays audit trail logs for the **ClearPass Device Insight** app.

The following table describes the fields displayed in the **Audit Trail** table:

Table 34: *Audit Trail Details*

| Parameter | Description |
|--------------------|--|
| Occurred On | Time stamp of the events for which the audit trails are shown. |
| IP Address | IP address of the client device. |
| Username | Username of the admin user who applied the changes. |
| Target | Group or device to which the changes were applied. |

Table 34: Audit Trail Details

| Parameter | Description |
|--------------------|---|
| Source | Tenant account in which the changes occurred. NOTE: This column is applicable only in the MSP mode. |
| Category | Type of modification and the affected device management category. |
| Description | A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click ⓘ to view the complete details of the event. For example, if an event was not successful, click the ellipsis to view the reason for the failure. |

Viewing Audit Trails in the Standard Enterprise Mode

The **Audit Trail** page in the Standard Enterprise Portal shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username
- IP Address
- Category
- Description
- Target

To view the **Audit Trail** logs perform the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Analyze**, click **Audit Trail**. The **Audit Trail** table is displayed with the following details:
 - **Occurred On**—Timestamp of the audit log. Use the sort option to sort the audit logs by date and time. Use the filter option to select a specific time range to display the audit logs.
 - **IP Address**—IP address of the client device.
 - **Username**—Username of the admin user who applied the changes.
 - **Target**—The group or device to which the changes were applied.
 - **Category**—Type of modification and the affected device management category. See [Classification of Audit Trails](#).
 - **Description**—A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click ⓘ to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.



To customize the **Audit Trail** table, click the eclipses ☰ icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Classification of Audit Trails

The audit trail is classified according to the type of modification and the affected device management category. The category can be one of the following:

- Alert Configuration
- API Gateway
- Configuration

- Device Management
- Federated User Activity
- Firmware Management
- Gateway Management
- Groups
- Guest
- Install Manager
- Label Management
- MSP
- RBAC
- Reboot
- SAML Profile
- Sites Management
- Subscription Management
- Templates
- Tools
- User Activity
- User Management
- Variables

Removing Devices

The device monitoring dashboards allow you to remove an offline device. However, you will not be able to remove a device completely from Aruba Central database, because the device entry remains in the **Device Inventory** page. The devices appearing in the **Device Inventory** page shows the hardware devices that belong to your account or purchase order.

For information on removing an offline device, see the following topics:

- [Deleting an Offline AP](#)
- [Deleting an Offline Switch](#)
- [Deleting an Offline Gateway](#)

Removing a Device from the Device Inventory Page

You cannot remove a device completely from Aruba Central, but you can unsubscribe the device. After you unsubscribe, the device status changes to **Unsubscribed** in the **Device Inventory** page. If you have more than one Aruba Central account and if another Aruba Central user adds this unsubscribed device to another Aruba Central account, the device entry is removed from the **Device Inventory** page in your Aruba Central account.

Users and Roles

Aruba Central users are broadly categorized as follows:

- Network Administrators—Network administrators manage, configure, and monitor devices in their respective network or organization using the Aruba Central Standard Enterprise interface.
- Service Provider Administrators—Service Provider administrators are referred to as the MSP administrators who create, manage, and monitor accounts for multiple organizations (tenants). For MSP accounts, the

Network Operations app provides a separate interface called the MSP View, using which MSP administrators can provision and manage their respective tenant accounts. Tenant account users' access is limited to their respective account or network setup. For more information on creating tenant accounts, see the *Aruba Central MSP User Guide*.

Within each Aruba Central account, the admin users of the respective accounts can configure and manage the following types of users:

- **System users**—Users who authenticate to the Aruba SSO server (public cloud deployments) or LocalDB servers (private cloud deployments). System users can access both the UI and API interface with their Aruba Central login credentials. Access for the system users is determined by the role to which they are mapped. For more information on configuring system users, see [Configuring System Users on page 136](#).
- **External users**—Users who log in to Aruba Central using an external authentication source. External user accounts are maintained by IT administrators of the respective organizations. External users are also referred to as federated users. To provide a secure and seamless sign-on experience for external users, Aruba Central supports a federation configuration module based on the SAML SSO framework. For more information on configuring the SAML SSO framework for federated users, see the [Aruba Central SAML SSO Solution Guide](#).

The following table lists the tasks that you can perform from the **Users and Roles** page:

Table 35: *Users and Roles—Tasks*

| Task | For more information... |
|--|---|
| Create, modify, or delete users | Configuring System Users on page 136 |
| Create, modify, or delete user roles | Configuring User Roles on page 139 |
| Resend email invitation to users | Resend Email Invite on page 137 |
| Enable Two-Factor Authentication (2FA) | Two-Factor Authentication on page 142 |
| Enable support access to debug issues | Support Access on page 144 |

Configuring System Users

In the **Account Home** page, the **Users & Roles** option under **Global Settings** allows you to create, modify, and delete users.



This section describes the procedure for configuring users in an enterprise account. For information on how to configure system users in the MSP mode, see the [Aruba Central Managed Service Provider User Guide](#).

Adding a System User

To add a user, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users and Roles** page is displayed.
2. Click **Add User**.
The **New User** window is displayed.
3. Configure the following parameters:
 - **Username**—Email ID of the user. Enter a valid email address.

- **Description**—Description of the user role. You can enter up to a maximum of 32 characters including alphabets, numbers, and special characters in the text field.
- **Language**—Select a language. The Aruba Central web interface is available in English, French, Spanish, German, Brazilian Portuguese, Chinese, and Japanese languages.
- **Account Home**—Select a user role for the **Account Home** page. If there are common modules between **Account Home** and other app(s), the **Account Home** user role has higher precedence. For example, the **Devices and Subscription** module in the **Network Operations** app.



If an application is not provisioned, that application is not listed in the **New User** pop-up window.

- **Network Operations**—Select a user role for the **Network Operations** application.
 - If you assign the user role **guestoperator**, **readonly**, or **readwrite**, from the **Select Groups** drop-down list, select group(s). By default, the **admin** user role has access to all groups.
- **ClearPass Device Insight**—Select a user role for the **ClearPass Device Insight** application. For more information on user roles, see [Configuring User Roles](#).

4. Click **Save**. An email invite is sent to the user with a registration link. Users can use this link to access Aruba Central.

The registration link in the email invite is valid for 15 days. The link expiry date is also mentioned in the registration email notification:



Click [here](#) to register your account.

If the link does not work, please copy and paste the following URL in the address bar of your browser:

The above link expires on **Dec 23 2019**

NEW USER

USERNAME

DESCRIPTION (OPTIONAL)

LANGUAGE

English

Account Home:

admin

Network Operations:

guestoperator

SELECT GROUPS

× topo-sim-group

× BOCSIM-GATEWAYS

Cancel

Save

Resend Email Invite

If any user has not received the email invite, complete the following steps to resend the invite:

1. Click **Actions** and slide the **Resend Invitation To Users** toggle button to the right.
2. Enter the email ID and click **Resend Invite**.

Viewing User Details

In the **Account Home** page, under **Global Settings**, click **Users & Roles**. The **Users** tab is displayed. The **List of Users** table displays the following information:

- Email ID of the user.
- Type of user. The user can be system user or external user.
- Description of the user.
- Role assigned for the **Network Operations** app.
- Role assigned for the **ClearPass Device Insight** app. This option is displayed only if the **ClearPass Device Insight** app is provisioned and if you have subscribed to the app.
- Role assigned for the **Account Home** page.
- Allowed groups for the user.
- Last active time of the user. If the last active time cell is blank, the user has not logged in after the product upgrade.

Editing a User

To edit a user account, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users** tab opens.
2. In the **List of Users** table, select the user and click the edit icon.
3. In the **Edit User <"Username">** window, modify description, role, or allowed groups.
4. Click **Save**.

Deleting a User

To delete a user account:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users** tab opens.
2. In the **List of Users** table, select the user and click the delete icon.
3. Confirm user deletion in the **Confirm Action** dialog box.

Viewing Audit Trail Logs for Users

Audit logs are generated when a new user is created and an existing user is modified or deleted from the Aruba Central account. It also records the login and logout activities of users.

To view audit logs for Aruba Central users:

1. In the **Account Home** page, under **Global Settings**, click **Audit Trail**.
The **Audit Trail** page is displayed.
2. To view audit logs for user addition, modification, or deletion, click the filter in the **Classification** column, and select **User Management**.
3. To filter audit logs about user activity, click the filter in the **Classification** column, and select **User Activity**.

Configuring User Roles

A role refers to a logical entity used for determining user access to devices and application services in Aruba Central. Users are always tagged to roles that govern the level of user access to the Aruba Central applications and services.



Access control for federated users is determined by the attributes set in the IDP.

Aruba Central supports a set of predefined roles with different privileges and access permissions. You can also configure custom roles.

Predefined User Roles

The **Users & Roles** page allows you to configure the following types of users with system-defined roles:

Table 36: *Predefined User Roles*

| Application | User Role | Privilege |
|--------------------------|---------------|--|
| Account Home | admin | Administrator for the Account Home page. If there are common modules between Account Home and other app(s), the Account Home user role has higher precedence and the user is granted permission if the operation is initiated from the Account Home page. |
| | readwrite | Can view and modify settings in the Account Home page and all Global Settings pages. |
| | readonly | Can view the Account Home page and all Global Settings pages. |
| Network Operations | admin | Administrator for the Network Operations application. Has access to Account Home > Global Settings . This is applicable only if the Account Home role is not set or is not conflicting. |
| | deny-access | Cannot view the Network Operations application. |
| | guestoperator | Has guest operator access for the Network Operations application. User does not have access to Account Home > Global Settings . |
| | readonly | Has read-only access to Account Home > Global Settings and the Network Operations application. |
| | readwrite | Has read-write access to Account Home > Global Settings and the Network Operations application. Has access to view and modify data using the Aruba Central UI or APIs. However, the user cannot execute APIs to: <ul style="list-style-type: none">■ Enable or disable MSP mode.■ Perform operations in the following pages:<ul style="list-style-type: none">● Account Home > Users & Roles● Network Operations application > Organization > Labels and Sites |
| ClearPass Device Insight | admin | Administrator for the ClearPass Device Insight application. |
| | deny-access | Cannot view the ClearPass Device Insight application. |
| | readonly | Can launch and view all the pages in the ClearPass Device Insight application. |

Custom Roles

Along with the predefined user roles, Aruba Central also allows you to create custom roles with specific security requirements and access control. However, only users with the administrator role and privileges can create, modify, clone, or delete a custom role in Aruba Central.

With custom roles, you can configure access control at the application level and specify access rights to view or modify specific application services or modules. For example, you can create a custom role that allows access to a specific applications like **Guest Management** or **Network Management** and assign it to a user.



MSP tenant account users cannot add, edit, or delete roles.

Adding a Custom Role

The following are the permissions that you can associate with a custom role:

- User roles with **Modify** permission can perform add, edit, or delete actions within the specific module.
- User roles with **View Only** permission can only view the specific module.
- User roles with **Block** permission cannot view that particular module.

To add a custom role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
2. Click the **Roles** tab.
3. Click **Add Role**. The **New Role** window is displayed.
4. Specify a name for the role.
5. From the drop-down list, select one of the following:
 - **Account Home**—To manage access to devices and subscriptions in Aruba Central.
 - **Network Operations**—To set permissions at the module level in the **Network Operations** application.
 - **ClearPass Device Insight**—To set permissions at the module level in the **ClearPass Device Insight** application. This option is displayed only if the **ClearPass Device Insight** app is provisioned and if you have subscribed to the app.
6. For Network Management and MSP modules, you can set access rights at the module level.

To set view or edit permissions or block the users from accessing a specific module, complete the following steps:

 - a. Click **Customize**.
 - b. Select one of the following options for each module as required:
 - **View Only**
 - **Modify**
 - **Block**
7. Click **Save**.
8. Assign the role to a user account as required.

Module Permissions

Aruba Central allows you to define user roles with **view** or **modify** permissions. You can also block user access to some modules. For example, if the **Guest Management** module is blocked for a specific user role, the corresponding pages are not displayed in the UI.

Aruba Central supports setting permissions for the following modules:

Table 37: *Permissions*

| Application | Module | Description |
|--------------------|--------------------------|---|
| Account Home | Devices and Subscription | Aruba recommends users to add devices and assign keys and subscriptions to devices in the Account Home page. |
| Network Operations | MSP | Allows users with administrator role and privileges to define user access to MSP modules such as Customer Management and Portal Customization. The MSP tenant account user does not have access to the MSP application. Even if a tenant account user is assigned a custom role having MSP application privileges: <ul style="list-style-type: none">■ Tenant account user does have access to the MSP application.■ MSP will not appear in the Account Home > Global Settings > Users & Roles > Roles > Allowed Applications list. |
| | Group Management | Allows users to create, view, modify, and delete groups and assign devices to groups. |
| | Devices and Subscription | Users cannot edit or set permissions for this module. Modify and Block options are disabled. By default, the View Only permission is set. |
| | Network Management | Allows users to configure, troubleshoot, and monitor Aruba Central-managed networks. |
| | Guest Management | Allows users to configure cloud guest splash page profiles. |
| | AirGroup | Allows users to define or block user access to the AirGroup pages. |
| | Presence Analytics | Allows users to access the Presence Analytics app and analyze user presence data. |
| | VisualRF | Allows user to access VisualRF and RF heatmaps. |
| | Unified Communications | Allows users to access the Unified Communications pages. |
| | Install Manager | Allows users to manage installer profiles and site installations. |
| | Reports | Allows users to view and create reports. |
| | Other Applications | Allows users to access other applications modules such as notifications and Virtual Gateway deployment service. |

| Application | Module | Description |
|--|--------------------------------|--|
| ClearPass Device Insight NOTE: This option is displayed only if the ClearPass Device Insight app is provisioned and if you have subscribed to the app. | Classified devices | Allows users to view or modify system and user-classified devices. |
| | Generic devices | Allows users to view or modify devices which are not classified by system or user. |
| | User classified devices | Allows users to view or modify user-classified devices. |
| | Discovery settings | Allows users to view, create, modify, or delete discovery settings. |
| | Application settings | Allows users to view or modify application level user settings |
| | Reports | Allows users to view create and view reports |
| | Other Applications | Allows users to define or block access to other applications. |

Viewing User Role Details

To view the details of a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
2. Click the **Roles** tab. The **Roles** tab displays the following information:
 - **Role Name**—Name of the user role.
 - **Allowed Applications**—The application(s) to which the user account is subscribed to.
 - **Assigned Users**—Number of users assigned to a role.

Editing a User Role

To edit a user role, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the edit icon.
4. In the **Edit Role** <"Rolename"> window, modify the permissions set for module(s).
5. Click **Save**.

Deleting a User Role

To delete a user role, ensure that the role is not associated to any user and complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
2. Click the **Roles** tab.
3. In the **List of Roles** table, select the role and click the delete icon.
4. Confirm role deletion in the **Confirm Action** dialog box.

Two-Factor Authentication

Aruba Central now supports two-factor authentication for both computers and mobile phones to offer a second layer of security to your login, in addition to password. When two-factor authentication is enabled on a

user account, the users can sign in to their Aruba Central account either through the mobile app or the web application, only after providing their password and the six-digit verification code displayed on their trusted devices.

When two-factor authentication is enabled at the customer account level, all the users belonging to the customer account are required to complete the authentication procedure when logging in to Aruba Central. If a user account is associated with multiple customer accounts and if two-factor authentication is enabled on one of these accounts, the user must complete the two-factor authentication during the login procedure.

If two-factor authentication is enabled on your accounts, you must install the Google Authenticator app on your devices such as mobile phones to access the Aruba Central application. When the users attempt to log in to Aruba Central with their credentials, the Google Authenticator app provides a six-digit verification code to complete the login procedure.

Installing the Google Authenticator App

For two-factor authentication, ensure that the Google Authenticator app is installed on your mobile device.

During the registration process, the Aruba Central application shares a secret key with the mobile device of the user over a secure channel when the user logs in to Aruba Central. The key is stored in the Google Authenticator app and used for future logins to the application. This prevents unauthorized access to a user account as this authentication procedure involves two-levels for secure transaction.

When you register your mobile device successfully, the Google Authenticator app generates a six-digit token for the second level authentication. The token is generated every thirty seconds.

Enabling Two-factor Authentication for User Accounts

To enable two-factor authentication, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Two-Factor Authentication (2FA)** toggle button to the right. The two-factor authentication is enabled for all the users associated with the account.

Two-factor Authentication for Aruba Central Web Application

When two-factor authentication is enabled for a customer account, the users associated with that customer account are prompted for two-factor authentication when they log in to Aruba Central.

To complete two-factor authentication, perform the following actions:

1. Access the Aruba Central website.
2. Log in with your credentials. If two-factor authentication is enforced on your account, the two-factor authentication page opens.
3. Install the Google Authenticator app on your mobile device if not already installed.
4. Click **Next**.
5. If this is your first login since two-factor authentication is enforced on your account, open Google Authenticator on your mobile device.
6. Scan the QR Code. If you are unable to scan the QR code, perform the following actions:
 - a. Click the **Problem in Reading QR Code** link. The secret key is displayed.
 - b. Enter this secret key in the Google Authenticator app.
 - c. Ensure that the **Time-Based** parameter is set. Aruba Central is added to the list of supported clients and a six-digit token is generated.
7. Click **Next**.
8. Enter the six-digit token.

9. Select the **Remember 2FA for 30 Days** check box if you want the authentication to expire only after 30 days.
10. Click **Finish**.

Two-factor Authentication for the Aruba Central Mobile App

Two-factor authentication must first be enabled for your account. If two-factor authentication is not enabled, you log in to the application directly after a successful SSO authentication.

To log in to Aruba Central app on your mobile device, perform the following actions:

1. Open the Aruba Central app on your mobile device.
2. Enter your username and password and click **Log in**. If the registration process is pending, an error message is displayed:

Please register for two-factor authentication in our web app to ensure secured authentication.

3. Enter the token. On successful authentication, the Aruba Central app opens.

Registering a New Mobile Device

If you have changed your mobile device, you need to install Google Authenticator app on your new device and register again using a web browser on your Desktop for two-factor authentication.

To register your new mobile device, complete the following steps:

1. Log in to Aruba Central web application. The two-factor authentication page is displayed.
2. Click the **Changed Your Mobile Device?** link.
3. To register your new device and receive a reset email with instructions, click **Send 2FA Reset Email**. A reset email with instructions will be sent to your registered email address.
4. Follow the instructions in the email and complete the registration.

Support Access

Aruba technical support may ask you to enable **Support Access** to debug issues. After you enable **Support Access**, the Aruba support team can access your Aruba Central account remotely. Only users with administrator role can enable **Support Access**.

Enabling Support Access

To enable **Support Access**, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the right.
3. Set password expiry by selecting the number of days and click **Get Password**. A new password is generated.
4. Copy the password and share it with the Aruba technical support representative.

Disabling Support Access

After the remote support session is complete, do the following to disable **Support Access**:

1. In the **Account Home** page, under **Global Settings**, click **Users & Roles**.
The **Users and Roles** page is displayed.
2. From the **Actions** menu, slide the **Support Access** toggle button to the left.

This chapter describes the various options available for viewing the device, client, and network details:

- [Overview on page 215](#)
- [Network Health Dashboard on page 214](#)
- [All Clients on page 233](#)
- [Application Visibility on page 251](#)
- [VisualRF on page 254](#)
- [Topology on page 262](#)
- [Alerts & Events on page 265](#)
- [Reports on page 275](#)

Overview

In the **Network Operations** app, perform the following steps to access the overall network summary page:

1. Set the filter to **All Devices**.
The Global dashboard is displayed.
2. Under **Manage > Overview**, the network summary page displays the following tabs:
 - **Summary**—Displays details such as the bandwidth usage in the network, client counts, and cluster-specific details. For more information, see [Summary](#).
 - **Network Health**—Displays vital information of the network sorted by site. For more information, see [Network Health Dashboard](#).
 - **WAN**—Displays information on WAN Health.
 - **AI Insights**—Displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization at AP. For more information, see [AI Insights](#).
 - **VisualRF**—Displays a page for viewing campuses, buildings, and floors within a network. For more information, see [Viewing Network Information](#).
 - **WiFi Connectivity**—Displays connection details of all the clients connected to an AP. For more information, see [Wi-Fi Connectivity](#).


APs

The **APs** monitoring dashboard provides all the metrics about the health, status, and clients information associated with the AP provisioned and managed through Aruba Central.

To view the Instant AP dashboard perform the following steps:

1. In the **Network Operations** app, use the filter bar to select a group.
2. Under **Manage**. Click **Devices > Access Points** to view the AP monitoring dashboard.
3. The **Access Points** dashboard includes the following contents:
 - **Usage**—Displays the overall usage metrics for the APs provisioned in your Aruba Central account.

- **Usage**—Displays the incoming and outgoing data traffic to and from the device.
- **Clients Count**—Displays the number of clients connected to an AP over a specific time period.
- **Bandwidth Usage Per Network**—Displays the incoming and outgoing traffic for all APs per SSID over a specific duration.
- **Client Count Per Network**—Displays the number of clients connected to an AP as per SSID over a specified time period.

4. Click the  list icon to display the AP list page.

Navigation and Granularity

To view more details about a specific AP, click the following contents:

- **Access Points**—Displays the total number of APs.
- **Up**—Displays the total number of APs that are up.
- **Down**—Displays the total number of APs that are down.
- **Radios**—Displays the total number of active radios.

Clicking each of the above component displays the list of APs in respective operational states in the AP list table. Clicking a specific AP in the table displays the corresponding AP details page.


Access Points Table

The APs table for the **Access Points**, **Up** and **Down** categories displays a list of APs with the following information:


- **Device Name**—Name of the AP.
- **Clients**—Clients connected to the AP.
- **Alerts**—Opens alerts related to APs.
- **Channel**—Channels assigned under Radio 1 and Radio 2.
- **Power**—The transmit power of Radio 1 and Radio 2 measured in decibels.
- **Utilization**—The percentage of time (normalized to 255) that the channels of Radio 1 and Radio 2 are sensed to be busy. The AP uses either the physical or the virtual carrier sense mechanism to sense a busy channel. This percentage not only depends on the data bits transferred but also with the transmission overhead that makes use of the channel.
- **Noise Floor**—The noise at the radio receivers of Radio 1 and Radio 2. Along with the thermal noise, Noise Floor may be affected by certain types of interference sources, though not all interference types result in increased noise floor. Noise Floor value may vary depending on the noise introduced by components used in the computer or client device.
- **IP Address**—IP address of the AP.
- **Model**—The model number of the AP.
- **Serial**—The serial number of the device.
- **Mode**—The radio mode such as access or monitor.
- **MAC**—MAC address of the AP.
- **Virtual Controller**—Name of the Virtual Controller.
- **Gateway Cluster**—Name of the Gateway Cluster associated with the AP.
- **Config Status**—The configuration changes associated with the AP.
- **Group**—Group to which the device belongs.
- **Labels**—Labels associated with the AP.
- **Site**—The site to which the device belongs.

- **Firmware Version**—The firmware version running on the AP.
- **Uptime**—Time since when the device is operational. The **Uptime** column is not applicable for offline devices and remains blank for all the devices in the **List of Offline APs** page.
- **Last Seen**—The last active time and date of the device. The **Last Seen** column is not applicable for online devices and remains blank for all the devices in the **List of Online APs** page.
- **Public IP**—IP address that is logged by servers when the device is connected through internet connection.
- **Search box**—The **Search** filter allows you to specify a criteria for searching devices. Aruba Central supports single column search. It filters the search results and sorts the list of devices based on the search string specified from a single column.

The **Search** filter is provided only for the **Device Name, IP Address, Model, Serial, Mode, MAC, Virtual Controller, Group, Labels, and Site** columns.

To expand or collapse the column view, click the column settings icon next to the last column of the table. By default, the AP list table displays the **Device Name, Clients, Alerts, Channel, Power, IP Address, and Model** columns. You can customize the view of AP list table with additional columns such as the **Utilization, Noise Floor, Serial, MAC, Virtual Controller, Gateway Cluster, Config Status, Group, Labels, Site, Firmware Version, Uptime, Last Seen, and Public IP**. These additional columns can be selected by clicking the  icon provided at the right corner of the table that displays the AP list. Click the **Reset** button provided in the drop-down list to reset the AP list with default columns only.

To delete a specific AP in the **List of Offline APs** page of the **Monitoring & Reports > Network Overview > APs** tab, click the AP listed in the AP list table. A confirmation message appears. Click the **Delete** button to delete the AP.

To download the **.csv** file of the AP list table, click the  icon provided at the right corner of the table and select the **Download CSV** option. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file in Microsoft Excel 2007 spreadsheet software, perform the following steps to view table with unicode values:

1. Open the Microsoft Excel 2007 software.
2. Click on the Data menu bar option.
3. Click on the **From Text** icon.
4. Browse to the location of the file that you want to import.
5. Select the file name and click **Import**.
6. The **Text Import** wizard is displayed.
7. Select the file type. For **.csv** format, select the **Delimited** option.
8. Select the **65001: Unicode (UTF-8)** option from the drop-down list that is displayed next to the **File** origin.
9. Click **Next**. The **Text Import Wizard-Step 1 of 3** page is displayed.
10. Place a check mark next to the delimiter such as the comma or full stop that was used in the file you wish to import into Microsoft Excel 2007.
11. The **Data Preview** window displays the data based on the selected delimiter.
12. Click **Next**. The **Text Import Wizard-Step 3 of 3** page is displayed. Select the appropriate data format for each column that you want to import.

Importing one or more columns is optional.

13. Click **Finish** to import the data into Microsoft Excel 2007.



When you click the **Radios** component in the AP list page, a table with the following columns are displayed:

- **Access Point**—Name of the AP.
- **Radio MAC Address**—The MAC address of the AP connected to the radio.
- **Band**—Displays the channel change based on both 2.4 GHz and 5 GHz radios.
- **Bandwidth**—The bandwidth of data transferred through the radios.
- **Channel**—Channels assigned under Radio 1 and Radio 2.
- **Utilization**—The percentage of time (normalized to 255) that the channels of Radio 1 and Radio 2 are sensed to be busy. The AP uses either the physical or the virtual carrier sense mechanism to sense a busy channel. This percentage not only depends on the data bits transferred but also with the transmission overhead that makes use of the channel.
- **Power(dBm)**—The transmit power of Radio 1 and Radio 2 measured in decibels.
- **Noise(dBm)**—The noise at the radio receivers of Radio 1 and Radio 2. Along with the thermal noise,

AP Details Page View

To view more details related to a specific AP, click the specific AP displayed in the AP list table under the following categories:

- **Access Points**—Displays the total number of APs.
- **Up**—Displays the total number of APs that are up.
- **Down**—Displays the total number of APs that are down.
- **Radios**—Displays the total number of active radios.

Filters

To set your dashboard view to show only the data pertaining to a group, label, site, or device, use the filter bar. By default, Aruba Central displays data for all devices in your Aruba Central account.

To set your dashboard view to show data for specific duration, use the filtering options in **Time Range** filter. By default, the data is displayed for a time range of 3 hours. To view the graphs for a different time range, click **Time Range** filter and select a time range of your choice. You can choose to view data for a time period of 3 hours, 1 day, 1 week, 1 month, and 3 months.

AP Details Panel

The AP details page includes a header panel that provides the following information on the AP:

- **Access Points**—Displays the MAC address of the AP along with a message describing the operational status of the device for the time range selected in the Temporal Filter.
- **Device Health**—Displays the health status of the device that is measured based on the CPU and memory utilization of the device. For example, **Good** or **Bad**.
- **Radio 1**—Displays the health of Radio 1 indicated as **Good** or **Bad**. The health of the radios are scored based on the Noise Floor and RF Utilization values.
- **Radio 2**—Displays the health of Radio 2 indicated as **Good** or **Bad**. The health of the radios are scored based on the Noise Floor and RF Utilization values.
- **Virtual Controller**—Displays the name of the Virtual Controller to which the AP is connected, if the AP details page belongs to a slave device. Clicking the Virtual Controller name displays the AP details page corresponding to the Virtual Controller. If the AP details page belongs to a master AP, then the **Virtual Controller** field displays **Self**.

The AP details page includes tabs that displays information specific to the AP.



The AP details page that is opened on Mozilla Firefox web browser displays blank sections in all the tabs when the time range is changed in the Temporal Filter or when the page undergoes auto-refresh. To populate data in the tabs, you must switch between the tabs of the AP details page or navigate back to the AP list view to revoke the AP details page.

Open Tools

The **Open Tools** button allows you access the troubleshooting utility to troubleshoot Access Point issues. For more information on troubleshooting Access Points, see [Advanced Device Troubleshooting](#).

Tabs in AP Details Page

To view information on the options displayed on the AP details page, click through the following:

- [Overview](#)
- [AI Insights](#)
- [Usage](#)
- [RF](#)
- [Spectrum](#)
- [Tunnels](#)
- [Location](#)
- [Events](#)
- [Actions](#)
- [Go Live](#)

Left Pane in AP Details Page

In the device context, the left pane of the AP details page displays device specific details in the following modules under **Manage**, **Analyze**, and **Maintain**:

- **Overview**—Displays the AP details page.
- **Device**—Displays all the tabs specific to device configurations. For more details, see [Deploying a Wireless Network Using Instant APs](#).
- **Clients**—Displays all the details of clients connected to the device. This tab also displays firewall session details of clients connected to the device.
- **Alerts & Events**—Displays all the alerts and events associated with the device. For more details, see [Access Point Alerts](#).
- **Audit Trail**—Displays all the trails and logs associated with the device. For more details, see [Viewing Audit Trails](#).
- **Tools**—Displays the tools required to troubleshoot network issues. For more details, see [Using Troubleshooting Tools](#).
- **Firmware**—Displays firmware specific details for the device. For more details, see [Managing Software Upgrades](#).

APs—Overview Tab

The **Overview** tab displays the AP device details, network information, radio details including the topology of clients connected to each radio, and the health status of the AP in the network. The **Overview** tab includes the following details:

Device

The **Device** section displays the following general information such as the state of the AP:

- **AP Model**—The AP hardware model.
- **Country Code**—Country code in which the AP operates.
- **MAC**—MAC address of the AP.
- **Serial Number**—Serial number of the AP.
- **Uptime**—Time since when the AP is operational.
- **Last Reboot Reason**—The reason for the latest rebooting of AP.
- **Firmware Version**—The firmware version running on the AP. If the device is running an older firmware version, this field prompts the user to upgrade to the latest firmware version along with the link to the **Maintenance > Firmware** page.
- **Configuration Status**—The time when the device configuration was modified lately.
- **Power Negotiation**—The power in watts (W) negotiated on the ethernet port of the device in a wired network.
- **Group**—The group to which the AP belongs.
- **Labels**—Labels associated with the AP. You can also add a new label to the AP by clicking the edit icon. To view all the labels associated with a device, hover your mouse over the **Labels** column.
- **Blink LEDs**—To enable the blinking of LEDs on the AP to identify the location. The default blinking time is set to 5 minutes and it automatically stops after that. To stop the blink manually, click **Stop Blinking**.
- **Site**—The site to which the AP device belongs.

Network

The **Network** section displays information of the network and interfaces to which the AP is connected. Along with the network profile name, the following fields are displayed in the **Network** section:

- **Speed/Duplex**—The speed of the network measured in Mbps. This field also indicates whether the network has a full-duplex or half-duplex communication.
- **VLANs**—Number of VLAN connections associated with the network.
- **Current Uplink**—Current uplink connection on the AP.
- **IP Address**—IP address of the AP.
- **Public IP Address**—IP address logged by servers when the AP device is connected through internet connection.
- **DNS Name Servers**—The server that has a directory of domain names and their associated IP addresses.
- **IPv4 Default Gateway**—A 32 bit value which is used to uniquely identify the device on a public network.
- **NTP Server**—The information on NTP Server.

Radios

The **Radios** section displays information related to **Radio 1** and **Radio 2** for 2.4 GHz and 5 GHz bands, and displays the following fields:

- **Mode**—The type of mode for Radio 1 and Radio 2.

- **Status**—The status of the AP connected to the radio.
- **Radio MAC Address**—The MAC address of the AP connected to the radio.
- **Channel**—The channels assigned under Radio 1 and Radio 2.
- **Power**—The transmit power of Radio 1 and Radio 2 measured in decibels.
- **Type**—The type of wireless LAN used for Radio 1 and Radio 2.
- **Clients**—The number of clients connected to the AP.
- **Wireless Networks**—The number of SSIDs configured in the network.

Data Path

The **Data Path** section displays the topology of clients connected to each of the radios of the AP, which in turn is connected to switches or gateways through VLAN.

Health Status

The **Health Status** trend graph indicates the health status of the device in the network for the time specified in the Time Range Filter. You can view information such as the Health Status, Noise Floor, CPU, memory, and channel utilization values when you move your mouse pointer to a specific area in the graph.

APs—AI Insights

The **AI Insights** tab in the AP context displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization.

To launch the **AI Insights** dashboard for APs, complete the following steps:

1. In the **Network Operations** app, use the filter to select an AP.
2. Under **Manage**, click **Devices > Access Points**.
3. Click a specific online AP in the table.

The **Access Point Details** page is displayed.

4. Click the **AI Insights** tab to view a list of AI Insights that are observed in the AP. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. Select one of the following time range from the **Time Range Filter** to view insight data:

- 3 hours—Displays 3 bar graphs with exact hourly data
- 1 day—Displays 24 bars with exact hourly data
- 1 week—Displays 7 bars with past 7 days' daily data
- 1 month—Displays 30 bars with past 30 days' daily data

The graphs represent severity in different colors:

- **Red**—High
- **Yellow**—Medium
- **Gray**—Low

Each insight further includes categories of information present in form of tabs like, reason, band, channel, SNR and so on. These tabs can be clicked and displays the detailed information found in that section of the Insight.

The **AI Insights** page displays the performance issues based on the following criteria:

- [Excessive AP Channel Changes](#)
- [Clients with Low SNR Uplink Connections](#)
- [AP with High Memory Utilization](#)
- [AP with High 2.4 GHz Airtime Utilization](#)
- [AP with High 5 GHz Airtime Utilization](#)

- [Frequent AP Transmit Power Changes](#)
- [AP with Missing Telemetry](#)
- [AP with High CPU Utilization](#)
- [Excessive AP Reboots](#)
- [MAC Authentication Failures](#)
- [4-way Handshake \(EAPOL Key\) Failures](#)
- [802.1x Authentication Failures](#)
- [High DHCP Failures](#)

Excessive AP Channel Changes

The **Excessive AP Channel Changes** insight displays information about AP radios on the network that changed channels excessively:

- **Reason**—Reason for which the AP might have changed the channels on the network. It might be due to different reasons such as interference, noise threshold, channel quality threshold, or empty channel for both the frequency bands (2.4 GHz and 5 GHz).
- **Clients**—MAC Address of the clients and the corresponding number of channel changes per client.
- **Channel**—Number of channel changes per channel for that AP during the selected time period. It shows a comparison of the channel change between the peer network and AP.
- **Band**—Channel change based on both 2.4 GHz and 5 GHz represented in pie chart format.

Clients with Low SNR Uplink Connections

The **Clients with Low SNR Uplink Connections** insight displays information about APs that have a low-quality signal-strength connection:

- **Clients**—List of connected clients experiencing low signal quality (minutes).
- **Band**—Devices experiencing a low signal-quality link using 2.4 GHz or 5 GHz radio bands.
- **Good vs Bad**—Amount of time (minutes) with Low SNR (Bad) and High SNR (Good) for all the clients. The data is represented in the form of a pie chart.
- **Tx Power**—Percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **SNR**—Average of all the connected clients' Signal-to-Noise Ratio overtime in both 2.4 GHz and 5 GHz band.

AP with High Memory Utilization

The **AP with High Memory Utilization** insight displays information about APs that have higher memory utilization:

- **Memory**—Average memory utilization for each AP.

AP with High 2.4 GHz Airtime Utilization

The **AP with High 2.4 GHz Airtime Utilization** insight displays the number of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day. When the AP Airtime Utilization Insight details page opens, it shows the total number of impacted AP radios for a specific period of time as selected in the **Time Range Filter**.

- **Root Causes**—Lists possible causes for this failure type, recommendations for resolving this issue (if available), and the percentage of individual failures attributed to each cause.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is

calculated from the severity of the utilization level and the duration of time that the channel was overutilized.

- **Hour of Day**—Hours of the day the network was most impacted by excessive AP airtime utilization.
- **Clients**—List of clients connected to 2.4 GHz AP radio.
- **Tx Power**—Percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **SNR**—Average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 2.4 GHz band.

AP with High 5 GHz Airtime Utilization

The **AP with High 5 GHz Airtime Utilization** insight displays the numbers of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and specific period of time as selected in the **Time Range Filter**.

- **Root Causes**—Lists possible causes for this failure type, recommendations for resolving this issue (if available), and the percentage of individual failures attributed to each cause.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Hour of Day**—Hours of the day the network was most impacted by excessive AP airtime utilization. The charts on this tab show the airtime utilization score for each hour of the day, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Clients**—List of clients connected to 5 GHz AP radio.
- **Tx Power**—Strength of the signal that the AP produces during the time it is transmitting signal to the client.
- **SNR**—Average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 5 GHz band.

Frequent AP Transmit Power Changes

The **Frequent AP Transmit Power Changes** insight displays AP radios that frequently changed transmit power:

- **Power Distribution**—Percentage of Tx power distribution (dBm) that each AP is spending over 2.4 GHz and 5 GHz bands.
- **Band**—Number of power changes in both the frequency bands by the AP (2.4 GHz or 5 GHz).

AP with Missing Telemetry

The **AP with Missing Telemetry** insight displays information about AP radios that has missing telemetry feed:

- **State**—The number of telemetry reports received by AP during the selected temporal filter duration.

AP with High CPU Utilization

The **AP with High CPU Utilization** insight displays information about AP with unusually high CPU utilization levels:

- **CPU**—CPU utilization of the AP.

Excessive AP Reboots

The **Excessive AP Reboots** insight displays the information about the APs that have been rebooted the maximum times and also the corresponding reason of the frequent reboots.

- **Reboots**—Number of reboots over time.

MAC Authentication Failures

The **MAC Authentication Failures** insight displays information about the frequent MAC authentication failures encountered during AP and client connectivity:

- **SSID**—List of SSIDs used by clients impacted by the issue, as well as the number of failures on that SSID.
- **BSSID**—Number of BSSIDs used by devices that frequently failed to complete MAC authentication.
- **Reason**—List of reasons that may explain why devices frequently failed MAC authentication and the number of errors that could be attributed to each cause.
- **Clients**—Number of clients that frequently failed to complete MAC authentication.

4-way Handshake (EAPOL Key) Failures

The **4-way Handshake (EAPOL Key) Failures** insight displays information about the frequent 4-way handshake failures encountered during AP and client connectivity:

- **SSID**—List of SSIDs used by clients impacted by the issue, as well as the number of failures on that SSID.
- **BSSID**—Number of BSSIDs used by devices that frequently failed to complete 4-way handshake authentication.
- **Reason**—List of reasons that may explain why devices frequently failed 4-way handshake authentication, and the number of errors that could be attributed to each cause.
- **Clients**—Number of clients that frequently failed to complete 4-way handshake authentication.

802.1x Authentication Failures

The **802.1x Authentication Failures** insight displays information about the frequent 802.1x authentication failures encountered by the AP:

- **SSID**—List of SSIDs used by clients impacted by the issue, as well as the number of failures on that SSID.
- **BSSID**—Number of BSSIDs used by devices that frequently failed to complete 802.1x authentication.
- **Reason**—List of reasons that may explain why devices frequently failed 802.1x authentication, and the number of errors that could be attributed to each cause.
- **Clients**—Number of clients that frequently failed to complete 802.1x authentication.
- **Server**—Number of servers that frequently failed to complete 802.1x authentication.

High DHCP Failures

The **High DHCP Failures** insight displays the information about the frequent DHCP failures encountered by the AP.

- **SSID**—List of SSIDs used by clients impacted by the issue, as well as the number of failures on that SSID.
- **BSSID**—Number of BSSIDs used by devices that frequently failed to complete DHCP authentication.
- **Reason**—List of reasons that may explain why devices frequently failed DHCP authentication, and the number of errors that could be attributed to each cause.
- **Clients**—Number of clients that frequently failed to complete DHCP authentication.

For more information, see [AI Insights](#).

APs—Usage Tab

The **Usage** tab displays the size of data transmitted through the AP. This tab includes the following details:

Throughput

The **Throughput** graph indicates the size of data sent to and received by the device in bits per second for the wired or wireless networks. For example, Eth 0 or Eth 1 wired network profiles and specific SSIDs of wireless networks. You can also view data for all the wireless SSIDs by selecting **All SSIDs** from the drop-down list. You can view the overall data usage measured in bytes in the **Overall Usage** field.

Clients

The **Clients** graph indicates the number of clients connected to the device for a selected time range in the Time Range Filter. You can select a specific SSID or all SSIDs, Eth0, or Eth 1 from the drop-down list provided in the **Clients** section.



You can also view the data for a specific time by moving the mouse on the graphs.

APs—Spectrum Tab

When the radios of Instant APs are set to spectrum scan mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference from neighboring Instant APs or non-WiFi devices such as microwaves and cordless phones. To enable the spectrum scan feature on a specific radio of an AP, see [Access Points Configuration](#).

When the spectrum scan feature is enabled, the Instant AP does not provide services to clients.



The spectrum scan feature is available only on Instant AP devices running Aruba Instant 8.5.0.1 firmware version and later. For more information on spectrum scanners, see [Spectrum Scan Feature](#).

The **Spectrum** tab displays the following details for all Wifi and non-Wifi devices associated to each radio in the following pages:

- Channel Utilization and Quality
- Non-Wifi Interferers List

Channel Utilization and Quality

By default, the **Spectrum** tab displays a page with device list with channel utilization and quality details graph corresponding to **Radio 1** and **Radio 2** radios of the AP. Click the **2.4 GHz** and **5 GHz** tabs on the **Channel Utilization and Quality** label to view the channel utilization and quality details graphs for the respective radios.

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the **Available**, **Interference**, and **Wifi Utilization** categories associated to **2.4 GHz** and **5 GHz** radios. You can view the following channel metrics when you hover the mouse over the **Channel Utilization** bar graph:

Table 38: *Channel Utilization Metrics*

| Metrics | Description |
|--------------------------|--|
| Channel | The channel number of 2.4 GHz or 5 GHz radio. |
| Available | The percentage of the channel currently available for use. |
| Interference | The percentage of the channel currently being used by non-Wi-Fi and Wi-Fi interferers. |
| Microwave | The percentage of the channel currently being used by microwaves. Common residential microwave ovens with a single magnetron are classified as a Microwave. These types of microwave ovens may be used in cafeterias, break rooms, dormitories, and similar environments. Some industrial, healthcare, or manufacturing environments may also have other equipment that functions like a microwave and may also be classified as a Microwave device. |
| Bluetooth | The percentage of the channel currently being used by bluetooth devices. Any device that uses the Bluetooth protocol to communicate in the 2.4 GHz band is classified as a Bluetooth device. Bluetooth uses a frequency hopping protocol. |
| Cordless Phone | The percentage of the channel currently being used by cordless phones. |
| Wi-Fi Utilization | The percentage of the channel currently being used by Wi-Fi devices. |

Quality

The **Quality** graph indicates the channel quality corresponding to each of the WiFi and non-WiFi devices connected to the radios. You can view the following channel metrics when you hover the mouse over the **Quality** bar graph:

Table 39: *Channel Quality Metrics*

| Metrics | Description |
|--------------------|---|
| Channel | The channel number of 2.4 GHz or 5 GHz radio. |
| Quality | Current relative quality of the channel. |
| Known APs | Number of valid Instant APs identified on the radio channel. |
| Unknown APs | Number of invalid or rogue Instant APs identified on the radio channel. |

| Metrics | Description |
|-------------------------|---|
| Max AP Signal | Signal strength of the Instant AP that has the maximum signal strength on a channel in dBm. |
| Max Interference | Signal strength of the non-Wi-Fi device that has the highest signal strength in dBm. |
| Max AP SSID | The network SSID with maximum APs. |
| Max AP BSSID | The network SSID with maximum APs. |

Non-WiFi Interferers List

Clicking the icon displays a page with a list of non-WiFi interferers detected by the spectrum scanner. The page displays a table with following details of non-WiFi interferers:

Table 40: *Non-WiFi Interferers Table*

| Metrics | Description |
|--------------------------|---|
| Type | Device type. This parameter can be any of the following: <ul style="list-style-type: none"> ■ Audio FF (fixed frequency) ■ Bluetooth ■ Cordless base FH (frequency hopper) ■ Cordless phone FF (fixed frequency) ■ Cordless network FH (frequency hopper) ■ Generic FF (fixed frequency) ■ Generic FH (frequency hopper) ■ Generic interferer ■ Microwave ■ Microwave inverter ■ Video ■ Xbox |
| ID | ID number assigned to the device by the spectrum monitor. Spectrum monitors assign a unique spectrum ID per device type. |
| Central Frequency | Center frequency of the signal sent from the device. |
| Bandwidth | Channel bandwidth used by the device in KHz. |
| Affected Channels | Radio channels affected by the wireless device. |
| Signal Strength | Strength of the signal sent from the device measured in dBm. |
| Duty Cycle | The device duty cycle. This value represents the percent of time the device broadcasts a signal. |
| First Seen | Time at which the device was first detected. |
| Last Seen | Time at which the device's status was updated. |



The data displayed in the Spectrum tab is refreshed every 15 seconds. Aruba Central displays the last recorded data for 30 minutes if the device turns offline.

Spectrum Scan Feature

Wireless networks operate in environments with electrical and RF devices that can interfere with network communications. Microwave ovens, cordless phones, and even adjacent Wi-Fi networks are all potential sources of continuous or intermittent interference.

The spectrum monitor (SM) software modules on Instant APs can examine the RF environment in which the Wi-Fi network is operating, identify interference, and classify its sources. An analysis of the results can then be used to quickly isolate issues associated with packet transmission, channel quality, and traffic congestion caused by contention with other devices operating in the same band or channel. SMs are Instant AP radios that gather spectrum data but do not service clients. Each SM scans and analyzes the spectrum band used by the SM's radio (2.4 GHz or 5 GHz).

The recorded spectrum is not reported to the virtual controller. A spectrum alert is sent to the virtual controller when a non-Wi-Fi interference device is detected.




In Aruba Central, the spectrum scan feature is available only on Instant AP devices running Aruba Instant firmware version 8.5.0.1 and later.

APs—Clients Tab

The **Clients** tab displays details of all the clients connected to a specific AP.

1. In the **Network Operations** app, click **Devices > Access Points**.



2. Click the  list icon to view the list of APs.
3. Click on a specific AP to view the AP details page.
4. Click the **Clients** tab on the left navigation to view the clients details corresponding to a specific AP.

The following tabs in **Client** page provide additional details about the client:

- **Summary** - This page displays a table that lists the clients connected to the AP. You can filter the clients based on the selection from the **Status** drop-down list.
- **Sessions** - This page displays details related to the firewall sessions maintained by the AP, and can be viewed only when you click on a specific client.



For more information, refer to [Wireless Client Overview](#).

APs—RF Tab

The **RF** tab displays the following details corresponding to **Radio 1** and **Radio 2** radios of the AP:

Channel Utilization

The **Channel Utilization** graph indicates the percentage of channel utilization for the selected time range from the Time Range Filter.

Noise Floor

The **Noise Floor** graph indicates the noise floor detected in the network to which the device belongs.

Frames

The **Frames** line graph indicates the trend of frames transmitted through the network. The frames can be one of the following types: **Drops**, **Errors**, and **Retries**. The graph indicates the status of data frames that were dropped, or encountered errors, or retried to be transferred, in a wireless network.

Channel Quality

The **Channel Quality** graph indicates the quality of channel in percentage.



You can also view the data for a specific time of the day by moving the mouse over the **Channel Utilization**, **Noise Floor**, **Frames**, and **Channel Quality** graphs.

RF Neighbors

The **RF Neighbors** table displays details on all the RF neighbors connected to the AP. The table includes the following mandatory columns:

- **RF Neighbor**—The MAC address of the neighboring devices that belong to the same RF group as the AP.
- **ESSID**—The ESSID of the neighboring device.
- **Channel**—The channels assigned under Radio 1 and Radio 2.
- **Signal**—The signal-to-noise ratio in decibels.
- **Type**—The type of RF neighbor in the network. For example, Neighbor, Interferer, or SuspectRogue.

APs—Tunnels Tab

The **Tunnels** tab provides two information on the following two sections:

VPNC

The **VPNC** tab provides information on VPN connections associated with the Virtual Controller along with information on the tunnels and the data usage through each of the tunnels. The VPN tab displays the following details:

Tunnels

The **Tunnels** table displays information on tunnels with the following columns:

- **Tunnel**—The type of the tunnels used in the VPN. For example, Primary, Secondary, or Backup.
- **Status**—The status of the tunnel.
- **Source**—The source address of the tunnel.
- **Destination**—The destination address of the tunnel.

Throughput Usage Per VPN

The **Throughput Usage Per VPN** graph indicates the successful data usage per VPN in Mbps for the primary or backup tunnel selected from the drop-down list. The **Throughput Usage Per VPN** displays a linear graph of sent and received data in the virtual private network.

Packet Loss

The **Packet Loss** graph indicates the percentage based on the number of packets lost during the data transmission in the VPN.



The **Tunnels** tab is displayed in the AP details page corresponding to Virtual Controllers only. This tab is not displayed for AP details page corresponding to slave or individual APs.

Gateway

The **Gateway** tab provides information on the gateways to which the AP is connected. The tab displays the following details:

Tunnels Summary

The **Tunnels Summary** section displays information on tunnels with the following details:

- **Total**—Total tunnels established.
- **Up**—Number of tunnels currently active.
- **Down**—Number of tunnels currently inactive.

The **Gateway** tab includes a table with the following tunnel details:

- **Gateway**—The name of the Gateway.
- **IP Address**—The IP address of the Gateway device.
- **Tunnel Status**—The status of the tunnel.
- **Tunnel Uptime**—The duration of the tunnel in active mode.
- **Last Key Received Time**—The time at which the Gateway key was received in order to establish a connection.

APs—Location Tab

The **Location** tab displays a sitemap or the floor plan showing the current location of the Instant AP device. The sitemap is derived from the Visual RF application, if Visual RF service is enabled for the Aruba Central account.

You can also edit the location of the Instant AP device by clicking the edit icon provided next to the address in the **Location** tab.

APs—Alerts & Events Tab

The **Alerts & Events** tab in the left navigation pane displays the total number of alerts, audit logs, and events generated for the AP. For more information, see [Access Point Alerts](#)

APs—Actions

The **Actions** tab displays the following list of actions that can be performed on the AP device. The **Actions** tab displays the following tasks that can be performed on the AP:

- **Reboot AP**—To reboot the AP. Clicking this option displays a confirmation message stating that all clients connected to the device will be disconnected. Click **Yes** to reboot the AP.
- **Reboot Swarm**—To reboot the AP cluster. Clicking this option displays the **APs in the swarm will reboot and all clients connected to those will be disconnected** confirmation message. Click **Yes** to reboot the swarm.
- **Tech. Support**—To enable the administrators to generate a tech support dump required for troubleshooting the device. Clicking the **Tech.Support** option displays the **Maintenance > Tools** page of Aruba Central.
- **Console**—To open the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device. Remote console access is supported only on VCs.




If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Live Instant AP Monitoring

Aruba Central supports live monitoring of AP details page corresponding to Instant APs that support Aruba Instant 8.4.0.0 firmware version and above. Aruba Central allows you to monitor live data that are updated in every 5 seconds, in the AP details page.

Enabling and Disabling Live Monitoring

To view the AP details page in a live-mode, perform the following steps:

1. In the **Network Operations** app, use the filter bar to select **All Devices**.
2. Under **Manage**, click **Devices > Access Points**. The AP dashboard is displayed.
3. Click the  list icon to display the AP list page.
4. The AP list page is displayed.



The Live Monitoring feature is not applicable for offline Instant APs.

5. Click the Instant AP entry in the **Access Points** table that supports Aruba Instant 8.4.0.0 firmware version and above. The AP details page is displayed.
6. Click the **Go Live** button at the right corner of the page to view live data.

The **Go Live** button remains grayed-out for all the AP details that are not associated with Instant AP devices running Aruba Instant 8.4.0.0 firmware version and above.



Aruba Central allows you to monitor live data for 15 minutes. After this time frame, Aruba Central reverts to the AP details page in a non-live mode to display the monitoring details for the time selected in the Time Range Filter. For more information on AP details page in a non-live mode, see [APs](#).

7. Click the **Stop Live** button manually to switch to the non-live mode.

AP Details in Go Live Mode

Clicking the **Go Live** button displays a page with the following two tabs:

Table 41: *AP Details in Go Live Mode*

| Card | Description |
|-----------------|--|
| Overview | Displays live data related to the radios of the Instant AP such as the radio mode, channels or bands of the radios, and the transmission power for each of the radios in the Mode , Channel/Band , and TX Power fields, respectively. This tab displays constant data until there are any changes to the state of radios such as the power value, channel value, and so on. |
| RF | Displays live graphs based on noise floor, frames, channel quality of the neighboring RF devices for 15 minutes or till the Stop Live button is clicked. This tab displays graphs in the Noise Floor , Frames , and Channel Quality cards for both 5 GHz and 2.4 GHz radios. |

Aruba Central allows you to monitor live data for 15 minutes. After this time frame, Aruba Central begins to display the monitoring details for the time selected in the Time Range Filter. For more information on AP Details page in a non-live mode, see [APs](#).



In **Go Live** mode, AP Details page updates and displays data for every 5 seconds.

The time range selected in the Time Range Filter becomes non-applicable when the **Go Live** button is enabled.


You can monitor one or more AP Details pages simultaneously on different tabs.

Renaming an AP

You can change the name of an AP provisioned in Aruba Central. The AP can be online or offline. When you rename an AP or a VC, the AP or VC does not reboot, and the client traffic is not affected. The new name must be a character string of up to 32 ASCII or non-ASCII characters, including spaces.

To rename an AP, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or Virtual Controller.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  **Configuration** icon to display the AP configuration dashboard.

4. Click the **Access Points** tab.

The **Access Points** page is displayed.

5. Hover the mouse over the AP or VC that you want to rename from the **Access Points** table.

6. Click the corresponding edit icon in the row.

The edit pane for modifying the AP parameters is displayed.

7. Under **Basic Info**, modify the AP or VC name in the **Name** field.

8. Click **Save Settings**.



The AP name is updated on the AP immediately. It might take up to 1 minute for the new AP name to get reflected in Central.



Renaming an AP depends on various privileges and access permissions that are assigned to each user to make configuration changes. For more information on various types of users and their respective roles, see [Users and Roles](#).

Deleting an Offline AP

To delete an offline AP:

1. In the **Network Operations** app, use the filter to select a group that has APs.
2. Under **Manage**, click **Devices > Access Points** to view the AP dashboard.
3. In the list view, click **Down** to view the list of offline APs in the **Access Points** table.
4. In the **Access Points** table, hover over the offline AP that you want to delete.



Clicking on the **Device Name** column displays the corresponding AP details page.

5. Click the corresponding delete icon in the row.


6. Click **Yes** in the resultant dialog box.

Monitoring Switches and Switch Stacks

The switch monitoring details are displayed on the switch dashboard and the switch details page. The switch dashboard and the switch details page are accessed from the **Network Operations** app.

The switch dashboard displays details about the health and status of switches and switch stacks. The switch details are provisioned and managed through Aruba Central. The switch dashboard displays the details in a chart and list view.



To view the switch list and chart details:

1. In the **Network Operations** app, use the filter to select a group that has switches.
2. Under **Manage**, click **Device(s) > Switches** to view the switch dashboard.
3. Click the  list icon to view the list of switches and their properties. The list view displays the following tabs:
 - **Switches**—Lists the details of both online and offline switches.
 - **Up**—Lists the details of switches that are currently up and connected to Aruba Central.
 - **Down**—Lists the details of switches that are currently down or not connected to Aruba Central.



The online switches are displayed with a green dot and offline switches are displayed with a red dot.


These tabs display the following details in a table:

- **Device Name**—Name of the switch or switch stack. For a switch stack, a stack icon is displayed next to the device name.
 - **Clients**—Number of clients connected.
 - **Alerts**—Number of alerts from the switch or switch stack.
 - **Model**—Model number of the switch. For a switch stack, the term **Stack** is displayed.
 - **Config Status**—configuration status of the switch or switch stack.
 - **Last Seen**—Date and time when the switch or switch stack was last connected.
 - **Usage**—Data usage on the switches.
 - **IP Address**—IP address of the switch or switch stack.
 - **MAC**—MAC address of the switch or switch stack.
 - **Firmware Version**—Firmware version of the switch or switch stack.
 - **Group**—Name of the group to which the switch is assigned.
 - **Labels**—Name of the label associated with the switch or switch stack.
 - **Site**—Site in which the switch or switch stack is provisioned.
 - **Uptime**—Duration for which the switch is operational.
 - **Serial/Stack ID**—Serial number of the switch or switch stack.
 - **Uplink Ports**—Uplink ports configured on the switch or switch stack.
 - **Port Utilization**—Utilization percentage of the port.
4. To download the switch details as a .csv file, click the  icon and click **Download CSV**. If the table contains unicode value, you must use a UTF-8 enabled software to view the contents. To view the file, open the file in a Microsoft Excel spreadsheet software.
 5. Click the  summary icon for a graphical view of the switch operations. The following information is displayed:
 - **Usage**—Indicates aggregate client data traffic detected on the switches.
 - **Clients**—Indicates the number of clients connected to the switch.
 6. To set the charts to show data for specific duration, use the options in the time range filter. By default, the data is displayed for a duration of 3 hours. To view the graphs for different durations, click the time

filter icon and select a time range of your choice. You can view data for 3 hours, 1 day, 1 week, 1 month, or 3 months.

Switch Details

To view the switch monitoring details:

1. In the **Network Operations** app, use the filter to select a group that has switches.
2. Under **Manage**, click **Device(s) > Switches** to view the switch dashboard.
3. Click the  list icon to view the list of switches and their properties.
4. In the **Device Name** column, click the name of the switch to view the details.

The **Switch Details** page is displayed with the following information:

- Header panel provides the following details:
 - **Operational status of the switch**—Displays a message describing the number of days since the last downtime of the switch. For example, No downtime in the last 3 days.
 - **Device Health**—Displays the health status of the switch as **Good** or **Bad**, which is measured based on the CPU and memory utilization of the switch. Hover over the status displayed to see the percentage of CPU and memory utilization.
- [Switches—Overview Tab](#)
- [Switches—Ports Tab](#)
- [Switches—PoE Tab](#)
- [Switches—VLANs Tab](#)
- [Switches—Routing Tab](#)
- [Switches—Hardware Tab](#)
- [Switches—Connected Tab](#)
- [Switches—Actions](#)

Switches—Overview Tab

The **Overview** tab provides a summary of the switch device details, network details, ports, hardware, uplink graph, usage graph, and details about the stack members.

Switch

The **Switch** section displays the following details:

- **Model**—Hardware model of the switch.
- **Location**—Current location of the switch.
- **Contact**—E-mail address of the contact person.
- **Commander**—Name of the commander switch.
- **Serial**—Serial number of the switch.
- **Uptime**—Time duration for which the switches are operational.
- **configuration**—configuration status of the switch.
- **Firmware Version**—Firmware version of the switch. If an updated version is available, the version number is displayed and you can click the link to navigate to the firmware management page and upgrade the firmware.
- **J-Number**—Part number of the switch.
- **MAC Address**—MAC address of the switch
- **Last Reboot**—Timestamp of when the switch was last rebooted.

- **Last Stats Received**—Timestamp of when the last statistics were received.
- **Firmware Status**—Displays whether a new firmware version is available.
- **Last Updated**—Timestamp of when the switch firmware was last changed.

Figure 22 *Switch Overview*

| SWITCH | | | |
|---|---|---|---------------------------------------|
| MODEL HP2920-24G-PoE+ Switch | J-NUMBER J9727A | LOCATION -- | CONTACT -- |
| SERIAL SG75FLX9HM | MAC ADDRESS f4:03:43:d4:2d:00 | UPTIME 46 Days 21 Hours 58 Minutes | LAST REBOOT Oct 04, 2019, 02:12:20 |
| CONFIGURATION Not in sync Last Sync: Nov 19, 2019, 17:11:20 | LAST STATS RECEIVED 20 Nov 2019 00:10:47 | FIRMWARE VERSION 16.06.0006 Update Available - 16.10.0002 | |
| GROUP Branch-2 | SITE AI-Testing | LABEL(S) -- | |

Network

The **Network** section displays the following details:

- **IP Address**—IP address of the switch.
- **Primary VLAN**—Default VLAN ID of the switch.
- **Stack/Standalone**—Indicates whether the switch is part of a stack or if it is a standalone switch.
- **Stack Members**—Total number of members in the stack.
- **Stack Topology**—Topology of the stack.
- **Stack ID**—Stack ID used to identify the stack.

Figure 23 *Network Details*

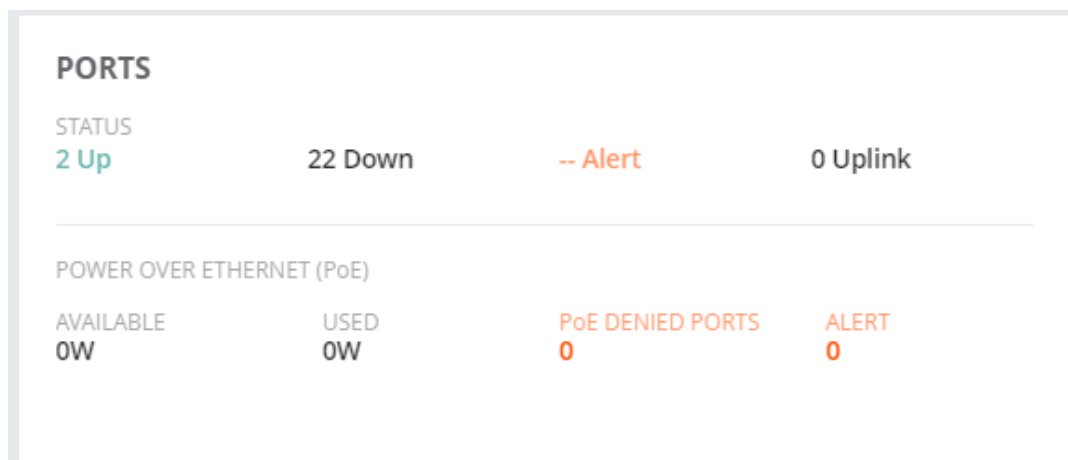
| NETWORK | | |
|--------------------------------|-------------------|----------------------|
| IP ADDRESS 10.8.130.249 | DEFAULT VLAN 1 | MANAGEMENT VLAN 1 |
| STACK/STANDALONE STANDALONE | | |

Ports

The **Ports** section displays the following details:

- **Status**—Number of ports in Up and Down state, and number of alerts.
- **Power Over Ethernet (PoE)**—Number of PoE ports enabled and disabled, and number of alerts.

Figure 24 *Port Summary*

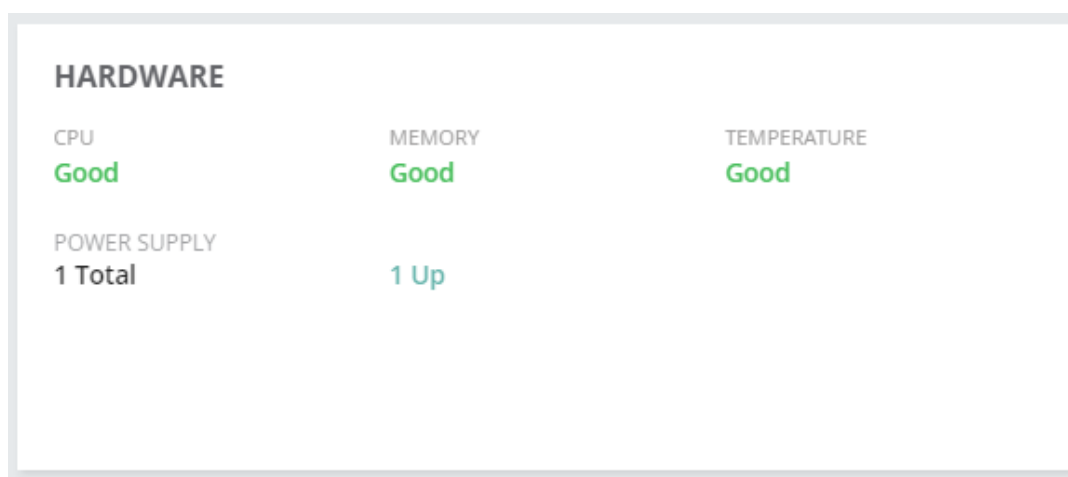


Hardware

The **Hardware** section displays the following details:

- **Power Supply**—Total number of power supplies and number of power supplies in Up state.
- **CPU**—CPU utilization status.
- **Memory**—Memory utilization status.
- **Temperature**—Temperature status. Hover your mouse over the status to view the temperature data.

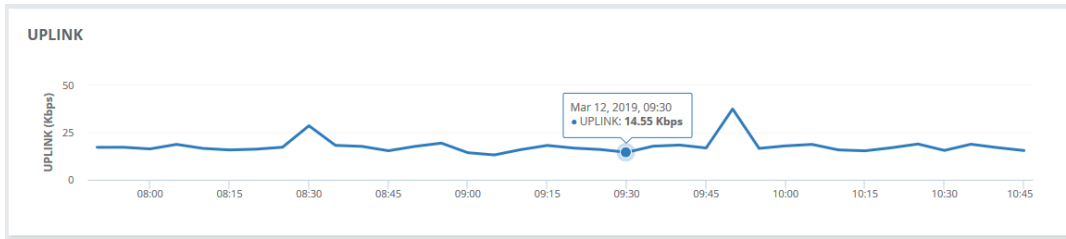
Figure 25 *Hardware Details*



Uplink

The **Uplink** section displays the uplink rate (bps) trend chart for the duration specified in the **Temporal sFilter**. Hover your mouse over the trend chart to view the uplink rate at a particular time.

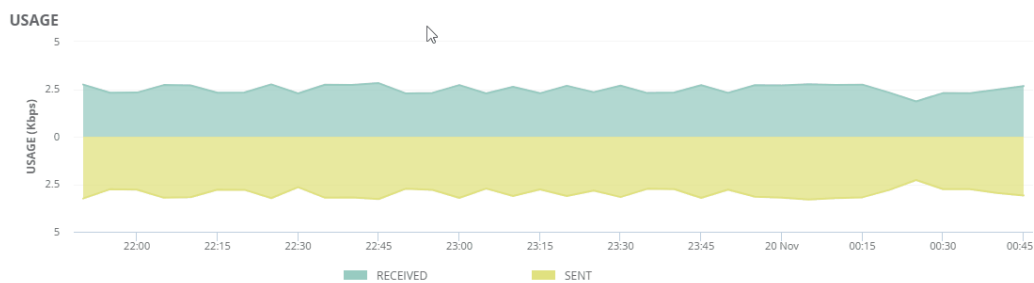
Figure 26 Uplink Trend Chart



Usage

The **Usage** section displays the trend chart for client data traffic detected on the switch. Hover your mouse over the trend chart to view data transmitted and received at a particular time.

Figure 27 Usage Graph



Stack Members

The **Stack Members** table displays the following details:

- Name of the stack member. Click on the name to navigate to the corresponding switch details page.
- Member ID.
- Model number.
- MAC address.
- Serial number.
- Role of the stack member—Commander or Standby.
- Status.
- Priority.

Figure 28 Stack Members Table

| STACK MEMBERS | | | | | | | |
|----------------------------------|-----------|------------------------|-------------------|------------|-----------|--------|----------|
| NAME | MEMBER ID | MODEL | MAC ADDRESS | SERIAL | ROLE | STATUS | PRIORITY |
| C2-2920-1-CMDR-1 | 1 | HP2920-24G-PoE+ Swi... | 14:58:d0:99:75:40 | SG48FLXYV7 | Commander | Down | |
| C2-2920-1-STBY-2 | 2 | HP2920-24G-PoE+ Swi... | 14:58:d0:99:96:80 | SG48FLXYVJ | Standby | Down | |

Switches—Ports Tab

The **Ports** tab displays the summary of ports, switch faceplate, and ports table.



To view a visual representation of the **Ports** tab, click [here](#).

Port Status

The **Port Status** section displays the total number of ports for the following:

- **Up**—Ports in up state
- **Down**—Ports in down state
- **Alert**—Alerts generated
- **Uplink**—Uplink ports

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover your mouse over the port to view the following details: port number, port name, type, speed, and trunk group.

Ports

The **Ports** table displays the following details:

- **Port**—Port number. Use the column filter to search for a particular port and use the sort option to sort the ports in ascending or descending order.
- **Name**—Name of the switch.
- **Status**—Status of the switch. Use the column filter to filter by status.
- **Type**—Type of switch port. Use the column filter to filter by type.
- **MTU (Bytes)**—MTU size of the switch.
- **Port Speed (Mbps)**—Port speed of the switch.
- **Trunk Group**—If the port is part of a trunk group, the name of the trunk group is displayed.
- **Mode**—Operational mode of the port.
- **Admin**—Admin status of the switch.
- **MAC Address**—MAC address of the switch.

Viewing Port-Level Information

Use one of the following options to navigate to the port and view port-level information:

- In the switch faceplate, click on the port number.
- In the Ports table, click the port number.

The port-level information page consists of the following sections:

- **Status**—The **Status** section displays the following details:
 - Operational status
 - Admin status
 - Type of port
 - Description
 - MAC address

- Name
- Untagged VLAN
- Trunk group
- Data received
- Data transmitted
- **Port Usage**—The **Port Usage** section provides a graphical representation of data received and transmitted by the port. Each line in the graph is a sum of the received and sent traffic for a given uplink port. Hover over the graph to view data for a particular time of the day.
- **Frame Counters**—The **Frame Counters** section provides a graphical representation of the interface frame counters. From the drop-down list, select one of the following options: **Unicast**, **Broadcast**, **Multicast**, **Discards**, or **Error**.

Switches—PoE Tab

The **PoE** tab displays details such as PoE status summary, PoE ports, and PoE consumption.



The **PoE** tab displays monitoring data only if the switch firmware version is 16.08.0001 or later.

PoE Status

The **PoE Status** section displays the following details:

- **Available**—Power available for consumption for the switch or stack.
- **Used**—Power used by various devices.
- **Remaining**—Power remaining to be utilized in the stack or device.
- **PoE Denied Ports**—Number of ports for which power is denied.

Faceplate

If the switch is a standalone switch, the faceplate of the switch is displayed. For a switch stack, faceplate of all the switches part of the stack is displayed. From the faceplate, click on the port to drill down and view port-level information. On the switch faceplate, hover your mouse over the PoE port to view the following details: port number, port name, type, class, and priority.

From the **Context** drop-down list, select the context:

- **POE-STATUS**—Displays the state of each port. The state can be: Uplink, Drawing, Enabled, Disabled, or Alert.
- **POE-CLASS**—Power class of the PoE port. The class can be: 0, 1, 2, 3, 4, or 5.
- **POE PRIORITY**—PoE priority configured on the port. The priority can be: Critical, High, or Low.



For a visual representation of how to set the context on the faceplate, click [here](#).

Ports PoE

The **Ports PoE** table displays the following details:

- **Port**—Port number.
- **PoE**—PoE state: Enabled or Disabled.
- **Class**—Power class of the PoE port.
- **Priority**—PoE priority: Critical, High, or Low.
- **Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.

- **Pre-STD Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
- **Alloc Actual**—Power actually being used on the port.
- **Alloc Configured**—The maximum amount of power allocated for the port.
- **PLC Type**—Physical layer classification type.

PoE Consumption

The **PoE Consumption** section displays a trend chart for the PoE power drawn from the Switch in watts. Hover your mouse over the trend chart to view the PoE power drawn at a particular time. For a stack, select the switch from the drop-down list to view the PoE consumption for the specific device.



For a visual representation of how to view PoE consumption for a switch stack, click [here](#).

Viewing PoE Port-Level Information

Use one of the following options to navigate to the PoE port and view port-level information:

- In the switch faceplate, click on the port number.
- In the **Ports PoE** table, click the port number.



For a visual representation of how to navigate to the PoE port level, click [here](#).

The port-level information page consists of the following tabs:

- [Summary](#)
- [Slot Info & PoE configuration](#)
- [LLDP Information](#)

Summary

The **Summary** tab consists of the following sections:

- **Summary**—Displays the following details:
 - **PSE Reserved Power**—Power reserved for the port in the Power Sourcing Equipment (PSE).
 - **PSE Voltage**—Total voltage, in volts (V), currently being delivered to the powered device connected to the port
 - **PD Power Draw**—Power drawn by the powered device.
 - **PD Amperage Draw**—Amperage drawn by the powered device.
 - **Over Current Count**—Number of times a powered device connected to the port attempted to draw more power than was allocated to the port.
 - **MPS Absent Count**—Number of times the powered device has no longer requested power from the port MPS is Maintenance Power Signature.
 - **Power Denied Count**—Number of power requests from the port that were denied because sufficient power was unavailable.
 - **Short Count**—Number of times the switch provided insufficient current to the powered device connected to the port.
- **PoE Consumption**—Displays the trend chart for PoE consumption and power available for the duration specified in the **Temporal Filter**.

Slot Info & PoE configuration

The **Slot Info & PoE configuration** tab consists of the following sections:

- **PoE Slot Information**—Displays the following details:
 - **Slot**—Slot where the port is located.
 - **Operation Status**—Displays PoE power is available for the slot: On, Off, or Faulty.
 - **Maximum Power**—Maximum PoE wattage available to provision active PoE ports in the slot.
 - **Power In Use**—PoE power currently being used by the slot.
 - **Usage Threshold**—Configured percentage of available PoE power provisioning the switch must exceed to generate a usage notice.
- **PoE configuration**—Displays the following details:
 - **PoE Power**—Displays whether PoE power is enabled on the port.
 - **Pre-Std Detect**—Displays whether PoE for pre-802.3af-standard powered devices is enabled on the switch: On or Off.
 - **PoE Port Status**—Current power status of the PoE port: Searching, Delivering, Disabled, or Fault.
 - **Power Priority**—Power priority configured on ports enabled for PoE: Low, High, or Critical.
 - **PLC Class Type**—Physical layer classification type.
 - **DLC Class Type**—Data link layer classification type.
 - **Configured Type**—If configured, shows the user-specified identifier for the port. If not configured, this field is empty.
 - **PoE Value configuration**—PoE power value configured for the port.

LLDP Information

The **LLDP Information** tab displays the following details:

- **PSE Allocated Power**—Power allocated for the port in the PSE.
- **PD Requested Power**—Power requested by the powered device.

Switches—VLANs Tab

The VLANs tab consists of the following sections:

- VLANs table
- Faceplate of the switch or switch stack

VLANs

The **VLANs** table displays the following details:

- **Name**—Displays the name of the VLAN. Click the sort icon to sort the VLAN names in the column.
- **ID**—Displays the VLAN ID associated with the VLAN.
- **Status**—Displays the status of the VLAN as Up or Down.
- **Type**—Displays the following types of VLANs:
 - **Regular VLAN**—A regular VLAN is a single broadcast domain.
 - **Private-Primary**—The regular VLAN which partitions one broadcast domain into multiple smaller broadcast sub-domains.
 - **Private-isolated**—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.

- **Private-Community**—Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN**—Displays the primary VLAN details.
- **Promiscuous**—Displays the promiscuous port value. A promiscuous port is a switch port that is connected to an uplink router, firewall, or other common gateway device, and can communicate with all ports within a private VLAN, including the ports in the isolated and community VLANs. By default, every primary VLAN port acts as a promiscuous port.
- **ISL**—Displays the Inter-switch Link port value (range). ISL port is also called PVLAN member port. ISL port is required in multi-switch PVLAN configurations to span the switches. The ISL port will automatically become a member of all VLANs within the PVLAN and it carries traffic from the primary VLAN and all secondary VLANs.
- **Tagged Ports**—Displays the ports that have marked the VLAN as tagged.
- **Untagged Ports**—Displays the ports that have marked the VLAN as untagged.
- **IP address**—Displays the IP address of the VLAN.
- **Voice**—Displays whether the Voice is enabled or disabled for the VLAN.
- **IGMP**—Displays whether the IGMP is enabled or disabled for the VLAN.
- **Jumbo**—Displays whether the Jumbo packets are enabled or disabled for the VLAN.

Faceplate

From the **VLANs** table, select a VLAN to view the tagged and untagged ports, promiscuous port, ISL port and the VLAN types in the faceplate.

The following is an illustration of the VLANs tab:

VLANs

| NAME | ID | STAT... | TAGGED PORTS | UNTAGGED PORTS | IP ADDRESS | VOICE | IGMP |
|--------------|----|---------|--------------|----------------|------------|----------|------|
| DEFAULT_VLAN | 1 | Up | | 1-24 | | DISABLED | -- |

PORTS FOR DEFAULT_VLAN
Check tagged and untagged port for a VLAN

Note: TAGGED ports are decorated with the P symbol. Other parts of the VLAN are UNTAGGED.

Legend: ■ VLAN PORT

aruba SWITCH 2920

Ports 1-24 are shown as green squares. Ports 1-11 are also marked with a 'P' symbol, indicating they are tagged ports.

Switches—Routing Tab



The **Routing** tab is displayed for the switches that run the firmware version 16.09 or later.

The **Routing** tab displays the following details:

- An overview of the routing information including:
 - **Total**—Displays the total number of routes on the switch.
 - **Static**—Displays the total number of static routes on the switch.
 - **Connected**—Displays the total number of connected routes on the switch.
- The routing details in the **Routing** table.

Routing

The **Routing** table displays the following details:

- **Destination**—Displays the network address of the destination route.
- **Gateway**—Displays the IP address of the gateway.
- **VLAN**—Displays the VLAN ID of the route destination.
- **Type**—Displays the following types of routes:
 - **Static**—The routes that are manually added to the routing table in the switch.
 - **Connected**—The routes that are directly connected to the interface.
- **Sub Type**—Displays the subtype of the route as Internal or External.
- **Metric**—Displays the measure used to calculate the best path to reach the destination. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.
- **Distance**—Displays the administrative distance of the route. The administrative distance helps routers determine the best route when there are multiple routes to the destination.



The routing information is displayed from the Aruba 3810 Series and Aruba 5400R switches in the network. The details displayed on the **Routing** tab are refreshed every five minutes.

Switches—Hardware Tab

The **Hardware** tab displays information related to power supplies, fans, utilization and temperature.

Hardware

The **Hardware** table displays the overall hardware summary:

- **ID**—Identity of the hardware.
- **Name**—Name of the device.
- **Power Supplies**
 - **Total**—Total number of power supplies.
 - **Up**—Number of power supplies in Up state.
 - **Down**—Number of power supplies in Down state.
- **Fans**
 - **Total**—Total number of fans.
 - **Up**—Number of fans in Up state.
 - **Down**—Number of fans in Down state.
- **Utilization**
 - **CPU**—Current CPU utilization percentage.
 - **Memory**—Current memory utilization percentage.
- **Temperature**

- **Current**—Current temperature.
- **Min**—Minimum temperature.
- **Max**—Maximum temperature.

Power Supplies

The **Power Supplies** table displays the following details:

- **Name**—Name of the power supply.
- **Status**—Current status of the power supply.

Fans

The **Fans** table displays the following details:

- **Name** —Name of the fan.
- **Status**—Current status of the fan.

CPU

The **CPU** section displays the current CPU utilization percentage and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the CPU utilization at a particular time.

Memory

The **Memory** section displays the current memory utilization percentage and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the memory utilization at a particular time.

Temperature

The **Temperature** section displays the current, minimum, and maximum temperature and trend chart for the duration specified in the **Temporal Filter**. Hover your mouse over the trend chart to view the temperature at a particular time.

Switches—Connected Tab

The **Connected** tab displays the following details:

- An overview of client devices and neighbour devices:
 - Client Devices—Displays the total number of client devices on the switch.
 - Neighbour Devices—Displays the total number of neighbour devices on the switch.
- The details of the client devices in the **Client Devices** table.
- The details of the neighbour devices in the **Neighbour Devices** table.

The following sections provide more information about the details displayed in the tables.

Client Devices

The **Client Devices** table displays the following details:

- **Name**—Displays the name of the client device.
- **Status**—Displays the status of the client as Connected, Disconnected, Failed_to_disconnect or Blacklisted.
- **Port**—Displays the port number of the switch the client device is connected to.
- **MAC Address**—Displays the MAC address of the client device.
- **IP Address**—Displays the IP address of the client device.
- **VLAN ID**—Displays the VLAN ID of the client device.

- **VLAN Name**—Displays the VLAN name of the client device.
- **VLAN Type**—Displays the following VLAN types of the client device:
 - Normal—The subnetwork which can group devices on separate physical LANs.
 - Primary—The standard VLAN that is partitioned to create a private VLAN.
 - Isolated—Secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.
 - Community—Secondary VLAN that forwards traffic between ports which belong to the same community and to the promiscuous ports.
- **Primary VLAN ID**—Displays the primary VLAN ID of the client device.
- **Primary VLAN Name**—Displays the primary VLAN name of the client device.
- **Authentication**—Displays the authentication type of the client device.
- **Usage**—Displays the total data usage by the client device for the selected time period.



The wired client will show up in the **Client Devices** table only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

Neighbour Devices

The **Neighbour Devices** table displays the following details:

- **MAC Address**—Displays the MAC address of the neighboring device.
- **Hostname**—Displays the hostname of the neighboring device.
- **IP Address**—Displays the IP address of the neighboring device.
- **Description**—Displays the description of the neighboring device.
- **Local Port**—Displays the local port number of the neighboring device.
- **Remote Port**—Displays the remote port number of the neighboring device.
- **Capabilities**—Displays the capabilities of the neighboring device.
- **VLAN ID(s)**—Displays the VLAN IDs of the neighboring device.

Switches—Actions

The **Actions** tab displays the various options available for remote administration of the switch. The following options are available:


- **Reboot**—Reboots the switch
- **Tech Support**—Allows the administrators to generate a tech support dump for troubleshooting the device.
- **Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.



If the Copy and Paste function from the keyboard shortcut keys (CTRL+C and CTRL+V) do not work in your web browser, use the Copy and Paste functions available under the menu options in the web browser.

Deleting an Offline Switch

To delete an offline switch:

1. In the **Network Operations** app, use the filter to select a group that has switches.
2. Under **Manage**, click **Devices > Switches**.
3. Click the  list icon to view the list of switches.

4. Select the offline switch that you want to delete by clicking any column on the row except the **Device Name** column.




Clicking device name in the **Device Name** column opens the corresponding switch details page.

5. In the pop-up window, click **Actions > Delete**.
6. Click **Yes** in the **Confirm Action** dialog box.

Assigning Uplink Ports

To assign uplink port(s):

1. In the **Network Operations** app, use the filter to select a group that has switches.
2. Under **Manage**, click **Device(s)>Switches**.
3. Click the  list icon for list view of the switches.
4. Select the switch for which you want to assign uplink port(s) by clicking any column on the row except the **Device Name** column.



Clicking on the **Device Name** column opens the corresponding switch details page.

5. In the pop-up window, click **Uplinks**.




For offline switches, click **Actions > Uplinks** in the pop-up window.

6. In the **Assign Uplink Ports/Trunks** dialog box, click the **Assigned Uplink Ports/Trunks** drop-down list.
7. Select the port(s), and click **Assign**.

Gateways

The **Gateways** monitoring dashboard provides rich metrics about the health and status of the SD-WAN devices provisioned and managed through Aruba Central.

Page Views

1. To view the Gateways dashboard, in the **Network Operations** app, use the filter to select a Branch Gateway group.
2. Under **Manage**, click **Overview>Gateways**. Then, click the  chart icon.

The **Gateways** dashboard includes the following contents:

- **Usage**—Displays the overall usage metrics for the Gateways provisioned in your Aruba Central account.
 - **Usage**—Displays the incoming and outgoing data traffic in the WAN network.
 - **WAN Compression**—Displays the data packet compression statistics for the WAN network. You can view the compressed, uncompressed, and saved bandwidth. By default, traffic between the Branch Gateway and VPN Concentrator is subject to compression.

- **WAN Tag Provider Distribution**—Displays the number of online and offline uplinks per WAN provider.
- **WAN Type Provider Distribution**—Displays the number of online and offline uplinks per WAN circuit type.
- **WAN Transport Health**—Displays the Mean Opinion Score (MOS) score trends for each uplink for the selected time range. The uplink health trend is plotted using health indicators such as Good, Fair, and Poor.
- **Model Distribution**—Displays the total percentage of Gateways distributed per hardware platform.
- **Firmware Distribution**—Displays the total percentage of Gateways distributed by software versions.



You can select the time range (3 hours, 1 day, 1 week, 1 month or 3 months) from the **Time Range** filter.

Gateway Details Page

To view the details of a specific Gateway perform the following steps:

1. In the **Network Operations** app, use the filter to select a Branch Gateway .
2. Under **Manage**, click **Overview > Summary**. The **Gateway Details** page is displayed.

The dashboard provides detailed information about the Gateway operational status. Live monitoring provides real time status about the following details.



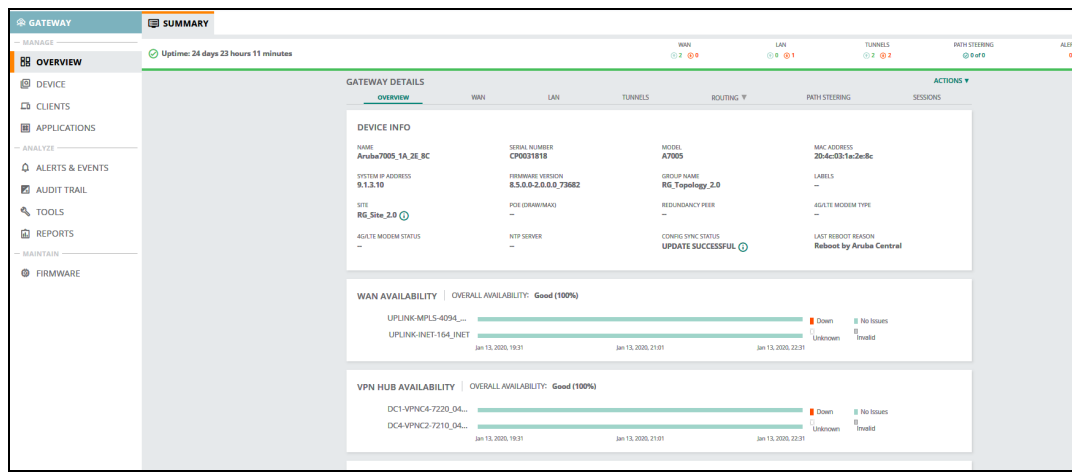
The default view of Gateways table shows only a few columns. To view the hidden columns, click the settings icon at the right side of the table. To reset the columns, click **Reset Columns**.

The header pane of the Gateways dashboard displays the following information:

- **Overview**
 - **Name**—Name of the Gateway. This column also includes a search filter to allow users to search for a Gateway.
 - **Serial Number**— Displays the serial number of the Gateway.
 - **Model**—Hardware model of the Gateway.
 - **MAC**—MAC address of the Gateway.
 - **System IP Address**—IP address of the Gateway.
 - **Firmware Version**—The current firmware revision of the Gateway.
 - **Group**—Group to which the Gateway is assigned.
 - **Labels**—Name of the label. Clicking the label name opens the per label details.
 - **Site**—Name of the site in which the Gateway is deployed.
 - **POE Draw/Max**—Displays the POE power drawn against the maximum allowed.
 - **Redundancy Peer**—Displays the status of the redundancy peer.
 - **4G/LTE Modem Type**—Displays the 4G modem type.
 - **4G/LTE Modem Status**—Displays the 4G modem status
 - **NTP Server**—Displays the NTP server details
 - **Config Sync Status**—Displays the configuration synchronization status.
 - **Last Reboot Reason**—Displays the reason for the last reboot.
 - **Uptime**—Displays the uptime of each Gateway.
 - **Serial**—Serial number of the Gateway.

- **WAN**—Displays the total number of WAN interfaces that are currently operational or down. On clicking a port, the dashboard displays WAN interface details.
- **LAN**—Displays the total number of LAN interfaces that are currently operational or down. On clicking a port, the dashboard displays LAN and VLAN interface details.
- **Tunnels**—Displays the total number of VPN tunnels that are currently active or down. On clicking a port tunnel, the dashboard displays VPN tunnel details.
- **Routing**—Displays details pertaining to the routing protocols such as BGP, OSPF, RIPv2 and Overlay.
- **Path Steering**—Displays the total number of path steering policies that are compliant with the performance criteria (SLAs) defined for each type of traffic.
- **Sessions**—Displays detailed information about the running sessions.

Figure 29 Summary page featuring the live monitoring status bar



Actions Drop-down List

The **Actions** drop-down list contains the following options:

- **Reboot Gateway**—Reboots the gateway.
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.
- **Clear IPsec SA**—Clears the IPsec Security Associations (SA).
- **Clear ISAKMP SA**—Clears the ISAKMP SA.

Tabs

The Gateway monitoring dashboard includes the following tab views:

- [Overview](#)
- [WAN](#)
- [LAN](#)
- [Tunnels](#)
- [Routing](#)
- [Path Steering](#)
- [Sessions](#)

Gateways—Overview Tab

After you onboard and configure the gateways, you can view the branch health, monitor the WAN uplink, and view gateway performance from the **Gateways** page.

1. In the **Network Operations** app, use the filter to select a Branch Gateway .
2. Under **Manage**, click **Overview > Summary**. The **Gateway Details** page is displayed.

The **Gateways** page displays the following details for the gateways that are deployed in the WAN network.

The **Overview** dashboard provides gateway device details, WAN availability and performance information, and the list of top applications. The **Overview** tab displays the following details:

Device Info

Figure 30 *Device Info*

| DEVICE INFO | | | |
|---|---|-----------------------|---|
| NAME VPN2-10-A7220_04_E6_B0 | GROUP NAME DC1 | MODEL A7220 | LOCATION -- |
| SERIAL NUMBER CW0006170 | POE (DRAW/MAX) -- | SITE -- | LABELS -- |
| MAC ADDRESS 00:1a:1e:04:e6:b0 | SYSTEM IP ADDRESS 1.1.1.2 | REDUNDANCY PEER -- | CURRENT FIRMWARE VERSION 8.4.0.0-bgp-dev_69145 |
| LAST REBOOT REASON Unknown reboot reason | CONFIG SYNC STATUS UPDATE SUCCESSFUL | | |

Displays the gateway device details. From the drop-down list, select **Overview** to view the following details:

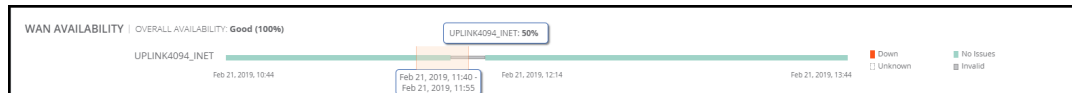
- **Name**—Name of the gateway.
- **Serial Number**—Serial number of the gateway.
- **MAC Address**—MAC address of the gateway.
- **Last Reboot Reason**—Reason for the last reboot.
- **Group Name**—Name of the group to which the gateway belongs.
- **POE (DRAW/MAX)**—The amount of power that the devices connected to the Branch Gateway consume and the maximum PoE power capacity. For example, if the value displayed is 6/120, the devices draw 6 watts and the maximum PoE power allocated is 120 watts.
- **System IP address**—IP address of the gateway.
- **Config Sync Status**—Status of the configuration sync.
- **Model**—Hardware model of the gateway.
- **Site**—Site name of the gateway location.
- **Redundancy Peer**—Displays the redundant gateway. Click the link to view the redundant gateway details. See the *Setting up Redundant Gateways for High Availability* section in the *Aruba Central Help Center*.
- **Location**—Physical location of the gateway.
- **Labels**—Labels attached to the gateway.
- **Current Firmware Version**—Firmware version running on the gateway.

The dashboard also displays additional overview information about WAN and VPN:

WAN Availability

Provides a graphical representation of the Branch Gateway's WAN uplink availability. The graph displays each WAN uplink availability for the selected time range. Availability is determined by default gateway, monitored IP, and data VPN Concentrator reachability.

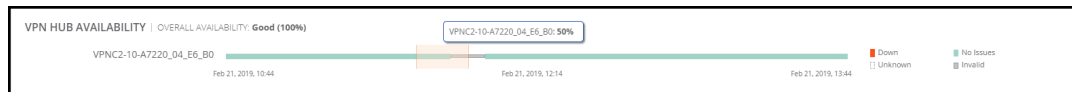
Figure 31 WAN Availability



VPN Hub Availability

Provides a graphical representation of the Branch Gateway's tunnel availability. Availability is determined by the probe settings configured using the **Health Check** option.

Figure 32 VPN Hub Availability



Aggregate WAN Usage

Displays the Branch Gateway's aggregate inbound and outbound traffic usage by WAN interface. Select one of the following options from the drop-down list:

Figure 33 Aggregate WAN Usage—All Traffic

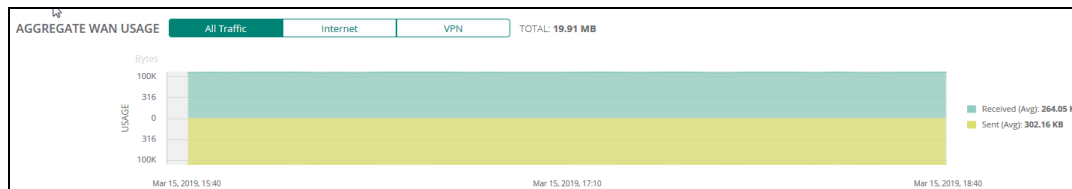


Figure 34 Aggregate WAN Usage—Internet

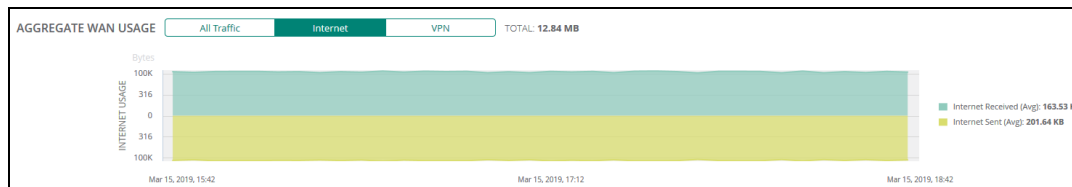
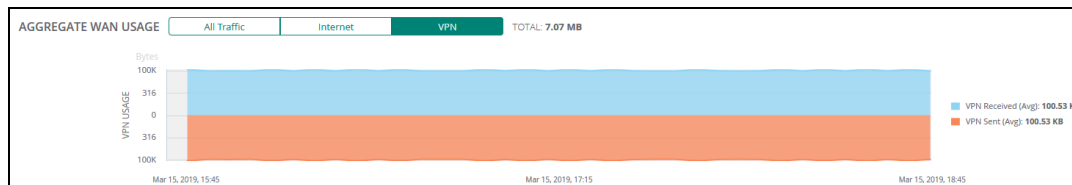


Figure 35 Aggregate WAN Usage—VPN



Aggregate WAN Compression

Displays the aggregate WAN compression details across all uplinks. The average bandwidth savings is displayed as a percentage. The compressed and uncompressed bandwidth is displayed as vertical grouped bar graphs. For more information about the process to enable data compression, see the *Configuring Uplink Interfaces* section in the *Aruba Central Help Center*.

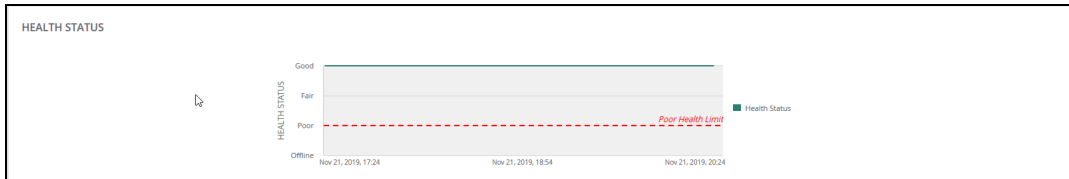
Figure 36 *Aggregate WAN Compression*



Health Status

Displays the health of the gateway in terms of CPU and memory usage.

Figure 37 *Health Status*



Gateway—WAN Tab

If the gateway is provisioned as a Branch Gateway, the **WAN** tab displays the following details:

- **Port Status**—Displays the WAN port status. Click a WAN port for more details.

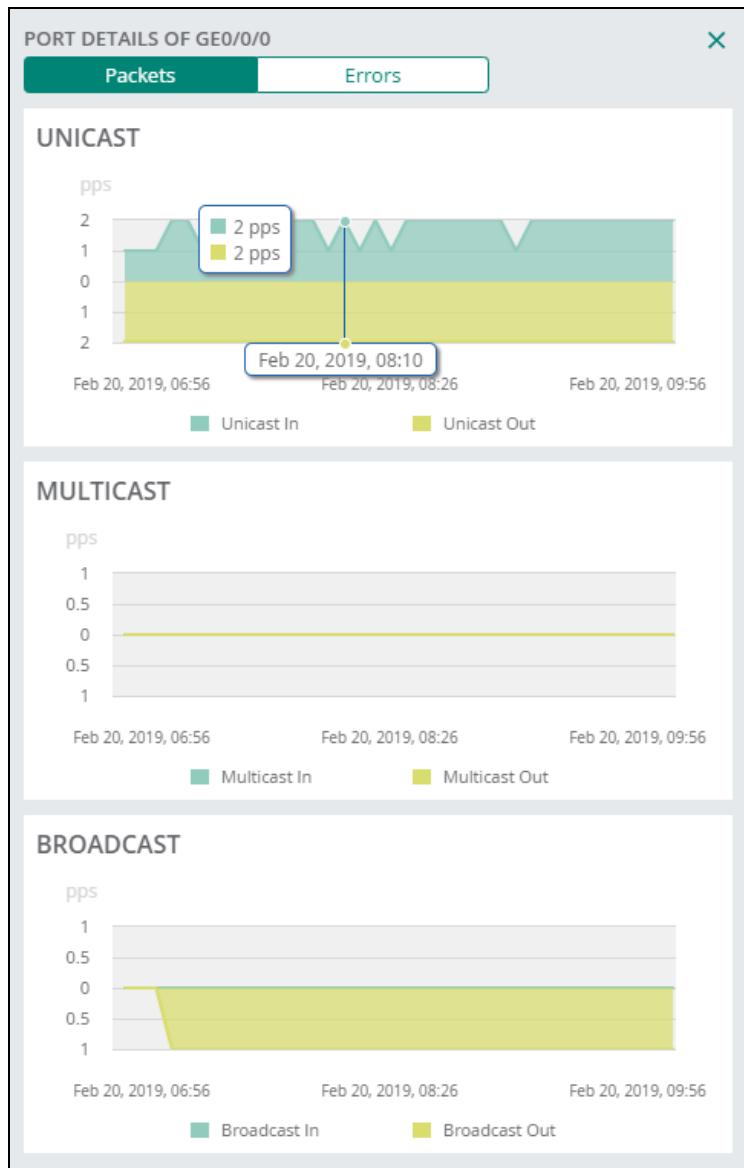
Figure 38 *Port Status*



In the **Port Status** table, click a port number to display the **Packets** and **Errors** details.

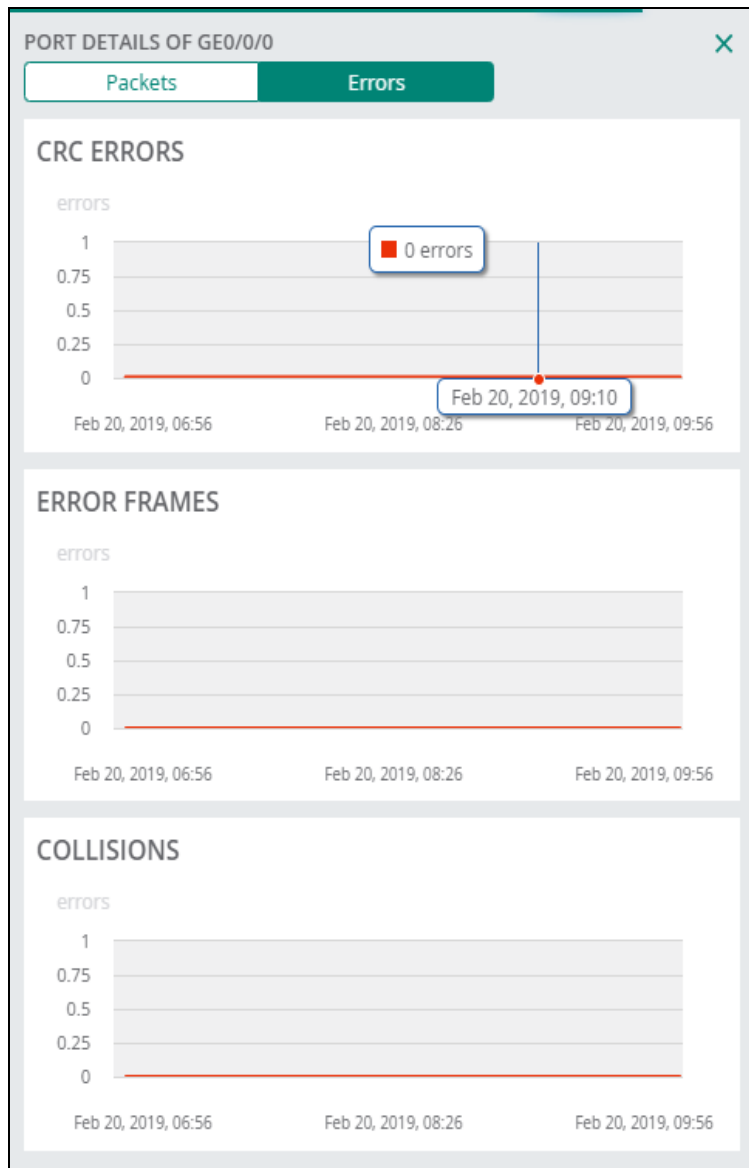
- The following graphs are displayed for the **Packets** interface:
 - **Unicast**—The number of unicast packets per second.
 - **Multicast**—The number of multicast packets per second.
 - **Broadcast**—The number of broadcast packets per second.

Figure 39 *Packet details of a port*



- The following graphs are displayed for the **Errors** interface:
 - **CRC Errors**—The number of cyclic redundancy errors logged.
 - **Error Frames**—The number of error frames logged.
 - **Collisions**—The number of collisions encountered.

Figure 40 Error details of a port



- **WAN Interfaces Summary**—The table lists the WAN interfaces and provides the total number of WAN interfaces. Displays the summary of WAN uplinks. The following details are displayed for the port:



Click the Settings icon to reset or set the default columns that are displayed.

- **Total WAN Interfaces**—Total number of WAN interfaces available.
- **Port**—Port number.
- **Provider Tag/Type**—Service provider uplink tag or type.
- **Type**—WAN interface type.
- **VLAN ID**—VLAN identification number.
- **Oper. State**—Operational status.
- **Loss**—Loss percentage.
- **Latency**—The latency in microseconds.
- **Private IP**—Private IP address.

- **Speed**—Indicated the type of connection, for example Auto, Full duplex or Half duplex.

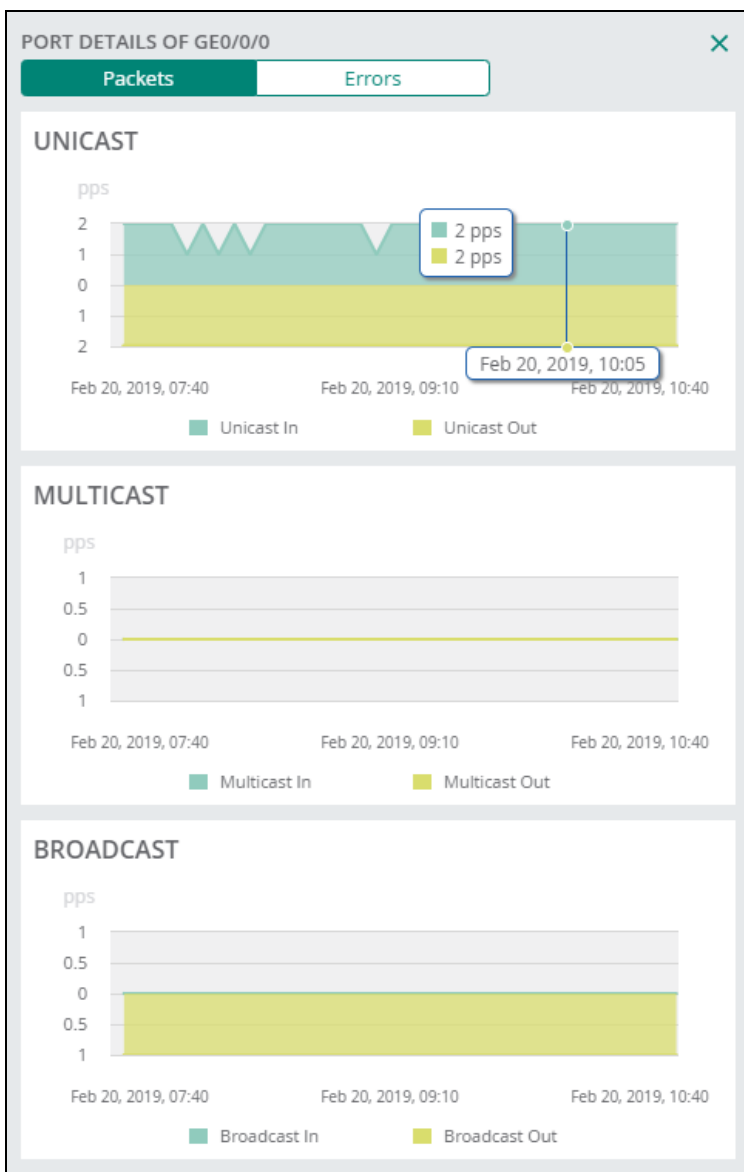
Figure 41 WAN interfaces summary

| WAN INTERFACES SUMMARY TOTAL WAN INTERFACES: 1 | | | | | | | | |
|--|---------------------|----------|---------|-------------|------|---------|----------------|------------|
| PORT | PROVIDER TAG/T... | TYPE | VLAN ID | OPER. STATE | LOSS | LATENCY | PRIVATE IP | SPEED |
| GE0/0/0 | uplink4094_internet | physical | 4094 | Up | 0 | 0.40% | 192.168.66.198 | 1 GbpsFull |

In the **WAN Interfaces Summary** table, click a port number to display the **Packets** and **Errors** details.

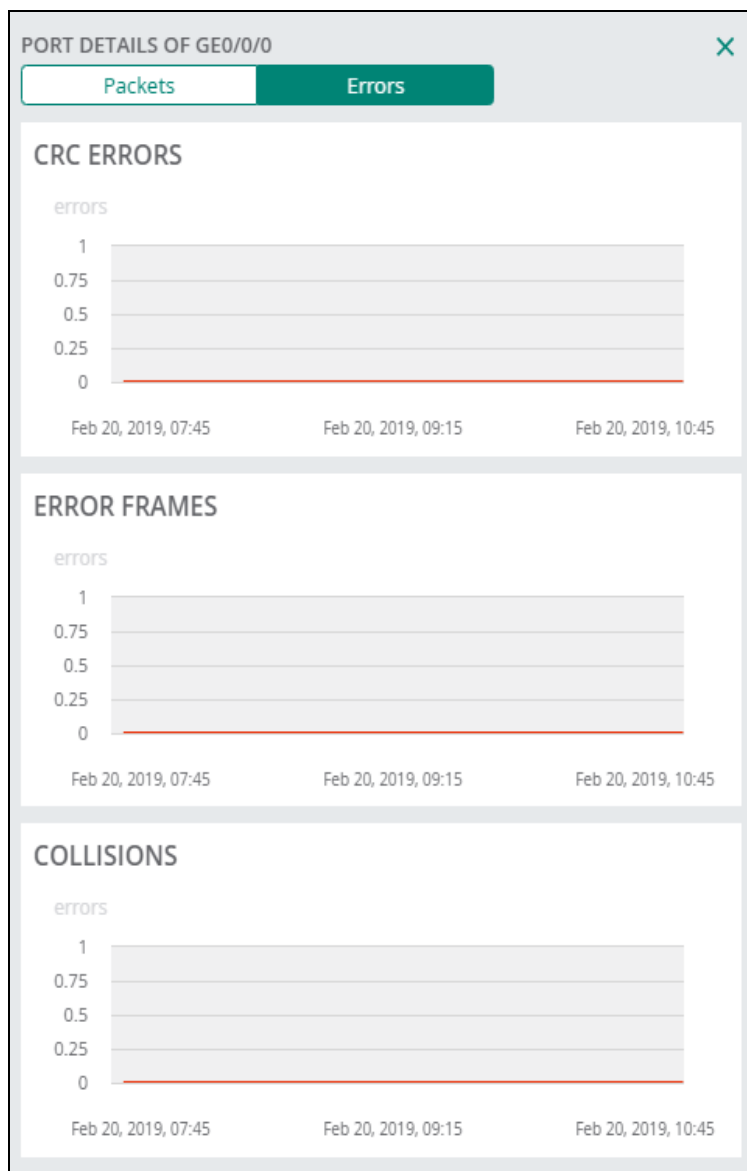
- The following graphs are displayed for the **Packets** interface:
 - **Unicast**—The number of unicast packets per second.
 - **Multicast**—The number of multicast packets per second.
 - **Broadcast**—The number of broadcast packets per second.

Figure 42 Packet details of an interface



- The following graphs are displayed for the **Errors** interface:
 - **CRC Errors**—The number of cyclic redundancy errors logged.
 - **Error Frames**—The number of error frames logged.
 - **Collisions**—The number of collisions encountered.

Figure 43 Error details of an interface



- **WAN Interface Details**—In the **WAN Interfaces Summary** table, select a **Provider Tag/Type** to view the WAN interface details.

The following details are displayed for the WAN interface:

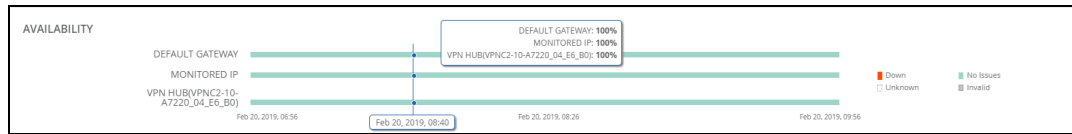
- **Status**—Operational status.
- **Provider Tag/Type**—Service provider uplink tag or type.
- **IP Address**—Private IP address.
- **Public IP Address**—Public IP address.
- **Default Gateway**—Default gateway.
- **Avg. MOS**—Indicates the transport health based on active monitoring probes. The field displays the average MOS score of all VPN probes.

Figure 44 WAN interface details

| WAN INTERFACES DETAILS UPLINK4094_INET/INTERNET ▼ | | | | | | |
|---|--------------------------|----------------|-------------------|-----------------|----------|--|
| STATUS | PROVIDER TAG/TYPE | IP ADDRESS | PUBLIC IP ADDRESS | DEFAULT GATEWAY | AVG. MOS | |
| UP | UPLINK4094_INET/INTERNET | 192.168.66.196 | 0.0.0.0 | 192.168.66.254 | 4.4 | |

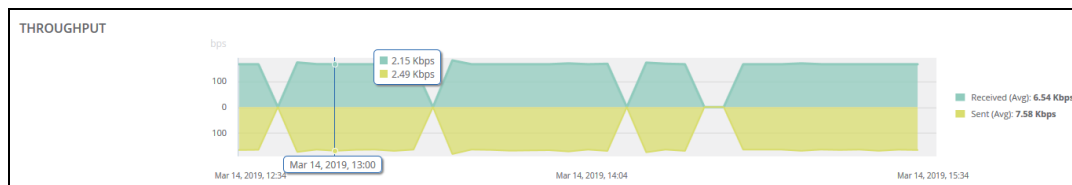
- **Availability**—Provides a graphical representation of the selected WAN interface's availability based on reachability. The graph shows the selected WAN port's ability to reach its default gateway, monitored IP, and VPN Concentrator.

Figure 45 *Availability of the interfaces*



- **Throughput**—Provides a graphical representation of the selected WAN interface's throughput. The graph displays the WAN interface's transmit and receive performance in Kbps.

Figure 46 *Throughput details*



- **WAN Usage**—Provides a snapshot of the WAN usage and is available for **All Traffic**, **Internet**, and **VPN** specific information. The graphs also display information that is sent and received.

Figure 47 *WAN Usage—All Traffic*

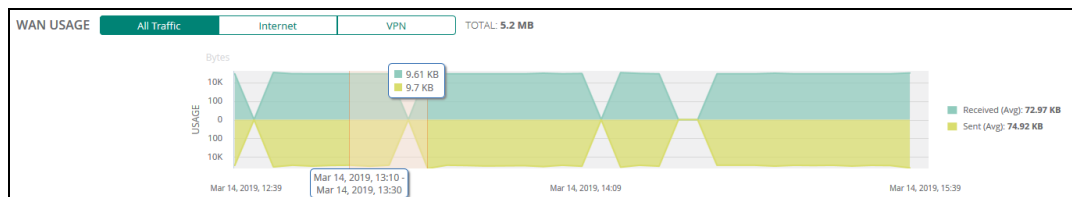


Figure 48 *WAN Usage—Internet*

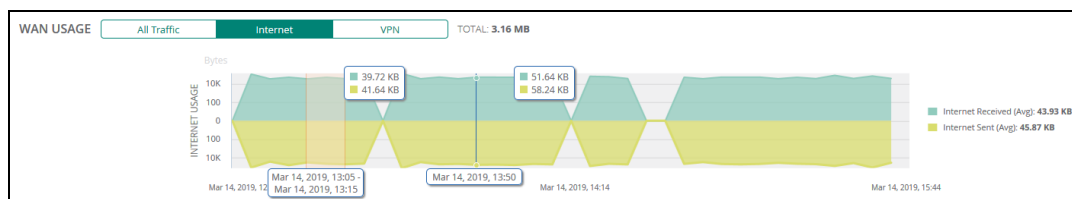
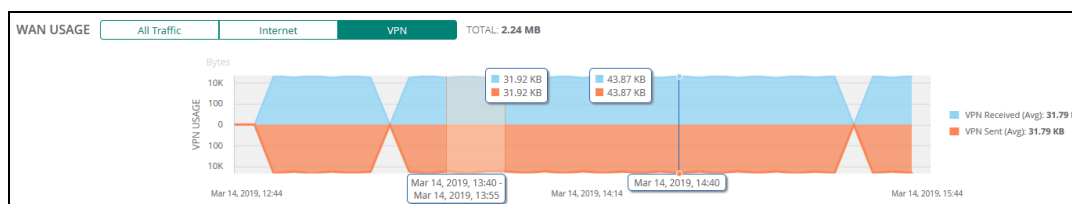


Figure 49 *WAN Usage—VPN*



- **WAN Compression**—Provides information on the percentage of optimized and non optimized packets and the average percentage of bandwidth saved.

Figure 50 WAN Compression information



- **Performance**—The Performance section displays the following details based on the interface that is selected:
 - **Latency**—The latency in milliseconds.
 - **Packet Loss**—Displays the packet loss in percentage.
 - **Jitter**—Displays the jitter in milliseconds.
 - **MOS Score**—Displays the MOS score.

Figure 51 Performance details



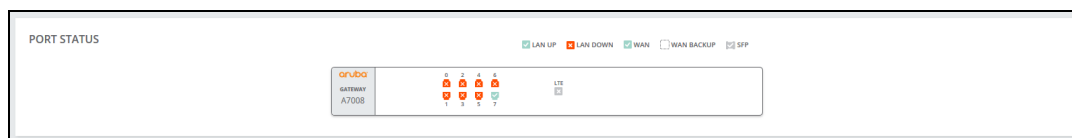
Live monitoring is enabled for sections that display the interface status, such as:

- The **Port Status**
- Operation state in the **WAN Interfaces Summary**
- Status of the **WAN Interfaces Details** and **Availability** graphs

Gateways—LAN Tab

- **Port Status**—Provides a graphical representation of the Branch gateway's LAN link availability. Also provides a quick view of the LAN port status. Click a LAN port to view the port detail graphs based on Packets or Errors.

Figure 52 LAN port status

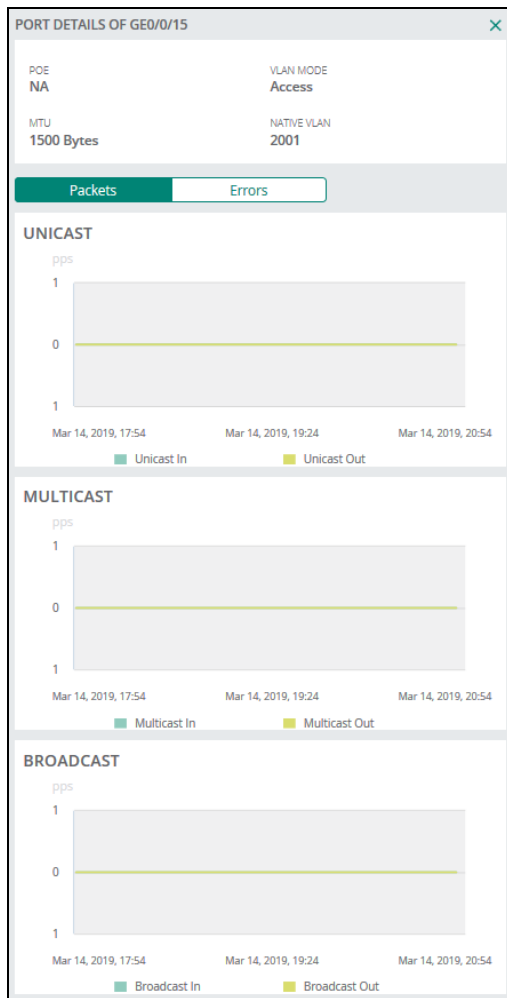


The following figure shows the Packet details displayed for the port:

- **Unicast**—The number of unicast packets per second.

- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

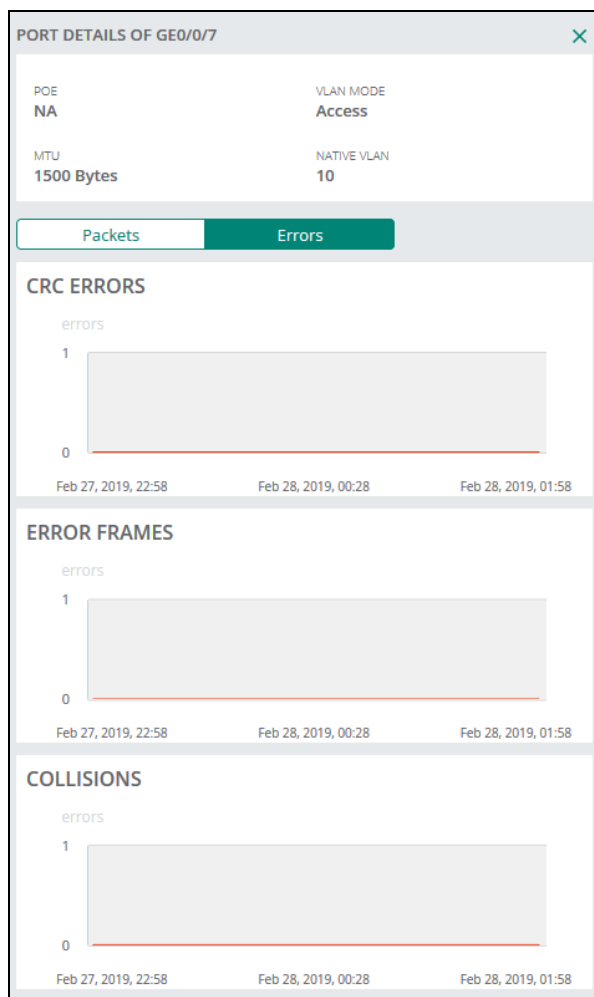
Figure 53 *Port Details—Packets*



The following figure shows the Error details displayed for the port:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

Figure 54 *Port Details—Errors*



- **LAN Interfaces Summary**—The table lists the LAN interfaces and provides the total number of LAN interfaces. Displays the summary of LAN interfaces. The following details are displayed for the port:
 - **Port**—Port number.
 - **Admin State**—Administrative state of the LAN interface.
 - **Oper. State**—Operational state of the LAN interface.
 - **Speed**—Speed.
 - **VLANs**—Range of VLANs.
 - **MTU**—MTU value.

Figure 55 *LAN Interfaces Summary*

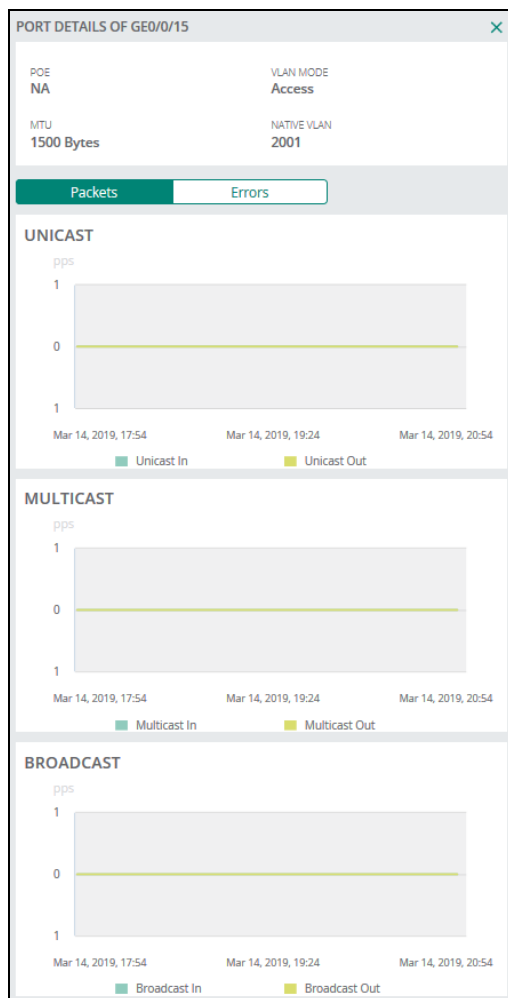
| LAN INTERFACES SUMMARY TOTAL LAN INTERFACES: 8 | | | | | |
|--|-------------|-------------|-------------|-------|------------|
| PORT | ADMIN STATE | OPER. STATE | SPEED | VLANs | MTU |
| GE0/0/0 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/1 | Enabled | Down | Auto/Auto | 400 | 1500 Bytes |
| GE0/0/2 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/3 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/4 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/5 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/6 | Enabled | Down | Auto/Auto | 1 | 1500 Bytes |
| GE0/0/7 | Enabled | Up | 1 Gbps/Full | 10 | 1500 Bytes |

Click a LAN port to view the port detail graphs based on Packets or Errors.

The following Packet details are displayed for the port:

- **Unicast**—The number of unicast packets per second.
- **Multicast**—The number of multicast packets per second.
- **Broadcast**—The number of broadcast packets per second.

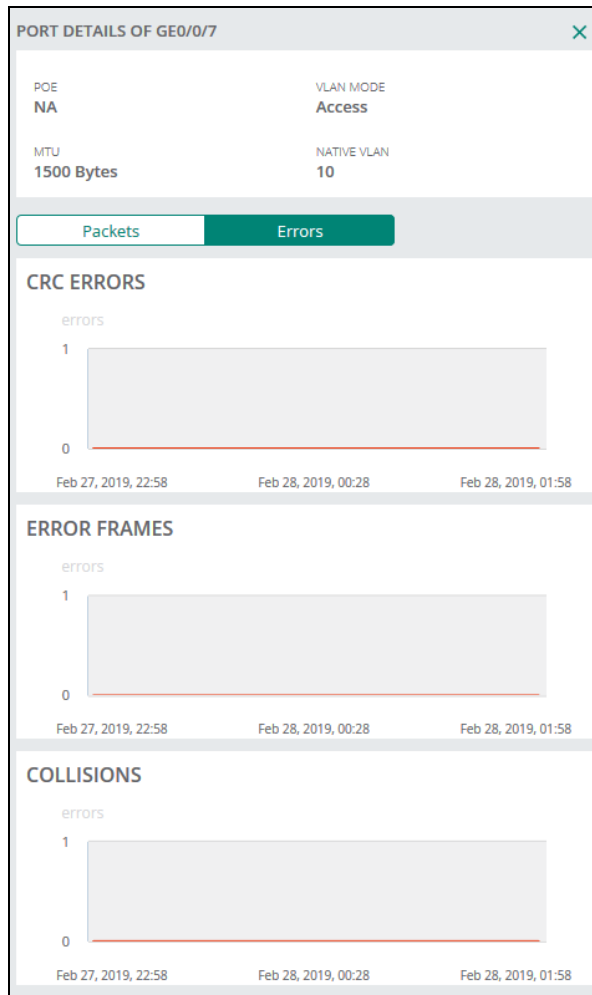
Figure 56 *Port Details—Packets*



The following Error details are displayed for the port:

- **CRC Errors**—The number of cyclic redundancy errors logged.
- **Error Frames**—The number of error frames logged.
- **Collisions**—The number of collisions encountered.

Figure 57 *Port Details—Errors*



- **VLAN Interfaces Summary**—The table lists the VLAN interfaces and provides the total number of VLAN interfaces. Displays the summary of VLAN interfaces. The following details are displayed:
 - **VLAN ID**—VLAN ID number.
 - **IP Address**—IP address.
 - **Admin State**—Administrative state of the VLAN interface.
 - **Oper. State**—Operational state of the VLAN interface.
 - **Addressing Mode**—Type of addressing mode.
 - **Description**—Description of the VLAN.

Figure 58 *VLAN Interfaces Summary*

| VLAN INTERFACES SUMMARY TOTAL VLAN INTERFACES: 4 | | | | | |
|--|--------------|-------------|-------------|-----------------|-------------|
| VLAN ID | IP ADDRESS | ADMIN STATE | OPER. STATE | ADDRESSING MODE | DESCRIPTION |
| 1 | | Disabled | Down | Static | |
| 7 | 7.7.7.2 | Disabled | Down | Static | |
| 33 | 3.3.3.3 | Disabled | Down | Static | |
| 4094 | 10.33.64.121 | Disabled | Down | Dynamic | |

- **DHCP Pools**—The table lists the DHCP pools and total number of DHCP pools. Displays the summary of DHCP pools. The following details are displayed:
 - **VLAN ID**—VLAN ID number.
 - **Pool Name**—Name of the DHCP pools.

- **Subnet**—IP address of the client subnet.
- **Pool size**—Size of the pool.
- **Lease time**—Lease time of the pool.
- **Free**—Number of addresses available.

Figure 59 *DHCP Pools*

| DHCP POOLS TOTAL DHCP POOLS: 1 | | | | | |
|----------------------------------|-----------|----------------|-----------|------------|------|
| VLAN ID | POOL NAME | SUBNET | POOL SIZE | LEASE TIME | FREE |
| 400 | vlan_400 | 172.30.10.0/24 | 253 | 12 hours | 99% |

- **Active Leases**—The table lists the active leases and the total number of active leases. Displays the summary of active leases. The following details are displayed:
 - **Pool Name**—Name of the DHCP pools
 - **IP Address**—IP address of the client subnet.
 - **MAC Address**—MAC address of the client.
 - **Start Date**—Start date and time of the lease.
 - **End Date**—End date and time of the lease.
 - **Remaining**—Remaining time for the lease to expire.

Figure 60 *Active Leases*

| ACTIVE LEASES TOTAL ACTIVE LEASES: 0 | | | | | |
|--|--------------|---------------|------------|----------|-----------|
| ▼ POOL NAME | ▼ IP ADDRESS | ▼ MAC ADDRESS | START DATE | END DATE | REMAINING |
| No data to display right now | | | | | |

Live monitoring is available for the following:

- **Port Status**
- Operational state of the LAN interface in **LAN Interfaces Summary** table.

Gateways—Tunnels Tab

To access the Tunnels section follow these steps:

1. On the **Gateways** page, click **List of Online Gateways**. The list of gateways connected in Aruba Central are displayed.
2. Click the gateway link for which you want to see the details. A dashboard showing the details of the selected gateway opens.
3. Click the **Tunnels** tab to view details about the Tunnels status and health.

The **Tunnels** tab displays the following details:

- **Tunnels Summary**
- **Tunnels Details**

The following details are displayed in the **Tunnels Summary** table:

- **Total**—Total number of VPN tunnels.
- **Up**—Number of VPN tunnels in UP state.
- **Down**—Number of VPN tunnels in DOWN state.
- **Peers**—Total number of VPN peers.

Figure 61 *Tunnels Summary*

| TUNNELS SUMMARY | | | |
|-----------------|----|------|-------|
| TOTAL | UP | DOWN | PEERS |
| 12 | 3 | 9 | 4 |

The following details are displayed in the **Tunnels Details** table:

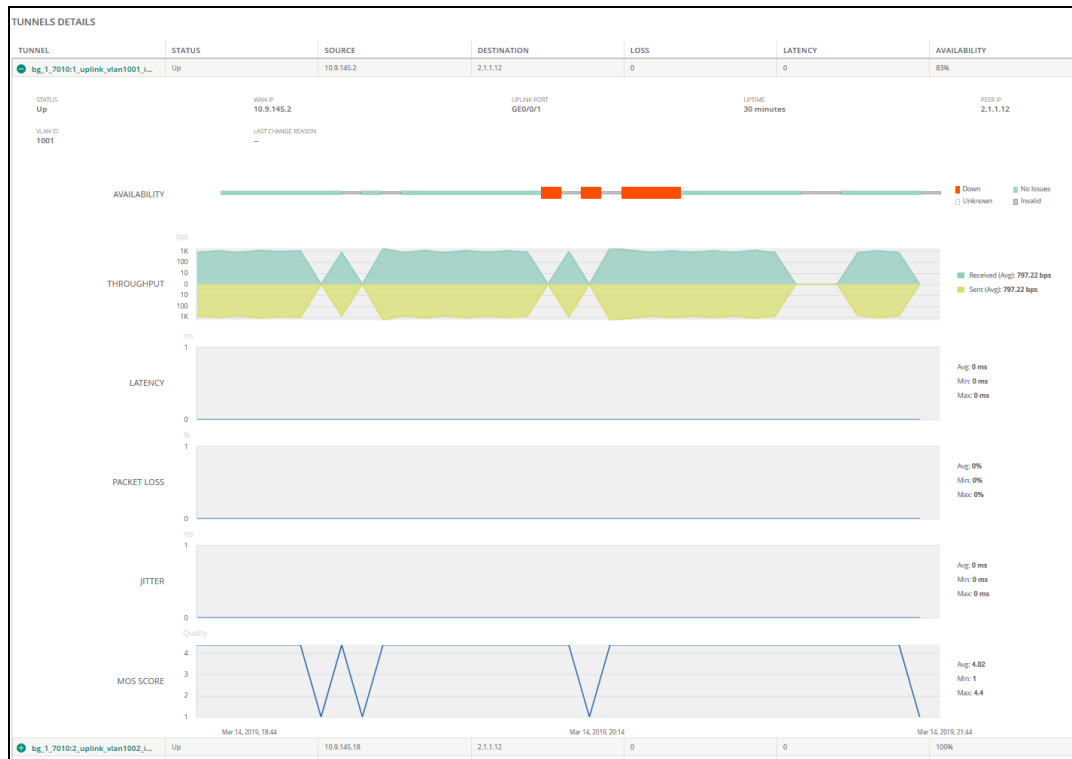
- **Tunnel**—Tunnel number.
- **Status**—Status of the tunnel.
- **Source**—Source IP address of the tunnel.
- **Destination**—Destination IP address of the tunnel.
- **Loss**—Percentage of packet loss.
- **Latency**—The latency in microseconds.
- **Availability**—Availability graph of the tunnel. Displays the percentage of time the tunnel was in UP state.

Figure 62 *Tunnels Details*

| TUNNELS DETAILS | | | | | | |
|---------------------------------|--------|--------------|-------------|------|---------|--------------|
| TUNNEL | STATUS | SOURCE | DESTINATION | LOSS | LATENCY | AVAILABILITY |
| 1 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.210.61 | 10.8.225.11 | | | 0 |
| 2 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.214.161 | 10.8.225.11 | | | 0 |
| 3 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.218.161 | 10.8.225.11 | | | 0 |
| 4 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.210.61 | 10.8.225.5 | | | 0 |
| 5 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.214.161 | 10.8.225.5 | | | 0 |
| 6 data-vpnc-00:1a:1e:04:b4d... | Down | 10.4.218.161 | 10.8.225.5 | | | 0 |
| 7 data-vpnc-00:1a:1e:04:cc6... | Up | 10.4.210.61 | 10.8.225.31 | 0 | 0.4ms | 97% |
| 8 data-vpnc-00:1a:1e:04:cc6... | Up | 10.4.214.161 | 10.8.225.31 | 0 | 0.60ms | 97% |
| 9 data-vpnc-00:1a:1e:04:cc6... | Up | 10.4.218.161 | 10.8.225.31 | 0 | 0.81ms | 97% |
| 10 data-vpnc-02:1a:1e:1d:72c... | Down | 10.4.210.61 | 6.6.6.11 | | | 0 |
| 11 data-vpnc-02:1a:1e:1d:72c... | Down | 10.4.214.161 | 6.6.6.11 | | | 0 |
| 12 data-vpnc-02:1a:1e:1d:72c... | Down | 10.4.218.161 | 6.6.6.11 | | | 0 |

- **Tunnel Info**—Select a tunnel to view the following details:
 - **Status**—Status of the tunnel.
 - **VLAN ID**—VLAN ID.
 - **WAN IP**—WAN IP address.
 - **Last Change Reason**—Reason for the last status change of the tunnel.
 - **Uplink Port**—Uplink port details.
 - **Uptime**—Amount of time the tunnel has been active since it was last reset.
 - **Peer IP**—Peer IP address.
 - **Availability**—Availability of the tunnel.
 - **Throughput**—Displays the inbound and outbound traffic rates for the selected tunnel.
 - **Latency**—Latency in microseconds.
 - **Packet Loss**—Percentage of packet loss.
 - **Jitter**—Jitter in microseconds.
 - **MOS Score**—MOS value.

Figure 63 Tunnel details-information



Live monitoring is enabled for sections that display the status, such as:

- The **Tunnels Summary**
- Status of the **Tunnels Details**

Gateways—Routing Tab

To access the Routing section follow these steps:

1. In the **Network Operations** app, use the filter to select a Branch Gateway.
2. Under **Manage**, click **Overview**. The Gateway **Summary** page is displayed.
3. Click the **Routing** tab to access the following route details for the gateway:

- **BGP**
- **OSPF**
- **Overlay**
- **RIP**
- **Route Table**

BGP

The **BGP** tab displays the following details for the gateway:

BGP Summary

- **Router ID**—Displays the Router ID.
- **AS Number**—Displays the private Autonomous System (AS) number.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes Learned**—Displays the number of routes that have been learned.

Figure 64 BGP—Summary

BGP SUMMARY

ENABLED

ROUTER ID: 172.100.0.1

AS NUMBER: 40000001

NEIGHBORS

1 UP | 1628 DOWN

ROUTES LEARNED

2

BGP DETAILS

ROUTES

TOTAL ROUTES: 4

LAST REFRESHED: 8:51:51 PM

| | NETWORK | NEIGHBOR | NEXTHOP | METRIC | LOCAL PREF | AS PATH | STATE | ROUTE SOURCE | ORIGIN |
|---|----------------|----------|-----------|--------|------------|---------|-------|--------------|------------|
| + | 54.1.1.0/24 | 24.1.1.1 | 24.1.1.1★ | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| + | 25.1.1.0/24 | 24.1.1.1 | 24.1.1.1★ | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| + | 24.1.1.0/24 | 24.1.1.1 | 24.1.1.1 | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| + | 172.100.0.0/24 | - | - | | | - | | | |

BGP Details

Displays the information categorized by **Neighbors** and **Routes**.

■ Neighbors

- **Total Neighbors**—Displays the total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Displays the available neighbors.
- **ASN**—Displays the private Autonomous System (AS) number.
- **State**—Displays the current state.
- **Type**—Neighbor type.
- **Last State Change**—Displays the last state change.
- **Down Count**—Displays the number of neighbors that are down.
- **Up Count**—Displays the number of neighbors that are up.
- **Hold Time**—Displays the time spent on hold.
- **Keep Alive Interval**—Displays the time set for the Keep Alive Interval.
- **Router ID**—Displays the Router ID.
- **Neighbor Version**—Displays the firmware version of the connected neighbors.
- **IP Precedence Value**—Displays the IP precedence.
- **Datagrams (Max = 1400Bytes)**—Displays existing datagrams.
- **Route Refresh**—Displays the latest route refresh.
- **Graceful Restart Capability**—Displays whether graceful restart is supported.
- **BGP Addtl-Paths Computation**—Displays the additional paths computation.
- **Recv Paths**—Displays the receive path information.
- **Send Paths**—Displays the send path information.
- **Source Address**—Displays the source information.
- **Nexthop**—Displays information about the next hop.
- **Link Address**—Displays the link address.
- **CFfg Hold Time**— Displays the minimum acceptable hold time.
- **CFfg Keep Alive Time**— Displays the configuration keep alive time.
- **IS Route Reflector**—Displays the net hop path.
- **IS Router Server**—Displays the IS Router Server details.
- **BGP Advertise-Best_External**—Displays the backup external route.
- **Up Time**—Displays the time that the connection has been up.

Figure 65 *BGP—Neighbors Details*

| BGP DETAILS NEIGHBORS ▼ TOTAL NEIGHBORS 2 LAST REFRESHED 8:46:19 PM ↻ | | | | | | |
|--|--------|-------------|-----------------------|------------|------------|------------|
| NEIGHBOR | ASN | STATE | LAST STATE CHANGE | DOWN COUNT | RECV PATHS | SEND PATHS |
| 24.1.1.1 | 200001 | Established | 20 Feb 2019, 06:54:05 | 0 | 0 | 0 |
| BGP NEIGHBOR 5.5.5.5 STATE: Established LAST STATE CHANGE: 20 Feb 2019, 06:54:05 TYPE: eBGP ASN: 2000001 DOWN COUNT: 0 UP COUNT: 0 HOLD TIME: 60/90 KEEPALIVE INTERVAL: 21/30 NEIGHBOR ROUTER ID: 5.5.5.5 NEIGHBOR VERSION: 4 IP PRECEDENCE VALUE: 192 DATAGRAMS (MAX = 1460 BYTES): 1.41 KB | | | | | | |
| NEIGHBOR CAPABILITIES ROUTE REFRESH: Advertised and received GRACEFUL RESTART CAPABILITY: Received | | | | | | |
| CAPABILITIES BGP ADOTL-PATHS COMPUTATION: Disabled BGP ADVERTISE-BEST-EXTERNAL: Disabled PATHS SENT: 0 RECEIVED: 0 | | | | | | |
| 35.1.1.1 | 100001 | Idle | - | 0 | 0 | 0 |
| BGP NEIGHBOR 0.0.0.0 STATE: Idle LAST STATE CHANGE: - TYPE: eBGP ASN: 100001 DOWN COUNT: 0 UP COUNT: 0 HOLD TIME: -/- KEEPALIVE INTERVAL: -/- NEIGHBOR ROUTER ID: 0.0.0.0 NEIGHBOR VERSION: 4 IP PRECEDENCE VALUE: 0 DATAGRAMS (MAX = 1460 BYTES): 0 Bytes | | | | | | |
| NEIGHBOR CAPABILITIES ROUTE REFRESH: Disabled GRACEFUL RESTART CAPABILITY: Disabled | | | | | | |
| CAPABILITIES BGP ADOTL-PATHS COMPUTATION: Disabled BGP ADVERTISE-BEST-EXTERNAL: Disabled PATHS SENT: 0 RECEIVED: 0 | | | | | | |

■ Routes

- **Total Routes**—Displays the total number of routes.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Network**—Connected network.
- **Neighbor**—Displays the available neighbors.
- **Nexthop**—Displays information about the next hop.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Local Pref**—Displays the outbound external path.
- **AS Path**—Displays the private Autonomous System path.
- **State**—Displays the connection state of the connection.
- **Route Source**—Displays the specific route the packet should take.
- **Origin**—Displays the origin attribute value.
- **Advertised to Upd-Grp**—Displays the Advertised Update-Group status.
- **Router ID**—Displays the router ID.

Figure 66 BGP—Routes Details

| BGP DETAILS ROUTES ▼ TOTAL ROUTES 4 LAST REFRESHED 8:53:52 PM ↻ | | | | | | | | | |
|---|-------------|----------|------------|--------|------------|----------|----------|--------------|------------|
| | NETWORK | NEIGHBOR | NEXTHOP | METRIC | LOCAL PREF | AS PATH | STATE | ROUTE SOURCE | ORIGIN |
| ● | 54.1.1.0/24 | 24.1.1.1 | 24.1.1.1 ★ | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| BGP ROUTE 54.1.1.0/24 ADVERTISED TO UPD-GRP: 0 | | | | | | | | | |
| | PATH | AS PATH | LOCAL PREF | STATE | ORIGIN | NEXTHOP | NEIGHBOR | ROUTER ID | TYPE |
| 1 | | 2000001 | 100 | VALID | INCOMPLETE | 24.1.1.1 | 24.1.1.1 | 5.5.5.5 | INTERNAL |
| ● | 25.1.1.0/24 | 24.1.1.1 | 24.1.1.1 ★ | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| BGP ROUTE 25.1.1.0/24 ADVERTISED TO UPD-GRP: 0 | | | | | | | | | |
| | PATH | AS PATH | LOCAL PREF | STATE | ORIGIN | NEXTHOP | NEIGHBOR | ROUTER ID | TYPE |
| 1 | | 2000001 | 100 | VALID | INCOMPLETE | 24.1.1.1 | 24.1.1.1 | 5.5.5.5 | INTERNAL |
| ● | 24.1.1.0/24 | 24.1.1.1 | 24.1.1.1 | 0 | 100 | 2000001 | Valid | Internal | Incomplete |
| BGP ROUTE 24.1.1.0/24 ADVERTISED TO UPD-GRP: 0 | | | | | | | | | |
| | PATH | AS PATH | LOCAL PREF | STATE | ORIGIN | NEXTHOP | NEIGHBOR | ROUTER ID | TYPE |
| 1 | | 2000001 | 100 | VALID | INCOMPLETE | 24.1.1.1 | 24.1.1.1 | 5.5.5.5 | INTERNAL |

RIP

The **RIP** tab displays the following details for the gateway:

RIP Summary

- **Enabled**—Implies that RIPv2 is enabled on the gateway device.
- **Version**—Displays the RIP version, RIPv1 or RIPv2. Currently, Aruba supports only RIPv2.
- **Interfaces**—Displays the number of interfaces that participates in the routing process.
- **Neighbors**—Displays the number of neighboring connections.
- **Routes**—Displays the number of routes advertised.
- **ECMP**—Displays the number of ECMPs available.
- **Infinity**—The hop count (16) assigned to unreachable devices (typically, any route that requires more than 15 hops).
- **Timers**—RIP uses timers to regulate its performance:
 - **Update** timer displays the interval between periodic routing updates. By default this is set to 30 seconds.
 - **Invalid** timer displays the time in seconds after which the route is marked invalid but is still available in the table. By default this is set to 180 seconds.
 - **Flush** timer displays the time duration after which the route is flushed out or removed from the table. By default this is set to 120 seconds.

Figure 67 RIP—Summary

| RIP SUMMARY ENABLED | | | | | | |
|-----------------------|------------|-----------|--------|------|----------|---|
| VERSION | INTERFACES | NEIGHBORS | ROUTES | ECMP | INFINITY | TIMERS |
| 2 | 1 | 3 | 3 | 16 | 16 | 30s 3m 2m UPDATE INVALID FLUSH |

RIP Details

Displays the information categorized by **Interfaces**, **Neighbors**, and **Routes**.

- **Interfaces**
 - **Name**—Displays the name of the interface.
 - **Address**—Displays the IP Address of the interface.

- **Cost**—Displays the cost associated.
- **State**—Displays the state of the connection (Up or Down).
- **Neighbors**—Displays the number of neighbors.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Next Update**—Time in seconds for the next update

Click on an interface listed in the table to view the following details:

- **RIP Interface**—Displays the name of the interface.
- **Address**—Displays the IP Address of the interface.
- **Mask**—Displays the subnet mask.
- **State**—Displays the state of the connection (Up or Down).
- **Port**—Displays the port number of the interface.
- **Version**—Displays the RIP protocol version.
- **Mode**—Displays the interface configuration mode.
- **Metric**—Displays the number of hop counts.
- **Passive**—Indicates whether the interface is operating in passive mode.
- **Split Horizon**—Indicates whether Split Horizon is implemented.
- **Poison Reverse**—Indicates whether Poison Reverse is implemented.
- **Authentication**—Displays the status of this option that is used for enabling RIP authentication mode for MD5.
- **Update Timer**—Displays the interval between periodic routing updates, by default this is set to 30 seconds.
- **Invalid Timer**—Displays the time in seconds after which the route is marked invalid but is still available in the table.
- **Flush Timer**—Displays the time duration after which the route is flushed out or removed from the table.

Figure 68 *RIP—Interfaces Details*

| RIP DETAILS | | INTERFACES ▼ | TOTAL INTERFACES: 1 | | LAST REFRESHED: 10:51:43 AM | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|---------------|---------------|---------------------|----------------|-----------------------------|----------------|---------|--|--|--|--|--|--|---------|------|-------|------|---------|------|--|-------------|---------------|----|-----|---|-----------|--|--------|---------|---------------|----------------|----------------|--------------|--|---|-------|------|------|------|-----|--|---------------|-------------|--|--|--|--|--|----|----|--|--|--|--|--|
| NAME | ADDRESS | COST | STATE | NEIGHBORS | NEXT UPDATE | AUTHENTICATION | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| vlan 4094 | 10.5.132.98 | 1 | up | 3 | 12s | NONE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| RIP INTERFACE VLAN 4094 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table> <tr> <td>DETAILS</td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>ADDRESS</td><td>MASK</td><td>STATE</td><td>PORT</td><td>VERSION</td><td>MODE</td><td></td></tr> <tr> <td>10.5.132.98</td><td>255.255.252.0</td><td>up</td><td>520</td><td>2</td><td>Multicast</td><td></td></tr> <tr> <td>METRIC</td><td>PASSIVE</td><td>SPLIT HORIZON</td><td>POISON REVERSE</td><td>AUTHENTICATION</td><td>UPDATE TIMER</td><td></td></tr> <tr> <td>1</td><td>false</td><td>true</td><td>true</td><td>None</td><td>30s</td><td></td></tr> <tr> <td>INVALID TIMER</td><td>FLUSH TIMER</td><td></td><td></td><td></td><td></td><td></td></tr> <tr> <td>3m</td><td>2m</td><td></td><td></td><td></td><td></td><td></td></tr> </table> | | | | | | | DETAILS | | | | | | | ADDRESS | MASK | STATE | PORT | VERSION | MODE | | 10.5.132.98 | 255.255.252.0 | up | 520 | 2 | Multicast | | METRIC | PASSIVE | SPLIT HORIZON | POISON REVERSE | AUTHENTICATION | UPDATE TIMER | | 1 | false | true | true | None | 30s | | INVALID TIMER | FLUSH TIMER | | | | | | 3m | 2m | | | | | |
| DETAILS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ADDRESS | MASK | STATE | PORT | VERSION | MODE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10.5.132.98 | 255.255.252.0 | up | 520 | 2 | Multicast | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| METRIC | PASSIVE | SPLIT HORIZON | POISON REVERSE | AUTHENTICATION | UPDATE TIMER | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | false | true | true | None | 30s | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| INVALID TIMER | FLUSH TIMER | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3m | 2m | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

- **Neighbors**
 - **Address**—Displays the IP address of the neighbor.
 - **Interface**—Displays the name of the interface.
 - **Metric**—Displays the number of hop counts.

- **Routes**— Displays the number of routes learned. Click the number for details of the routes learned.
- **Last Seen**— Displays the last seen time duration in *nD nH nM nS* format.

Figure 69 *RIP—Neighbors Details*

| RIP DETAILS NEIGHBORS ▼ TOTAL NEIGHBORS: 3 LAST REFRESHED: 10:53:10 AM ↻ | | | | | | | |
|--|-----------|--------|--------|-----------|--|--|--|
| ADDRESS | INTERFACE | METRIC | ROUTES | LAST SEEN | | | |
| 10.5.132.143 | vlan 4094 | 1 | 1 | 9s | | | |
| 10.5.132.47 | vlan 4094 | 1 | 2 | 20s | | | |
| 10.5.132.97 | vlan 4094 | 1 | 2 | 22s | | | |

■ Routes

- **Route**—Displays the route.
- **Next Hop**—Displays information about the next hop.
- **Metric**— Displays the number of hop counts.
- **Tag**—Displays the tag number associated with the route attribute that is set.
- **Expires**—Displays the time in *nD nH nM nS* format after which the route expires.

Figure 70 *RIP—Routes Details*

| RIP DETAILS ROUTES ▼ TOTAL ROUTES: 3 LAST REFRESHED: 10:54:31 AM ↻ | | | | | | | |
|--|--------------|--------|-----|---------|--|--|--|
| ROUTE | NEXTHOP | METRIC | TAG | EXPIRES | | | |
| 172.5.132.0/24 | 10.5.132.47 | 2 | 0 | 2m 48s | | | |
| 10.5.132.0/22 | 10.5.132.143 | 2 | 0 | 2m 58s | | | |
| | 10.5.132.47 | 2 | 0 | 2m 48s | | | |
| | 10.5.132.97 | 2 | 0 | 2m 45s | | | |
| 2.2.1.7/32 | 10.5.132.97 | 2 | 0 | 2m 45s | | | |

OSPF

The **OSPF** tab displays the following details for the gateway:

OSPF Summary

- **Status**—Status is either Enabled or Disabled.
- **Router ID**—The routers identification details.
- **Areas**—Area type as specified in the OSPF parameters.
- **Interfaces**—Displays the current interface.

- **Neighbors**—Displays the number of neighbors available.
- **Active LSA**—Displays the Active Link-State Advertisements.
- **Retransmit LSA**—Displays the Retransmitted Link-State Advertisements.

Figure 71 OSPF—Summary

| OSPF SUMMARY ENABLED ROUTER ID:1.1.1.2 | | | | | |
|--|-----------------|-----------|------------|----------------|--|
| AREAS | INTERFACES | NEIGHBORS | ACTIVE LSA | RETRANSMIT LSA | |
| 1 | 1 | 3 | 264 | 0 | |
| OSPF DETAILS NEIGHBORS ▼ TOTAL NEIGHBORS:3 LAST REFRESHED 9:17:18 PM ↻ | | | | | |
| NEIGHBOR | ADDRESS | INTERFACE | PRIORITY | STATE | |
| 192.168.164.100 | 192.168.164.100 | Vlan164 | 1 | ↕ | |
| 1.1.1.1 | 192.168.164.99 | Vlan164 | 1 | ↕ | |
| 10.53.9.9 | 192.168.164.101 | Vlan164 | 1 | ↕ | |

OSPF Details

Displays the information categorized by **Neighbors**, **Interfaces**, **Areas**, and **Link State Databases**.

■ Neighbors

- **Total Neighbors**—The total number of neighbors.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Neighbor**—Details of the neighbors.
- **Address**—IP address of the neighbor.
- **Interface**—Displays the current interface for the neighbor.
- **Priority**—Displays the priority of each neighbor.
- **State**—Displays the state of the connection.
- **Area**—Displays the area of the neighbor.
- **Options**—Available neighbor options.
- **Dead Timer**—Displays the required time to wait before the neighbor connection is dead.
- **Retransmit Timer**—Displays the time between OSPF and LSA retransmissions.

Figure 72 OSPF—Neighbor details

| OSPF SUMMARY ENABLED ROUTER ID:1.1.1.2 | | | | | |
|--|-----------------|-----------|------------|----------------|--|
| AREAS | INTERFACES | NEIGHBORS | ACTIVE LSA | RETRANSMIT LSA | |
| 1 | 1 | 3 | 264 | 0 | |
| OSPF DETAILS NEIGHBORS ▼ TOTAL NEIGHBORS:3 LAST REFRESHED 9:17:18 PM ↻ | | | | | |
| NEIGHBOR | ADDRESS | INTERFACE | PRIORITY | STATE | |
| 192.168.164.100 | 192.168.164.100 | Vlan164 | 1 | ↕ | |
| 1.1.1.1 | 192.168.164.99 | Vlan164 | 1 | ↕ | |
| 10.53.9.9 | 192.168.164.101 | Vlan164 | 1 | ↕ | |

■ Interfaces

- **Total Interfaces**—The total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Name**—Name of the interface.
- **Area**—Displays the logical collection of devices that share the same area.
- **Address**—IP address of the interface.
- **Mask**—IP mask of the interface.
- **State**—Displays the state of the connection.

- **Type**—Displays the type of connection.
- **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
- **Neighbor Count** —Displays the number of neighbors.
- **ID**—Displays the interface ID.
- **Address**—Displays the IP address of the interface.
- **Priority**—Displays the priority of the interface to determine the default router.
- **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
- **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
- **Retransmit Timer** —Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Click on an interface listed in the table to view the following details:

- **Type**—Displays the type of connection.
- **Area**—Displays the logical collection of devices that share the same area.
- **Address**—IP address of the interface.
- **Mask**—IP mask of the interface.
- **Cost**—Displays the cost associated with the OSPF traffic on the tunnel interface.
- **State**—Displays the state of the connection.
- **Priority**—Displays the priority of the interface to determine the default router.
- **Neighbor Count**—Displays the number of neighbors.
- **Dead Timer**—Displays the time interval after which a router is declared dead if hello packets are not received.
- **Hello Timer**—Displays the time interval between the hello packets to be sent on the interface.
- **Retransmit Timer**—Displays the retransmit interval time for link state advertisements.
- **Authentication**—Displays the status of this option that is used for enabling OSPF authentication mode for MD5.

Figure 73 OSPF— Interfaces details

OSPF SUMMARY

ENABLED | ROUTER ID:1.1.1.2

AREAS

1

INTERFACES

1

NEIGHBORS

3

ACTIVE LSA

264

RETRANSMIT LSA

0

OSPF DETAILS

INTERFACES

TOTAL INTERFACES:1 | LAST REFRESHED 9:20:21 PM

| NAME | AREA | ADDRESS | COST | STATE | NEIGHBOR COUNT |
|---|------|----------------|------|---------|----------------|
| <div><div></div><div>Vlan-164</div></div> | 0 | 192.168.164.97 | 1 | DROTHER | 3 |

OSPF INTERFACE

VLAN-164

TYPE: BCAST

AREA: 0

ADDRESS: 192.168.164.97

MASK: 255.255.255.0

COST: 1

STATE: DROTHER

PRIORITY: 0

NEIGHBOR COUNT: 3

DEAD TIMER: 40s

HELLO TIMER: 10s

RETRANSMIT TIMER: 5s

AUTHENTICATION: None

DESIGNATED ROUTER

ID: 192.168.164.100

ADDRESS: 192.168.164.100

BACKUP DESIGNATED ROUTER

ID: 1.1.1.1

ADDRESS: 192.168.164.99

■ Areas



Click the Settings icon to reset or set the default columns that are displayed.

- **Total Areas**—The total number of areas.

- **Last Refreshed**—Indicates when the last refresh was completed.
- **Area**—Displays the logical collection of devices that share the same area.
- **Type**—Displays the type of connection.
- **Interface count**—Displays the interface count.
- **SPF Count**—Displays the Shortest Path First count.
- **Default Count**—Displays the default count.
- **Enable Summary**—Displays if summary collection is enabled.

Figure 74 OSPF—Areas details

| OSPF SUMMARY ENABLED ROUTER ID:1.1.1.2 | | | | | |
|--|-----------------|-----------------|-------------------|---------------------|----------------|
| AREAS 1 | INTERFACES 1 | NEIGHBORS 3 | ACTIVE LSA 264 | RETRANSMIT LSA 0 | |
| OSPF DETAILS AREAS ▼ TOTAL AREAS:1 LAST REFRESHED 9:23:26 PM ↻ | | | | | |
| AREA | TYPE | INTERFACE COUNT | SPF COUNT | DEFAULT COST | ENABLE SUMMARY |
| 0 | Normal | 1 | 38 | 1000 | false |

■ Link State Databases



Click the Settings icon to reset or set the default columns that are displayed.

- **Total Link State Database**—The total number of Link State Databases.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Link ID**—Displays the router ID of the originating router.
- **Advertising Router**—Displays the routes that is advertising the link-state.
- **Area**—Displays the logical collection of devices that share the same area.
- **LSA Type**—Displays the aggregation type.
- **Age**—Displays the age of the OSPF LSA.
- **State**—Displays the state of the connection.
- **Seq No.**—Displays the 32-bit OSPF Sequence number.
- **Checksum**—Displays the 16-bit checksum for the OSPF packet.

Figure 75 OSPF—Link State Databases details

| OSPF DETAILS LINK STATE DATABASE ▼ TOTAL LSAs:264 LAST REFRESHED 9:22:13 PM ↻ | | | | |
|---|--------------------|------|----------|---------|
| LINK ID | ADVERTISING ROUTER | AREA | LSA TYPE | AGE |
| 192.202.1.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.2.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.3.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.4.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.5.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.6.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.7.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.8.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.9.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.10.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.11.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.12.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.13.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.14.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.15.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.16.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |
| 192.202.17.0 | 192.168.164.100 | 0 | EXTERNAL | 29m 29s |

- **LSA types**—There are various LSA types available and they are listed here:
 - **Router**—The Router page displays the following details:
 - Flags
 - Link ID

- Link Data
- Link Type
- Metric
- **Network**—The Network page displays the following details:
 - Mask
 - Attached router
- **Network Summary**—The Network Summary page displays the following details:
 - Address
 - Mask
 - Metric
- **ASBR Summary**—The ASBR Summary page displays the following details:
 - ASBR
 - Metric
- **External**—The External page displays the following details:
 - Mask
 - Metric
 - Type
 - Route Tag
 - Forwarding Address

Overlay

The **Overlay** tab displays the following details for the gateway:



Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

■ Overlay Summary

- **Status**—Status is either Enabled or Disabled.
- **Site**—Displays the site location.
- **Control Connections**—Displays the number of active control connections.
- **Interfaces**—Displays the number of active interfaces.
- **Routes Advertised**—Displays the number of routes that are advertised.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 76 Overlay—Summary

| OVERLAY SUMMARY ENABLED SITE 00:1A:1E:04:E6:B0 | | | | |
|---|-----------------|-----------------|--------------------------|---------------------|
| CONTROL CONNECTIONS 1 UP 0 DOWN | | INTERFACES 1 | ROUTES ADVERTISED 256 | ROUTES LEARNED 0 |
| OVERLAY DETAILS ROUTES ADVERTISED ▼ TOTAL ROUTES ADVERTISED: 256 LAST REFRESHED: 9:29:25 PM ↻ | | | | |
| ROUTE | NEXTHOP | INTERFACE | ORIGIN | COST |
| 192.202.1.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.2.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.3.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.4.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.5.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.6.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.7.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.8.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.9.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.10.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.11.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.12.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.13.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.14.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.15.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.17.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |
| 192.202.18.0/24 | 192.168.164.100 | vlan 164 | OSPF | 10 |

- **Overlay Details**—Displays the information categorized by **Control Connections**, **Interfaces**, **Routes Advertised**, and **Routes Learned**.
- **Control Connections**



Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

- **Total Control Connections**—Displays the total number of control connections.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Control Plane Peers**—Displays the Control Plane Peers.
- **State**—Displays the state of the connection.
- **Last State Change**—Indicates the Last State Change.
- **Down Count**—Displays the Down Count.
- **Routes Advertised**—Displays the advertised routes.
- **Routes Learned**—Displays the number of routes that are learned.

Figure 77 Overlay Details —Control Connections

| OVERLAY DETAILS CONTROL CONNECTIONS ▼ TOTAL CONTROL CONNECTIONS: 1 LAST REFRESHED: 10:47:53 PM ↻ | | | | | |
|--|-----------------------|---------------------------------|------------|-------------------|----------------|
| CONTROL PLANE PEERS | STATE | LAST STATE CHANGE yyyy-mm-dd | DOWN COUNT | ROUTES ADVERTISED | ROUTES LEARNED |
| Overlay Route Orchestrator | OAP CHANNEL CONNECTED | 14 Mar 2019, 20:45:28 | 17 | 1 | 267 |

- **Interfaces**



Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

- **Total Interfaces**—Displays the total number of interfaces.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Interfaces**—Displays the number of active interfaces.
- **State**—Displays the state of the interface.
- **Tunnel Destination**—Displays the destination address.
- **Uptime**—Amount of time the tunnel has been active since it was last reset.

- **Routes Learned**—Displays the number of routes that are learned.

Figure 78 *Overlay Details —Interfaces*

| OVERLAY DETAILS INTERFACES ▼ TOTAL INTERFACES: 1 LAST REFRESHED: 9:35:39 PM ↻ | | | |
|---|-------|--------------------|----------------|
| INTERFACES | STATE | TUNNEL DESTINATION | ROUTES LEARNED |
| default-vpnip-master-ipsecmap-20-4c:03:30:00:a4-uplink4094_inet | Up | Aruba7005_30_00_A4 | 0 |

■ Routes Advertised

Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information.

- **Route**—Displays the route name.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.
- **Flags**—Lists the number of active flags.
- **Origin**—Origin of the route.
- **Cost**—Cost associated with the route.

Figure 79 *Overlay Details—Routes Advertised*

| OVERLAY DETAILS ROUTES ADVERTISED ▼ TOTAL ROUTES ADVERTISED TO OVERLAY: 1 LAST REFRESHED: 10:54:47 PM ↻ | | | | | |
|---|---------|-----------|-----------|-----------|------|
| ROUTE | NEXTHOP | INTERFACE | FLAGS | ORIGIN | COST |
| 2.1.1.2/32 | 0.0.0.0 | vlan 10 | RTO LOCAL | Connected | 0 |

■ Routes Learned

- **Total Routes Learned**—Displays the total number of routes that are learned.
- **Last Refreshed**—Indicates when the last refresh was completed.
- **Route**—The route IP address and subnet.
- **Age (Last Updated)**—Last updated date.
- **Origin**—Origin of the connection, for example, Connected or Overlay.
- **Flags**—Lists the number of active flags.
- **Nexthop**—Displays information about the next hop.
- **Interface**—Displays the number of active interfaces.

Figure 80 *Overlay Details—Routes Learned*

| OVERLAY DETAILS ROUTES LEARNED ▼ TOTAL ROUTES LEARNED FROM OVERLAY: 9 LAST REFRESHED: 5:45:01 PM ↻ | | | | | | |
|--|----------------|----------------------|-----------|------|---------|--------------------------------------|
| | ROUTE | AGE (LAST UPDATED) | ORIGIN | COST | NEXTHOP | INTERFACE |
| ⊕ | 172.168.1.0/24 | 7 JUN 2019, 21:09:18 | OSPF | 10 | VPNC1* | data-vpnc-00:1a:1e:04:ce:b8-ATT_inet |
| | | | | | | data-vpnc-00:1a:1e:04:ce:b8-ATT_mpls |
| | | | Connected | 1 | VPNC2 | data-vpnc-00:1b:2e:04:ce:b9-ATT_inet |
| | | | | | | data-vpnc-00:1b:2e:04:ce:b9-ATT_mpls |
| ⊕ | 10.2.0.0/16 | 7 JUN 2019, 21:09:18 | BGP | 999 | VPNC3* | data-vpnc-00:1c:2e:04:ce:c0-ATT_inet |
| ⊕ | 192.168.0.0/16 | 7 JUN 2019, 21:09:18 | Static | 5 | VPNC4* | |
| ⊕ | 10.1.1.0/24 | 7 JUN 2019, 21:09:18 | Overlay | 100 | VPNC1* | data-vpnc-00:1a:1e:04:ce:b8-ATT_inet |
| | | | | | | data-vpnc-00:1a:1e:04:ce:b8-ATT_mpls |

Route Table



Click the Settings icon to reset or set the default columns that are displayed.

Click the filter icon on each column header row to filter the displayed information

The **Route Table** tab displays the following route details for the gateway:

■ Route Summary

- **Capacity**—Number of routes supported.
- **Connected**—Number of connected routes.
- **Default**—Number of default routes.
- **Static**—Number of static routes.
- **Dynamic**—Number of dynamic routes.
- **Overlay**—Number of overlay connections.

Figure 81 *Routes Summary*

| ROUTES SUMMARY | | | | | |
|----------------|-----------|---------|--------|---------|---------|
| CAPACITY | CONNECTED | DEFAULT | STATIC | DYNAMIC | OVERLAY |
| --- | --- | --- | --- | --- | --- |

■ Routes

- **Last Refreshed**
- **Route**—The route IP address and subnet.
- **Nexthop**—Displays information about the next hop.
- **Protocol**—Routing protocol. Possible values are **CONNECTED**, **STATIC**, **IKE**, **OVERLAY**, **BGP**, or **OSPF**.
- **Type**—The type of connection.
- **Metric**—Distance for static routes. For a given route destination, there can be multiple next hops. A route metric enables the gateway to prefer one route over another or load-balance when the metric is the same.
- **Flags**—Route flags that indicate the flags for the selected routes.

Figure 82 *Routes details*

| ROUTES LAST REFRESHED: 4:47:42 AM | | | | |
|-------------------------------------|-------------|-----------|---------|--------|
| ROUTE | NEXTHOP | PROTOCOL | TYPE | METRIC |
| 0.0.0.0/0 | 10.3.52.254 | Default | Default | 1 |
| 3.3.3.0/24 | - | Connected | - | - |
| 10.3.52.0/24 | - | Connected | - | - |
| 172.30.10.0/24 | - | Connected | - | - |

Gateways—Path Steering Tab

In the **Path Steering** tab, you can view traffic path steering details for the Dynamic Path Steering policies configured on the Branch Gateway. The tab also displays the number of policies that are compliant along with the total number of policies configured on the Branch Gateway.

From the list of Dynamic Path Steering policies, select the policy for which you want to view the path steering details.

The **Path Steering** section displays the following information:

■ Path Steering Summary

- **State**—Displays whether the path steering feature is enabled.
- **Policy Compliance**—Displays the compliance status of all the configured policies.

Figure 83 Path Steering Summary

| | |
|-----------------------|----------------------------|
| PATH STEERING SUMMARY | |
| STATE | POLICY COMPLIANCE 1 / 1 |

- **Path Steering Details** section displays the following information:
 - **Policy Name**—The name of the Dynamic Path Steering policy
 - **Bandwidth**—The threshold percentage set for bandwidth utilization
 - **Latency**—The threshold value set for a round-trip ping time in milliseconds
 - **Jitter**—The threshold value set for jitters in packet transmission in milliseconds
 - **Packet Loss**—The percentage of packet loss allowed for the traffic type
 - **Path Preference**—The path preference in the primary, secondary, and tertiary order
 - **Status**—The compliance status of the uplinks
 - **Overall Compliance**—Overall compliance (%) of the policy

Figure 84 Path Steering Details

| PATH STEERING DETAILS | | | | | | | | |
|-----------------------|-------------|---------------------------|---------|--------|-------------|-----------------------------|-----------|------------------|
| | POLICY NAME | EXPECTED THRESHOLD VALUES | | | | PATH PREFERENCE | STATUS | OVERALL COMPL... |
| | | BANDWIDTH | LATENCY | JITTER | PACKET LOSS | | | |
| + | default | 80% | 0ms | 0ms | 1% | public_inet,private_mpls | Compliant | 100.00% |
| + | seel-lab | 0% | 150ms | 150ms | 1% | private_mpls,public_inet | Compliant | 100.00% |
| + | voz | 0% | 80ms | 15ms | 0% | private_mpls => public_inet | Compliant | 100.00% |

Click a policy to view the **Compliance Summary** that consists of the **Status** and **Session** information.

- **Status**—Provides a graphical representation of the configured uplink statuses. The following details are displayed:
 - Overall status
 - The status of each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Hover over the status bar to view the compliance status details of all the configured uplinks. You can view the compliance status of the uplinks and the probe IPs. If the probe IPs are non-compliant, it displays the reason for non-compliance such as latency, jitter, or packet loss. The following list contains the various colors and the corresponding compliance status:

- **Green**—An uplink is **Compliant** when all of the associated probe IPs meet the set SLAs and threshold settings.
- **Orange**—An uplink is **Partially Compliant** when you have multiple probe IPs and not all of them are compliant.
- **Red**—An uplink is **Non-Compliant** when all of the probe IPs are non-compliant.
- **Yellow**—This is the **Hold Period** when an uplink changes it's status from Non-compliant to Compliant (usually the first 3 minutes of the transition phase).
- **Grey**—Uplink status is **Unknown** when the Dynamic Path Steering feature does not send any compliance information to the cloud.
- **Sessions**—Provides a graphical representation of the total number of sessions. The following details are displayed:
 - Overview
 - The sessions count on each of the uplinks configured for the Dynamic Path Steering policy on that gateway

Figure 85 Path Steering Details—Compliance Summary



- **Event Logs**—When an uplink becomes non-compliant, an event is recorded, when the same uplink becomes compliant adhering to the set SLAs, another event is recorded. The **Event Logs** table provides information about all such events. It displays the timestamp and a detailed event statement that contains the policy name, the uplink name, the probe IP, and the reason for non-compliance, if it is a non-compliance event.

Figure 86 Event Logs

| EVENT LOGS | |
|-----------------------|--|
| DATE & TIME | EVENT STATEMENT |
| yyyy-mm-dd | |
| 10 May 2019, 12:34:23 | Policy : overlay applied on Uplink : uplink_1_inet Probing : 10.8.239.46 has become Compliant. |
| 10 May 2019, 12:34:13 | Policy : overlay applied on Uplink : uplink_1_inet Probing : 10.8.239.46 has become Non Compliant due to 40.0% Packet Loss |
| 10 May 2019, 06:56:28 | Policy : overlay applied on Uplink : uplink_1_inet Probing : 10.8.239.46 has become Compliant. |
| 10 May 2019, 06:41:16 | Policy : overlay applied on Uplink : uplink_1_inet Probing : 10.8.239.46 has become Non Compliant due to 77.0ms Latency |
| 10 May 2019, 06:25:54 | Policy : overlay applied on Uplink : uplink_1_inet Probing : 10.8.239.46 has become Compliant. |
| 10 May 2019, 06:15:18 | Policy : overlay applied on Uplink : uplink_2_mpls Probing : 10.8.239.46 has become Compliant. |

Live monitoring is enabled for sections that display status, such as:

- The **path Steering Summary**
- Real time state of the **Event Logs**

Application Visibility



The **Visibility** dashboard displays charts showing client traffic trends to application, application categories, website categories, and websites of a specific security reputation score. To view the traffic classification based on application, application category, and website category, you must enable **Application Visibility** service on Branch Gateways.

To view application usage metrics for Aruba Gateways:

1. In the **Network Operations** app, use the filter to select a Gateway group or a Gateway.
2. Under **Manage**, click **Applications > Visibility**.

The Visibility dashboard is displayed.



Click the Table  and the Summary  icons on the **Application** and **Websites** sections to toggle between the dashboard views.

The **Applications** section displays the following:

- **Application / Categories**—Displays the top N application categories based on total bandwidth usage. Apart from the top N, the rest of the application categories are grouped under the **Unclassified** category.
 - **Applications**—Displays top N applications based on total bandwidth usage. Apart from the top N, the rest of the applications are grouped under the **Unclassified** category. Click the **+** next to the service name to expand the view and display additional information.
 - **Categories**—Displays the top N web categories based on total bandwidth usage. Apart from the top N, the rest of the web categories are grouped under the **Unclassified** category.
 - **Usage**—Displays the bandwidth usage of each application.
 - **Sent**—Displays the amount of data sent.
 - **Received**—Displays the amount of data received.

Figure 87 Applications

The screenshot shows the 'APPLICATIONS' tab in the Aruba Central interface. It displays a table with columns: APPLICATION, CATEGORY, USAGE, SENT, and RECEIVED. The table lists various network services and their bandwidth usage.

| APPLICATION | CATEGORY | USAGE | SENT | RECEIVED |
|----------------------|-----------------|------------------|--------|----------|
| TCP | Network Service | 1.4 MB (27.70%) | 1.4 MB | 0 B |
| HTTPS | Web | 1005 KB (19.73%) | 871 KB | 134 KB |
| Google Generic | Google SAAS | 336 KB (6.61%) | 336 KB | 0 B |
| SSL | Encrypted | 49 KB (0.97%) | 49 KB | 0 B |
| Server Message Block | Network Service | 36 KB (0.70%) | 36 KB | 0 B |
| HTTP | Web | 35 KB (0.69%) | 35 KB | 0 B |
| Netbios Name Service | Network Service | 18 KB (0.36%) | 18 KB | 0 B |
| Spotify | Streaming | 13 KB (0.25%) | 13 KB | 0 B |
| baidu.com | Web | 9 KB (0.18%) | 9 KB | 0 B |
| ISAKMP | Encrypted | 648 B (0.01%) | 648 B | 0 B |

The **Websites** tab displays the following tables:

- **Reputation and Usage**—Displays the reputation and usage percentage.
- **Category and Usage**—Displays the WebCC category and the usage percentage.

Figure 88 Websites

The screenshot shows the 'WEBSITES' tab in the Aruba Central interface. It displays two tables side-by-side.

| REPUTATION | USAGE |
|---------------|---------|
| Moderate Risk | 90.665% |
| Trustworthy | 9.335% |

| CATEGORY | USAGE |
|--------------------------------|-----------------|
| Unclassified | 3.9 MB (90.21%) |
| Business and Economy | 390 KB (8.88%) |
| Computer and Internet Security | 40 KB (0.91%) |

Gateways—Sessions Tab

The **Sessions** tab displays the following information:

- **Session Summary**—Displays a summary of all the running sessions.
- **Sessions**—Displays filtered session information.

The following details are displayed in the **Session Summary** pane:

- **Current entries**—Displays the number of current and active entries.
- **Max entries**—Displays the total entries made with the time period.
- **High watermark**—Displays the highest number of active entries.
- **Allocation failures**—Displays the number of failed allocations.
- **Denied entries**—Displays the number of entries that were denied.

The **Sessions** pane displays information filtered by the **IP Address** entered in the text box.


Click the Settings icon  to reset or set the default columns that are displayed.



Click the Filter icon and enter the keyword or ip address to filter the information.

The Session table displays information about:

- **Application**—Displays the list of applications.
- **Source IP**—Displays the source IP address.
- **Destination IP**—Displays the destination IP address.
- **Protocol**—Displays the communication protocol used.
- **Source port** —Displays the source port number.
- **Dest port** —Displays the destination port number used by the application.
- **Action**—Displays the application specific action.
- **Flags**—Displays the applied flags. Hover over the information icon to see the Legend for the flag description.
- **Packets**—Displays the number of packets.
- **Bytes**—Displays the amount of data (in bytes and mega bytes) consumed by the application.
- **State**—Displays the connection state of the application. The state can either be Active, Inactive, or Denied.
- **Start Time**—Displays the start time.
- **Receive Time**—Displays the receive time.
- **WEBCC Category**—Displays the WEBCC category.
- **WEBCC Reputation**—Displays the WEBCC reputation.
- **WEBCC Score**—Displays the WEBCC score.
- **Application Category**—Displays the application category.

To view additional information of individual sessions click the drop down  icon to expand and display session specific information. The following information is displayed:

- **Details**
 - **User role**—Displays the user role name.
 - **User policy rule (ACE)**—Displays the user policy rule.
 - **Start time**—Displays the session start time.
 - **Receive time**—Displays the session receive time.
 - **WebCC category**—Displays the WebCC categorization.
 - **WebCC reputation**—Displays the site reputation.
 - **Application category**—Displays the application category.
- **Nexthop**
 - **Uplink interface**—Displays the uplink interface details.
 - **Uplink VLAN**—Displays the uplink VLAN details.
 - **Tunnel**—Displays the tunnel details.
- **Matching PBR**
 - **Policy Name (RACL)**—Displays the policy name.

- **Policy Rule (RACE)**—Displays the policy rule.
- **Dynamic Path Selection (DPS)**
 - **Policy name**—Displays the policy name.
 - **Path preference**—Displays the path interface details.
 - **Compliance**—Displays the compliance details.
 - **Matching Policy Rule**—Displays the matching policy rule.



Matching PBR and Dynamic Path Selection (DPS) tables require SD-WAN version 2.0.0.1 or higher.

Figure 89 Session summary and session information

SESSIONS LAST REFRESHED: 7:11:46 PM

FILTERS FILTERED ENTRIES: 60

IP ADDRESS

| APPLICATION | SOURCE IP | DESTINATION | SOURCE PORT | DEST PORT | ACTION | FLAGS | PACKETS | BYTES | STATE |
|----------------------|----------------|--------------|-------------|-----------|--------|-------|---------|----------|----------|
| ICMP | 10.5.132.42 | 10.5.132.1 | 9800 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |
| Nat-t | 10.5.132.42 | 54.180.99.29 | 4500 | 4500 | Permit | F C | 321100 | 46.55 MB | Active |
| ICMP | 10.5.132.42 | 10.5.132.1 | 50412 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |
| ICMP | 10.5.132.1 | 10.5.132.42 | 9812 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| Netbios Name Service | 10.5.135.255 | 10.5.132.98 | 137 | 137 | Permit | F Y | 0 | 0 Bytes | Inactive |
| ICMP | 10.5.132.1 | 10.5.132.42 | 50416 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| Nat-t | 1.4.1.2 | 10.5.132.42 | 4500 | 4500 | Permit | F | 224765 | 32.58 MB | Active |
| Nat-t | 10.53.9.178 | 10.5.132.42 | 4500 | 4500 | Permit | F Y | 0 | 0 Bytes | Inactive |
| - | 10.5.132.80 | 10.5.132.116 | 1716 | 56024 | Permit | C A | 1 | 52 Bytes | Active |
| ICMP | 10.5.132.42 | 10.5.132.1 | 3832 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |
| - | 34.211.217.249 | 10.5.132.42 | 443 | 44326 | Permit | - | 221844 | 11.91 MB | Active |
| ICMP | 10.5.132.1 | 10.5.132.42 | 3828 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| ICMP | 10.5.132.1 | 10.5.132.42 | 3844 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| ICMP | 10.5.132.42 | 10.5.132.1 | 45592 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |
| ICMP | 10.5.132.1 | 10.5.132.42 | 50400 | 0 | Permit | I F | 1 | 28 Bytes | Active |

Figure 90 Session Details

CURRENT ENTRIES: 85 MAX ENTRIES: 458575 HIGH WATERMARK: 1447 ALLOCATION FAILURES: 0 DENIED ENTRIES: 4

SESSIONS LAST REFRESHED: 9:16:41 PM

FILTERS FILTERED ENTRIES: 85

IP ADDRESS

| APPLICATION | SOURCE IP | DESTINATION | SOURCE PORT | DEST PORT | ACTION | FLAGS | PACKETS | BYTES | STATE |
|---------------------------|----------------|---------------|-------------|-----------|--------|-------|---------|-----------|----------|
| HyperText Transfer Pro... | 10.132.72 | 52.38.149.117 | 59503 | 443 | Permit | Y | 0 | 0 Bytes | Inactive |
| Nat-t | 10.5.132.42 | 54.180.99.29 | 4500 | 4500 | Permit | F C | 328580 | 47.63 MB | Active |
| ICMP | 10.5.132.42 | 10.5.132.1 | 19156 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |
| User Datagram Protocol | 10.53.9.152 | 10.5.132.67 | 4500 | 13793 | Permit | F C A | 2 | 448 Bytes | Active |
| - | 35.163.174.225 | 10.5.132.84 | 443 | 42784 | Permit | C A | 1 | 52 Bytes | Active |
| Nat-t | 1.4.1.2 | 10.5.132.42 | 4500 | 4500 | Permit | F | 230001 | 33.34 MB | Active |
| - | 35.162.204.126 | 10.5.132.75 | 2083 | 61071 | Permit | C A | 1 | 52 Bytes | Active |
| ICMP | 10.5.132.1 | 10.5.132.42 | 37200 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| - | 10.5.132.139 | 35.160.24.134 | 61605 | 2083 | Permit | Y A | 0 | 0 Bytes | Inactive |
| Nat-t | 10.53.9.178 | 10.5.132.42 | 4500 | 4500 | Permit | F Y | 0 | 0 Bytes | Inactive |
| ICMP | 10.5.132.1 | 10.5.132.42 | 49880 | 0 | Permit | I F | 1 | 28 Bytes | Active |
| ICMP | 10.5.132.42 | 10.5.132.1 | 50400 | 2048 | Permit | I F C | 1 | 28 Bytes | Active |

Deleting an Offline Gateway

To delete an offline Gateway:

1. In the **Network Operations** app, use the filter to select a Branch Gateway group.
2. Under **Manage**, click **Devices** > **Gateways**.

3. From the **Gateways** table, select the Gateway that you want to delete. To select a Gateway, click on any column except **Device Name**.



Clicking on a device name in the **Device Name** column opens the Gateway dashboard.

4. Click **Delete**.
5. Confirm deletion.

WIDS Events

Overview

With Aruba Central, you can quickly identify and act on interfering devices that can be later considered for investigation, restrictive action, or both. Once the interfering devices are discovered, Aruba Central sends alerts to your network administrators about the possible threat and provides essential information needed to locate and manage the threat.

Viewing Intrusion Details Page

To view the intrusion detail page in order to find information on interfering devices, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, site, or a label.
2. Under **Manage**, click **Security**. The **Intrusion Detection** tab is selected by default.

Intrusion Detection System Events Configuration

The type and severity of Intrusion Detections raised by an AP is configurable and affects the data that is seen in Security. For more information on configuring IDS for APs, see the [Configuring IDS Parameters on APs on page 343](#).

Monitoring WIDS Events

The **Manage > Security** tab provides a summary of the total number of wireless attacks detected for a given duration.

Intrusion Detection

By default, the **Intrusion Detection** tab is selected and displays the list of WIDS events.


The **WIDS Events** table displays the following information:

- Infrastructure attacks—Displays the number of infrastructure attacks detected in the network.
- Client attacks—Displays the number of client attacks detected in the network.

Table 42: WIDS Events

| Fields | Description |
|---------------------|---|
| Event Type | The type of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the event types based on your requirement. |
| Category | Category of the intrusion or attack, infrastructure or client attack. Click the drop-down arrow at the column heading to filter the category that you want to display. |
| Level | The level of the intrusion or attack detected. Click the drop-down arrow at the column heading to filter the attack level. |
| Time | Time of the intrusion or attack. |
| Station MAC | MAC address of the station under attack or BSSID of the AP under attack. |
| Detecting AP | The MAC address of the device that detected the intrusion or attack. |
| Radio Band | Radio band on which the intrusion was detected. There are two radio band signals available, 2.4 GHZ and 5 GHZ. Click the drop-down arrow at the column heading to filter the radio band where the intrusion was detected. |
| Description | Details of the attack or the intrusion. |

Note the following important points:

- Clicking  icon enables you to customize the **Events** table columns or set it to the default view.
- To view the details of each event that is generated, click the arrow against each row in the table.
- Intrusions are displayed for a selected time period based on the time selected in **Time Range Filter**. Security displays data for a maximum time period of 1 week because the volume of data that is collected is huge.

Generating Alerts for Security Events

Aruba Central supports configuring alerts for IDS events. To generate alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Analyze**, click **Alerts & Events** and then click the settings icon to display the alert configuration dashboard.
3. Select **Access Point** tab to display the AP dashboard. Aruba Central supports three alert types for identifying interfering devices:
 - Rogue AP Detected
 - Infrastructure Attacks Detected
 - Client Attack Detected
4. Select an alert and click **+** to enable the alert with default settings. To configure alert parameters, click on the alert tile (anywhere within the rectangular box) and do the following:
 - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning.



For a few alerts, you can configure threshold value for one or more alert severities. To set the threshold value, select

the alert and in the **exceeds** text box, enter the value. The alert is triggered when one of the threshold values exceed the duration.

b. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:

- **Group**—Select a group to limit the alert to a specific group.
- **Label**—Select a label to limit the alert to a specific label.
- **Sites**—Select a site to limit the alert to a specific site.

c. **Notification Options**

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
- **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information, see [Webhooks on page 487](#).

d. Click **Save**.

For more information on how to configure Alerts, see [Configuring Alerts on page 267](#).

Generating Reports for Security Events

Aruba Central supports generating reports for IDS events. To generate reports, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Analyze**, click **Reports**.
3. In the **Reports** page, click **Create Report**. . For more information on how to create Reports, see [Reports on page 275](#)


Network Health Dashboard




The Network Health dashboard displays information of the network sorted by site. This dashboard displays information on network devices and WAN connectivity of individual sites.

To launch the **Network Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Network Health** to launch the **Network Health** dashboard.

The **Network Health** dashboard has two views, you can toggle between them by clicking on the view icons.

 **Summary**— This view displays the vital network information of individual sites on cards mapped by geographical location. Sites are marked with location pins- red pin for a site with potential issues and green pin for a site with no issues. To view the information card of a site, click on the location pin of a site.

 **List**— This view displays the global network report in a list sorted according to individual sites. Clicking on the site name will take you to the **Site Health** dashboard page. The data columns listed in the page can be managed by clicking on the hamburger icon (≡) on the right of the column header. The report can be filtered by clicking on the filter labels below the column name. Selecting a filter label filters the results based on the field values of the column in ascending or descending order, sites with zero issues will not be displayed. The order of the results displayed can be toggled by clicking the  or  icon beside the filter.

The **Network Health** dashboard displays the information listed in the table below.

Table 43: *Network Health Dashboard.*

| Header | Description |
|---------------------------------|---|
| Site Name | The name of the site. Clicking on the site name will take you to the Site Health dashboard page (Site > Overview > Site Health tab). To search for a site by name, click on the Site Name label and enter the name of the site. |
| AI Insights | The number of AI Insight reports available for the site. The reports are organized by degree- High , Medium , and Low depending on the number of events in the network. |
| Number of Devices | |
| Status | The number of devices that are in Up or Down state in a site. Hover your mouse over a field with one or more down devices in the column to view the following details. : <ul style="list-style-type: none">■ WLAN Devices Down■ Wired Devices Down■ Branch Devices Down |
| High Memory Usage | The number of devices with high memory utilization in the site. Hover the mouse over a field in the column to view the following details: <ul style="list-style-type: none">■ WLAN High Memory■ Wired High Memory■ Branch High Memory |
| High CPU Usage | The number of devices with high CPU usage in the site. Hover the mouse over a field in the column to view the following details: <ul style="list-style-type: none">■ WLAN CPU High■ Wired CPU High■ Branch CPU High |
| High Channel Utilization | The number of APs with a higher channel utilization in the 5 GHz and 2.4 GHz radio bands. |
| High Noise | The number of APs with high RF noise in the 5 GHz and 2.4 GHz bands. |
| WAN | |
| Uplink Status | Displays the uplink connectivity status of devices in the site. The data is classified into two columns: devices with no issues and devices with no uplink connectivity. |
| Tunnel Status | Displays the connectivity status of tunnels in the site. The data is classified into two columns: tunnels with no issues and tunnels with no connectivity. |

Overview

In the **Network Operations** app, perform the following steps to access the overall network summary page:

1. Set the filter to **All Devices**.

The Global dashboard is displayed.

2. Under **Manage > Overview**, the network summary page displays the following tabs:

- **Summary**—Displays details such as the bandwidth usage in the network, client counts, and cluster-specific details. For more information, see [Summary](#).
- **Network Health**— Displays vital information of the network sorted by site. For more information, [Network Health Dashboard](#).

- **WAN**—Displays information on WAN Health.
- **AI Insights**—Displays information on AP performance issues such as excessive channel changes, excessive reboots, airtime utilization, and memory utilization at AP. For more information, see [AI Insights](#).
- **VisualRF**—Displays a page for viewing campuses, buildings, and floors within a network. For more information, see [Viewing Network Information](#).
- **WiFi Connectivity**—Displays connection details of all the clients connected to an AP. For more information, see [Wi-Fi Connectivity](#).

Summary

The **Summary** tab displays details such as the bandwidth usage, client count, top APs by usage, top 5 clients, top AP clusters by usage, top AP clusters by clients, and WLAN network details of the selected group. By default, the graphs are plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** link.

Table 44: *Summary pane*

| Data Pane Item | Description |
|------------------------------------|--|
| Time Range Filter | Allows you to select a time range for the graphs displayed on the Overview pane. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. |
| Bandwidth Usage Graph | Displays the aggregate incoming and outgoing data traffic of all clients in the selected group. |
| Clients count | Displays the total number of clients connected to an AP over a specific duration. |
| Top APs By Usage | Displays the list of top APs that utilize the maximum bandwidth in the network. Bandwidth usage includes the sum total of data transmitted and received on the radio interfaces and wired clients connected to the AP. |
| Top 5 Clients | Displays the top five clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The Top 5 Clients table displays data only for the clients that are connected to the network for a total duration of two or more hours. |
| Top IAP Clusters By Usage | Displays the list of top AP clusters that utilize the maximum bandwidth in the network. |
| Top IAP Clusters by Clients | Displays the list of top AP clusters connected to the client that utilize the maximum bandwidth in the network. |
| WLANs | Displays the list of SSIDs configured. The WLANs table displays the SSID details such the name, type, security settings, and the clients connected on the network. To expand or collapse the column view, click the column settings icon next to the last column in the table. |

Site Health Dashboard

The **Site Health** dashboard displays details of wired and wireless devices deployed on the site. This page includes information on client connectivity statistics, change logs, health of devices, and RF health of the site.

To launch the **Site Health** dashboard, complete the following procedure:

1. In the **Network Operations** app, use the filter bar to select a site.
2. Under **Manage**, click **Overview > Site Health** to launch the **Site Health** dashboard.

Alternatively, the **Site Health** dashboard can be accessed by selecting a site from the **Network Health** dashboard page. The **Site Health** dashboard displays the information listed in the table below:

Table 45: *Site Health Dashboard*

| Content | |
|-----------------------------------|---|
| Name | Name of the site. |
| Location | Location of the site. |
| APs | Number of APs deployed on the site. |
| Switches | Number of switches deployed on the site. |
| Gateways | Number of gateways deployed on the site. |
| Summary Statistics | A graphical representation of the number of clients (wired and wireless) and their bandwidth usage for the selected time range. |
| Change Log | A visual representation of change logs for configuration, firmware, and reboot changes in the selected time range. Select a column in the graph and click on the Config Log , Firmware Log and Reboot Log button to view detailed information logs on the corresponding events in the site. |
| System Health Indicators | |
| Down Devices | <p>This graph shows the count of devices with DOWN status. The graph displays the following information:</p> <ul style="list-style-type: none"> ■ Total number of devices ■ Number of unique devices that were DOWN ■ Minimum and maximum device downtime. <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with DOWN status and their Up and Down time in percentage. You can also add other metrics such as CPU, Memory, 5 GHz and 2.4 GHz Channel Utilization, and 5 GHz and 2.4 GHz Noise Floor by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the filter icon (🔍) and entering the name of the device.</p> |
| High CPU & High Memory | <p>This graph shows the total count or percentage of devices with high CPU utilization and high memory utilization.</p> <ul style="list-style-type: none"> ■ High CPU Utilization—This graph displays the total number of devices, number of unique devices with high CPU utilization, and minimum and maximum number of devices with high CPU utilization. You can also view the total count or percentage of maximum and minimum number of devices with high CPU utilization for a specific time when you hover your mouse over the graph. ■ High Memory Utilization—This graph displays the total number of devices, number of unique devices, the minimum and maximum number of devices with high memory utilization. You can also view the total count or percentage of maximum and minimum number of devices with high memory utilization for specific time when you hover your mouse over the graph. ■ Threshold Setting Widget—You can also choose to view the graph details based one of the |

Table 45: Site Health Dashboard






| Content | |
|--------------------------------------|---|
| | <p>following criteria by clicking the () icon and selecting any of the following options:</p> <ul style="list-style-type: none"> ■ >70% CPU utilization ■ >80% CPU utilization ■ >90% CPU utilization ■ >70% memory utilization ■ >80% memory utilization ■ >90% memory utilization <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum values. You can add other metrics such as 5 GHz and 2.4 GHz Channel Utilization , 5 GHz and 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the filter icon () and entering the name of the device.</p> |
| RF Health Indicators | |
| 5 GHz Utilization and Noise | <p>This graph displays the total count or percentage of devices with high channel utilization and high noise floor levels for 5 GHz band.</p> <ul style="list-style-type: none"> ■ Device Details—The graph displays total number of devices, number of unique devices with high 5 GHz channel utilization and high noise floor levels, and the minimum and maximum number of devices with high channel utilization. You can also view the total count of maximum and minimum number of devices with high 5 GHz channel utilization and noise for a specific time when you hover your mouse over the graph. ■ Threshold setting—You can also choose to view the graph details based one of the following criteria by clicking the () icon and selecting any of the following options: <ul style="list-style-type: none"> ■ >60% 5 GHz Utilization ■ >70% 5 GHz Utilization ■ >80% 5 GHz Utilization ■ >-75 dBm 5 GHz Noise ■ >-80 dBm 5 GHz Noise ■ >-85 dBm 5 GHz Noise <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with high CPU utilization and memory utilization with their individual minimum and maximum CPU utilization values. You can add other metrics such as CPU, Memory, 2.4 GHz Channel Utilization, 2.4 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the filter icon () and entering the name of the device.</p> |
| 2.4 GHz Utilization and Noise | <p>This graph displays the total count or percentage of devices with a higher channel utilization and high noise floor levels for 2.4 GHz channel.</p> <ul style="list-style-type: none"> ■ Device Details—The graph displays the total number of devices, number of unique devices with high 2.4 GHz channel utilization and noise floor levels, minimum and maximum number of devices with high channel utilization and noise levels. You can also view the total count of maximum and minimum number of devices with high 2.4 GHz Utilization and Noise for a specific time when you hover your mouse over the graph. ■ Threshold Setting widget —You can also choose to view the graph details based one of the following criteria by clicking the () icon and selecting any of the following options: <ul style="list-style-type: none"> ■ >60% 2.4 GHz Utilization |

Table 45: *Site Health Dashboard*

| Content | |
|---|---|
| | <p>>70% 2.4 GHz Utilization</p> <p>>80% 2.4 GHz Utilization</p> <p>>-75 dBm 2.4 GHz Noise</p> <p>>-80 dBm 2.4 GHz Noise</p> <p>>-85 dBm 2.4 GHz Noise</p> <p>To view more details, select a time range in the graph and click on See Devices. A pop-up window displays the details of devices with 2.4 GHz channel utilization and 2.4 GHz noise floor with their individual minimum and maximum values. You can add other metrics such as CPU, Memory, 5 GHz Channel Utilization, 5 GHz Noise Floor, and Device Down time for the devices by clicking on the Add Metric button. A particular device can be filtered from the list by clicking on the filter icon (🔍) and entering the name of the device.</p> |
| <p>NOTE: The threshold setting widget (⚙️) is visible only when you bring the mouse pointer closer to its position slightly above the right-hand side of each graph.</p> | |

Wi-Fi Connectivity

The **Wi-Fi Connectivity** page displays an overall view of the connection details for all clients that are connected to or tried to connect to each connection phase. The connection phases include **Association**, **Authentication**, **DHCP**, and **DNS**.

The connectivity details can also be viewed at a group or a site level. By default, the graphs on the **Wi-Fi Connectivity** page is plotted for a time range of 3 hours. To view the graphs for a different time range, click the **Time Range Filter** link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, and, 1 month.

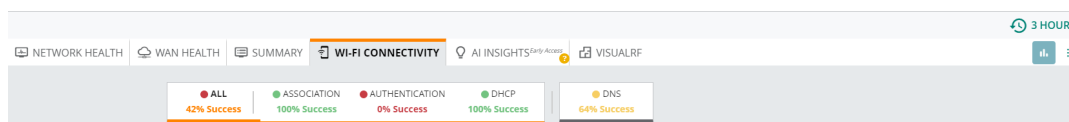
This section includes the following topics:

- [Connectivity Summary Bar](#)
- [Connection Experience](#)
- [AI Insights](#)
- [Connection Problems](#)
- [Connection Events](#)

Connectivity Summary Bar

The connectivity summary bar displays the details of all clients in percentage. It displays the percentage success rate of each stage for the users to know the network performance.

Figure 91 *Connectivity Summary Bar*



The following table describes the information displayed in each section:

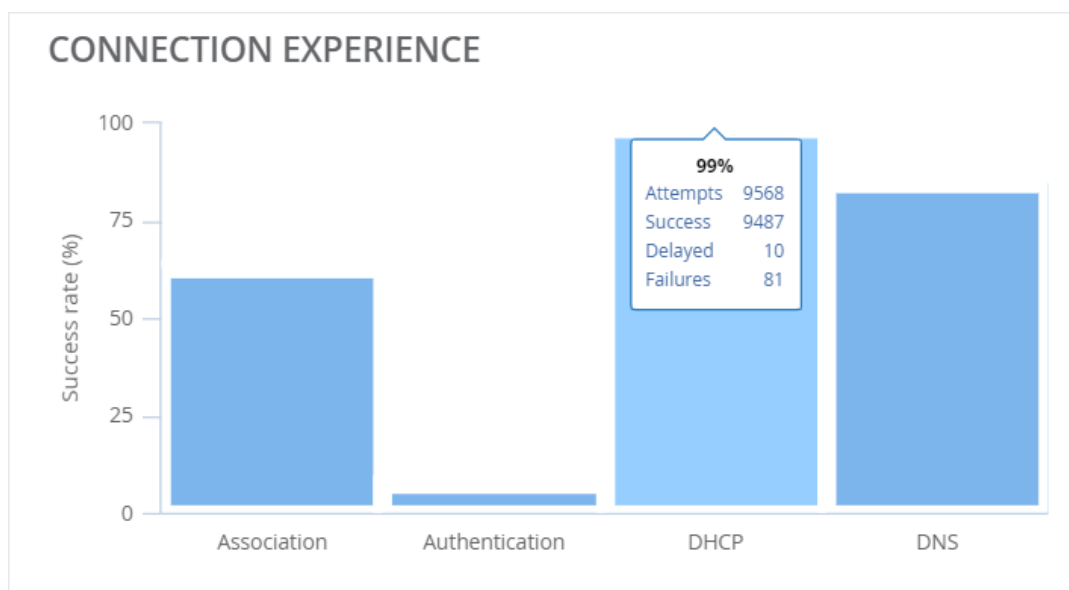
Table 46: *Connectivity Summary Bar*

| Field | Description |
|----------------|---|
| All | Displays the aggregated success percentage of Association, Authentication, and DHCP for all clients connected to the network. |
| Association | Displays the percentage of successful attempts made by a client to connect to the network. |
| Authentication | Displays the percentage of successful attempts of client authentication. |
| DHCP | Displays the percentage of successful attempts of DHCP requests and responses when onboarding a client. |
| DNS | Displays the percentage of successful attempts in the detected DNS resolutions, when a client is connected to the network. |

Connection Experience

The **Connection Experience** tile displays the overall success percentage, total number of attempts, number of successful attempts, total delays, and the total failures for each of the stages based on the selected time range filter. To view the connection experience for each individual stage, select the stage type from the **Connectivity Summary** bar, the **Connection Experience** gets charted for the selected stage.

Figure 92 *Connection Experience tile*



AI Insights

The **AI Insights** tile provides a list of AI Insights generated for a selected time range. To view the details, click on a selected **AI Insight**. The page gets redirected to the AI Insights under the **AI Insights** page. Click each of the listed AI Insight for a detailed analysis based on the impact on the network. For more information on AI Insights, see [AI Insights](#).

AI-Insights is not implemented for **Association** and **DNS**. AI Insights is not implemented at a Group level also. The page displays **No AI Insights observed**.

For a visual representation of viewing an AI Insight, click [here](#).



NOTE

Connection Problems

The **Connection Problems** tile displays the details of **Failures** and **Delays** graphically for each of the categories from the drop-down list. Each graph displays the top five MAC addresses or SSID based on the selected category. Each category in the **Connection Problems** drop-down lists changes based on the selected stage in the **Connectivity Summary** bar. Selecting the required category from the drop-down displays the failures and delays in a pie chart with percentage, and a bar graph with the number of failures and delays. Hover the cursor over each graph to view the number of failures or delays for each stage.

Figure 93 *Connection Problems Tile*



The following table describes the information displayed in each connection category based on the selected stage:

Table 47: *Connection Problems Rolls-ups*

| Data Pane Content | Description |
|-----------------------|--|
| All | <p>Displays the details of the failures and delays that occurred during a client connection. The chart displays the failure details of Association, Authentication, and DHCP for each client. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Stage ■ By Clients ■ By Access Points ■ By Band ■ By SSID |
| Association | <p>Charts the details of the failures and delays that occurred during a client association. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Reason |
| Authentication | <p>Charts the details of the failures and delays that occurred during a client authentication. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Type ■ By Clients ■ By Access Points ■ By Band ■ By SSID ■ By Server |
| DHCP | <p>Charts the details of the failures and delays that occurred during the attempts of DHCP requests and responses by a client. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Clients ■ By Access Points ■ By Reason |
| DNS | <p>Charts the details of the failures and delays that occurred during the attempts in detected DNS resolutions when a client is connected to the network. The Connection Problems drop-down list includes the following categories:</p> <ul style="list-style-type: none"> ■ By Access Points ■ By Reason ■ By Server |

Connection Events

Connection Events table details out the list of delays and failures for each client based on the client MAC

addresses. Click the  icon to view the connection events table. Click the **Connection Events** drop down to filter the events **By Clients** or **By Access Points**. The **Connection Events** table displays the following information:

Table 48: *Connection Events*

| Data Pane Content | Description |
|-------------------|--|
| MAC Address | Displays the MAC address of the client. |
| Delays | Displays the delays that occurred during the event. |
| Failures | Displays the failure details that occurred during the event. |

AI Insights

The AI Insights dashboard displays a report of network events that could possibly affect the quality of the overall network performance. These are anomalies observed at the access point, connectivity, and client level observed in the network for the selected time range. Each insight report provides specific details on the occurrences of these events for easy debugging.

To launch the **AI Insights** dashboard, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > AI Insights** to launch the **AI Insights** page.

All AI Insights observed for the network are listed in the **AI Insight** dashboard in the **All Devices** context. Alternatively, AI Insights reports for a specific site, access point, or a client can be viewed by selecting the appropriate context. A summary of AI Insights generated for a site is displayed in the **Network Health** dashboard.



AI Insights are displayed for the time range selected. Select the time range from the **Time Range Filter** (🕒) to filter reports.

AI Insights Categories

AI Insights are categorized in high, medium, and low priorities depending on the number of occurrences.

- **Red**—High priority
- **Yellow**—Medium priority
- **Gray**—Low priority

AI Insights listed in the dashboard are sorted from high priority to low priority. The description indicates the network event and the number of occurrences of that event for the selected context and time period defined. Clicking on the description displays a graph displaying number of events over time and tables with other specific information. Hover the pointer over graphs to view specific count of events and click on a tab to view the corresponding table information.



Tables displayed within each AI Insights report vary on the scope selected.

| | | |
|---|---|---|
| ● AP with High Memory Utilization (15 Access Points) | Access Points are experiencing higher than normal memory utilization | ▼ |
| ● 802.1x Authentication Failures (227995 failures) | Users connecting to WiFi using 802.1x authentication are experiencing higher than normal failures | ▼ |
| ● 4-Way Handshake (EAPOL Key) Failures (197458 failures) | Users connecting to WiFi using PSK authentication are experiencing higher than normal failures | ▼ |
| ● AP with Missing Telemetry (8 radios) | Access Points telemetry data is not reaching Aruba Central | ▼ |
| ● Clients with Excessive 2.4 GHz Dwell Time (4 % client devices) | Dual band capable devices are spending a significant amount of time on the 2.4 GHz band | ▼ |
| ● Excessive AP Channel Changes (2011 Channel Changes) | Access Point radios are changing channels excessively | ▼ |
| ● High DHCP Failures (27670 failures) | Client DHCP failures are greater than normal client DHCP failures | ▼ |
| ● Frequent AP Transmit Power Changes (40 power changes) | Access Point radios are changing power levels more than normal | ▼ |
| ● Excessive AP Reboots (2 reboots) | Access Points are rebooting more than normal | ▼ |

The **AI Insights** dashboard displays reports on the following network events. The list describes the insights followed by the information tables available for the insight:

- [802.1X Authentication Failures](#)
- [4-way Handshake \(EAPOL Key\) Failures](#)
- [AP with Missing Telemetry](#)
- [AP Transmit Power Recommendation](#)
- [AP with High 2.4 GHz Airtime Utilization](#)
- [AP with High 5 GHz Airtime Utilization](#)
- [AP with High Memory Utilization](#)
- [Clients with Excessive 2.4 GHz Dwell Time](#)
- [Excessive AP Channel Changes](#)
- [Excessive AP Reboots](#)
- [Frequent AP Transmit Power Changes](#)
- [Clients with Low SNR Uplink Connections](#)
- [AP with High CPU Utilization](#)
- [High DHCP Failures](#)
- [MAC Authentication Failures](#)

802.1X Authentication Failures

The **802.1X Authentication Failures** insight displays excessive 802.1X authentication failures observed in the network. The graph displays the number of 802.1X authentication failures observed across time:

- **SSID**—Graph of the percent of 802.1X authentication failures sorted by SSIDs.
- **Reason**—Graph of the percent of 802.1X authentication failures sorted by reason for failure.
- **Clients**—Information of clients that failed 802.1X authentication.
- **Access Points**—Number of 802.1X authentication failures observed at an AP and its details.
- **AP Model**—Displays a graph of the percent of 802.1X authentication failures sorted by AP models.
- **FW Version**—Graph of the percent of 802.1X authentication failures sorted by AP firmware version.
- **Server**—Graph of the percent of 802.1X authentication failures sorted by authentication servers.
- **Sites**—Number of 802.1X authentication failures observed in a site.

4-way Handshake (EAPOL Key) Failures

The **4-way Handshake (EAPOL Key) Failures** insight reports on excessive 4-way handshake failures observed in the network. The graph displays the number of 4-way handshake (EAPOL Key) failures observed across time.

- **SSID**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by SSIDs.
- **Reason**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by reason for failure.
- **Clients**—Information of clients that failed 4-way handshake authentication.
- **Access Points**—Number of 4-way handshake (EAPOL Key) failures observed at an AP and its details.
- **AP Model**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by AP models.
- **FW Version**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by AP firmware version.
- **Sites**—Number of 4-way handshake (EAPOL Key) failures observed in a site.

AP with Missing Telemetry

The **APs Missing Telemetry** insight displays AP radios that missed sending telemetry data to Aruba Central. The graph displays the number of 2.4 GHz and 5 GHz radios that failed to send telemetry data across time.

- **Access Points**—Information on missing telemetry reports sorted by APs.
- **Sites**—Information on missing telemetry reports reported at APs in a site.

AP Transmit Power Recommendation

The **AP Transmit Power Recommendation** insight provides recommendation for transmit power setting to optimize the network. The recommendations are arrived upon based on the analytics of **Frequent AP Transmit Power Changes** insight.

- **Recommendation**—Current setting and the recommended setting for the 2.4 GHz and 5 GHz radio band.
- **Band**—Graph of the percent of minutes the transmit power varied in the 2.4 GHz and 5 GHz bands.
- **SSID**—Graph of the percent of minutes the transmit power varied in the 2.4 GHz and 5 GHz band sorted by SSIDs.

AP with High 2.4 GHz Airtime Utilization

The **AP High 2.4 GHz Airtime Utilization** insight displays the number of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day.

- **Root Cause**—Lists the possible causes for this failure type and recommended actions for resolving this issue.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Hours of the Day**—Graph of which hours of the day the network was most impacted by excessive AP airtime utilization.
- **Tx Power**—Graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **SNR**—Graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 2.4 GHz band and 5 GHz band.
- **Access Points**—High 2.4 GHz Airtime utilization information for individual APs.
- **Sites**—High 2.4 GHz Airtime utilization information classified by site.

AP with High 5 GHz Airtime Utilization

The **AP High 5 GHz Airtime Utilization** insight displays the numbers of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and specific period of time as selected in the **Time Range Filter**.

- **Root Cause**—Lists possible causes for this failure type and recommendations for resolving this issue.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Hours of the Day**—Hours of the day the network was most impacted by excessive AP airtime utilization. The charts show the airtime utilization score for each hour of the day, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Clients**—List of clients connected to 5 GHz AP radio.
- **Tx Power**—Strength of the signal that the AP produces during the time it is transmitting signal to the client.
- **SNR**—Average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 5 GHz band.
- **Access Points**—High 5 GHz Airtime utilization information for individual APs.
- **Sites**—High 5 GHz Airtime utilization information classified by site.

AP with High Memory Utilization

The **APs with High Memory** insight displays information about APs that have higher memory utilization.

- **Access Points**—Average memory utilization for each AP.
- **FW Version**—Pictorial graph of APs with high memory utilization classified by AP software versions.
- **AP Model**—Pictorial graph of APs with high memory utilization classified by AP models.
- **Sites**—APs with high memory information classified by site.

Clients with Excessive 2.4 GHz Dwell Time

The **Clients with Excessive 2.4 GHz Dwell Time** insight reports on dual band capable clients that spent more time in the 2.4 GHz band instead of the 5 GHz bands. The graph displays the percentage of clients over dwelling in the 2.4 GHz band across time.

- **Access Points**—Number of clients dwelling in the 2.4 GHz band observed at an AP.
- **Clients**—Client information and the time spent in the radio bands.
- **Device Type**—Graph of the percent of clients dwelling in the 2.4 GHz band sorted by client device type.
- **Sites**—Number of clients and APs impacted in a site.

Excessive AP Channel Changes

The **Excessive Channel Changes** insight displays information about AP radios on the network that changed channels excessively.

- **Reason**—Reason for which the AP might have changed the channels on the network. It might be due to different reasons such as interference, noise threshold, channel quality threshold, or empty channel for both the frequency bands (2.4 GHz and 5 GHz).
- **Clients**—MAC Address, name, and the corresponding number of channel changes for each client.
- **Channel**—Number of channel changes per channel for that AP during the selected time period. It shows a comparison of the channel change between the peer network and AP.
- **Band**—Channel change based on both 2.4 GHz and 5 GHz represented in pie chart format.

- **Access Points**—Channel change information for individual APs.
- **AP Model**—Pictorial graph of the channel changes classified by AP models.
- **FW version**—Pictorial graph of channel changes classified by AP software versions.
- **Sites**—Excessive channel change information classified by site.

Excessive AP Reboots

The **Excessive AP Reboots** insight displays the information about APs that have been rebooted the maximum times and also the corresponding reason of the frequent reboot. The graph shows the number of AP reboots observed across time.

- **Access Points**—Number of reboots observed at an AP.
- **Reboots**—Number of reboots over time.
- **FW Version**—Graph of AP reboots observed in a particular firmware version.
- **AP Model**—Graph of AP reboots observed in a particular firmware version.
- **Sites**—Number of reboots observed at APs in a site.

Frequent AP Transmit Power Changes

The **Frequent AP Transmit Power Changes** insight reports on AP radios that frequently changed transmission power levels. The graph displays the number of AP Transmit power change events observed across time.

- **Access Points**—Count of power transmit changes observed at an AP.
- **Power Changes Over Time**—Graphs of power transmit changes observed across time for 2.4 GHz and 5 GHz radio.
- **Power Distribution**—Graph of percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band.
- **Band**—Graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.
- **Variance**—Graph of the percentage of variance in transmission power across number of APs in that power variance for the 2.4 GHz and 5 GHz band.
- **Sites**—Count of power changes observed at a site.

Clients with Low SNR Uplink Connections

The **Low SNR Links** insight report shows information about access points that have a low-quality signal-strength connection.

- **Access Points**— Displays the list of APs experiencing low signal quality (minutes).
- **Clients**— Displays the list of connected clients experiencing low signal quality (minutes).
- **Band**— Displays if devices experiencing a low signal-quality link were using 2.4 GHz or 5 GHz radio bands.
- **Good vs Bad**— Displays the amount of time (minutes) with Low SNR (Bad) and High SNR (Good) for all the clients. The data is represented in the form of a pie chart.
- **Tx Power**— Displays the percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **Client Type**— Displays the device type experiencing low signal quality.
- **Sites**— Displays the list of APs and Clients experiencing low signal quality at a particular site.

AP with High CPU Utilization

The **APs with High CPU** insight shows information about AP with unusually high CPU utilization levels.

- **Access Points**—Average memory utilization for each AP.
- **FW Version**—Pictorial graph of APs with high memory utilization classified by AP software versions.

- **AP Model**—Pictorial graph of APs with high memory utilization classified by AP models.
- **Sites**—APs with high memory information classified by site.

High DHCP Failures

The **High DHCP Failures** insight reports on excessive client to AP DHCP failures observed in the network. The graph displays the number of DHCP failures observed across time.

- **SSID**—Graph of the percent of DHCP failures sorted by SSIDs.
- **Reason**—Graph of the percent of DHCP failures sorted by reason for failure.
- **Clients**—Information of clients that failed DHCP handshake.
- **Access Points**—Number of failures observed at an AP and its details.
- **AP Model**—Graph of the percent of DHCP failures sorted by AP models.
- **FW Version**—Graph of the percent of DHCP failures sorted by AP firmware version.
- **Sites**—Number of DHCP failures and APs impacted in a site.

MAC Authentication Failures

The **MAC Authentication Failures** insight reports on excessive MAC authentication failures observed in the network. The graph displays the number of MAC authentication failures observed across time.

- **SSID**—Graph of the percent of MAC authentication failures sorted by SSIDs.
- **Reason**—Graph of the percent of MAC authentication failures sorted by reason for failure.
- **Clients**—Information of clients that failed MAC authentication.
- **Access Points**—Number of MAC authentication failures observed at an AP and its details.
- **AP Model**—Graph of the percent of MAC authentication failures sorted by AP models.
- **FW Version**—Graph of the percent of MAC authentication failures sorted by AP firmware version.
- **Sites**—Number of MAC authentication failures observed in a site.

Sites—AI Insights

The **AI Insights** dashboard in the site context displays a report of network events that could possibly affect the quality of the overall network performance for a particular site. These are anomalies observed at the access point, connectivity, and client level in the site for the selected time range. Each Insight report provides specific details on the occurrences of these events for easy debugging.

To launch the **AI Insights** dashboard for site, complete the following steps:

1. In the **Network Operations** app, use the filter to select a site.
2. Under **Manage**, click **Overview > AI Insights** to launch the **AI Insights** page.

AI Insights observed in the site are listed in the **AI Insights** dashboard in this context. It displays the data for that particular site selected by the user.



AI Insights reports are displayed for the time range selected. The user can select the time range from the **Time Range Filter** (🕒).

Each insight further includes categories of information present in form of tabs like, reason, band, channel, SNR, and so on. These tabs can be clicked and displays the detailed information found in that section of the Insight.

The **AI Insights** page displays the performance issues based on the following criteria:

- [802.1X Authentication Failures](#)
- [4-way Handshake \(EAPOL Key\) Failures](#)

- [AP with Missing Telemetry](#)
- [AP with High 2.4 GHz Airtime Utilization](#)
- [AP with High 5 GHz Airtime Utilization](#)
- [AP with High Memory Utilization](#)
- [Clients with Excessive 2.4 GHz Dwell Time](#)
- [Excessive AP Channel Changes](#)
- [Excessive AP Reboots](#)
- [Frequent AP Transmit Power Changes](#)
- [Clients with Low SNR Uplink Connections](#)
- [AP with High CPU Utilization](#)
- [High DHCP Failures](#)
- [MAC Authentication Failures](#)

802.1X Authentication Failures

The **802.1X Authentication Failures** insight displays excessive 802.1X authentication failures observed in the network. The graph displays the number of 802.1X authentication failures observed across time:

- **SSID**—Graph of the percent of 802.1X authentication failures sorted by SSIDs.
- **Reason**—Graph of the percent of 802.1X authentication failures sorted by reason for failure.
- **Clients**—Information of clients that failed 802.1X authentication.
- **Access Points**—Number of 802.1X authentication failures observed at an AP and its details.
- **AP Model**—Displays a graph of the percent of 802.1X authentication failures sorted by AP models.
- **FW Version**—Graph of the percent of 802.1X authentication failures sorted by AP firmware version.
- **Server**—Graph of the percent of 802.1X authentication failures sorted by authentication servers.

4-way Handshake (EAPOL Key) Failures

The **4-way Handshake (EAPOL Key) Failures** insight reports on excessive 4-way handshake failures observed in the network. The graph displays the number of 4-way Handshake (EAPOL Key) failures observed across time.

- **SSID**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by SSIDs.
- **Reason**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by reason for failure.
- **Clients**—Information of clients that failed 4-way handshake authentication.
- **Access Points**—Number of 4-way handshake (EAPOL Key) failures observed at an AP and its details.
- **AP Model**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by AP models.
- **FW Version**—Graph of the percent of 4-way handshake (EAPOL Key) failures sorted by AP firmware version.

AP with Missing Telemetry

The **APs Missing Telemetry** insight displays AP radios that missed sending telemetry data to Aruba Central. The graph displays the number of 2.4 GHz and 5 GHz radios that failed to send telemetry data across time.

- **Access Points**—Information on missing telemetry reports sorted by APs.

AP with High 2.4 GHz Airtime Utilization

The **AP High 2.4 GHz Airtime Utilization** insight displays the number of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and time of day.

- **Root Cause**—Lists the possible causes for this failure type and recommended actions for resolving this issue.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Hours of the Day**—Graph of which hours of the day the network was most impacted by excessive AP airtime utilization.
- **Tx Power**—Graph of Tx Power distribution (dBm) for both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **SNR**—Graph of the average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 2.4 GHz band and 5 GHz band.
- **Access Points**—High 2.4 GHz Airtime utilization information for individual APs.

AP with High 5 GHz Airtime Utilization

The **AP High 5 GHz Airtime Utilization** insight displays the numbers of AP radios whose Wi-Fi channel utilization deviated from the normal utilization range, as compared to other APs broadcasting in the same location, RF band, and specific period of time as selected in the **Time Range Filter**.

- **Root Cause**—Lists possible causes for this failure type and recommendations for resolving this issue.
- **Channel**—Chart of AP radio channels that experienced excessive AP airtime utilization. It displays the channels impacted by this issue over the selected time period, sorted by airtime utilization score, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Hours of the Day**—Hours of the day the network was most impacted by excessive AP airtime utilization. The charts show the airtime utilization score for each hour of the day, which is calculated from the severity of the utilization level and the duration of time that the channel was over utilized.
- **Clients**—List of clients connected to 5 GHz AP radio.
- **Tx Power**—Strength of the signal that the AP produces during the time it is transmitting signal to the client.
- **SNR**—Average Signal-to-Noise Ratio of the AP in different percentiles (25th, 50th, 75th, 90th, 99th) in 5 GHz band.
- **Access Points**—High 5 GHz Airtime utilization information for individual APs.

AP with High Memory Utilization

The **APs with High Memory** insight displays information about APs that have higher memory utilization.

- **Access Points**—Average memory utilization for each AP.
- **FW Version**—Pictorial graph of APs with high memory utilization classified by AP software versions.
- **AP Model**—Pictorial graph of APs with high memory utilization classified by AP models.

Clients with Excessive 2.4 GHz Dwell Time

The **Clients with Excessive 2.4 GHz Dwell Time** insight reports on dual band capable clients that spent more time in the 2.4 GHz band instead of the 5 GHz bands. The graph displays the percentage of clients over dwelling in the 2.4 GHz band across time.

- **Access Points**—Number of clients dwelling in the 2.4 GHz band observed at an AP.
- **Clients**—Client information and the time spent in the radio bands.
- **Device Type**—Graph of the percent of clients dwelling in the 2.4 GHz band sorted by client device type.

Excessive AP Channel Changes

The **Excessive Channel Changes** insight displays information about AP radios on the network that changed channels excessively.

- **Reason**—Reason for which the AP might have changed the channels on the network. It might be due to different reasons such as interference, noise threshold, channel quality threshold, or empty channel for both the frequency bands (2.4 GHz and 5 GHz).
- **Clients**—MAC Address, name, and the corresponding number of channel changes for each client.
- **Channel**—Number of channel changes per channel for that AP during the selected time period. It shows a comparison of the channel change between the peer network and AP.
- **Band**—Channel change based on both 2.4 GHz and 5 GHz represented in pie chart format.
- **Access Points**—Channel change information for individual APs.
- **AP Model**—Pictorial graph of the channel changes classified by AP models.
- **FW version**—Pictorial graph of channel changes classified by AP software versions.

Excessive AP Reboots

The **Excessive AP Reboots** insight displays the information about APs that have been rebooted the maximum times and also the corresponding reason of the frequent reboot. The graph shows the number of AP reboots observed across time.

- **Access Points**—Number of reboots observed at an AP.
- **Reboots**—Number of reboots over time.
- **FW Version**—Graph of AP reboots observed in a particular firmware version.
- **AP Model**—Graph of AP reboots observed in a particular firmware version.

Frequent AP Transmit Power Changes

The **Frequent AP Transmit Power Changes** insight reports on AP radios that frequently changed transmission power levels. The graph displays the number of AP Transmit power change events observed across time.

- **Access Points**—Count of power transmit changes observed at an AP.
- **Power Changes Over Time**—Graphs of power transmit changes observed across time for 2.4 GHz and 5 GHz radio.
- **Power Distribution**—Graph of percentage of time spent across power levels for the time period in the 2.4 GHz and 5 GHz band.
- **Band**—Graph of the percent of number of changes observed in the 2.4 GHz and 5 GHz bands.
- **Variance**—Graph of the percentage of variance in transmission power across number of APs in that power variance for the 2.4 GHz and 5 GHz band.

Clients with Low SNR Uplink Connections

The **Low SNR Links** insight report shows information about access points that have a low-quality signal-strength connection.

- **Access Points**— Displays the list of APs experiencing low signal quality (minutes).
- **Clients**— Displays the list of connected clients experiencing low signal quality (minutes).
- **Band**— Displays if devices experiencing a low signal-quality link were using 2.4 GHz or 5 GHz radio bands.
- **Good vs Bad**— Displays the amount of time (minutes) with Low SNR (Bad) and High SNR (Good) for all the clients. The data is represented in the form of a pie chart.
- **Tx Power**— Displays the percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band during the time it is transmitting signal to the client.
- **Client Type**— Displays the device type experiencing low signal quality.

AP with High CPU Utilization

The **APs with High CPU** insight shows information about AP with unusually high CPU utilization levels.

- **Access Points**—Average memory utilization for each AP.
- **FW Version**—Pictorial graph of APs with high memory utilization classified by AP software versions.
- **AP Model**—Pictorial graph of APs with high memory utilization classified by AP models.

High DHCP Failures

The **High DHCP Failures** insight reports on excessive client to AP DHCP failures observed in the network. The graph displays the number of DHCP failures observed across time.

- **SSID**—Graph of the percent of DHCP failures sorted by SSIDs.
- **Reason**—Graph of the percent of DHCP failures sorted by reason for failure.
- **Clients**—Information of clients that failed DHCP handshake.
- **Access Points**—Number of failures observed at an AP and its details.
- **AP Model**—Graph of the percent of DHCP failures sorted by AP models.
- **FW Version**—Graph of the percent of DHCP failures sorted by AP firmware version.

MAC Authentication Failures

The **MAC Authentication Failures** insight reports on excessive MAC authentication failures observed in the network. The graph displays the number of MAC authentication failures observed across time.

- **SSID**—Graph of the percent of MAC authentication failures sorted by SSIDs.
- **Reason**—Graph of the percent of MAC authentication failures sorted by reason for failure.
- **Clients**—Information of clients that failed MAC authentication.
- **Access Points**—Number of MAC authentication failures observed at an AP and its details.
- **AP Model**—Graph of the percent of MAC authentication failures sorted by AP models.
- **FW Version**—Graph of the percent of MAC authentication failures sorted by AP firmware version.

For more information about AI Insights at a global context, see [AI Insights Categories](#).

All Clients

The **Clients** page provides a list view of all the clients connected to the network. You can filter clients based on the network the clients are connected to. The page displays key client information and also allows you to view a specific client detail page.

By default, the **Clients** page displays a unified list of all clients for the selected group. The list of clients is populated for a time range of 3 hours. To view the list of clients for a different time range, click the **Time Range Filter** and select the required time period. Total data usage for the selected time period is displayed above the client summary bar.

To filter clients based on the device to which the clients are connected, select the device type from the **Clients** drop-down list:

- **All**—Displays a list of all the clients connected to the network.
- **AP**—Displays a list of clients connected to the Instant AP.
- **Switch**—Displays a list of clients connected to the switch.
- **Gateway**—Displays a list of clients connected to the Aruba Gateway.



The wired client will show up in the **All Clients** page only if the client is connected to an Aruba 2540 Series, Aruba 2920 Series, Aruba 2930F Series, Aruba 2930M Series, Aruba 3810 Series, or Aruba 5400R Series switch.

To filter clients based on the network to which the clients are connected, click the network type from the **Client Summary** bar:

- **Wireless**—Displays a list of clients connected to the wireless network.
- **Wired**—Displays a list of clients connected to the wired network.

The **Clients** table lists the details of each client. By default, the table displays the following columns: **Client Name**, **Status**, **IP Address**, **Connected To**, **VLAN**, **Connected To**, **Link**, **AP Role**, **Gateway Role**, and **Health**. Click the ellipsis icon to perform additional operations:

- **Download CSV**—Downloads the client details in the .csv file format.
- **Select All**—Selects all columns.
- **Reset Columns**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. For example, in the **Client Name** column, enter the name of the client and in the **Status** column, select from one of the predefined filter criteria: **Connected**, **Offline**, or **Failed**.

Table 49: All Client Details

| Column Names | Applicability | Description |
|---------------------|--|---|
| Client Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Username, hostname, or MAC address of the client. Click the client name to view the Summary page. |
| Status | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch | <p>Client connection status. Use the filter option to view the following:</p> <ul style="list-style-type: none"> ■ Connected clients ■ Offline clients ■ Failed clients. <p>Hover the cursor over the status column to view a pop-up summary based on the connection status. The status summary is populated based on the status type. Each status type and the summary is described below:</p> <p>Connected:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ IP address—Client IP address ■ Connected Since—Date and time at which the client was connected. ■ Health Score—Device health. <p>Offline:</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ IP address—Client IP address ■ Connected Since—Date and time at which the client was connected. ■ Last Seen Time—Date and time the client was last connected. <p>Failed</p> <ul style="list-style-type: none"> ■ Client name—Name of the client. ■ Authentication—Authentication type of the client. ■ Last Seen Time—Date and time the client was last connected. ■ Failure Stage—Status of the client that failed to connect. ■ Failure Reason—Reason for the client failure. |
| IP Address | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch | IP address of the client. |
| VLAN | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | VLAN of the device to which the client is connected. |
| Connected To | <ul style="list-style-type: none"> ■ All | AP name, Switch name, or Gateway name. This is the first layer 2 hop for the client. If the device does not have a name, the MAC address is displayed. |
| Link | <ul style="list-style-type: none"> ■ All | Displays the SSID for wireless clients and the port number for wired clients. |
| AP Role | <ul style="list-style-type: none"> ■ All ■ AP | Role assigned by the Instant AP. |
| Gateway Role | <ul style="list-style-type: none"> ■ All ■ Gateway | Role assigned by the Aruba Gateway. |
| Health | <ul style="list-style-type: none"> ■ All ■ AP ■ Gateway | <p>Client health. The value can be one of the following:</p> <ul style="list-style-type: none"> ■ Poor—0-25 ■ Fair—26-50 ■ Good—51-100 |

Table 49: All Client Details

| Column Names | Applicability | Description |
|-----------------------|--|---|
| Failure Stage | <ul style="list-style-type: none"> ■ All ■ AP | Failure status of the client that failed to connect. The failure reasons could be: <ul style="list-style-type: none"> ■ Association error ■ MAC authentication error ■ 802.1X authentication error ■ Key exchange error ■ DHCP error ■ Captive Portal error |
| Group Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Group name of the device managed by Aruba Central. |
| Site Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Name of the site in which the devices managed by Aruba Central are installed. |
| MAC Address | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | MAC address of the client. |
| Hostname | <ul style="list-style-type: none"> ■ All ■ AP ■ Gateway | Host name of the client. |
| User Name | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Username of the client. |
| Key Management | <ul style="list-style-type: none"> ■ All ■ AP | Security mode used by the client. |
| Authentication | <ul style="list-style-type: none"> ■ All ■ AP | Authentication type. |
| IPv6 Address | <ul style="list-style-type: none"> ■ All ■ AP | IPv6 address of the client. |
| Capabilities | <ul style="list-style-type: none"> ■ All ■ AP | Client capabilities. |
| Usage | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Total data usage for the selected time period. |
| OS | <ul style="list-style-type: none"> ■ All ■ AP ■ Gateway | Operating system of the client. |

Table 49: *All Client Details*

| Column Names | Applicability | Description |
|------------------------|--|--|
| Last Seen Time | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Date and time when the client was last seen. |
| Connected Since | <ul style="list-style-type: none"> ■ All ■ AP ■ Switch ■ Gateway | Date and time since when the client was connected. |
| AP Name | <ul style="list-style-type: none"> ■ All ■ AP | Name of the Instant AP. |
| AP Mac Address | <ul style="list-style-type: none"> ■ All ■ AP | MAC address of the Instant AP. |
| Channel/Band | <ul style="list-style-type: none"> ■ All ■ AP | Last connected channel and band. |
| Switch Name | <ul style="list-style-type: none"> ■ All ■ Switch | Name of the switch. |
| Port | <ul style="list-style-type: none"> ■ All ■ Switch ■ Gateway | Port number of the switch. |
| Gateway Name | <ul style="list-style-type: none"> ■ All ■ Gateway | Name of the Aruba Gateway. |

Client Overview

The **Clients** page displays the details of clients connected to the devices in Aruba Central and their connectivity status. The overview page displays the total number of clients, bandwidth usage, and the application usage by the clients connected to the wired and wireless networks. The following table describes the information displayed in each section:

Table 50: *Client Overview Page*

| Data Pane Content | Description |
|--------------------------|---|
| Time Range Filter | By default, the graphs on the Clients page are plotted for a time range of 3 hours. To view the graphs for a different time range, click the Time Range Filter link. You can choose to view graphs for a time period of 3 hours, 1 day, 1 week, 1 month and 3 months. However, the Distribution data (Client OS) under the Distribution tab does not honor the time range you selected in the time range filter. |
| Total | Displays the total number of clients. |
| Wireless | Displays the total number of clients connected to wireless network. |

| Data Pane Content | Description |
|---------------------|---|
| Wired | Displays the total number of clients connected to the wired network. |
| Usage | Displays the Bandwidth Usage of the incoming and outgoing throughput traffic for all the clients during a specific time range. The graph will not show any data for the clients that are connected to the network for less than two hours. |
| Distribution | Displays the type of client device connected to the wireless network. |
| Top N | Displays a list of clients connected to the currently available SSIDs that utilize the maximum bandwidth in the network. The Top Clients by Usage table displays data only for the clients that are connected to the network for a total duration of two or more hours. |

Wireless Client Overview

The overview page displays the client summary details and client sessions details for the selected wireless client. The section includes the following topics:

- [Viewing Clients Connected to Wireless Networks](#)
- [Wireless Client Summary](#)
- [Wireless Client Sessions](#)
- [Applications](#)
- [Live Events](#)
- [Events](#)

Viewing Clients Connected to Wireless Networks

To view the details of a client connected to the wireless network:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the client table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network.
6. Enter the client name in the **Client Name** column and then click the client name. The **Client Summary** page is displayed.
7. Additionally, click **Sessions** to view the client sessions details.

Wireless Client Summary

The wireless client summary page displays the client summary bar and the wireless client details.

Wireless Client Summary

The client summary bar displays the client connection, device health, and transmission rate along with name of the device the client is connected to. The **Summary** bar displays the following information:

Table 51: *Client Summary Bar*

| Field | Description |
|----------------------|--|
| Connection status | Connection status of the client. Connection status is updated immediately on state change. |
| Device Health | Signal strength of the client device. The signal strength value is displayed in percentage: <ul style="list-style-type: none">■ 0-25—Poor■ 26-50—Fair■ 50-100—Good |
| SNR | SNR for the client as measured by the AP. The SNR value is displayed in decibels: <ul style="list-style-type: none">■ 0-20—Poor■ 21-35—Fair■ >35—Good |
| TX Rate | Data transmission rate. |
| RX Rate | Data reception rate. |
| Connected To | Name of the AP that broadcasts the SSID to which the client is connected. Click the name of the AP to view the device details page. |

Wireless Client Details

The wireless **Client Details** page displays the client overview details, connectivity summary, location, UCC, and AirGroup information for the selected client. The client details page includes the following topics:

- [Overview](#)
- [AI Insights](#)
- [Connectivity](#)
- [Location](#)
- [UCC](#)
- [AirGroup](#)

Overview

The **Overview** tab displays information about the type of data path that the client uses, the network and connectivity details, and basic client details such as IP address of the client, type of encryption etc. The following table describes the information displayed in each section:

Table 52: *Overview Tab*

| Section | Description |
|-------------------|--|
| Data Path | Displays the data path of the client in the network. Click the AP icon to view the AP details page. The data path can be one of the following: <ul style="list-style-type: none">■ Client > SSID > AP■ Client > SSID > AP > Switch■ Client > SSID > AP > Switch > Gateway■ Client > SSID > AP > Gateway |
| Client | Displays the following information: <ul style="list-style-type: none">■ Username—User name of the client.■ Hostname—Hostname of the client.■ Client Type—Type of the client device.■ IP Address—IP address of the client.■ MAC Address—MAC address of the client.■ Manufacturer—Manufacturer of the client device.■ Encryption—Type of client encryption.■ Connected Since—Date and time since when the client is connected.■ Device OS—Operating system running on the client device. |
| Network | Displays the following information: <ul style="list-style-type: none">■ VLAN—Displays the VLAN ID on which the client is connected to the AP.■ VLAN Derivation—Displays the VLAN derivation method used for assigning an IP address to the client. Aruba devices can assign a static or dynamically derived IP address from a DHCP pool to the clients.■ AP Role—Displays the role assigned to the client by the AP.■ AP Derivation—Displays the role derivation method used for assigning a role to a client. For example, clients that authenticate successfully can be assigned a default role as per the AAA profile.■ Gateway Role—Displays the role assigned to the client by the Gateway.■ Auth Server—Server that last authenticated the client device. The field displays the IP address of the server that performed either 802.1X or MAC authentication for the client device. If the client connects to the network through 802.1X and MAC authentication, Aruba Central displays only the IP address of the server that performed 802.1X authentication.■ DHCP Server—DHCP server that last assigned IP address to the client. |
| Connection | Displays the following information: <ul style="list-style-type: none">■ Channel—Radio channel assigned to the client.■ Band—Radio band on which the client is connected.■ Client Capabilities—Capabilities of the client device.■ Client Max Speed—Wireless link data transfer speed.■ LEDs on AP—Enables or disables the LED indication on the corresponding AP to which the client is connected. |

AI Insights

The **AI Insight** tab displays information about client performance and connectivity issues such as, excessive 2.4 GHz dwell and low SNR links. AI Insights are displayed for a selected time period based on the time selected in **Time Range Filter**. The user can select 3 hours, 1 week, 1 day, or 1 month to view the insight data. Each AI Insight type displays the AI Insight label, AI Insight graph, and AI Insight chart. Further, the Insights include categories of information present in form of tabs like, reason, band, channel, SNR and so on. These tabs are

clickable and display the detailed information found in that section of the Insight. For more information on AI Insights, see [AI Insights](#).

AI Insight Label

Each AI insight label includes the type of insight, the severity of each insight, the percentage of the failures, and a short description of the insight. Click the insight to view the graphical representation of the details. The labels represent severity in different colors:

- **Red**—High
- **Yellow**—Medium
- **Grey**—Low

AI Insight Graph

Each AI insight graph is displayed based on the severity of the insight for that hour or the day. The graph is displayed based on the selected **Time Range Filter**. The chart can be viewed for a time range of:

- **3 hours**—Displays the graph for a time range of 3 hours.
- **1 day**—Displays the graph for a time range of 24 hours with hourly data.
- **1 week**—Displays the graph for the last 7 days.
- **1 month**—Displays the graph for the last 30 days.
- **3 months**—Displays the graph for the last 3 months.

The graphs represent severity in different colors:

- **Red**—High
- **Yellow**—Medium
- **Grey**—Low

AI Insight Chart

Each AI insight displays a roll-up for each type based on the details such as SSID, BSSID, Reason, or Server. These roll-ups provide details of each reason and the total number of failures.



3 months Time Range Filter is not supported. If the user selects 3 months in the Time Range Filter, it displays 1 month time series.

The **Client AI Insights** tab displays the performance issues based on the following criteria:

Pre-Shared Key (PSK) Authentication Failures

The **Pre-Shared Key (PSK) Authentication Failures** insight shows information about the number of users that frequently failed to connect to a wireless network due to WPA issues. Each insight further displays details of:

- **SSID**—Lists the SSIDs used by the client that are impacted by the issue and the total number of failures for that SSID.
- **BSSID**—Lists the number of BSSIDs used by the client that frequently failed to complete MAC authentication.
- **Reason**—List of reasons that may explain why client frequently failed MAC authentication and the number of errors that could be attributed to each cause.

802.1X Authentication Failures

The **802.1X Authentication Failures** insight shows information about the number of users and devices per day that frequently failed to complete 802.1X authentication. Each insight further displays details of:

- **SSID**—Lists the SSIDs used by the client that are impacted by the issue and the total number of failures for that SSID.
- **BSSID**—Lists the number of BSSIDs used by the client that frequently failed to complete MAC authentication.
- **Reason**—List of reasons that may explain why client frequently failed MAC authentication and the number of errors that could be attributed to each cause.
- **Server**—List the servers that frequently failed the 802.1X authentication.

MAC Authentication Failures

The **MAC Authentication Failures** insight shows information about the number of users failing to get authenticated due to multiple reasons. Each insight further displays details of:

- **SSID**—Lists the SSIDs used by the client that are impacted by the issue and the total number of failures for that SSID.
- **BSSID**—List the number of BSSIDs used by the client that frequently failed to complete MAC authentication.
- **Reason**—List of reasons that may explain why client frequently failed MAC authentication and the number of errors that could be attributed to each cause.

High DHCP Failures

The **High DHCP Failure** insight shows information about the number of DHCP failures. Each insight further displays details of:

- **SSID**—Lists the SSIDs used by the client that are impacted by the issue and the total number of failures for that SSID.
- **BSSID**—Lists the number of BSSIDs used by the client that frequently failed to complete MAC authentication.
- **Reason**—List of reasons that may explain why client frequently failed MAC authentication and the number of errors that could be attributed to each cause.

Clients with Excessive 2.4 GHz Dwell Time

The **Clients with Excessive 2.4 GHz Dwell Time** insight shows information about the number of dual-band (2.4 GHz and 5 GHz) devices that spend a significant amount of time in the 2.4 GHz band. 5 GHz channels are often preferable, as they typically offer faster Wi-Fi connections and lower levels of interference than 2.4 GHz channels. Each insight further displays details of:

- **Band**—Lists if devices experiencing a low signal-quality link were using 2.4 GHz or 5 GHz radio bands. The graph on this tab shows the proportion of time (minutes) and usage of the client.
- **Tx Power**—Lists the percentage of Tx Power distribution (dBm) in both the 2.4 GHz and 5 GHz band.
- **SNR**—Lists the percentage of SNR (dB) in both 2.4 GHz and 5 GHz band.

Clients with Low SNR Uplink Connections

The **Clients with Low SNR Uplink Connections** insight shows information about client devices that have a low-quality signal-strength connection to their access point. Each insight further displays details of:

- **SNR**—Lists four views, Signal-to-Noise Ratio, Data Rate, Upload and Download overtime for the selected temporal filter.
- **Band**—Lists if devices experiencing a low signal-quality link were using 2.4 GHz or 5 GHz radio bands. The graph on this tab shows the proportion of time and usage of the client.
- **Good vs Bad**—Lists the amount of time (minutes) with Low SNR (Bad) and High SNR (Good). The data is represented in the form of a pie chart.
- **By AP**—Lists the total time (High and Low SNR) that the client connected to all the APs in the network.

Connectivity

The **Connectivity** tab displays information about the overall throughput usage, roaming events, and latency. The following table describes the information displayed in each section:

Table 53: *Connectivity Tab*

| Section | Description |
|-------------------------------------|---|
| Throughput | Displays the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the Throughput pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the Time Range Filter link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. |
| Roaming Events & Latency | <p>Displays the details of a roaming event and the latency of the client. When a wireless client roams between two APs, the destination AP creates an event. By default, the Roaming Events & Latency table displays data for the last 3 hours. To view the table for a different time range, click the Time Range Filter link. You can choose to view the data for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months. The Roaming Events & Latency displays two views, grid view and trend view. The grid view displays the following information:</p> <ul style="list-style-type: none">■ Date/Time—Displays the time of occurrence of the client roaming/ association events.■ SSID—The SSID to which the client is connected.■ Latency(ms)—Roaming Latency in milliseconds between source and destination AP.■ To BSSID—The BSSID of the destination AP.■ Source AP—AP to which the client was connected.■ Destination AP—AP to which the client is connected.■ Roaming Type—The type of roam.■ Band—Radio band on which the client is connected.■ RSSI(dBm)—Received Signal Strength Indicator (RSSI) on the client, estimated measure of power level that the client is receiving from the AP. <p>The trend view displays a chart that shows the percentage of high latency roaming events, total roaming events, and the number of high latency roaming events at a particular instance based on the value selected in the Time Range Filter. Clicking the chart icon brings you back to the grid view.</p> |

Location

The **Location** tab displays the current physical location of the client device on the floor map.

UCC

The **UCC** tab displays the detailed call records for the client if any. To view this data, ensure that the **Unified Communication** application service is enabled on the APs. The following table describes the information displayed in each session:

Table 54: *UCC Tab*

| Section | Description |
|----------------------|--|
| Calls | Displays the total number of calls. The call quality is displayed as: <ul style="list-style-type: none">■ Good■ Fair■ Poor■ Unknown |
| Client Health | Displays the health of the client. |
| Session Type | Displays the type of the call or session. For example, audio, or video, or desktop sharing. |
| Quality | Displays the quality of the call. |

AirGroup

The **AirGroup** displays the details of the servers a client is connected to. The following table describes the information displayed in each session:

Table 55: *AirGroup Tab*

| Section | Description |
|---------------------|--|
| Hostname | Displays the host name. |
| MAC Address | Displays the MAC address of the server the client is connected to. |
| IP Address | Displays the IP address. |
| Role | Displays the user role assigned to the client. |
| Service | Displays the type of service. |
| VLAN | Displays the connected VLAN details. |
| Connected To | Displays the network the client is connected to. |

Wireless Client Sessions

The client sessions page consists of the firewall session details for the client connected to an AP or a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application, Source IP, Destination IP, Source Port, Destination Port, Action, Flags, Packets, Bytes,** and **State**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 56: *Sessions Tab*

| Section | Description |
|-----------------------|---|
| Application | Displays the list of applications. |
| Source IP | Displays the source IP address. |
| Destination IP | Displays the destination IP address. |
| Protocol | Displays the communication protocol used. |
| Source Port | Displays the source port number. |
| Dest Port | Displays the destination port number. |
| Action | Displays the application specific action. |

Table 56: Sessions Tab

| Section | Description |
|-----------------------------|--|
| Flags | Displays the active flags |
| Packets | Displays the number of packets. |
| Bytes | Displays the total number of bytes. |
| State | Displays the connection state of the application. The state can either be Denied, Active, or Inactive. |
| Start Time | Displays the start time. |
| Receive Time | Displays the receive time. |
| WebCC Category | Displays the WebCC category. |
| WebCC Reputation | Displays the WebCC reputation. |
| WebCC Score | Displays the WebCC score. |
| Application Category | Displays the application category. |



Client **Sessions** is supported only if the Instant AP is running Aruba Instant 8.6.0.0 firmware version or later versions.

For details on the AP client sessions refer, [APs—Clients Tab](#). For details on the Branch Gateway client sessions refer, [Gateways—Sessions Tab](#).

Applications

The **Applications** page provides you the client details for passive motoring of the client connected to a wireless network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see [Application Visibility on page 251](#).

Live Events

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. You can live troubleshoot clients connected to a wireless network. For more information on live troubleshooting a client, see [Live Events](#).



Live troubleshooting can be performed for wireless clients only.

Events

The **Events** page displays the details of events generated by the AP and client association. By default, the table displays the following columns: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 57: *Events Tab*

| Section | Description |
|--------------------|---|
| Occurred On | Displays the time at which the event occurred. |
| Event Type | Displays the type of the event. |
| Description | Displays the detailed description of the event. |
| Device MAC | Displays the MAC address of the device. |
| BSSID | Displays the BSSID. |

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table. For more information on Events, see [Alerts & Events](#)

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information on Tools, see [Using Troubleshooting Tools](#).

Live Client Monitoring

Click **Go Live** to start live monitoring of the client. Live monitoring is supported only if the Instant AP is running 8.4.0.0 firmware version. Live monitoring stops after 15 minutes. At any point, you can click **Stop Live** to go back to the historical view.

Five seconds after you start live monitoring, the following data starts getting populated:

- **Usage** graph—The Instant AP sends bandwidth usage data every five seconds and the usage graph is live for 15 minutes.
- For the following fields, data is refreshed every five seconds and the average for the last 60 seconds is displayed:
 - **Device Health**
 - **SNR**
 - **TX Rate**

- **RX Rate**

Disconnecting a Wireless Client from an AP

To disconnect a wireless client from an online AP:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the client table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the name of the wireless client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network, enter the client name in the **Client Name** column, and click the client name.
6. From the **Actions** drop-down list, click **Disconnect from AP**. The clients gets disconnected from the AP.



The **Actions** drop-down is disabled if the AP is offline.

Live Events

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis. Live troubleshooting is supported only if the Instant AP is running 8.4.0.0 firmware version or a later version.



The live troubleshooting can only be performed at a site level or for a specific wireless client.

Live troubleshooting can be performed on a wired client only when the Instant AP is running Aruba Instant 8.5.0.0 firmware version or later versions.

Troubleshooting a Client

Aruba Central allows you to troubleshoot issues related to a client or a site in real time for detailed analysis.

To troubleshoot a client at a site level, perform the following steps:

1. In the **Network Operations** app, use the filter bar to select a site.
2. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
3. Enter the MAC address of the client and click **Start Troubleshooting**.

To troubleshoot a wireless client, perform the following steps:

1. In the **Network Operations** app, use the filter bar to select a group, a label, a site or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the client table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the client name to view the client details page. If there are many clients connected to the network, click **Wireless** to filter the clients connected to the wireless network and enter the client name in the **Client Name** column and then click the client name. The **Client Summary** page is displayed.
6. Under **Analyze**, click **Live Events**. The **Live Events** page is displayed.
7. The client live troubleshooting starts automatically for the selected client.

The status of the troubleshooting is displayed every minute. The troubleshooting session runs for a duration of 15 minutes. You can stop live troubleshooting at any point by clicking **Stop Troubleshooting** to go back to the historical view.

After the live troubleshooting session ends, the details of the events are displayed in the live events table.

Live Events Details

The following details are captured and displayed in the live events table:

- **Occurred On**—Displays the timestamp of the event. Use the filter option to filter the events by date and time.
- **AP Name**—Displays the name of the AP the client is connected to. Use the filter option to select a specific AP.
- **Category**—Displays the category of the event. Use the filter option to filter the events by category.
- **Description**—Displays a description of the event. Use the filter option to filter the events based on description.

Wired Client Overview

The overview page displays the client summary details and client sessions details for the selected wired client. The section includes the following topics:

- [Viewing Clients Connected to Wired Networks](#)
- [Wired Client Summary](#)
- [Wired Client Sessions](#)

Viewing Clients Connected to Wired Networks

To view the details of a client connected to the wired network:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Clients**. The clients overview page is displayed.
3. Click the list icon to view the clients table.
4. By default, the **Clients** table displays a unified list of clients for the selected group.
5. Click the name of the wired client to open the corresponding **Client Details** page. If there are many clients connected to the network, click **Wired** to filter the clients connected to the wired network.
6. Enter the client name in the **Client Name** column, and click the client name. The client **Summary** page is displayed.
7. Additionally, click **Sessions** page to view client sessions details.

Wired Client Summary

The wired client summary page displays the client summary bar and the wired client details.

Wired Client Summary

The wired client summary page displays the client summary bar and the client details. The **Summary** bar displays the following information:

Table 58: *Client Summary Bar*

| Field | Description |
|-------------------|--|
| Connection status | Connection status of the client. Connection status is updated immediately on state change. |
| Connected To | Name of the Gateway to which the client is connected. Click the name of the Gateway to view the device details page. |

Wired Client Details

The wired **Client Details** page displays the client overview details, connectivity summary, UCC, and AirGroup information for the selected client. The client details page includes the following topics:

- [Overview](#)
- [Connectivity](#)
- [UCC](#)
- [AirGroup](#)

Overview

The **Overview** tab consists of three sections. The following table describes the information displayed in each section:

Table 59: *Overview Tab*

| Section | Description |
|---------------------|--|
| Data Path | Displays the data path of the client in the network. Click the device icon to view the corresponding device details page. The data path can be one of the following: <ul style="list-style-type: none">■ Client > Wired Profile > AP■ Client > Wired Profile > AP > Switch■ Client > Wired Profile > AP > Switch > Gateway■ Client > Wired Profile > AP > Gateway■ Client > Switch■ Client > Switch > Gateway■ Client > Gateway |
| Client Info | Displays the following information: <ul style="list-style-type: none">■ Username—User name of the client.■ Hostname—Hostname of the client.■ Client Type—Type of the client device.■ IP Address—IP address of the client.■ MAC Address—MAC address of the client.■ Manufacturer—Manufacturer of the client device.■ Connected Since—Date and time since when the client is connected.■ Device OS—Operating system running on the client device. |
| Network Info | Displays the following information: <ul style="list-style-type: none">■ VLAN—VLAN ID on which the client is connected to the AP.■ Gateway Role—Gateway role associated to the client.■ Port—Gateway port to which the client is connected. |

Connectivity

The **Connectivity** tab displays information about the incoming and outgoing throughput traffic for the client during a specific time range. By default, the graph on the **Throughput** pane is plotted for a time range of 3 hours. To view the graph for a different time range, click the **Time Range Filter** link. You can choose to view the graph for a time period of 3 hours, 1 day, 1 week, 1 month, or 3 months.

UCC

The **UCC** tab displays the detailed call records for the client if any. To view this data, ensure that the **Unified Communication** application service is enabled on the Gateway. The following table describes the information displayed in each session:

Table 60: *UCC Tab*

| Section | Description |
|----------------------|---|
| Calls | Displays the total number of calls. The call quality is displayed as: <ul style="list-style-type: none"> ■ Good ■ Fair ■ Poor ■ Unknown |
| Client Health | Displays the health of the client. |
| Session Type | Displays the type of the call or session. For example, audio, or video, or desktop sharing. |
| Quality | Displays the quality of the call. |

AirGroup

The **AirGroup** displays the details of the servers a client is connected to. The following table describes the information displayed in each session:

Table 61: *AirGroup Tab*

| Section | Description |
|---------------------|--|
| Hostname | Displays the host name. |
| MAC Address | Displays the MAC address of the server to which the client is connected. |
| IP Address | Displays the IP address. |
| Role | Displays the user role assigned to the client. |
| Service | Displays the type of service. |
| VLAN | Displays the connected VLAN details. |
| Connected To | Displays the network to which the client is connected. |

Wired Client Sessions

The client sessions page consists of the firewall session details for the client connected to a Branch Gateway. The **Sessions** page displays information filtered by the IP address of the client. The **Sessions Summary** pane displays the device the client is connected to, total number of sessions, and the time stamp of when the page was last refreshed.

The **Sessions** table lists the details of each session. By default, the table displays the following columns: **Application, Source IP, Destination IP, Source Port, Destination Port, Action, Flags, Packets, Bytes,** and **State**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each session:

Table 62: *Sessions Tab*

| Section | Description |
|-----------------------------|--|
| Application | Displays the list of applications. |
| Source IP | Displays the source IP address. |
| Destination IP | Displays the destination IP address. |
| Protocol | Displays the communication protocol used. |
| Source Port | Displays the source port number. |
| Dest Port | Displays the destination port number. |
| Action | Displays the application specific action. |
| Flags | Displays the active flags |
| Packets | Displays the number of packets. |
| Bytes | Displays the total number of bytes. |
| State | Displays the connection state of the application. The state can either be Denied, Active, or Inactive. |
| Start Time | Displays the start time. |
| Receive Time | Displays the receive time. |
| WebCC Category | Displays the WebCC category. |
| WebCC Reputation | Displays the WebCC reputation. |
| WebCC Score | Displays the WebCC score. |
| Application Category | Displays the application category. |



Client **Sessions** is supported only if the Instant AP is running Aruba Instant 8.6.0.0 firmware version or later versions.

For details on the Branch Gateway client sessions refer, [Gateways—Sessions Tab](#).

Applications

The **Applications** page provides you the client details for passive motoring of the client connected to a wired network. The **Visibility** dashboard provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard. The tab consists of a list view and a graph view. The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**

For more information about enabling **Application Visibility**, list of supported Instant APs, and the data displayed on the **Applications** and **Websites** sections, see [Application Visibility on page 251](#).

Events

The **Events** page displays the details of events generated by the AP and client association. By default, the table displays the following columns: **Occurred On**, **Event Type**, and **Description**. Click the ellipsis icon to perform additional operations:

- **Autofit columns**—Adjusts the column width of the table to fit the page evenly.
- **Reset to default**—Resets the table view to the default columns.

If a filter icon appears next to the column header, click it and enter the filter criteria or select a filter criteria. The following table describes the information displayed in each event:

Table 63: *Events Tab*

| Section | Description |
|--------------------|---|
| Occurred On | Displays the time at which the event occurred. |
| Event Type | Displays the type of the event. |
| Description | Displays the detailed description of the event. |
| Device MAC | Displays the MAC address of the device. |
| BSSID | Displays the BSSID. |

To download events into a CSV format, click the download button. Aruba Central generates the CSV report of all the events for the selected client.

You can also filter the events based on the type of events, click the **Click here for Advance Filtering**. Select the type of events from the list and click **Filter**. The events under the selected categories get listed in the **Events** table. For more information on Events, see [Alerts & Events](#)

Tools

The **Tools** page is automatically filtered based on the client you select. This enables network administrators to perform checks on the client and debug client connectivity issues. For more information on Tools, see [Using Troubleshooting Tools](#).

Application Visibility

The **Manage > Applications** tab provides detailed information on data usage by the clients connected to APs and Branch Gateways in the network. Clicking the **Applications** tab displays a **Visibility** dashboard that provides a summary of client traffic and their data usage to and from applications, and websites. You can also analyze the client traffic flow using the graphs displayed in the **Visibility** dashboard.

Application Visibility is supported for Instant APs running 6.4.3.1-4.2.0.0 or later release version.

Aruba Central supports Application Visibility monitoring, DPI configuration, and web filtering for IAP-103, RAP-108/109, IAP-114/115, RAP-155, IAP-224/225, IAP-274/275, IAP-228, IAP-277, IAP-205, IAP-214, and IAP-324/325, IAP-304/305, IAP-207, IAP-334, IAP-314/315, IAP-344/345, IAP-504/505, IAP-535/534 and IAP-555.



The Instant AP-104/105, Instant AP-134/135, RAP3WNP, and Instant AP-175 devices support only web policy enforcement.

Visibility Dashboard

The **Visibility** dashboard displays metrics and graphs related to client traffic flow in the following sections:

- **Applications**
- **Websites**
- **Blocked Traffic**

To view the client traffic details, ensure that the DPI access rules are enabled on the Instant AP device.

The **Blocked Traffic** section is only displayed in **All Devices** level in the **Network Operations > Global > Applications** page.



Applications

The **Applications** section includes a table view and a graph view related to the client traffic flow to and from various applications.

Table View in Application Section

The **Applications** section displays a table with details on the client traffic flow to and from various applications. The table in the **Applications** section displays the following columns:

- **Application**—Name of the application.
- **Category**—The category to which the application belongs. The application can belong to any of the categories, for example, **Unclassified**, **Standard**, **Social Networking**, **Streaming**, **Web**, **Cloud File Storage**, **Instant Messaging** and so on.
- **Usage**—The usage size by the respective application.
- **Sent**—The size of data sent from the application.
- **Received**—The size of data received by the application.

Graph View in Applications Section

Click the graph icon in the Applications section to display bar graphs indicating the traffic flow in the following two tabs:

- **Applications**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified applications listed in the **Applications** table. The legend beside the bar graphs displays the list of applications to which the traffic flow is detected. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application same as displayed in legend section,
- **Categories**—The stacked bar graph in this tab displays details of the client traffic flowing to or from the top five classified application categories listed in the **Applications** table. By hovering the mouse on the bar graph, you can view the size of data flowing to and from the application categories same as displayed in legend section.

These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in the last three hours.

Websites

The **Websites** section includes a table view and a bar graph view related to the client traffic flow and their data usage by various websites.

Table View in Websites Section

The **Websites** section displays tables with the following details:

- **Reputation**—The reputation of the application categories, for example, **Trustworthy**, **incomplete**, **Moderate Risk**, **Low Risk**, **High Risk** and so on. The reputations are set based on the risk levels exhibited by the application categories.
- **Usage**—The percentage of data usage by application categories based on their reputation.
- **Category**—The category of the client traffic that sends and receives data, for example, **Unclassified**, **Social Networking**, **Streaming**, **Web**, **Cloud File Storage**, **Instant Messaging** and so on.
- **Usage**—The size and percentage of data usage by the corresponding categories.

Graph View in Websites Section

Clicking the graph icon corresponding to the **Websites** section displays bar graphs for the following two tabs:

- **Reputation**—The stacked bar graph in the **Reputation** tab displays details of client traffic flow for the top five reputations listed in the **Websites** table.
- **Web Categories**—The stacked bar graph in the **Web Categories** tab displays details of client traffic flow for the top five web categories listed in the **Websites** table. You can view the size of data flowing to and from each of the web categories by hovering the mouse on the bar graph. The legend beside the bar graphs displays the list of websites based on its reputation, to which the traffic flow is detected.

These graphs are displayed for a specific time frame (3 Hours, 1 Day, 1 Week, 1 Month, 3 Months). By default, the graphs display real-time client traffic data or usage trend in the last three hours.

The Applications (Apps) and Web Categories charts are also displayed in the **Applications** pages for the Group, Site, All device, APs, and Gateways levels.

Application Visibility data is updated every 0th minute of every hour. The data population on the **Applications > Visibility** dashboard may be delayed by an hour when compared to the Application Visibility data displayed in the **Applications** pages for the Group, Site, All device, APs, and Gateways levels

Blocked Traffic

Based on the group selection from the **Blocked Traffic** drop-down list, the **Blocked Traffic** section of the **Application > Visibility** dashboard allows you to view the following information:

- Blocked devices of the selected group as CSV file.
- The number of user sessions that are blocked. This information is displayed under **Blocked Sessions**.

The blocked traffic details are shown only for the APs on which the Application Visibility or DPI ACLs are enabled.

Downloading Blocked Session Details

To download the blocked session details in the CSV format, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select **All Devices**.
2. Under **Manage**, click **Applications**. The visibility dashboard is displayed.
3. To download the blocked sessions report, select the device group from the **Select Group** drop-down. If the device group is already selected from the **Groups** drop-down on the filter bar, the page displays the group name and the number of sessions blocked for the clients connected to devices in that group.
4. Click **Download CSV**. Aruba Central generates the CSV report with data from the last 7 days.

The CSV file shows up to 50000 blocked sessions for a single Instant AP cluster.



VisualRF

VisualRF allows you to plan sites, create and manage floor plans, and provision APs. You can use VisualRF Plan to do basic planning procedures, such as, creating a floor plan and provisioning APs.

VisualRF provides a real-time picture of the radio environment of your wireless network and the ability to plan the wireless coverage of new sites. For a better understanding of your wireless network, you must know the location of your devices and users, and the RF environment of your network. The VisualRF puts this information at your fingertips through integrated mapping and location data.

VisualRF uses sophisticated RF fingerprinting to accurately display coverage patterns and calculate the location of every wireless device in range. VisualRF does not require dedicated RF sensors or a costly additional location appliance, because it gathers all the necessary information from your existing devices.



VisualRF is supported only on Instant APs running 6.5.2.0 or later.

In VisualRF, do not use the internet browser for back and front navigation. Instead, use the breadcrumbs.

VisualRF offers the following features:

- Floor plan import and creation.
- Pictorial navigation that allows you to view the floor plans associated with Instant APs, associated clients, buildings, and floors.
- Accurate calculation of the location of all associated client devices (laptops and Phones) using RF data from your devices.
- A tree view that allows you to navigate to a specific campus.
- A map view that shows the location of devices and heatmaps that depict the strength of RF coverage in each location.
- Unique URLs when you drill down to a site, campus, or building map, in the following formats: `/vrf`, `/vrf/site/<id>`, `/vrf/campus/<id>`, and `/vrf/building/<id>`

VisualRF Dashboard

To view the VisualRF dashboard:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.

The VisualRF dashboard allows you to set your view to one of the following options:

- Network—Click the network icon, to navigate to a specific site.
- Map—The map view displays the location of the sites. Clicking on a specific site leads you to a campus, buildings, floor plans, and devices.
 - You can also search for a specific site in the search box.
 - To move or drag a site to different location on the map, click the lock icon.
- List—The list view provides a complete list of sites, links to the corresponding buildings and floor plans, size of the floor, gridsize, the number of APs on the floor, and the number of clients connected to APs on the floor.

Viewing Network Information

The **Network** link displays a page for viewing campuses, buildings, and floors within a network. You can click the **Map** link to view the site map. Click the **List** link to view the list of sites.

To view more information, perform the following actions:

- To view the details of a network within a campus, select a campus, and click on a building within the selected campus.
- To view the floor plan, select a floor. The floor plan displays the APs and associated clients on that floor.
- To view information about the devices, select an AP or client.

Customizing the Floor Plan View

To customize your floor plan view, click the **View** tab on the right sliding panel. The **View** tab displays the list of campuses and the devices.

- To increase the icon size of campus, click the arrow next to **Campuses**.
- Click **APs** to view the details of the Instant AP and the RF environment.
- Click **Clients** to view the client details.

Viewing Campus, Sites, Buildings, and Floors

The VisualRF navigation menu on the right pane consists of the **Properties**, **View**, and **Edit** tabs. The following table describes the menu options available for network locations such as campus, building, and floor.

Table 64: *VisualRF—Network Menu Options*

| Networks Property Tab | View Tab | Edit Tab |
|--|---|---|
| Displays the total number of APs, buildings, clients, and floors | Displays the following menu options: <ul style="list-style-type: none">■ Campuses<ul style="list-style-type: none">● Displays the complete list of campus sites within your network. Click the links to view details of the campus sites.● Enables or disables the campus icons on the map.● Allows you to decrease or increase campus icon size on the map.■ Labels—Shows or hides the labels assigned to campus sites. | Displays the following menu options: <ul style="list-style-type: none">■ Select All—Selects all campus sites. You can perform the following actions when the campus sites are selected:<ul style="list-style-type: none">● Remove—Removes the selected sites.● Bill of Materials—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details.● Auto match planned devices—Automatically matches the devices that are planned for deployment and reloads the page.■ Undo—Cancels the previous action.■ New Floorplan—Allows you to create a new floor plan■ Set Background—Allows you set a background image. You can upload a custom image or set a specific location from the world map as a background.■ New Campus—Allows you create a new campus.■ Auto-arrange Campuses—Arranges campus icons on the map. |

Table 65: VisualRF—Campus Menu Options

| Campus Property Tab | View Tab | Edit Tab |
|---|---|---|
| Displays the name of campus and the total number of APs in the campus site. | <p>Displays the following menu options:</p> <ul style="list-style-type: none"> ■ Buildings <ul style="list-style-type: none"> ● Displays the complete list of buildings within the campus. Click the links to view the details of the buildings in the campus site. ● Enables or disables the building icons on the map. ● Allows you to decrease or increase the building icon size on the map ■ Labels—Shows or hides the labels assigned to buildings. | <p>Displays the following menu options:</p> <ul style="list-style-type: none"> ■ Select All—Selects all buildings. You can perform the following actions when buildings are selected: <ul style="list-style-type: none"> ● Remove—Removes the selected buildings. ● Navigate—Navigates to the building. ● Bill of Materials—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details. ● Auto match planned devices—Automatically matches the devices that are planned for deployment and reloads the page. ■ Export Floor Plans—Exports the floor plan of a specific floor. ■ Undo—Cancels the previous action ■ New Floorplan—Allows you to create a new floor plan. ■ Set Background—Allows you set a background image. You can upload a custom image or set a specific location from the world map as a background. ■ New Building—Allows you to create a new building. ■ Auto-arrange Buildings—Arranges building cons on the map. |

Table 66: VisualRF—Building Menu Options

| Building Property Tab | View Tab | Edit Tab |
|---|---|--|
| Displays the name and location details of the building, and the total number of floors and APs in the building. | Displays the complete list of floors in the building. Click the links to view the floor plan of the floors in the building. | <p>Displays the following menu options:</p> <ul style="list-style-type: none"> ■ Select All—Selects all floors. You can perform the following actions when floors are selected: <ul style="list-style-type: none"> ● Remove—Removes the selected buildings. ● Navigate—Navigates to the building. ● Bill of Materials—Enables showing or hiding heatmap, speed, sensor coverage, wired range and other details. ● Auto match planned devices—Automatically matches the devices that are planned for deployment and reloads the page. ● Duplicate—Creates a duplicate of the selected floor. ■ Export Floor Plans—Exports the floor plan of a specific floor. ■ Undo—Cancels the previous action. ■ New Floorplan—Allows you to create a new floor plan. |

Table 67: *VisualRF—Floor Menu Options*

| Property Tab | View Tab | Edit Tab |
|--|---|---|
| <p>Displays the floor details, total number of APs on the floor, and clients.. The Advanced option allows you to set the values to indicate if the environment is related to an office space, cubicles, offices, or concrete.</p> | <p>Displays the following menu options:</p> <ul style="list-style-type: none"> ■ Devices—Displays APs, and Clients devices detected on the floor. ■ AP Overlay—Shows the heatmap for the current and adjacent floors. ■ Floor Plan Features—Displays the following details: <ul style="list-style-type: none"> ● Grid Lines—Allows you to change the grid size and color. ● Labels—Shows or hides the labels tagged to the devices on the floor. ● Origin—To ensure that multi-floor heatmaps display properly, ensure that your floor plans are vertically aligned. VisualRF uses the origination point for this alignment. By default, the origin appears in the upper left corner of the floor plan. You can drag and drop the origin point to the correct position. ● Regions—Displays the regions defined within a floor plan. For example, you can define two small regions of high density clients within a larger floor plan with lower client density. ● Walls—Displays walls drawn on the floor. | <p>Displays the following menu options:</p> <ul style="list-style-type: none"> ■ Drawing—Allows you to draw a region or wall for the floor. ■ Devices—Allows you to add and delete the already deployed or planned devices. ■ Actions—Displays the following options: <ul style="list-style-type: none"> ● Select All—Selects all floors. ● Export Floor Plans—Exports the floor plan of a specific floor. ● Undo—Cancels the previous action. ● New Floorplan—Allows you to create a new floor plan. ● Auto Match Planned Devices—Automatically matches the devices that are planned for deployment and reloads the page. ● Refresh—Refreshes the page. |

Viewing AP Overlay Information

The AP Heatmap overlay displays information for adjacent floors to determine how the bleed through from adjacent floors affects the viewed floor. Besides the current floor, you can view all floors, or data from APs located on the floor above or below.

The **AP Overlay > Heatmap** option allows you to view details of signal cutoff, and for each radio band and floors. The **Heatmap** option also allows you to change the overlay display to grid.

Viewing Client Devices

VisualRF displays only associated client devices. To view the client devices on a floor plan, navigate to the floor plan and click the **Devices > Clients** in the **View** tab. Clicking on **Clients** shows or hides the client icons on the floor plan. The client device presence is marked with symbol of a mobile phone. The floor plan also shows the Instant AP to which the client device is associated.

Planning and Provisioning Devices

VisualRF provides the capability to plan campuses, buildings, floors, and location for device provisioning before the actual deployment. Using VisualRF, you can create a floor plan and add devices to the floor plan.

The planning and provisioning workflow includes the following procedures:

Creating a Campus

To create a new campus, perform the following actions:

1. In the **Network Operations** app, use the filter to select **All Devices**.
 2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
 3. Click **Floor Plans > Network** view.
 4. Click the **Network** slide out pane on the right and then click the **Edit** link.
 5. Click **New Campus**.
 6. Enter the name of the campus and click **Save**. The new campus icon appears on the campus background.
 7. To set a background image for the campus, complete the following steps:
 - a. Click **Set Background**.
 - To set a custom background, select the **Custom Image** option and upload the image file.
 - To set the background to a specific geographical map, click the **World Map** option and select the country map from the drop-down list.
 - b. Click **Save**.
 - c. Drag the new campus icon to the appropriate location on the map background, or right-click the background.
- Or
- d. Click **Auto Arrange Campuses** to arrange the campus in alphabetical order across the background.

Creating a Building

To create a building, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click **Floor Plans > Network** view.
4. Select the campus under which you want to create a building. The **Campus** slide out pane is displayed.
5. Click the **Edit** tab.
6. Click **New Building**. Enter the following information:

Table 68: *New Building Configuration Parameters*

| Field | Description |
|-----------------------|---|
| Name | Name of the building located in an existing campus. |
| Address | Building or Campus address. |
| Latitude | Latitude of the building. |
| Longitude | Longitude of the building. |
| Ceiling Height | The normal distance between floors in the building (in feet). This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. |
| Attenuation | Enter the attenuation loss (in dBm) between floors. This value can be overridden as each floor is created, but this is the default value for every new floor added to the system. |

- Click **Save**. You can add multiple buildings if required.
- To automatically arrange buildings, click **Auto-arrange Buildings**.

Creating a Floor Plan

VisualRF allows you to add, modify, and import a floor plan background image file. When importing RF plans ensure that the devices from the device catalog are included.

To create a new floor plan, complete the following steps:

- In the **Network Operations** app, use the filter to select **All Devices**.
- Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
- Click **Floor Plans > Network** view.
- Click the **Edit** tab in the **Network** slide out panel.
- Click **New Floorplan**. The **New Floorplan** pop-up window is displayed.
- Click **Choose File** and locate a floor plan image file from your local file system. You can import the floor plan image file in the bmp, jpg, jpeg, gif, and png format.
- Select the campus and building from the **Campus** and **Building** drop-down lists, respectively.
- Assign a floor name and a floor number in the **Floor name** and **Floor number** text boxes, respectively.
- Click **Save**.
- You can define new floor by clicking the **Define New Floor** option on the top right corner.
- The **Define New Floor** includes the following option:
 - Scale**— Shows the dimensions of the floor.
 - Region**—Allows you to define floorplan boundary and planning region.
 - CAD Layer**—Allows you to import walls from the CAD file.
 - Access Points**—Allows you to add the AP's to the floor plan.
- Click **Next** button after you set the **Scale**, **Region**, and **CAD layer** for the floor.
- To add a planned AP, under **Access Points > Planned APs**, select the device type from the **Type** dropdown menu.
- In the **Count** field, enter the number of devices to add to the new floor.
- Click and drag the **Deployment Type** slider bar to adjust data rates for a high density or low density environment.
- Optionally, click the **Advance** link to configure the advance deployment options.

- a. **Service Level:** Select **Speed** or **Signal** to plan coverage by adjusting the data rate requirements (speed) or AP signal strength settings. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.
- b. **Client Density:** In the **Max Clients** field, set the anticipated number of clients that will be stationed in the floor. In the **Clients Per AP** field, enter the maximum number of clients supported by each radio. Click **Calculate AP Count** to recalculate the suggested number of APs based on these settings.

17. Click **Add APs to Floorplan** to add the planned APs to the floor.

18. Click **Finish**.

19. To remove the planned device from the floorplan, right-click on that device and click **Remove**.

Importing a Floor Plan

To import a floor plan exported from VisualRF Plan, AirWave, or Aruba Central, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click the **Import** menu option.
4. Click **Choose File** and select the floor plan zip file to import.
5. Click **Upload**. When an import is complete, the UI displays a notification to alert the user.

Modifying Floor Plan Properties

To edit the properties of an existing floor plan, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click **Floor Plans > Network** view.
4. Click **List**. The list of sites is displayed.
5. Click the floor number or floor name link. The **<Floor Name>** slide out pane is displayed.
6. Click **Properties** to modify the following properties.

Table 69: *Floor Plan Properties*

| Setting | Default | Description |
|---------------------|----------------|--|
| Floor Name | Floor [Number] | A descriptive name for the floor. It inherits the floor number as a name if nothing is entered. |
| Floor Number | 0.0 | The floor number. You can enter negative numbers for basements. NOTE: Each floor plan within a building must have a unique floor number. |
| Width | N/A | These fields display the current width of the floor plan. To change these settings, click the Measure icon and measure a portion of the floor. |
| Height | N/A | These fields display the current height of the floor plan. To change these settings, click the Measure icon and measure a portion of the floor. |
| Gridsize | 5 x 5 feet | Size of the grid. Decreasing the grid size will enable the location to place clients in a small grid which will increase accuracy. |
| Advanced | | |
| Environment | N/A | Environment indicator. The values on the slider range from 1–4 to indicate if the environment is related to an open space, cubicles, offices, or concrete. |

7. Click **Save**.

Adding Devices to the Floor Plan

You can add the planned devices (for example, APs) or the already deployed devices to floor plan.

To add the already deployed devices to the floor plan, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click **Floor Plans > Network** view.
4. Click **List**. The list of sites is displayed.
5. Click the floor number or name link. The **<Floor Name>** slide out pane is displayed.
6. Click **Edit**.
7. Click the **Add Deployed Devices**. A list of devices is displayed.
8. Expand the group containing the APs which need to be provisioned on this floor plan. Note that by default, devices that have already been added to VisualRF are hidden. To show them, clear the **Hide APs that are already added** check box at the bottom of the list.
9. Click and drag an AP (or a Group or Folder of APs) to its proper location on the floor.
10. To remove a device from the floor plan, right-click that device and then click **Remove**.

To add planned devices when creating a new floor plan, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click **Floor Plans > Network** view.
4. Click **List**. The list of sites is displayed.
5. Click the floor number or name link. The **<Floor Name>** slide out pane is displayed.
6. Click **Edit**.
7. Click **Add Planned Devices** and select a device type (model) from the list of available devices.
8. Click and drag the device to the desired location on the floor.
9. To Auto-match the planned devices, click **Auto-Match Planned Devices** from the **Action** tab.
10. To remove a planned device from the floor plan, right-click on that device and then click **Remove**.

Printing a Bill of Materials Report

To generate a Bill of Materials (BOM) Report from within VisualRF, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Manage**, click **Overview > Visual RF**. The VisualRF dashboard is displayed.
3. Click **Floor Plans > Network**.
4. Right-click a campus icon, a building icon, or a building floor and select **Bill of Materials**. A report pop-up window opens.
5. Select options such as heatmap, speed, sensor coverage, wired range, summary, and include kit, serial number, notes.
6. Select **OK**.

VisualRF APIs

Aruba Central supports the following APIs for retrieving client location and floor plan information:

- **GET /visualrf_api/v1/campus**—Retrieves a list of all campus sites.

- **GET /visualrf_api/v1/campus/{campus_id}**—Retrieves information about a specific campus and its buildings.
- **GET /visualrf_api/v1/building/{building_id}**—Retrieves information about specific building and its floors.
- **GET /visualrf_api/v1/floor/{floor_id}**—Retrieves details about a specific floor.
- **GET /visualrf_api/v1/floor/{floor_id}/image**—Retrieves background image from a specific floor plan.
- **GET /visualrf_api/v1/floor/{floor_id}/access_point_location**—Retrieves information about the location of the APs on a specific floor plan.
- **GET /visualrf_api/v1/access_point_location/{macaddr}**—Retrieves location details of a specific AP.
- **GET /visualrf_api/v1/client_location/{macaddr}**—Retrieves location details of a specific client.
- **GET /visualrf_api/v1/floor/{floor_id}/client_location**—Retrieves information about the location of clients on a specific floor.

For more information on APIs, see [Aruba Central APIs](#) and refer to API documentation at <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Topology

The **Topology** map in Aruba Central provides a graphical representation of the site including the network layout, details of the devices deployed and the health of the WAN uplinks and tunnels. The minimum required ArubaOS version for Topology is ArubaOS version 8.1.0.0-1.0.1.1.

Before You Begin

To view the topology map ensure that LLDP is enabled. On switches, LLDP is enabled by default. On Branch Gateways, if the port type is LAN, LLDP is enabled by default.

The topology map filters devices based on sites. To view the topology map, ensure that you have assigned the devices to sites. For more information, see [Assigning Devices to Sites](#).

For more information, see the following sections in the Aruba Central Help Center:

- [Configuring Ports for LAN Interfaces](#)
- [Configuring Other Parameters for Port](#)

Viewing the Topology Map

To access the topology map:

1. In the **Network Operations** app, use the filter to select a site for which you want to view the topology map.
2. Under **Manage**, click **Overview > Topology**.

The topology map provides a pictorial view of the devices deployed in the branch site, uplink health, and tunnel status. A task pane on the right provides a summary of the devices, uplinks, and tunnel details. The red and green indicators show the current status and health of the WAN uplinks and tunnels.

- To view the name, type, and hardware model of the device, hover over the device.
- To view details of the uplink interfaces, click the lines on the map.
- To know the tunnel mapping, hover over the tunnel or the uplink, and the uplink path is highlighted.
- To change the zoom level, click the zoom icons.
- In case of High Availability, the redundant gateway tunnel details are also displayed in the **Details** tab under **HA Tunnels** when you select the uplink or the tunnel.

Grouping VPN Concentrators

If the tunnels in the overlay are orchestrated, the VPN Concentrators are grouped according to their hub groups. You can also see the group preference order marked as primary, secondary or tertiary. For more information, see [Configuring the SD-WAN Overlay Network](#). However, if the tunnels are configured manually, the VPN Concentrators are grouped according to their sites. If the VPN Concentrators are not associated with any site, they are grouped based on their hub groups. For manual tunnels, the Data Center group preference is not displayed.

If you have a combination of gateways in a single site, with one gateway configured as a manual tunnel and the other gateway configured as an orchestrated tunnel, both the tunnels are treated as manual and the VPN Concentrators are grouped based on their sites. If there are no associated sites, they are grouped according to their hub groups.

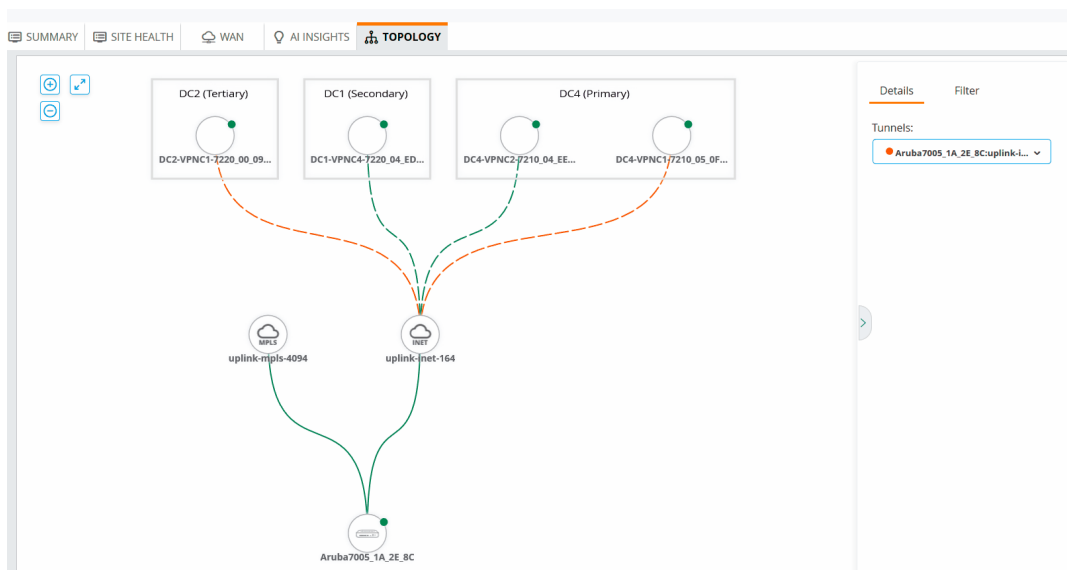


Various combinations of configurations in a single site are not recommended.

Example of a Topology Map:

An example of a Site Topology where the VPN Concentrators are grouped based on their hub groups.

Figure 94 Site Topology



Active tunnels are green in color and inactive tunnels are red in color. If there are multiple tunnels connecting to a VPN Concentrator, and even if one of those tunnels is down, the tunnel mapping is displayed in red dotted lines.

Details and Filter Pane

The Details and Filter pane consists of the following tabs:

- **Details**—Provides a detailed summary of the devices, uplink interfaces, and tunnels. It also highlights the status of the device and uplinks.
- **Filter**—Allows you to apply a filter criteria to display devices on the map. The following options are available:
 - **Switch**—Filters out switches.
 - **IAP**—Filters out Instant Access Points.
 - **VPNC**—Filters out VPNCs and Virtual gateways.

- **Security Cloud**—Filters out Zscaler and Palo Alto Prisma Access™ Cloud Service.

For example, if you set the filter to VPN, only the VPN details are displayed. Similarly, you can set the filter to show or hide the devices that are linked on uplink ports.

The **Details** tab displays the following information:

Table 70: *Contents of the Details Tab*

| Type | Description |
|---|---|
| Device details | |
| Branch Gateway | Displays the following details: <ul style="list-style-type: none"> ■ Name—Hostname of the Branch Gateway. ■ Serial—Serial number of the Branch Gateway. ■ IP—IP address of the Branch Gateway. ■ MAC—MAC address of the device. ■ Type—Type of device deployment. For Branch Gateways, the type shows up as Gateway. ■ Model—Hardware model of the device. ■ Status—Operational status of the device. ■ Health—Operational health of the device. |
| Switch | Displays the following details: <ul style="list-style-type: none"> ■ Name—Hostname of the switch. ■ Serial—Serial number of the switch. ■ IP—IP address of the switch. ■ MAC—MAC address of the switch. ■ Type—Type of the device. ■ Model—Hardware model of the switch. ■ Status—Operational status of the switch. ■ Health—Operational health of the switch. |
| Switch Stack | Displays the following details: <ul style="list-style-type: none"> ■ Name—Hostname of the switch. ■ IP—IP address of the switch. ■ MAC—MAC address of the switch. ■ Type—Type of the device. ■ Stack Role—Role of the switch in the stack. ■ Model—Hardware model of the switch. ■ Status—Operational status of the switch stack. ■ Health—Operational health of the switch stack. ■ Stack Members—Lists the members of the stack, the role (member or commander), and state. |
| Instant AP | Displays the following details: <ul style="list-style-type: none"> ■ Name—Hostname of the Instant AP. ■ Serial—Serial number of the Instant AP. ■ IP—IP address of the Instant AP. ■ MAC—MAC address of the Instant AP. ■ Type—Type of the device. ■ Model—Hardware model of the Instant AP. ■ Status—Up and down arrows indicating the operational status of the Instant AP. ■ Health—Operational health of the Instant AP. |
| Tunnel, Uplink, and Edge details | |
| Tunnel | Displays the following information about tunnels configured on the Branch Gateway: <ul style="list-style-type: none"> ■ Map Name—Tunnel interface. ■ Peer MAC—MAC address of the peer device with which the tunnel was established. ■ Local MAC—MAC address of the Branch Gateway. ■ Source IP—Source IP address from where the traffic originates. |



| Type | Description |
|--------|--|
| | <ul style="list-style-type: none"> ■ Destination IP—IP address to which the traffic is sent. ■ Established Time—Timestamp showing when the tunnel was established. ■ VLAN—VLAN ID of the tunnel. ■ Source Serial—Source Serial of the tunnel. |
| Uplink | <p>Displays the following information about uplinks configured on the Branch Gateway:</p> <ul style="list-style-type: none"> ■ Uplink Type—Type of the uplink. ■ VLAN—VLAN ID of the uplink. ■ Link Status—Uplink status. ■ Description—Description of the uplink. ■ WAN Status—WAN status. ■ IP Address—IP address of the WAN interface. ■ Public IP—Public IP address. ■ Device MAC—MAC address of the device. ■ Serial—Serial number of the device. ■ Port Number—Port number of the device. ■ Tunnels—List of tunnels mapped to the uplink. A green bullet icon indicates that the tunnel is up and a red bullet icon indicates that the tunnel is down. |
| Edge | <p>Displays the following information about the link:</p> <ul style="list-style-type: none"> ■ Interface numbers—The devices' interface numbers. ■ Interface—Interface number of the individual device. <ul style="list-style-type: none"> ● Serial—Serial number of the individual device. ● Device Name—The name of the individual device. ● Port Number—The Port number of the individual device. <p>NOTE: In case of Branch Office Controller (BOC) to Switch link, if a peer Branch Gateway link is configured for redundancy, link details are displayed for the peer Branch Gateway to switch link as well.</p> |

Alerts & Events

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management.

Viewing the Alerts Summary

To view a summary of alerts and events and acknowledge alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, site, or label.
 2. Under **Analyze**, click **Alerts & Events** to view the alert and events dashboard. The **Alerts & Events** dashboard offers a graphical view, list view, and a configuration view.
 3. Optionally, click the summary  icon to view the graphs displaying alerts and events. Select each tab, **All**, **Access Point**, **Switch**, or **Gateway** to view the graphs pertaining to each device type. To view the list of alerts, click the list  icon.
- By default, the **Alerts** tab is selected and the **Open Alerts** table is displayed. The table displays all the generated alerts. The Alerts bar categorizes the alerts as **Critical**, **Major**, **Minor**, and **Warning**.
4. Optionally, click **Acknowledge All** to acknowledge all the alerts at once.

Important Points:

- Once an alert is acknowledged, the alert is moved to the **Acknowledged** tab.
- All **Acknowledged Alerts** can be viewed when the **Show Acknowledged Alerts** button is ON.
- If the user does not acknowledge an alert, the alert is suppressed for 5 minutes. The alert notification is then sent to the user every 5 minutes in case the issue still persists.


- If the user acknowledges an alert, the alert is suppressed until the issue is resolved. After resolving the issue, if it re-occurs the alert is sent again.

5. Optionally, enable the **Show Acknowledged Alerts** button to display the list of acknowledged alerts.

The following table describes the information displayed in each column of the **Alerts** table:


Table 71: *Alerts pane*

| Data Pane Content | Description |
|--------------------|--|
| Occurred On | Displays the timestamp of the alert. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the alerts. |
| Category | Displays the category of the alert. Use the filter option to filter the alert by category. |
| Label | Displays the label name of the alert. |
| Site | Displays the site name of the alert. |
| Group | Displays the group name of the alert. |
| Severity | Displays the severity level of the alert. The severity can be Critical , Major , Minor , or Warning . |
| Description | Displays a description of the alert. Use the search option in filter bar to filter the alert based on description. |

To customize the **Alerts & Events** table, click the eclipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Viewing the Events Summary

To view a summary of events, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group, device, site, or label.
2. Under **Analyze**, click **Alerts & Events**. The **Alert & Events** page is displayed. The **Alerts & Events** dashboard offers a graphical view, list view, and a configuration view.
3. In the **Alerts & Events** summary bar, click **Events**. By default the list view is selected and a consolidated list of events is displayed in the events table.
4. Optionally, click the summary  icon to view the graphs displaying alerts and events. Select each tab, **All**, **Access Point**, **Switch**, or **Gateways** to view the graphs pertaining to each device type.

Advanced Event Filtering

Aruba Central allows you to filter the events based on the event types. To filter events based on event types, complete the following steps:

1. In the **Events** page, click **Click here for advanced filtering** to filter the events based on event types.
2. Select the event type and click **Filter**. You can select multiple event types from the advanced filtering option.


3. The events table displays the list of events generated in each event type. The filter summary bar displays the total number of events in the selected category and the type(s) of events.
4. Optionally, to clear advanced filtering option, from the events summary bar, click **Clear All**. The advanced filtering gets cleared.

The following table describes the information displayed in each column of the **Events** table:

Table 72: *Events pane*


| Data Pane Content | Description |
|------------------------|--|
| Occurred On | Displays the timestamp of the event. Use the sort option to sort the events by date and time. Use the filter option to select a specific time range to display the events. |
| Device Type | Displays the type of the device, Access Point, Gateway, Switch. Use the filter option to filter events by device types. |
| Device Hostname | Displays the host name of the device where the event is generated. |
| Device MAC | Displays the MAC address of the device. |
| Client MAC | Displays the MAC address of the device to which the client is connected. |
| BSSID | Displays the BSSID of the device. |
| Event Type | Displays the type of the event. |
| Description | Displays the description of the event. Use the column filter to filter an event based on the description. |

To customize the **Alerts & Events** table, click the eclipses  icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Aruba Central allows you to download the global list of events to your local browser. Click  to download the events list in a CSV format.

Configuring Alerts

To configure alerts, complete the following steps:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed.
3. In the **Alerts & Events** page, click the configuration  icon. The **Alert Severities & Notifications** is displayed.
4. Use the tabs to navigate between the alert categories. Select an alert and click + to enable the alert with default settings. To configure alert parameters, click on the alert tile and do the following:
 - a. **Severity**—Set the severity. The available options are Critical, Major, Minor, and Warning. By default, the following alerts are enabled and the severity is **Major**:
 - Virtual Controller Disconnected

- Rogue AP Detected
- New User Account Added
- Switch Detected
- Switch Disconnected



For a few alerts, you can configure threshold value for one or more alert severities. Enter a value in the **exceeds** text box to set a threshold value for the alerts. The alert is triggered when one of the threshold values exceed the duration.

b. **Duration**—Enter the duration in minutes.

c. **Device Filter Options**—(Optional) You can restrict the scope of an alert by setting one or more of the following parameters:

- **Group**—Select a group to limit the alert to a specific group.
- **Label**—Select a label to limit the alert to a specific label.
- **Device**—Select a device to limit the alert to a specific device.
- **Sites**—Select a site to limit the alert to a specific site.

d. **Notification Options**

- **Email**—Select the **Email** check box and enter an email address to receive notifications when an alert is generated. You can enter multiple email addresses, separate each value with a comma.
- **Webhook**—Select the **Webhook** check box and select the Webhook from the drop-down list. For more information, see [Webhooks on page 487](#).

e. Click **Save**.

f. **Add Rule**—(Optional) For a few alerts, the **Add Rule** option appears. For such alerts, you can add additional rule(s). The rule summaries appear at the top of the page.



You can use the **Search box**, to search for alerts using keywords.

User Alerts

Aruba Central allows you to configure and enable the following user management alerts:

- **New User Account Added**—Generates an alert when a new user account is added. This alert is enabled by default and the alert severity is **Major**.
- **User Account Deleted**—Generates an alert when a user account is deleted.
- **User Account Edited**—Generates an alert when a user account is edited.

Switch Alerts

Aruba Central allows you to configure and enable the following switch alerts:

- **New Switch Connected**—Generates an alert when a new switch is connected.
- **Switch Disconnected**—Generates an alert when a switch is disconnected. This alert is enabled by default and the alert severity is **Major**. In the **Duration** field, enter the duration after which the alert must be generated. The default value is 10 minutes.
- **Switch Mismatch Config**—Generates an alert when there is a mismatch in switch configuration.
- **Switch Hardware Failure**—Generates an alert when the switch hardware fails. The following are the typical hardware failures for Aruba and MAS switches:

Aruba switches

- Fan failure.

- Power supply failure.
- Redundant power supply failure.
- High temperature.
- Management module failures—Management module failed self-test or lost communication with management module.
- Slot failure—Lost communications detected, slot self-test failure or unsupported module, or chassis hot swap failure.
- Fabric power failure.
- Internal power supply: Fan failure.
- Internal power supply failure.
- Internal power supply main PoE power failure.
- Internal power supply: Main inlet exceeds/within total fault count.
- Bad driver—Too many undersized/giant packets.
- Bad transceiver—Excessive jabbering.
- Bad cable—Excessive CRC/alignment errors.
- Too long cable—Excessive late collisions.
- Over bandwidth—High collision or drop rate.
- Broadcast storm—Excessive broadcasts.
- Duplex mismatch HDx—Duplex mismatch. Reconfigure to Full Duplex.
- Duplex mismatch FDx—Duplex mismatch. Reconfigure port to Auto.
- Link flap—Rapid detection of link faults and recoveries.

MAS switches

- Fan failure.
- High temperature.
- **Switch CPU Utilization**—Generates an alert when the switch CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Memory Utilization**—Generates an alert when the switch memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Switch Port Tx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data transmission rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data transmission rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Rx Rate**—In the **Transform Function** drop-down, select either **absolute** or **percentage**. Select **absolute** to generate an alert if the data reception rate of the port (in terms of Mbps) exceeds the threshold value. Select **percentage** to generate an alert if the data reception rate of the port (in terms of utilization as a percentage of total bandwidth available) exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Input Errors**—Generates an alert when the percentage of input errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.

- **Switch Port Output Errors**—Generates an alert when the percentage of output errors on the port exceeds the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Switch Port Duplex Mode**—Generates an alert when the port is operating in half-duplex mode. In the **Interface** field, enter the interface name.
- **Switch PoE Utilization**—Generates an alert when the PoE utilization for a port exceeds the critical and major threshold value. This alert is enabled by default and the alert severity is **Critical**. You can add additional rule(s) for this alert.

Gateway Alerts

You can configure the following alerts for the SD-WAN and Gateway appliance-related events:

- **SLA DPS Compliance Violations**—Generates an alert when the WAN policy does not meet the compliance criteria.
- **New Gateway Connected**—Generates an alert when a new Branch Gateway is connected.
- **Gateway Disconnected**—Generates an alert when a Branch Gateway is disconnected.
- **Blocked Session Detected**—Generates an alert when a blocked session is detected.
- **Gateway CPU Utilization**—Generates an alert when the Branch Gateway CPU utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Memory Utilization**—Generates an alert when the Branch Gateway memory utilization exceeds the threshold value. You can add additional rule(s) for this alert.
- **Gateway Emergency Mode**—Generates an alert when a gateway enters the emergency mode, where all the uplinks are down and the backup uplink is activated.
- **OSPF Session Error**—Generates an alert when an OSPF session fails.
- **BGP Session Error**—Generates an alert when a BGP session fails.
- **Gateway Base License Capacity Limit Exceeded**—Generates an alert when a Gateway with Foundation-Base Capacity subscription exceed the client capacity threshold.
- **WAN Health-Check Failure**—Generates an alert when WAN health check fails.
- **WAN VPN-Peer Unreachable**—Generates an alert when the WAN VPN peer is unreachable.
- **VPN Peer Failover**—Generates an alert when the VPN peer fails over.
- **WAN Uplink Status Change**—Generates an alert when the WAN uplink status changes.
- **WAN Uplink Autonegotiation State Change**—Generates an alert when the WAN uplink automatic negotiation status changes.
- **WAN Uplink Input Errors**—Generates an alert when the WAN uplink input errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink Output Errors**—Generates an alert when the WAN uplink output errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **WAN Uplink PHY Errors**—Generates an alert when the WAN uplink PHY errors exceed the threshold value. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **DHCP Pool Consumption Alert**—Generates an alert when the DHCP pool consumption exceeds the threshold value. In the **Subnet** field, enter the subnet address to filter the alert based on subnet.
- **IPSec Establishment Failure**—Generates an alert when the IPSec tunnel fails to establish.
- **IPSec SA Down**—Generates an alert when the IPSec SA is down.
- **All IPSec SAs Down**—Generates an alert when all the IPSec SAs are down.
- **CFG-SET Advertisement Failure**—Generates an alert when the CFG-SET advertisement fails.

- **Uplink Flapping**—Generates an alert when the uplink state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Tunnel Flapping**—Generates an alert when the tunnel state changes frequently. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **Uplink Speed Flapping**—Generates an alert when the uplink speed changes. In the **Interface** field, enter the interface name. You can add additional rule(s) for this alert.
- **EST Enrollment Failure**—Generates an alert when the Virtual Gateway fails to enroll with the EST server.
- **VGW VM Down**—Generates an alert when an Aruba Virtual Gateway deployed as a Virtual Machine is down.
- **Gateway Cluster VLAN Mismatch**—Generates an alert when one or more gateway(s) in a cluster have a mismatch in the VLAN.
- **Gateway Joining Cluster**—Generates an alert when a gateway joins the cluster.
- **Gateway Leaving Cluster**—Generates an alert when a gateway leaves the cluster.
- **Gateway Cluster Leader Change**—Generates an alert when there is cluster leader change.
- **Gateway Cluster Client Capacity**—Generates an alert when the cluster client capacity exceeds the configured threshold.
- **Gateway Firmware Upgrade Failed**—Generates an alert when there is a firmware upgrade failure.

Access Point Alerts

Aruba Central allows you to configure and enable the following IAP alerts:

- **New Virtual Controller Detected**—Generates an alert when a new virtual controller is detected.
- **Virtual Controller Disconnected**—Generates an alert when a virtual controller is disconnected. This alert is enabled by default and the alert severity is automatically set to **Major**. To customize the alert trigger, enter a duration in minutes, in the **Duration** field. By default, the trigger to generate the alert is set to 10 minutes.
- **New AP Detected**—Generates an alert when a new Instant AP is detected.
- **AP Disconnected**—Generates an alert when an Instant AP is disconnected. This alert is enabled by default and the alert severity is automatically set to **Major**. To customize the alert trigger, enter a duration in minutes, in the **Duration** field. By default, the trigger to generate the alert is set to 15 minutes.
- **Rogue AP Detected**—Generates an alert when a rogue Instant AP is detected. This alert is enabled by default and the alert severity is **Major**.
- **Infrastructure Attack Detected**—Generates an alert when an infrastructure attack is detected.
- **Client Attack Detected**—Generates an alert when a client attack is detected.
- **Uplink Changed**—Generates an alert when an uplink has changed.
- **Modem Unplugged**—Generates an alert when the modem is unplugged.
- **Modem Plugged**—Generates an alert when the modem is plugged.
- **AP CPU Utilization**—Generates an alert when the Instant AP CPU utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **AP Memory Utilization**—Generates an alert when the Instant AP memory utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Insufficient Power Supplied**—Generates an alert when the IAP is supplied with lesser power than the required power.

- **Radio Channel Utilization**—Generates an alert when the Instant AP radio channel utilization exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Radio Noise Floor**—Generates an alert when the Noise Floor (dBm) exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. From the **Band** drop-down, select the spectrum band: **2.4 GHz** or **5 GHz**. You can add additional rule(s) for this alert.
- **Connected Clients per VC**—Generates an alert when the number of connected clients to the VC exceeds the threshold value. In the **Duration** field, enter the duration after which the alert must be generated. You can add additional rule(s) for this alert.
- **Connected Clients per AP**—Generates an alert when the number of connected clients to the AP exceeds the threshold value. You can enter the threshold value after which the alerts must be generated. The recommended value is 15 minutes and above. You can add additional rule(s) for this alert.

Connectivity Alerts

Aruba Central allows you to configure and enable the following connectivity alerts:

- **DNS Delay Detected**—Generates an alert when DNS delay is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DNS Failure Detected**—Generates an alert when DNS failure is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Delay Detected**—Generates an alert when DHCP delay is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **DHCP Failure Detected**—Generates an alert when DHCP failure is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Authentication Delay Detected**—Generates an alert when authentication delay is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Authentication Failure Detected**—Generates an alert when authentication failure is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Association Delay Detected**—Generates an alert when client association delay is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.
- **Association Failure Detected**—Generates an alert when client association failure is detected. The **Duration** field displays the duration after which the alert is generated. The default value is 30 minutes. You can add additional rule(s) for this alert.

WAN Health Alerts

Aruba Central allows you to configure and enable the following WAN Health alerts:

- **Application Unreachable**—Generates an alert when the application is not reachable.
- **High Latency Detected**—Generates an alert when high latency is detected.
- **Low Download Rate Detected**—Generates an alert when the download rate over the WAN network is detected to be low.

- **Low Upload Bandwidth Detected**—Generates an alert when the upload bandwidth over the WAN network is detected to be low.
- **Low Download Bandwidth Detected**—Generates an alert when the download bandwidth over the WAN network is detected to be low.
- **High Download Packet Loss Detected**—Generates an alert when there is a high download packet loss over the WAN network.
- **High Download Jitter Detected**—Generates an alert when there is a high download jitter detected.
- **High Connection Time Detected**—Generates an alert when the connection time to the WAN network is high.
- **Health Check Failed**—Generates an alert when the health check fails.
- **High Upload Packet Loss Detected**—Generates an alert when there is a high upload packet loss detected.
- **High Upload Jitter Detected**—Generates an alert when there is a high upload jitter detected.

Audit Alerts

Aruba Central allows administrators to enable alerts for configuration changes at group level. The **Config Change Detected** alert is under **Audit** tab. Configuration change alerts are intended for administrators handling large distributed network. Alerts are triggered under the following scenarios:

- Create New Template
- Update Existing Template
- Variable Upload
 - Device Level: Sends an alert with additional parameters such as serial number and MAC address of the device.
 - Group Level: Sends an alert with respective group name.
 - Configuration restore
- Configuration change at Device Level
- Configuration change at Group Level

The alert content includes the following information:

- Group Name
- Device Type
- User ID
- Config Change
- Device Serial number and MAC Address

The following table describes the behavior of the alert and alert content depending on the user action,

Table 73: Config Alert Behavior

| User Action | Group Name | Device Type | User ID | Config Change | Device Serial/ MAC |
|--|--|----------------------|---------|------------------------------|--------------------|
| Created a template | Template group name | IAP/ Switch. Gateway | User ID | No Content | NO |
| Updated existing template | Template group name | IAP/ Switch/ Gateway | User ID | Changed content is displayed | NO |
| Uploaded variable at device level | Group name to which the device belongs | IAP/ Switch/ Gateway | User ID | No Content | YES |
| Uploaded variable at group level | Template group name | IAP/ Switch/ Gateway | User ID | No Content | NO |
| Made configuration at the device level | Group name to which the device belongs | IAP/ Switch/ Gateway | User ID | Changed content is displayed | YES |
| Made configuration change at the group level | UI group name | IAP/ Switch/ Gateway | User ID | Changed content is displayed | NO |

Site Alerts

Aruba Central allows you to configure and enable this alert for aggregated device disconnections. The **Aggregated Device Disconnections** alert is under **Site** tab. It is intended to reduce the number of alerts that are generated for customers that prefer to have a single notification or a handful of notifications for mass outages where several devices may go down simultaneously in a given site.

For example, if site alerts are configured with **Severity** as Major, **Duration** being 10 minutes, and **Site** as site1, a single alert saying “Aggregated Device Disconnects” is raised on the user interface for every set of device belonging to “site1” that goes down within 10 minutes of the first DOWN event limited to 100 devices per alert. Any device that is not a part of “site1” is treated as not being aggregated.

The alert content includes the following information for each device:

- Hostname
- Device Serial Number
- MAC Address
- IP Address




Unlike other alerts types, site alerts will not be auto closed.

Viewing Enabled Alerts

To view alerts that you have enabled, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group, device, site, or label.
2. Under **Analyze**, click **Alerts & Events**. The **Alerts & Events** page is displayed.

3. In the **Alerts & Events** page, click the configuration  icon. The **Alert Severities & Notifications** is displayed.
4. In the **Alert Severities & Notifications** page, click **Enabled**. Use the tabs to navigate between the alert categories. The alerts enabled for each category are displayed in the respective tabs.

Reports

The Aruba Central dashboard enables you to create various types of reports. You can create recurrent reports or configure the reports to run on demand. To create a report, you must have read/write privileges or Admin rights.

The **Reports** page has the following sections:

- **Create**—Creates a report that can run instantly, on scheduled time, or recurrent reports.
- **Manage**—Edits or deletes the scheduled reports.
- **Browse**—Lists all the archived reports.



For a visual representation of viewing an AI Insight, click [here](#).

This section includes the following topics:

- [Report Categories](#)
- [Creating a Report](#)
- [Editing a Report](#)
- [Viewing a Report](#)
- [Downloading a Report](#)
- [Deleting a Report](#)

Report Categories

Aruba Central allows you to create various types of reports based on your network requirements. The report types supported by Aruba Central are:

- **Clients**
- **Infrastructure**
- **Security Compliance**
- **Applications**

The following table lists the different types of reports under each report category:

Table 74: *Clients Reports*

| Section | Description |
|-------------------------|---|
| Client Inventory | <p>Displays the client details summarized by all aggregation fields. The report includes the following details:</p> <ul style="list-style-type: none">■ Client count by SSID■ Client count by role■ Client count by connection mode■ client count by connection type■ Client count by OS■ Client count by vendors |
| Client Session | <p>Displays the details of client sessions aggregated by OS / Connection Mode / SSID / Role / MAC Vendor. The report includes the following details:</p> <ul style="list-style-type: none">■ Clients■ Sessions■ Traffic■ Session Data by OS / Connection Mode / SSID / Role / MAC Vendor■ Clients by OS / Connection Mode / SSID / Role / MAC Vendor■ Time Spent by OS / Connection Mode / SSID / Role / MAC Vendor■ Data Usage by OS / Connection Mode / SSID / Role / MAC Vendor■ Client Device OS / Connection Mode / SSID / Role / MAC Vendor■ Top 10 clients by usage filtered based on SSID |
| Client Usage | <p>Displays the client usage and count details. The report includes the following details:</p> <ul style="list-style-type: none">■ Client Usage■ Top 10 clients by usage filtered based on SSID■ Client Count■ Top 10 applications by usage■ Top 10 web categories by usage■ Top 10 app categories■ Web reputation |
| Guest | <p>Displays the guests, and guest session details for all the SSIDs for a specific time period. NOTE: Guest report does not support location based filtering for any selected device group or site label to ensure end user privacy protection.</p> |

Table 75: Infrastructure Reports

| Section | Description |
|----------------------------------|--|
| Capacity Planning | <p>Displays the throughput and client density information for devices provisioned in Aruba Central. The report includes the following details:</p> <ul style="list-style-type: none"> ■ Subscription Utilization: Total Subscription, Used subscriptions, and Available subscriptions ■ Top 25 APs by usage ■ Top 25 switches by usage ■ Top 25 APs by peak client ■ Top-25 APs by average client |
| Configuration & Audit | <p>Displays the configuration and audit logs for all the device management, configurations, and user management events triggered in Aruba Central. The report includes the following details:</p> <ul style="list-style-type: none"> ■ Configuration Audit Status ■ Aruba Switches Configuration Audit Status ■ Virtual Controllers Configuration Audit Status |
| Infra Inventory | <p>Displays the inventory and subscription information for the devices that are online during a specific duration. The report includes the following details:</p> <ul style="list-style-type: none"> ■ Subscription Utilization: Total Subscription, Used subscriptions, and Available subscriptions ■ Subscription Keys ■ Number of APs ■ Number of Switches ■ Number of Gateways ■ Firmware Version Summary (IAP) ■ Firmware Version Summary (Switch) ■ Firmware Version Summary (Gateway) ■ Devices by Site ■ Model and Firmware version (IAP) ■ Model and Firmware version (Switch) ■ Model and Firmware version (Gateway) ■ AP interfaces summary |
| Network | <p>Displays the following parameters:</p> <ul style="list-style-type: none"> ■ Top 20 Sites By Availability ■ Bottom 20 Sites By Availability ■ Top 20 Sites By WLAN Usage ■ Bottom 20 Sites By WLAN Usage ■ Number of APs ■ AP Model ■ Top Ten Clients By Usage filtered based on SSID ■ Device Types (Current) ■ Top Ten APs By Usage ■ Total Usage By SSID ■ Wireless Clients by SSID ■ Peak and Average Wireless Data Usage ■ Number of Switches ■ Switch Model ■ Top Ten Switches by Usage ■ Top Ten Ports by Usage ■ Wired Peak and Average Uplink Stats ■ Number of Gateways ■ Gateway Model |

Table 75: Infrastructure Reports

| Section | Description |
|-----------------------------|---|
| New Infra Inventory | <p>Displays the inventory and subscription information to the devices that are newly added in Aruba Central. The report includes the following details:</p> <ul style="list-style-type: none"> ■ Subscription Utilization: Total Subscription, Used subscriptions, and Available subscriptions ■ Subscription Keys ■ APs Added by Model ■ APs Added by Group ■ Switches Added by Model ■ Switches Added by Group ■ Total APs ■ Total Switches |
| Resource Utilization | <p>Displays the details of infrastructure devices that exceeded the configured thresholds on a daily, weekly, and monthly basis. The report includes the following details:</p> <ul style="list-style-type: none"> ■ Resource Utilization Threshold ■ CPU/Memory Compliance ■ Sites with Non-Compliant Devices ■ Non-Compliance by Device Type ■ Non-Compliant Access Points ■ Non-Compliant Switches |
| RAPIDS | Displays the details of all rogue or interfering devices in Aruba Central. |
| RF Health | <p>Displays the following RF usage statistics for the AP radios.</p> <ul style="list-style-type: none"> ■ Problem Radios (5 GHz / 2.4 GHz) ■ Most Noise (5 GHz / 2.4 GHz) ■ Most Errors (5 GHz / 2.4 GHz) ■ Most Utilized by Channel Usage (5 GHz / 2.4 GHz) ■ Least Utilized by Channel Usage (5 GHz / 2.4 GHz) ■ Most Channel Changes (5 GHz / 2.4 GHz) ■ Most Transmission Power Changes (5 GHz / 2.4 GHz) ■ Radio with Least Goodput (5 GHz / 2.4 GHz) <p>NOTE: For APs that support 5 GHz dual band in synchronization with Aruba Instant 8.3.0.0, the Device column in the RF Health Report shows the radio number of the operating radio along with the model number of the device.</p> |
| WAN Availability | <p>Displays WAN overlay and underlay availability information.</p> <p>The Underlay report contains the following details:</p> <ul style="list-style-type: none"> ■ Branch Gateway <ul style="list-style-type: none"> ● Site ● Serial Number ● Host name ● MAC ■ Uplink <ul style="list-style-type: none"> ● Name ● Type ● VLAN ■ %Uptime ■ Uptime ■ Downtime <p>The Overlay report contains the following details:</p> <ul style="list-style-type: none"> ■ Branch Gateway <ul style="list-style-type: none"> ● Site ● Serial Number ● Host name |

Table 75: Infrastructure Reports

| Section | Description |
|-----------------------|--|
| | <ul style="list-style-type: none"> ● MAC ■ Uplink <ul style="list-style-type: none"> ● VLAN ■ Tunnel <ul style="list-style-type: none"> ● Name ● SIP ● DIP ■ %Uptime ■ Uptime ■ Downtime |
| WAN Inventory | <p>Displays a list of Branch Gateways onboarded. The report is segregated by ArubaOS software version and contains the following information:</p> <ul style="list-style-type: none"> ■ Software Version ■ Site Name ■ Serial Number ■ Host name ■ MAC ■ IP Address ■ Model ■ Status ■ Street Address |
| WAN Compliance | <p>Displays the worst performing or best performing links according to the SLA compliance violations. The report contains the following details:</p> <ul style="list-style-type: none"> ■ Policy Name ■ Branch Gateway <ul style="list-style-type: none"> ● Site ● Serial Number ● Host Name ● MAC ■ Uplink <ul style="list-style-type: none"> ● Name ● Type ■ Value <ul style="list-style-type: none"> ● Compliance |

Table 75: Infrastructure Reports

| Section | Description |
|---------------------------------------|---|
| WAN Transport Health | <p>Displays the top N links with probed values. The report contains the following details:</p> <ul style="list-style-type: none"> ■ Report Name ■ Report Type ■ Date Run ■ Periodicity ■ Title ■ Probe Destination IP ■ Branch Gateway <ul style="list-style-type: none"> ● Site ● Serial Number ● Host name ● MAC ■ Uplink <ul style="list-style-type: none"> ● Name ● Uplink ■ Value <ul style="list-style-type: none"> ● Either Loss (%) |
| WAN Utilization | <p>Displays WAN bandwidth utilization information for Underlay, Overlay, and Uplinks. The report contains the following details:</p> <ul style="list-style-type: none"> ■ Branch Gateway <ul style="list-style-type: none"> ● Site ● Serial Number ● Host name ● MAC ■ Uplink <ul style="list-style-type: none"> ● Name ● Type ● VLAN ■ Usage <ul style="list-style-type: none"> ● Average Bandwidth (Mbps) ● SLA Bandwidth (Mbps) ● %Utilization |
| WAN Web Content Classification | <p>Displays the details of Reputation, Categories, and Destination Countries. The report can categorize information by:</p> <ul style="list-style-type: none"> ■ Transport Type— Internet or VPN. ■ Top N Count—Top N count of events, the number should be between 1-250. ■ Classify On—Classify the report on geo location, web category, or web reputation. ■ Report type— Choose either a complete summary report or blocked urls report. ■ Report Period—Choose the time period for the report from: <ul style="list-style-type: none"> ● Last day ● Last seven days ● Last 30 days ● Custom Range ■ Recurrence—Set the recurrence for the report generation. <p>The reports contain the following Device Details:</p> <ul style="list-style-type: none"> ■ Site—Location of the Gateway or VPNC. ■ Serial #—Serial number of the device. ■ Hostname—The hostname. ■ MAC—Device MAC address. <p>The report also contains the top 5 Web Reputation, Web Category, Destination, and total usage details. If required, a user can generate a report for web traffic going over a VPN.</p> |

Table 76: Security Compliance Reports

| Section | Description |
|----------------------------|--|
| PCI Compliance | Displays the PCI Compliance result as Fail or Pass . |
| Security Compliance | Displays the security compliance results. The report includes the following details: <ul style="list-style-type: none"> ■ Rogue APs ■ Total Rogue APs Detected ■ Wireless Intrusions ■ Total Wireless Intrusions |

Table 77: Applications Reports

| Section | Description |
|--------------|--|
| AppRF | Displays application usage report for a specific device group. The report displays the following widgets: <ul style="list-style-type: none"> ■ Top 10 applications accessed by the clients ■ Top 10 web categories accessed by the clients ■ Top 10 applications for device types ■ Others |
| UCC | Displays the security compliance results. The report includes the following details: <ul style="list-style-type: none"> ■ Rogue APs ■ Total Rogue APs Detected ■ Wireless Intrusions ■ Total Wireless Intrusions |

Creating a Report

You can generate reports for devices associated with a group, multi-group, label, or site level. You can also set a periodicity for running the reports.



Although your page view is set to a specific group, site, or label, you can create reports for a different group, site, or label. However, if your page view is set to an Instant AP cluster or Switch, you can schedule report generation only for that Instant AP cluster or Switch.

To create a report:

1. In the **Network Operations** app, under **Analyse**, click **Reports**. The reports overview page is displayed.
2. Click **Create**. The **Reports** page is displayed.
3. Select one of the categories from the page display and click on the type of report you wish to create.
4. Under **Context**, select one of the following options:
 - a. **Groups**
 - b. **Sites**
 - c. **Labels**
5. To generate reports for the devices attached to a group, select **Groups** and then select a device group.
6. To generate reports for devices attached to a label, click **Labels** and then select a label.
7. To generate reports for devices deployed on a specific site, click **Sites** and select a site.

For **Client Session** report, the **Show Detailed Report** option is available only for a selected site. Selecting this option restricts the **Report Period** to **Last Day** and **Custom Range** only. Selecting custom range enables you to select a one day time range from the particular day till the last seven days only.

8. To set the threshold values for a **Resource Utilization** report, select the AP, Switch, and Gateway thresholds under the **Threshold** window.
9. Click **Next**.
10. Under **Report Period**, select one of the following options:
 - a. **Last day**
 - b. **Last 7 days**
 - c. **Last 30 days**
 - d. **Custom Range**
11. Click **Next**.
12. Select one of the recurrent options:
 - a. **One time (now)**
 - b. **One time (Later)**
 - c. **Every day**
 - d. **Every week**
 - e. **Every month**
13. Under **Report Information**, add a report title, and an optional email address to receive the report as email.
14. Select **PDF** and/or **CSV**, to specify the format of the report to receive the email.
15. Click **Generate**. The report gets generated is displayed under the **Generated Reports** tab. The report gets emailed as an attachment to the email address provided. If not, you can download the **PDF** and/or **CSV** from the **Generated Reports** table.
16. If you selected **One Time** as the option in step 12, the report will display under **Archived Reports**. If the report is scheduled for a later time, the details will display under **Scheduled Reports**.

Editing a Report

To edit a report:

1. From the **Network Operations** app, under **Analyze**, click **Reports**. The reports overview page is displayed.
2. Click **Manage**.
3. Under **Scheduled Reports**, select a report and then click the edit icon. The **Create Report** page is displayed.
4. Click **Next**. The **Context** page is displayed.
5. Under **Context**, select one of the following options:
 - a. **Groups**
 - b. **Sites**
 - c. **Labels**
6. To generate reports for the devices attached to a group, select **Groups** and then select a device group.
7. To generate reports for devices attached to a label, click **Labels** and then select a label.
8. To generate reports for devices deployed on a specific site, click **Sites** and select a site.
9. Click **Next**.
10. Under **Report Period**, select one of the following options:
 - a. **Last day**
 - b. **Last 7 days**

- c. **Last 30 days**
 - d. **Custom Range**
11. Click **Next**.
 12. Select one of the recurrent options:
 - a. **One time (now)**
 - b. **One time (Later)**
 - c. **Every day**
 - d. **Every week**
 - e. **Every month**
 13. Select the **Run Time** for generating the report at a specific time.
 14. Under **Report Information**, add a report title, and an optional email address to receive the report as email.
 15. Select **PDF** and/or **CSV**, to specify the format of the report to receive the email.
 16. Click **Generate**. The report gets generated is displayed under the **Generated Reports** tab. The report gets emailed as an attachment to the email address provided. If not, you can download the **PDF** and/or **CSV** from the **Generated Reports** table.
 17. If you selected **One Time** as the option in step 12, the report will display under **Archived Reports**. If the report is scheduled for a later time, the details will display under **Scheduled Reports**.

Viewing a Report

To view a report:

1. From the **Network Operations** app, under **Analyze**, click **Reports**. The reports overview page is displayed.
2. Click **Browse**. The **Report** table is displayed. Existing reports are listed under **Generated Reports** page.
3. Under **Generated Reports**, click the report name. The report details are displayed.

Downloading a Report

To download a report:

1. From the **Network Operations** app, under **Analyze**, click **Reports**. The reports overview page is displayed.
2. Click **Browse**. The **Report** table is displayed. Existing reports are listed under **Generated Reports** page.
3. Under **Generated Reports**, hover the cursor over the report name. The PDF, CSV, Email, and Delete icons are displayed.
4. Click **PDF** or **CSV** to download the report. The report gets downloaded to the local system.
5. Optionally, click the email icon to generate an email attachment of the report.

You can also download the report from the report details page. Click **PDF**, **CSV**, or email icon to select the format.

Deleting a Report

To delete a report, perform the following steps:

1. From the **Network Operations** app, under **Analyze**, click **Reports**. The reports overview page is displayed.
2. Click **Browse**. The **Report** table is displayed. Existing reports are listed under **Generated Reports** page.

3. Under **Generated Reports**, hover the cursor over the report name. The PDF, CSV, Email, and Delete icons are displayed.
4. Click the delete icon. The selected report gets deleted.

Deleting Multiple Reports

To delete multiple reports, perform the following steps:

1. From the **Network Operations** app, under **Analyze**, click **Reports**. The reports overview page is displayed.
2. Click **Browse**. The **Report** table is displayed. Existing reports are listed under **Generated Reports** page.
3. Under **Generated Reports**, select multiple reports by clicking each row. A pop-up displays the number of selected rows.



Clicking the **Report Name** displays the corresponding report details page. To select multiple reports, click any column apart from the Report Name and select the required reports.

4. Click the delete icon within the pop-up. The **Delete Report** window appears.
5. Click **Yes** to delete the selected reports. The selected reports get deleted.

Viewing Audit Trails in the Standard Enterprise Mode

The **Audit Trail** page in the Standard Enterprise Portal shows the total number logs generated for all device management, configuration, and user management events triggered in Aruba Central. You can search or filter the audit trail records based on any of the following columns:

- Occurred on (Custom Range)
- Username
- IP Address
- Category
- Description
- Target

To view the **Audit Trail** logs perform the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Analyze**, click **Audit Trail**. The **Audit Trail** table is displayed with the following details:
 - **Occurred On**—Timestamp of the audit log. Use the sort option to sort the audit logs by date and time. Use the filter option to select a specific time range to display the audit logs.
 - **IP Address**—IP address of the client device.
 - **Username**—Username of the admin user who applied the changes.
 - **Target**—The group or device to which the changes were applied.
 - **Category**—Type of modification and the affected device management category. See [Classification of Audit Trails](#).
 - **Description**—A short description of the changes such as subscription assignment, firmware upgrade, and configuration updates. Click ⓘ to view the complete details of the event. For example, if an event was not successful, clicking the ellipsis displays the reason for the failure.



To customize the **Audit Trail** table, click the eclipses ☰ icon to select the required columns, or click **Reset to default** to set the table to the default columns.

Classification of Audit Trails

The audit trail is classified according to the type of modification and the affected device management category. The category can be one of the following:

- Alert Configuration
- API Gateway
- Configuration
- Device Management
- Federated User Activity
- Firmware Management
- Gateway Management
- Groups
- Guest
- Install Manager
- Label Management
- MSP
- RBAC
- Reboot
- SAML Profile
- Sites Management
- Subscription Management
- Templates
- Tools
- User Activity
- User Management
- Variables

Instant APs offer an enterprise-grade networking solution with a simple setup. The WLAN solution with Instant APs supports simplified deployment, configuration, and management of Wi-Fi networks.

Instant APs run the Aruba Instant software that virtualizes Aruba Mobility Controller capabilities on 802.11 APs and offers a feature-rich enterprise-grade Wi-Fi solution. Instant APs are often deployed as a cluster. An Instant AP cluster includes a master AP and set of other APs that act as slave APs.

In an Instant deployment scenario, only the first AP or the master AP that is connected to a provisioning network is configured. All other Instant APs in the same VLAN join the master AP and inherit the configuration changes. The Instant AP clusters are configured through a common interface called Virtual Controller. A Virtual Controller represents the combined intelligence of the Instant APs in a cluster.

Supported Deployment Modes

Aruba Instant APs can be deployed in the following modes in Aruba Central:

- **Cluster mode**—In this mode, several Instant APs form a cluster when connected to a provisioning network and an master Instant AP is elected. In the cluster mode, new Instant AP onboarded to Aruba Central can join an existing Instant AP cluster.
- **Standalone mode**—In this mode, individual Instant APs are provisioned in groups and managed from Aruba Central.

Configuration and Management

Network administrators can manage Instant APs through the Aruba Instant UI, Aruba Central, or AirWave management system.

For information on how to configure Instant APs using the Aruba Instant UI, see the *Aruba Instant User Guide*.

For more information on how to deploy, provision, manage, and monitor Instant APs from Aruba Central, see the following topics:

- [Supported Instant APs on page 29](#)
- [Provisioning Instant APs on page 287](#)
- [Configuring Device Parameters on page 290](#)
- [Configuring Network Profiles on Instant APs on page 300](#)
- [Configuring Time-Based Services for Wireless Network Profiles on page 336](#)
- [Configuring ARM and RF Parameters on Instant APs on page 338](#)
- [Configuring IDS Parameters on APs on page 343](#)
- [Configuring Authentication and Security Profiles on Instant APs on page 347](#)
- [Configuring Instant APs for VPN Services on page 378](#)
- [Configuring DHCP Pools and Client IP Assignment Modes on Instant APs on page 384](#)
- [Configuring Services on page 391](#)
- [Configuring Uplink Interfaces on Instant APs on page 400](#)
- [Configuring Enterprise Domains on page 406](#)
- [Configuring Syslog and TFTP Servers for Logging Events on page 409](#)
- [Resetting an AP on page 411](#)

- [Mapping Instant AP Certificates on page 412](#)
- [Configuring APs Using Templates on page 413](#)
- [Managing Variable Files on page 99](#)

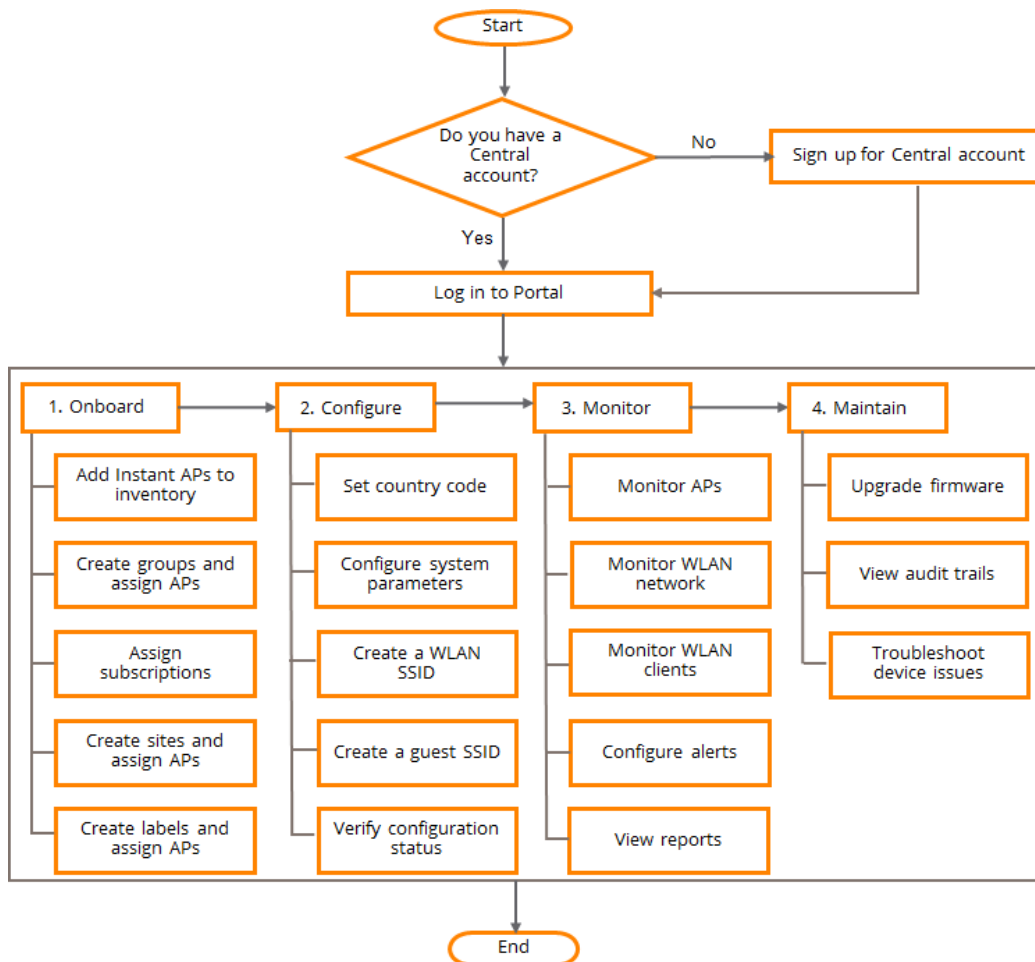
Provisioning Instant APs

The following figure illustrates the procedure for bringing up Instant APs and configuring a basic WLAN setup. To view a detailed description of the tasks, click the task link in the flowchart.



When you click a task in the flowchart, the linked topic opens in a pop-up window. After you browse through the topic, click outside the pop-up window to return to this page.

Figure 95 *Getting Started—Instant APs*



Deploying a Wireless Network Using Instant APs

This section describes how to configure WLAN SSIDs, radio profiles, DHCP profiles, VPN routes, security and firewall settings, uplink interfaces, logging servers on Instant APs.

For more information on Instant AP configuration, see the following topics:

- [Configuring Device Parameters on page 290](#)
- [Configuring Network Profiles on Instant APs on page 300](#)
- [Configuring Time-Based Services for Wireless Network Profiles on page 336](#)

- [Configuring ARM and RF Parameters on Instant APs on page 338](#)
- [Configuring IDS Parameters on APs on page 343](#)
- [Configuring Authentication and Security Profiles on Instant APs on page 347](#)
- [Configuring Instant APs for VPN Services on page 378](#)
- [Configuring DHCP Pools and Client IP Assignment Modes on Instant APs on page 384](#)
- [Configuring Services on page 391](#)
- [Configuring Uplink Interfaces on Instant APs on page 400](#)
- [Configuring Enterprise Domains on page 406](#)
- [Configuring Syslog and TFTP Servers for Logging Events on page 409](#)
- [Resetting an AP on page 411](#)
- [Mapping Instant AP Certificates on page 412](#)

Setting Country Code

The initial Wi-Fi setup of an Instant AP requires you to specify the country code for the country in which the Instant AP operates. This configuration sets the regulatory domain for the radio frequencies that the Instant AP uses. The available 20 MHz, 40 MHz, or 80 MHz channels are dependent on the specified country code.

Country Code Configuration in Aruba Central from UI

If you provision a new Instant AP without the country code, Aruba Central exhibits the following behavior:

Table 78: *Instant AP Provisioned To Aruba Central*

| Country Code Configured at Instant AP | Country Code Configured in Group | Behavior |
|---------------------------------------|----------------------------------|---|
| No | Yes | The country code of the group is pushed to the newly added Instant AP. |
| No | No | Aruba Central displays the Country Code not set. Config not updated message in the Audit Trail. A notification is also displayed at the bottom of the main window to set the country code of the new Instant AP. To set the country code, perform the following actions: <ol style="list-style-type: none"> 1. Click Set Country Code Now link on the notifications pane. The Set Country Code pop up is displayed. 2. Select the device and click the edit icon. 3. Specify a country code from the Country Code drop-down list. 4. Click Save. |




If an Instant AP already has a country code, and then joins the Central using ZTP configuration, the country code of the Instant AP is retained. In this case, Central would not push the group's country code.

Setting Country Code at Group Level

To set the country code of the Instant AP at the group level, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **General**. The page to set the configurations for the group is displayed.
7. Select the country code for Instant AP from the **Set Country code for group** drop-down list.
8. Click **Save Settings**.
9. Reboot Instant AP for changes to take effect.




By default, the value corresponding to the **Set Country code for group field** is empty. This indicates that any Instant AP with different country codes can be a part of the group.



Once the **Set Country code for group** field is set, the field cannot revert to the default value. When the country code of the group is changed, the country code of the already connected Instant AP also will be updated accordingly.

Setting Country Code at Device Level

To set the country code of the Instant AP at the device level, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **General**. The page to set the configuration for the device is displayed.
7. Click the edit icon.
8. Select the new country code from the **Country Code** drop-down list.
9. Click **OK**.
10. Reboot Instant AP for changes to take effect.



By default, the value corresponding to the **Country code** is the country code set at the group level which can be then modified at the device level from the drop-down list. The country code of the Instant AP will always be the most recently set country code at the group level or device level.

Country Code Configuration at Group Level from API

Aruba Central provides an option to set and get the country code at group level through the APIs in **API Gateway**.

To set or get the country code at group level through API:

1. In the Account Home, go to **API Gateway**.
2. Click the **Authorized Apps & Tokens** tab and generate a token key.
3. Download and copy the generated token.
4. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page is displayed.
5. On the left navigation pane, select **Configuration** from the **URL** drop-down list.
6. Paste the token key in the **Token** field and press enter.
7. Click **NB UI Group Configuration**. The following options are displayed:

- **Set country code at group level ([PUT]/configuration/v1/country)** — This API allows to set country code for multiple groups at once. Aruba Central currently allows country codes of up to 50 Instant AP device groups to be configured simultaneously. To set the country codes of multiple groups, enter the group names and country code as inputs corresponding to the **groups** and **country** labels respectively in the script { "groups": ["string"], "country": "string" } within the **set_group_config_country_code** text box.
- **Get country code set for group ([GET]/configuration/v1/{group}/country)** — This API allows to retrieve the country code set for a specific Instant AP group. To get the country code information of the Instant AP group, enter the name of the group for which the country code is being queried corresponding to the **country** label in the script { "country": "string" } within the **group** text box.



The APIs for setting and retrieving country code information are not available for the Instant AP devices deployed in template groups.

The following are the response messages displayed in the **Set country code at group level** and **Get country code set for group** sections:

Table 79: Response Messages

| Set country code at group level | Get country code set for group |
|---|---|
| <ul style="list-style-type: none"> ■ 201 - Successful operation ■ 400 - Bad Request ■ 401 - Unauthorized access, authentication required ■ 403 - Forbidden, do not have write access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress | <ul style="list-style-type: none"> ■ 400 - Bad Request ■ 401 - Unauthorized access authentication required ■ 403 - Forbidden, do not have read access for group ■ 413 - Request-size limit exceeded ■ 417 - Request-size limit exceeded ■ 429 - API Rate limit exceeded ■ 500 - Internal Server Error ■ 503 - Service unavailable, configuration update in progress |

For further details on API help, refer to <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Configuring Device Parameters

To configure device parameters for an Instant AP, complete the following steps:


1. In the **Network Operations** app, use the filter bar to select a group.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. To edit an AP, click the edit icon for that AP. The edit pane for modifying the Instant AP parameters is displayed.
5. Configure the parameters described below:

Table 80: Access Points Configuration

| UI | Parameters | Description |
|-------------------|------------------------------------|--|
| Basic Info | Name | Configures a name for the Instant AP. You can specify a character string of up to 32 ASCII or non-ASCII characters. |
| | AP Zone | Configures the Instant AP zone. For Instant APs running firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. Aruba recommends that you do not configure zones in both SSID and in the Per AP settings of an Instant AP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see <i>Aruba Instant User Guide</i> . |
| | RF Zone | Allows you to create an RF zone for the AP. With RF zone, you can configure different power transmission settings for APs in different zones or sections of a deployment site. For example, you can configure power transmission settings to make Wi-Fi available only for the devices in specific areas of a store. You can also configure separate RF zones for the 2.4 GHz and 5 GHz radio bands for the Instant APs in a cluster. For more information, see Configuring Radio Parameters on page 342 . Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors. |
| | Swarm Mode | Allows to set one of the following operation modes: Cluster —Allows Instant AP join an Instant AP cluster. Standalone —Allows Instant AP to function in the standalone mode. After changing the AP operation mode, ensure that you reboot the AP. |
| | Preferred Master | Provisions the Instant AP as a master Instant AP. By default, the Preferred Master toggle button remains disabled. |
| | IP Address for Access Point | Allows IP to get an IP address from the DHCP server. By default, the Instant APs obtain IP address from a DHCP server. The users can also assign a static IP address to the Instant AP. To specify a static IP address for the Instant AP, complete the following steps: Enter the new IP address for the Instant AP in the IP Address text box. Enter the subnet mask of the network in the Netmask text box. Enter the IP address of the default gateway in the Default Gateway text box. Enter the IP address of the DNS server in the DNS Server text box. Enter the domain name in the Domain Name text box. |
| Radio | Mode | Select any of the following options: Access —In the Access mode, the Instant AP serves clients, while also monitoring for rogue Instant APs in the background. <ul style="list-style-type: none"> ■ Monitor—In the Monitor mode, the Instant AP acts as a dedicated monitor, scanning all channels for rogue Instant APs and clients. ■ Spectrum Monitor—In the Spectrum Monitor mode, the Instant AP functions as a dedicated full-spectrum RF monitor, scanning all channels to detect interference, whether from the |

| UI | Parameters | Description |
|--------------------------|----------------------------------|--|
| | | <p>neighboring Instant APs or from non-Wi-Fi devices such as microwaves and cordless phones.</p> <p>NOTE: In the Monitor and Spectrum Monitor modes, the Instant APs do not provide access services to clients.</p> <p>NOTE: In the dual 5 GHz band, the Mode remains as Access and is non-editable. This dual 5 GHz band is only supported on AP-344 and AP-345 that run on Instant AP 8.3.0.0. For more information, see the Configuring Dual 5 GHz Radio Bands on an Instant AP section. To get accurate monitoring details and statistics, it is highly recommended to reboot the Instant APs once the Instant APs are toggled from the 2.4/5 GHz mode to dual 5 GHz radio mode or vice-versa.</p> |
| | | <p>You can configure a radio profile on an Instant AP either manually or by using the Adaptive radio management assigned (ARM) feature.</p> <p>ARM is enabled on Aruba Central by default. It automatically assigns appropriate channel and power settings for the Instant APs.</p> |
| | | <p>You can also Administrator Assigned and select the number of channels in the Channel drop-down list. In the Transmit Power field, enter the signal strength measured in dBm.</p> |
| External Antenna | Antenna Gain | <p>If the Instant AP has external antenna connectors, you need to configure the transmit power of the system. You can also measure or calculate additional attenuation between the device and the antenna before configuring the antenna gain. For more information, see the Configuring External Antenna section.</p> |
| | Antenna Polarization Type | <p>The wireless bridge's integrated antenna sends a radio signal that is polarized in a particular direction. The antenna's receive sensitivity is also higher for radio signals that have the same polarization. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction. To maximize the performance of the wireless link, both antennas must be set to the same polarization direction.</p> |
| Installation Type | Installation Type | <p>Configure the Installation Type of the Instant AP you have selected. The Installation Type drop-down consists of the following options:</p> <ul style="list-style-type: none"> ■ Indoor ■ Outdoor <p>You can either select the Indoor option to change the installation to Indoor mode or select the Outdoor option to change the installation to the Outdoor mode.</p> <p>The options in the Installation Type drop-down are listed based on the Instant AP model.</p> |

| UI | Parameters | Description |
|--------|------------------------|---|
| Mesh | Mesh enable | Enable this option to allow mesh access points to form mesh network. The mesh feature ensures reliability and redundancy by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network. For more information, see the Aruba Mesh Network and Mesh Instant AP section. |
| | Clusterless mesh name | Enter the name of mesh access points that do not belong to any cluster. The Clusterless mesh name field is disabled when the Mesh enable option is enabled. |
| | Clusterless mesh key | Enter the key of the mesh access points that do not belong to any cluster. The Clusterless mesh key field is disabled when the Mesh enable option is enabled. |
| | Retype | Re-enter the clusterless mesh key. The Retype is disabled when the Mesh enable option is enabled. |
| Uplink | Uplink Management VLAN | The uplink traffic on Instant AP is carried out through a management VLAN. However, you can configure a non-native VLAN as an uplink management VLAN. After an Instant AP is provisioned with the uplink management VLAN, all management traffic sent from the Instant AP is tagged to the management VLAN. To configure a non-native uplink VLAN, click Uplink and specify the VLAN in Uplink Management VLAN . |
| | Eth0 Bridging | If you want to convert the Eth0 uplink port to a downlink port, enable Eth0 Bridging . Enable this option to support wired bridging on the Ethernet 0 port of an Instant AP. |
| | USB Port | Enable the USB port if you do not want to use the cellular uplink or 3G/4G modem in your current network setup. |
| | PEAP User | Create the PEAP user credentials for certificate based authentication. Provide the user name and password in the Username and Password field for creating the PEAP user. |

6. Click **Save Settings**.

7. Reboot the Instant AP.

Configuring External Antenna

If your Instant AP has external antenna connectors, you need to configure the transmit power of the system. The configuration must ensure that the system's EIRP is in compliance with the limit specified by the regulatory authority of the country in which the Instant AP is deployed. You can also measure or calculate additional attenuation between the device and antenna before configuring the antenna gain. To know if your Instant AP device supports external antenna connectors, see the *Installation Guide* that is shipped along with the Instant AP device.

EIRP and Antenna Gain

The following formula can be used to calculate the EIRP limit related RF power based on selected antennas (antenna gain) and feeder (Coaxial Cable loss):

$$\text{EIRP} = \text{Tx RF Power (dBm)} + \text{GA (dB)} - \text{FL (dB)}$$


The following table describes this formula:

Table 81: *Formula Variable Definitions*

| Formula Element | Description |
|--------------------|---|
| EIRP | Limit specific for each country of deployment |
| Tx RF Power | RF power measured at RF connector of the unit |
| GA | Antenna gain |
| FL | Feeder loss |

Configuring Antenna Gain

To configure antenna gain for Instant APs with external connectors, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Access Points**. The **Access Points** page is displayed.
5. Click the edit icon corresponding to an AP.
6. Under **Basic Info**, select the access point to configure and then click **Edit**.
7. Select **Radio** and select **External Antenna** to configure the antenna gain value. This option is available only if the selected AP supports external antennas.
8. Enter the antenna gain values in dBm for the 2.4 GHz and 5 GHz bands.
9. Click **Save Settings**.


Adding an Instant AP

To add an Instant AP to Aruba Central, assign an IP address and a subscription.

After an Instant AP is connected to the network and if the **Auto Join Mode** feature is enabled, the Instant AP inherits the configuration from the virtual controller and is listed in the **Access Points** tab.

Deleting an Instant AP from the Network

To delete an Instant AP from the network:

1. In the **Network Operations** app, use the filter bar to select a group.
2. Under **Manage**, click **Devices > Access Points** to view the AP monitoring dashboard.
3. Click the  list icon to display the AP list page.
4. Click **Access Points**.
5. Hover over the mouse on the AP name from the table.
6. Click the delete icon.
7. Click the **Delete** icon.
8. Click **OK** to confirm deletion.

Configuring System Parameters for an AP

To configure system parameters for an AP cluster, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **General** and configure the following parameters:

Table 82: *System parameters*

| Data Pane Item | Description |
|-----------------------------------|--|
| Virtual Controller | <p>This parameter configuration is only applicable for APs that operate in a cluster deployment environment.</p> <p>To configure the virtual controller name and IP address, click edit icon and update the name and IP address. The IP address serves as a static IP address for the multi-AP network. When configured, this IP address is automatically provisioned on a shadow interface on the AP that takes the role of a virtual controller. The AP sends three ARP messages with the static IP address and its MAC address to update the network ARP cache.</p> <p>Name—Name of the virtual controller.</p> <p>IP address—IPv4 address configured for the virtual controller. The IPv4 address uses the 0.0.0.0 notation.</p> <p>IPv6 address—IPv6 address configured for the virtual controller. You can configure IPv6 address for the virtual controller only if the Allow IPv6 Management feature is enabled. IPv6 is the latest version of IP that is suitable for large-scale IP networks. IPv6 supports a 128-bit address to allow 2¹²⁸, or approximately 3.4×10³⁸ addresses while IPv4 supports only 2³² addresses.</p> <p>The IP address of the IPv6 host is always represented as eight groups of four hexadecimal digits separated by colons. For example <code>2001:0db8:0a0b:12f0:0000:0000:0000:0001</code>. However, the IPv6 notation can be abbreviated to compress one or more groups of zeroes or to compress leading or trailing zeroes; for example <code>2001:db8:a0b:12f0::0:0:1</code>.</p> |
| Set Country code for group | <p>To configure a country code for the AP at the group level, select the country code from the Set Country code for group drop-down list. By default, no country code is configured for the AP device groups.</p> <p>When a country code is configured for the group, it takes precedence over the country code setting configured at the device level.</p> |
| Timezone | <p>To configure a time zone, select a time zone from the Timezone drop-down list.</p> <p>If the selected timezone supports DST, the UI displays the "The selected country observes Daylight Savings Time" message.</p> |
| Preferred Band | <p>Assign a preferred band by selecting an appropriate option from the Preferred Band drop-down list.</p> <p>Reboot the AP after modifying the radio profile for changes to take effect.</p> |
| NTP Server | <p>To facilitate communication between various elements in a network, time synchronization between the elements and across the network is critical. Time synchronization allows you to: Trace and track security gaps, network usage, and troubleshoot network issues. Validate certificates.</p> <p>Map an event on one network element to a corresponding event on another.</p> <p>Maintain accurate time for billing services and similar.</p> <p>NTP helps obtain the precise time from a server and regulate the local time in each network element. Connectivity to a valid NTP server is required to synchronize the AP clock to set the correct time. If NTP server is not configured in the AP network, an AP reboot may lead to variation in time data.</p> |

Table 82: *System parameters*

| Data Pane Item | Description |
|--|--|
| | <p>By default, the AP tries to connect to pool.ntp.org to synchronize time. The NTP server can also be provisioned through the DHCP option 42. If the NTP server is configured, it takes precedence over the DHCP option 42 provisioned value. The NTP server provisioned through the DHCP option 42 is used if no server is configured. The default server pool.ntp.org is used if no NTP server is configured or provisioned through DHCP option 42.</p> <p>To configure an NTP server, enter the IP address or the URL of the NTP server and reboot the AP to apply the configuration changes.</p> |
| Virtual Controller Netmask Virtual Controller Gateway Virtual Controller VLAN | <p>This parameter configuration is only applicable for APs that operate in a cluster deployment environment.</p> <p>The IP configured for the virtual controller can be in the same subnet as AP or can be in a different subnet. Ensure that you configure the virtual controller VLAN, gateway, and subnet mask details only if the virtual controller IP is in a different subnet.</p> <p>Ensure that virtual controller VLAN is not the same as native VLAN of the AP.</p> |
| DHCP Option 82 XML | <p>The Option 82 is not applicable for Cloud APs.</p> <p>Option 82 can be customized to cater to the requirements of any ISP using the master AP. To facilitate customization using a XML definition, multiple parameters for Circuit ID and Remote ID options of DHCP Option 82 are introduced.</p> <p>The XML file is used as the input and is validated against an XSD file in the master AP. The format in the XML file is parsed and stored in the DHCP relay which is used to insert Option 82 related values in the DHCP request packets sent from the client to the server.</p> <p>From the drop-down list, select one of the following XML files:</p> <p>default_dhcpopt82_1.xml default_dhcpopt82_2.xml</p> <p>For information related to the Option 82 drop-down list, see Option 82 on page 388.</p> |
| Dynamic CPU Utilization | <p>APs perform various functions such as wired and wireless client connectivity and traffic flows, wireless security, network management, and location tracking. If an AP is overloaded, prioritize the platform resources across different functions. Typically, the APs manage resources automatically in real time. However, under special circumstances, if dynamic resource management needs to be enforced or disabled altogether, the dynamic CPU management feature settings can be modified.</p> <p>To configure dynamic CPU management, select any of the following options from Dynamic CPU Utilization.</p> <p>Automatic—When selected, the CPU management is enabled or disabled automatically during run-time. This decision is based on real time load calculations taking into account all different functions that the CPU needs to perform. This is the default and recommended option.</p> <p>Always Disabled in all APs—When selected, this setting disables CPU management on all APs, typically for small networks. This setting protects user experience.</p> <p>Always Enabled in all APs—When selected, the client and network management functions are protected. This setting helps in large networks with high client density.</p> |
| Auto Join Mode | <p>When enabled, APs can automatically discover the virtual controller and join the network. The Auto Join Mode feature is enabled by default.</p> |
| APs allowed for Auto-Join Mode | <p>When Auto Join is enabled, the APs are automatically discovered and are allowed to join the cluster.</p> <p>When the Auto Join feature is disabled on the AP, the list of allowed APs on Aruba Central may not be synchronized or up-to-date. In such cases, you can manually add a list of APs that can join the AP cluster in the Aruba Central UI.</p> <p>To manually add the list of allowed AP devices, complete the following steps:</p> <p>From the group selector, select the desired AP.</p> <p>Under System, click the Manage APs link next to APs allowed for Auto-Join Mode field.</p> <p>Add the MAC address of AP that you want to allow.</p> |

Table 82: *System parameters*

| Data Pane Item | Description |
|----------------------------------|--|
| | Click Save Settings . |
| Allow IPv6 Management | Enables IPv6 address configuration for the virtual controller. You can configure an IPv6 address for a virtual controller IP only when Allow IPv6 Management feature is enabled. |
| Uplink switch native VLAN | Allows you to specify a VLAN ID, to prevent the AP from sending tagged frames for clients connected on the SSID that uses the same VLAN as the native VLAN of the switch. By default, the AP considers the native VLAN of the upstream switch, to which it is connected, as the VLAN ID 1. |
| Terminal Access | When enabled, the users can access the AP CLI through SSH. |
| Console Access | When enabled, the users can access AP through the console port. |
| WebUI Access | If an AP is connected to Aruba Central, you can use this option to disable AP Web UI access and any communication via HTTPS or SSH. If you enable this option, you can manage the AP only from Aruba Central. |
| Telnet Server | When enabled, the users can start a Telnet session with the AP CLI. |
| LED Display | Enables or disables the LED display for all APs in a cluster. The LED display is always enabled during the AP reboot. |
| Extended SSID | Extended SSID is enabled by default in the factory default settings of APs. This disables mesh in the factory default settings. For AP devices that support Aruba Instant 8.4.0.0 firmware versions and above, you can configure up to 14 SSIDs. By enabling Extended SSID, you can create up to 16 networks. |
| Deny Inter-user Bridging | If you have security and traffic management policies defined in upstream devices, you can disable bridging traffic between two clients connected to the same AP on the same VLAN. When inter-user bridging is denied, the clients can connect to the Internet but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. To disable inter-user bridging, move the slider to the right. |
| Deny Local Routing | If you have security and traffic management policies defined in upstream devices, you can disable routing traffic between two clients connected to the same AP on different VLANs. When local routing is disabled, the clients can connect to the Internet but cannot communicate with each other, and the routing traffic between the clients is sent to the upstream device to make the forwarding decision. To disable local routing, move the slider to the right. |
| Dynamic RADIUS Proxy | If your network has separate RADIUS authentication servers (local and centralized servers) for user authentication, you may want to enable Dynamic RADIUS proxy to route traffic to a specific RADIUS server. When Dynamic RADIUS proxy is enabled, the IP address of the virtual controller is used for communication with external RADIUS servers. To enable Dynamic RADIUS Proxy , you must configure an IP address for the Virtual Controller and set it as a NAS client in the RADIUS server profile. |
| Dynamic TACACS Proxy | If you want to route traffic to different TACACS servers, enable Dynamic TACACS Proxy . When enabled, the AP cluster uses the IP address of the Virtual Controller for communication with external TACACS servers. If an IP address is not configured for the Virtual Controller, the IP address of the bridge interface is used for communication between the AP and TACACS servers. However, if a VPN tunnel exists between the Instant AP and TACACS server, the IP address of the tunnel interface is used. |

Table 82: System parameters


| Data Pane Item | Description |
|---|---|
| Cluster Security | <p>This parameter is required to be set only for APs that operate in a cluster deployment environment.</p> <p>Enables or disables the cluster security feature. When enabled, the control plane communication between the AP cluster nodes is secured. The Disallow Non-DTLS Slaves toggle appears. Enable this toggle to allow slave APs to join a DTLS enabled cluster. For secure communication between the cluster nodes, the Internet connection must be available, or at least a local NTP server must be configured.</p> <p>After enabling or disabling cluster security, ensure that the configuration is synchronized across all devices in the cluster, and then reboot the cluster.</p> <p>The Disallow Non-DTLS Slaves toggle is only supported in AP devices supporting Aruba Instant 8.4.0.0 firmware versions and above.</p> |
| Low Assurance PKI | <p>Enable this option to allow low assurance devices that use non-TPM chip, in the network. To enable the cluster security feature, set the Low Assurance PKI toggle to Enable. For more information on <i>Low Assurance PKI</i>, refer to <i>Cluster Security</i> section in <i>Aruba Instant User Guide</i>. The Low Assurance PKI toggle is supported in AP devices running Aruba Instant 6.5.3.0 firmware versions and later..</p> |
| Mobility Access Switch Integration | <p>Enables LLDP protocol for Mobility Access Switch integration. With this protocol, APs can instruct the Switch to turn off ports where rogue access points are connected, as well as take actions such as increasing PoE priority and automatically configuring VLANs on ports where APs are connected.</p> |
| URL Visibility | <p>Enables URL data logging for client HTTP and HTTPS sessions and allows APs to extract URL information and periodically log them on ALE for DPI and application analytics.</p> |

7. Click **Save Settings**.

Configuring VLAN Name and VLAN ID

Aruba Central allows you to map VLAN name to a VLAN ID for the ease of identifying the existing VLANs.

To map a VLAN Name to a VLAN ID, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group are displayed.
6. Click the **Named VLAN Mapping** section.
7. Click the + icon in the **Named VLAN Mapping** section. The **VLAN Name to VLAN ID Mapping** page is displayed.
8. Enter the VLAN Name and VLAN ID that is required to be mapped.
9. Click **OK**. The **VLAN Name to VLAN ID Mapping** table in the **Named VLAN Mapping** section lists all the mapped VLAN.

You can find the Named VLAN Mapping feature applied in the following fields of corresponding UI pages of Aruba Central:

- The **VLANID** field in the **VLAN** tab when **Custom** for Instant AP Assigned and **Static** for External DHCP server assigned is selected during WLAN SSID creation. For more information, see [Configuring Wireless Network Profiles on Instant APs](#).

- The **VLANID** field in the **Ports > Add SSID > VLAN** tab when **Custom** for **Instant AP Assigned** and **Static** for **External DHCP server assigned** is selected during wired port profile creation.
- The **Access Rule** page of the **Ports > Access** tab and the **WLANS > Access** tab when you add rules for selected roles. Select **VLAN Assignment** as the rule type in the **Access Rule** page to find the mapped VLAN name in the **VLAN ID** field.



You can also map VLAN ID to a VLAN name when you customize the **Client VLAN Assignment** configuration in **VLANs** tab during network profile creation. For more information, see [VLAN Assignment](#).

Points to remember

- The maximum number of Named VLAN ID mappings allowed in Aruba Central is **32**.
- VLAN mapping cannot be performed if the VLAN name does not exist.
- The VLAN mapping record is deleted from the **VLAN Name to VLAN ID Mapping** table when the VLAN name is deleted.
- You can only map a single VLAN id to a VLAN name.
- The VLAN name field is not case-sensitive.

Configuring Dual 5 GHz Radio Bands on an Instant AP

Aruba Central provides an option to retrieve the radio numbers of Instant AP through the APIs. It also provides an option to filter AP details using radio numbers in the Monitoring dashboard.



For regular Instant APs with non-dual band, Central automatically assigns radio 1 to 2.4 GHz band and radio 0 to 5 GHz band respectively.

To get the radio numbers through API:

1. In the Account Home page, click **API Gateway**.
2. Click **APIs** tab.
3. Click the link displayed in the **APIs** tab of the **API Gateway**. The **Central Network Management APIs** page is displayed.
4. On the left navigation pane, select **Monitoring** from the **URL** drop-down list.
5. Click **API Reference > AP**. The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 83: APIs to Get Radio Number in APs

| API | Description |
|--|---|
| [GET]/monitoring/v1/aps/{serial}/neighbouring_clients | Allows you to filter data of neighbouring clients for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the data of neighbouring clients for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the data of neighbouring clients for a specific radio number. |
| [GET]/monitoring/v1/aps/rf_summary | Retrieves information on RF summary such as channel utilization and noise floor in positive, errors, drops for a given time period. This API can also be used to filter RF health statistics for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the RF health statistics for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the RF health statistics for a specific radio number. |
| [GET]/monitoring/v1/aps/bandwidth_usage | This API can also be used to filter out bandwidth usage data for a specific radio number in a given time period. When there is no radio number entered in the radio_number field, the API filters the bandwidth usage for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the bandwidth usage for a specific radio number. |

6. On the left navigation pane, click **API Reference > Client**.

7. The following APIs allow you to retrieve the radio number for the total number of clients connected:

Table 84: APIs to Get Radio Number in Connected Clients

| API | Description |
|--|--|
| [GET]/monitoring/v1/clients/count | This API is used to filter out the data for connected clients for a specific radio number of AP in a given time period. When there is no radio number entered in the radio_number field, the API filters the clients count for both radio 0 and radio 1. It is mandatory to provide the serial number of the AP to get the total count of clients for a specific radio number. |

For further details on API help, refer to <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Configuring Network Profiles on Instant APs

This section describes the following procedures:

- [Configuring Wireless Network Profiles on Instant APs on page 300](#)
- [Configuring Wireless Networks on Guest Users on Instant APs on page 313](#)
- [Configuring Wired Port Profiles on Instant APs on page 328](#)
- [Editing a WLAN Profile on page 332](#)
- [Deleting a Network Profile on page 333](#)

Configuring Wireless Network Profiles on Instant APs

You can configure up to 14 SSIDs. By enabling **Extended SSID** in the **System > General** tab, you can create up to **16** networks.



If more than 16 SSIDs are assigned to a zone and the extended zone option is disabled, an error message is displayed.

Creating a Wireless Network Profile

To configure WLAN settings, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS** tab, to create a new SSID profile, click **+ Add SSID**. The **Create a New Network** pane is displayed.
5. In **General** tab, enter a name that is used to identify the network in the **Name (SSID)** text box.
6. Under **Advanced Settings**, configure the parameters as mentioned in the [Advanced WLAN Configuration Parameters](#) table.

Table 85: *Advanced WLAN Configuration Parameters*

| Parameter | Description |
|--|--|
| Broadcast/Multicast | |
| Broadcast Filtering | Select any of the following values: <ul style="list-style-type: none">■ All—The Instant AP drops all broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols.■ ARP—The Instant AP drops broadcast and multicast frames except DHCP and ARP, IGMP group queries, and IPv6 neighbor discovery protocols. Additionally, it converts ARP requests to unicast and sends frames directly to the associated clients. By default, the Instant AP is configured to ARP mode.■ Unicast ARP Only—This option enables Instant AP to convert ARP requests to unicast frames thereby sending them to the associated clients.■ Disabled—The Instant AP forwards all the broadcast and multicast traffic is forwarded to the wireless interfaces. |
| DTIM Interval | The DTIM Interval indicates the DTIM period in beacons, which can be configured for every WLAN SSID profile. The DTIM interval determines how often the Instant AP delivers the buffered broadcast and multicast frames to the associated clients in the power save mode. Range is 1 to 10 beacons. The default value is 1, which means the client checks for buffered data on the Instant AP at every beacon. You can also configure a higher DTIM value for power saving. |
| Multicast Transmission Optimization | Select the check box if you want the Instant AP to select the optimal rate for sending broadcast and multicast frames based on the lowest of unicast rates across all associated clients. When this option is enabled, multicast traffic can be sent up to a rate of 24 Mbps. The default rate for sending frames for 2.4 GHz is 1 Mbps and that for 5 GHz is 6 Mbps. This option is disabled by default. |
| Dynamic Multicast Optimization | Select the check box to allow Instant AP to convert multicast streams into unicast streams over the wireless link. Enabling DMO enhances the quality and reliability of streaming video, while preserving the bandwidth available to the non-video clients. NOTE: When you enable DMO on multicast SSID profiles, ensure that the DMO feature is enabled on all SSIDs configured in the same VLAN. |

| Parameter | Description |
|---|---|
| Dynamic Multicast Optimization Channel Utilization Threshold | Specify a value to set a threshold for DMO channel utilization. With DMO, the Instant AP converts multicast streams into unicast streams as long as the channel utilization does not exceed this threshold. The default value is 90% and the maximum threshold value is 100%. When the threshold is reached or exceeds the maximum value, the Instant AP sends multicast traffic over the wireless link. NOTE: This option will be enabled only when Dynamic Multicast Optimization is enabled. |
| Transmit Rates (Legacy Only) | |
| 2.4 GHz | If the 2.4 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 1 Mbps and maximum transmission rate is 54 Mbps. |
| 5 GHz | If the 5 GHz band is configured on the Instant AP, specify the minimum and maximum transmission rates. The default value for minimum transmission rate is 6 Mbps and maximum transmission rate is 54 Mbps. |
| Zone | |
| Zone | Specify the zone for the SSID. If a zone is configured in the SSID, only the Instant AP in that zone broadcasts this SSID. If there are no Instant APs in the zone, SSID is broadcast. If the Instant AP cluster has devices running Aruba Instant firmware versions 6.5.4.7 or later, and 8.3.0.0 or later, you can configure multiple AP zones by adding zone names as comma separated values. NOTE: Aruba recommends that you do not configure zones in both SSID and in the device specific settings of an Instant AP. If the same zones are configured in SSID and Per AP settings, APs may broadcast the SSIDs, but if the SSIDs and Per AP settings have different zones configured, it may lead to a configuration error. For more information on AP zones, see <i>Aruba Instant User Guide</i> . |
| Bandwidth Control | |
| Airtime | Select this to specify an aggregate amount of airtime that all clients in this network can use for sending and receiving data. Specify the airtime percentage. |
| Each Radio | Select this to specify an aggregate amount of throughput that each radio is allowed to provide for the connected clients. The value ranges from 1 through 65535. |
| Downstream | Enter the downstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per User check box. NOTE: The bandwidth limit set in this method is implemented at the device level and not cluster level. |
| Upstream | Enter the upstream rates within a range of 1 to 65,535 Kbps for the SSID users. If the assignment is specific for each user, select the Per user check box. NOTE: The bandwidth limit set in this method is implemented at the device level and not cluster level. |
| Enable 11n | When this option is selected, there is no disabling of High-Throughput (HT) on 802.11n devices for the 5 GHz radio band. If HT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, HT is enabled on all SSIDs. NOTE: If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check box to disable VHT on these devices. |
| Enable 11ac | When this option is selected, VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. |

| Parameter | Description |
|--|---|
| | NOTE: If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check box to disable VHT on these devices. |
| Enable 11ax | When this option is selected, VHT is enabled on the 802.11ax devices. If VHT is enabled for a radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. |
| WiFi Multimedia | |
| Background Wifi Multimedia Share | Allocates bandwidth for background traffic such as file downloads or print jobs. Specify the appropriate DSCP mapping values within a range of 0–63 for the background traffic in the corresponding DSCP mapping text box. Enter up to 8 values with no white space and no duplicate single DHCP mapping value. |
| Best Effort Wifi Multimedia Share | Allocates bandwidth or best effort traffic such as traffic from legacy devices or traffic from applications or devices that do not support QoS. Specify the appropriate DSCP mapping values within a range of 0–63 for the best effort traffic in the corresponding DSCP mapping text box. |
| Video Wifi Multimedia Share | Allocates bandwidth for video traffic generated from video streaming. Specify the appropriate DSCP mapping values within a range of 0–63 for the video traffic in the corresponding DSCP mapping text box. |
| Voice Wifi Multimedia Share | Allocates bandwidth for voice traffic generated from the incoming and outgoing voice communication. Specify the appropriate DSCP mapping values within a range of 0–63 for the voice traffic in the corresponding DSCP mapping text box. NOTE: In a non-WMM or hybrid environment, where some clients are not WMM-capable, you can allocate higher values for Best Effort Wifi Multimedia share and Voice Wifi Multimedia Share to allocate a higher bandwidth to clients transmitting best effort and voice traffic. |
| Traffic Specification (TSPEC) | Select this check box to set if you want the TSPEC for the wireless network. The term TSPEC is used in wireless networks supporting the IEEE 802.11e Quality of Service standard. It defines a series of parameters, characteristics and Quality of Service expectations of a traffic flow. |
| TSPEC Bandwidth | Enter the bandwidth for the TSPEC. |
| Spectralink Voice Protocol (SVP) | Select this check box to opt for SVP protocol. |
| WiFi Multimedia Power Save (U-APSD) | Select this check box to enable WiFi Multimedia Power Save (U-APSD). The U-APSD is a power saving mechanism that is an optional part of the IEEE amendment 802.11e, QoS. |
| Miscellaneous | |
| Band | Select a value to specify the band at which the network transmits radio signals in the Band drop-down list. You can set the band to 2.4 GHz , 5 GHz , or All . The All option is selected by default. |
| Content Filtering | Select this check box to route all DNS requests for the non-corporate domains to OpenDNS on this network. |
| Primary Usage | Based on the type of network profile, select one of the following options: <ul style="list-style-type: none"> ■ Mixed Traffic—Select this option to create an employee or guest network profile. The employee network is used by the employees in an organization and it supports passphrase-based or 802.1X-based authentication methods. Employees can access the |

| Parameter | Description |
|--------------------------------------|--|
| | <p>protected data of an enterprise through the employee network after successful authentication. The guest network is created for guests, visitors, contractors, and any non-employee users who use the enterprise Wi-Fi network. The VC assigns the IP address for the guest clients. Captive portal or passphrase-based authentication methods can be set for this wireless network. Typically, a guest network is an unencrypted network. However, you can specify the encryption settings when configuring a guest network.</p> <ul style="list-style-type: none"> ■ Voice Only—Select this option to configure a network profile for devices that provide only voice services such as handsets or applications that require voice traffic prioritization. <p>NOTE: When a client is associated with the voice network, all data traffic is marked and placed into the high priority queue in QoS.</p> |
| Inactivity Timeout | Specify an interval for session timeout. If a client session is inactive for the specified duration, the session expires and the users are required to log in again. You can specify a value within the range of 60–3600 seconds. The default value is 1000 seconds. |
| Deauth Inactive Clients | Select this option to allow the Instant AP to send a de-authentication frame to the inactive client and the clear client entry. |
| Hide SSID | Select this check box if you do not want the SSID to be visible to users. |
| Disable Network | Select this check box if you want to disable the SSID. When selected, the SSID is disabled, but is not removed from the network. By default, all SSIDs are enabled. |
| Can Be Used Without Uplink | Select this check box if you do not want the SSID profile to use the uplink. |
| Max Clients Threshold | Specify the maximum number of clients that can be configured for each BSSID on a WLAN. You can specify a value within the range of 0– 255. The default value is 64. |
| ESSID | Specify the identifier that serves as an identification and address for the device to connect to a wireless router which can then access the internet. If the ESSID value defined is not the same as the profile name, the SSID can be searched based on the ESSID value and not by its profile name. |
| Out of service (OOS) | <p>Configures the SSID state when a connection link of the AP is down. To configure out of service for an SSID, the link condition of the AP and the SSID state must be configured. The SSID can be enabled or disabled automatically when the following conditions are met:</p> <ul style="list-style-type: none"> ■ VPN down - Connection to the VPN network is down. ■ Uplink down - The uplink connection of the AP is down. ■ Internet down - The connection to the Internet is down. ■ Primary uplink down - The primary uplink connection of the AP is down. <p>The SSID status changes according to the configuration when the link condition is met. For example, when Internet down, Disabled is set for Out of Service, the SSID is disabled when the Internet connection is down and is changed back to enabled when the Internet connection is restored.</p> <p>NOTE: When Internet Down condition is set in the SSID, the AP checks for uplink by pinging the IP defined in the Failover Internet IP. To configure the Failover Internet IP, see Switching Uplinks based on the Internet Availability.</p> |
| OOS time (global) | Configure a hold time interval in seconds within a range of 30–300 seconds, after which the out-of-service operation is triggered. For example, if the VPN is down and the configured hold time is 45 seconds, the effect of this out-of-service state impacts the SSID availability after 45 seconds. |
| Local Probe Request Threshold | Specify a threshold value to limit the number of incoming probe requests. When a client sends a broadcast probe request frame to search for all available SSIDs, this option controls system response for this network profile and ignores probe requests if required. You can specify a RSSI value within range of 0–100 dB. |

| Parameter | Description |
|------------------------------------|---|
| Min RSSI for auth request | Enter the minimum RSSI threshold for authentication requests. |
| Deny Inter User Bridging | Disables bridging traffic between two clients connected to the same SSID on the same VLAN. When this option is enabled, the clients can connect to the Internet, but cannot communicate with each other, and the bridging traffic between the clients is sent to the upstream device to make the forwarding decision. |
| Deny Intra VLAN Traffic | Disables intra VLAN traffic to enable the client isolation and disable all peer-to-peer communication. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP. This feature enhances the security of the network and protects it from vulnerabilities. For more information, see Client Isolation . |
| Management Frame Protection | Set this option to Enable to provide high network security by maintaining data confidentiality of management frames. The Management Frame Protection (MFP) establishes encryption keys between the client and Instant AP using 802.11i framework. For more information, see Management Frames Protection . |
| Time Range Profiles | |
| Time Range Profiles | Click + New Time Range Profile to create a new time range profile. For more information, see Configuring Time-Based Services for Wireless Network Profiles on page 336 . |

Configuring VLAN Settings for Wireless Network

To configure VLAN settings for an SSID, complete the following steps:

1. In the **VLAN** tab, select any of the following options for **Client IP Assignment**:
 - **Instant AP assigned**—When selected, the client obtains the IP address from the VC.
 - **External DHCP server assigned**—When selected, the client obtains the IP address from the network.
2. Based on the type of client IP assignment mode selected, you can configure the VLAN assignment for clients as described in the following table:

Table 86: VLAN Assignment

| Parameter | Description |
|--------------------------------------|---|
| Instant AP assigned | <p>On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on Instant APs on page 384.</p> <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none"> ■ Internal VLAN—By default, the client VLAN is assigned to the native VLAN on the network. The DHCP server automatically assigns the IP address from VLAN 3333 to the client. ■ Custom—Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, enter the scope of VLAN that is allowed in the VLAN ID text box. Click the Show Named VLANs section to view all the named VLANs mapped to VLAN ID. Click the + Add Named VLAN icon and enter the VLAN Name and VLAN ID that is required to be mapped. Clicking OK populates the named VLAN in the VLAN Name to VLAN ID Mapping table. <p>NOTE: You can also map VLAN ID to VLAN Names in the System tab of AP configuration page. For more information, see Configuring VLAN Name and VLAN ID.</p> |
| External DHCP server assigned | <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none"> ■ Static —Allows you to specify a VLAN id of single VLAN, or a comma separated list of VLANs, or a range of VLANs for all clients on this network, in the VLAN ID text box. You can also select the VLAN name that is mapped to the VLAN id from the scroll-down list provided next to the VLAN ID text box. If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. ■ Dynamic—Assigns the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules by clicking the + sign. The New VLAN Assignment Rule page is displayed to enter details such as attribute, operator, string and VLAN ID. For more information, see Configuring VLAN Assignment Rule. ■ Native Vlan—Assigns the client VLAN to the native VLAN. |

3. Click **Next** to configure security settings.

Configuring Security Settings for Wireless Network

To configure security settings for mixed traffic or voice network, complete the following steps:

1. In the **Security** tab, specify any one of the following options in the **Security Level**:
 - **Enterprise**—On selecting the security level, the authentication options applicable to the network are displayed.
 - **Personal**—On selecting **Personal** security level, the authentication options applicable to the personalized network are displayed.
 - **Captive Portal**—On selecting **Captive Portal** security level, the authentication options applicable to the captive portal is displayed. For more information on captive portal, see [Configuring Access Points Ports Networks on Guest Users on Instant APs](#).
 - **Open**—On selecting **Open** security level, the authentication options applicable to an open network are displayed.



The default security setting for a network profile is **Personal**.

2. Based on the security level specified, configure the following basic parameters:

Table 87: Basic WLAN security settings

| Data Pane Item | Description |
|----------------|---|
| Key Management | <p>For Enterprise security level, select any of the following options from Key Management:</p> <p>WPA-2 Enterprise—Select this option to use WPA-2 security. The WPA-2 Enterprise requires user authentication and requires the use of a Radius server for authentication.</p> <p>Both (WPA-2 & WPA)—Select this option to use both WPA-2 and WPA security.</p> <p>WPA Enterprise—Select this option to use both WPA Enterprise.</p> <p>Dynamic WEP with 802.1X—If you do not want to use a session key from the RADIUS Server to derive pairwise unicast keys, set Session Key for LEAP to Enabled. This is required for old printers that use dynamic WEP through LEAP authentication. The Session Key for LEAP feature is Disabled by default.</p> <p>WPA-3 Enterprise(GCM 256)—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text.</p> <p>WPA-3 Enterprise(CCM 128)—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text.</p> <p>When WPA-2 Enterprise and Both (WPA2-WPA) encryption types are selected and if 802.1x authentication method is configured, OKC is enabled by default. If OKC is enabled, a cached PMK is used when the client roams to a new AP. This allows faster roaming of clients without the need for a complete 802.1x authentication. OKC roaming can be configured only for the Enterprise security level.</p> |
| | <p>For Personal security level, select an encryption key from Key Management. For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 Personal keys, specify the following parameters:</p> <p>Passphrase Format: Select a passphrase format. The options available are 8-63 alphanumeric characters and 64 hexadecimal characters.</p> <p>Enter a passphrase in Passphrase and reconfirm.</p> <p>For Static WEP, specify the following parameters:</p> <p>Select an appropriate value for WEP key size from the WEP Key Size. You can specify 64-bit or 128-bit.</p> <p>Select an appropriate value for Tx key from Tx Key.</p> <p>Enter an appropriate WEP Key and reconfirm.</p> <p>For MPSK-AES, configure the authentication server.</p> |
| | <p>For Captive Portal security level, select an encryption key from Key Management. For WPA-2 Personal, WPA Personal, Both (WPA-2&WPA), and WPA-3 keys, specify the following parameters:</p> <p>Passphrase Format: Select a passphrase format. The options are available are 8-63 alphanumeric characters and 64 hexadecimal characters.</p> <ul style="list-style-type: none"> ■ Enter a passphrase in Passphrase and reconfirm. <p>For Static WEP, specify the following parameters:</p> <ul style="list-style-type: none"> ■ Select an appropriate value for WEP key size from the WEP Key Size. You can specify 64-bit or 128-bit. ■ Select an appropriate value for Tx key from Tx Key. ■ Enter an appropriate WEP Key and reconfirm. <p>For information on configuring captive portal, see Configuring Wireless Networks on Guest Users on Instant APs on page 313.</p> |
| | <p>For Open security level, the Key Management includes Open, and Enhanced Open options.</p> |

| Data Pane Item | Description |
|------------------------------|---|
| EAP Offload | <p>This option is applicable to Enterprise security levels only. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, set EAP Offload to Enabled. Enabling EAP Offload can reduce network traffic to the external RADIUS server by terminating the authorization protocol on the Instant AP. By default, for 802.1X authorization, the client conducts an EAP exchange with the RADIUS server, and the Instant AP acts as a relay for this exchange. When EAP Offload is enabled, the Instant AP by itself acts as an authentication server and terminates the outer layers of the EAP protocol, only relaying the innermost layer to the external RADIUS server. It can also reduce the number of exchange packets between the Instant AP and the authentication server.</p> <p>Instant supports the configuration of primary and backup authentication servers in an EAP termination-enabled SSID.</p> <p>If you are using LDAP for authentication, ensure that Instant AP termination is configured to support EAP.</p> |
| Authentication Server | <p>Configure the following parameters:</p> <p>MAC Authentication—Set the MAC Authentication option to Enabled to enable MAC address based authentication for Personal, Captive Portal, and Open security levels.</p> <p>Primary Server—Set a primary authentication server. The Primary Server option appears only for Enterprise security level, internal and external captive portal types. Select one of the following options from the drop-down list:</p> <p>Internal Server—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users. To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs on page 356.</p> <p>Aruba Central allows you to configure an external RADIUS server, TACACS or LDAP server, and External Captive Portal for user authentication.</p> <p>Secondary Server—To add another server for authentication, configure another authentication server.</p> <p>Authentication Survivability—If an external server is configured for authentication, you can enable authentication survivability. Specify a value in hours for Cache Timeout to set the duration after which the authenticated credentials in the cache expires. When the cache expires, the clients are required to authenticate again. You can specify a value within range of 1 to 99 hours. By default, authentication survivability is disabled.</p> <p>Load Balancing—Set this to Enabled if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Dynamic Load Balancing between Authentication Servers on page 356.</p> |
| Users | <p>Click Users to add the users. The registered users of Employee type will be able to access the users of Enterprise network. To add a new user, click + Add User and enter the new user in the Add User page. The Primary Server option appears only for Enterprise security level, internal and external captive portal types.</p> |

3. Based on the security level specified, specify the following parameters in the **Advanced Settings** section:

Table 88: Advanced WLAN security settings

| Data pane item | Description |
|---|---|
| Use Session Key for LEAP | Select this option to use the session key for Lightweight Extensible Authentication Protocol. This option is available only for Enterprise level. |
| Opportunistic Key Caching (OKC) | Select the Opportunistic key caching (OKC) options that helps reduce the time needed for authentication. When OKC is used, multiple APs can share Pairwise Master Keys (PMKs) among themselves, and the station can roam to a new access points that has not visited before and reuse a PMK that was established with the current AP. OKC allows the station to roam quickly to an access point it has never authenticated to, without having to perform pre-authentication. OKC is available specifically on WPA2 SSIDs only. |
| MAC Authentication for Enterprise Networks | <p>To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled. For Enterprise security level, the following options are available:</p> <ul style="list-style-type: none"> ■ Perform MAC Authentication Before 802.1X — Select this to use 802.1X authentication only when the MAC authentication is successful. ■ MAC Authentication Fail-Thru — On selecting this, the 802.1X authentication is attempted when the MAC authentication fails. <p>If MAC authentication is enabled, configure the following parameters:</p> <ul style="list-style-type: none"> ■ Delimiter Character—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled. ■ Uppercase Support—Set to Enabled to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled. |
| Reauth Interval | <p>Specify a value for Reauth Interval. When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients.</p> <p>If the re-authentication interval is configured:</p> <ul style="list-style-type: none"> ■ On an SSID performing L2 authentication (MAC or 802.1X authentication): When re-authentication fails, the clients are disconnected. If the SSID is performing only MAC authentication and has a pre-authentication role assigned to the client, the client will get a post-authentication role only after a successful re-authentication. If re-authentication fails, the client retains the pre-authentication role. ■ On an SSID performing both L2 and L3 authentication (MAC with captive portal authentication): When re-authentication succeeds, the client retains the role that is already assigned. If re-authentication fails, a pre-authentication role is assigned to the client. ■ On an SSID performing only L3 authentication (captive portal authentication): When re-authentication succeeds, a pre-authentication role is assigned to the client that is in a post-authentication role. Due to this, the clients are required to go through captive portal to regain access. |
| Blacklisting | By default, this option is disabled. To enable blacklisting of the clients with a specific number of authentication failures, select Blacklisting and specify a value for Max Authentication Failures . The users who fail to authenticate the number of times specified in Max Authentication Failures field are dynamically blacklisted. By default, the Blacklisting option is disabled. |
| Enforce DHCP | <p>Enforces WLAN SSID on Instant AP clients. When DHCP is enforced:</p> <ul style="list-style-type: none"> ■ A layer-2 user entry is created when a client associates with an Instant AP. ■ The client DHCP state and IP address are tracked. ■ When the client obtains an IP address from DHCP, the DHCP state changes to complete. ■ If the DHCP state is complete, a layer-3 user entry is created. ■ When a client roams between the Instant APs, the DHCP state and the client IP address is synchronized with the new Instant AP. |

| Data pane item | Description |
|-----------------------------------|--|
| WPA3 Transition | Enable this option to allow transition from WPA3 to WPA2 and vice versa. The WPA3 Transition appears only when WPA3 is selected in the Key Management for Personal , Captive Portal , and Open level. |
| Legacy Support | Enable this option to allow backward compatibility of encryption modes in networks. The Legacy Support appears only when WPA3 is selected in the Key Management for Personal , Captive Portal , and Open level. |
| Accounting | <p>To enable accounting, select the Accounting option. On enabling this option, the APs post accounting information to the RADIUS server at the specified Accounting Interval. Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Disabled—To disable the accounting option. ■ Use authentication server—To select authentication servers and the accounting time interval in minutes. ■ Use separate servers—To select specific accounting and mention the accounting interval time in minutes. |
| Use IP for Calling Station | <p>Enable this option to configure client IP address as calling station ID. When this option is enabled, the following options are displayed:</p> <ul style="list-style-type: none"> ■ Called Station ID Type—Select any of the following options for configuring called station ID: <ul style="list-style-type: none"> ● Access Point Group—Uses the VC ID as the called station ID. ● Access Point Name—Uses the host name of the Instant AP as the called station ID. ● VLAN ID—Uses the VLAN ID of as the called station ID. ● IP Address—Uses the IP address of the Instant AP as the called station ID. ● MAC address—Uses the MAC address of the Instant AP as the called station ID. ■ Called Station Include SSID—Appends the SSID name to the called station ID. <p>NOTE: The Called Station ID Type detail can be configured even if the Use IP for Calling Station ID is set to Disable.</p> <ul style="list-style-type: none"> ■ Called Station ID Delimiter—Sets delimiter at the end of the called station ID. ■ Max Authentication Failures—Sets a value for the maximum allowed authentication failures. |

| Data pane item | Description |
|----------------------------|--|
| Delimiter Character | Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled. |
| Uppercase Support | Select this option to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled. |
| Fast Roaming | <p>Enable the following fast roaming features as per your requirement:</p> <ul style="list-style-type: none"> ■ 802.11r—Select 802.11r option to enable 802.11r roaming. Selecting this enables fast BSS transition. The fast BSS transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. The 802.11r option is not available for Enterprise level. Once you enable the 802.11r, the following text box is displayed: <ul style="list-style-type: none"> ● MDID— In the MDID text box, enter the mobility domain identifier to configure a mobility domain identifier. In a network of standalone Instant APs within the same management VLAN, 802.11r roaming does not work. This is because the mobility domain identifiers do not match across Instant APs. They are auto-generated based on a virtual controller key. You can set a mobility domain identifier for 802.11r SSIDs. For standalone Instant APs in the same management VLAN, 802.11r roaming works only when the mobility domain identifier is configured with the same value. ■ 802.11k—Select 802.11k to enable 802.11k roaming. The 802.11k protocol enables Instant APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Instant APs and clients send neighbor reports, beacon reports, and link measurement reports to each other. ■ 802.11v— Select 802.11v to enable 802.11v based BSS transition. The 802.11v standard defines mechanisms for wireless network management enhancements and BSS transition management. It allows the client devices to exchange information about the network topology and RF environment. The BSS transition management mechanism enables an AP to request a voice client to transition to a specific AP, or suggest a set of preferred APs to a voice client, due to network load balancing or BSS termination. It also helps the voice client identify the best AP to transition to as they roam. |

4. Click **Next** to configure access rules.

Configuring ACLs for User Access to a Wireless Network

You can configure up to 64 access rules for a wireless network profile. To configure access rules for a network, complete the following steps:

1. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The CPPM Settings table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed. For more information on Downloadable User Roles feature, see [Configuring Network Port Profile AssignmentDownloadable User Roles](#).

The **Downloadable User Role** feature is optional.



The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

2. Click the action corresponding to the server. The **Edit Server** page is displayed.

Viewing Wireless SSIDs Summary Table

The **Network Summary** page now displays all the settings configured in the **General, Security, VLANs,** and **Access** tabs. Click **Finish** to complete the network profile creation and save the settings.


Management Frames Protection

Aruba Central supports the Management Frame Protection (MFP) feature in networks that include Aruba Instant APs 8.5.0.0 firmware version and later. This feature protects networks against forged management frames spoofed from other devices that might otherwise disrupt a valid user session.

The MFP increases the security by providing data confidentiality of management frames. MFP uses 802.11i framework that establishes encryption keys between the client and Instant AP.

Enabling Management Frames Protection Feature for Wireless Networks in Aruba Central

To enable the MFP feature, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS** page, click + **Add SSID**. The **Create a New Network** pane is displayed.
5. In the **General** tab, click **Advanced Settings**,
6. Expand **Miscellaneous**.
7. Set the **Management Frames Protection** toggle to **Enable**.
8. Click **Next** to go to the VLANs settings.



The MFP configuration is a per-SSID configuration. The MFP feature can be enabled only on WPA2-PSK and WPA2-enterprise SSIDs. The 802.11r fast roaming option will not take effect when the MFP is enabled.

Client Isolation

Aruba Central supports the Client Isolation feature isolates clients from one another and disables all peer-to-peer communication within the network. Client isolation disables inter-client communication by allowing only client to gateway traffic from clients to flow in the network. All other traffic from the client that is not destined to the gateway or configured servers will not be forwarded by the Instant AP.

This feature enhances the security of the network and protects it from vulnerabilities. Client Isolation can only be configured through the CLI. When Client Isolation is configured, the Instant AP learns the IP, Subnet Mask, MAC, and other essential information of the gateway and the DNS server. A subnet table of trusted destinations is then populated with this information. Wired servers used in the network should be manually configured into this subnet table to serve clients. The destination MAC of data packets sent by the client is validated against this subnet table and only the data packets destined to the trusted addresses in the subnet table are forwarded by the Instant AP. All other data packets are dropped.




Client Isolation feature is supported only in IPv4 networks. This feature does not support AirGroup functionalities and affects Chromecast and Airplay services.

Enabling Client Isolation Feature for Wireless Networks in Aruba Central

To enable the Client Isolation feature, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS** tab, click + **Add SSID**. The **Create a New Network** pane is displayed.
5. Click **Advanced Settings** and expand **Miscellaneous**,
6. Set the **Deny Intra VLAN Traffic** toggle to **Enable**.
7. Click **Next**.

Configuring Wireless Networks on Guest Users on Instant APs

Instant APs support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centers, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an Instant AP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the Instant AP.

The Instant AP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**— Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
 - **Internal Authenticated**— When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
 - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.

Selecting **None** disables the captive portal authentication.

For information on how to create splash page profiles, see the following sections:

- [Creating a Wireless Network Profile for Guest Users on page 314](#)
- [Configuring an Internal Captive Portal Splash Page Profile on page 314](#)
- [Configuring an External Captive Portal Splash Page Profile on page 316](#)
- [Configuring a Cloud Guest Splash Page Profile on page 318](#)
- [Disabling Captive Portal Authentication on page 319](#)

Creating a Wireless Network Profile for Guest Users

To create an SSID for guest access, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. In the WLANs tab, to create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
5. Under **Basic Settings**, enter a name that is used to identify the network in the **Name (SSID)** box.
6. If configuring a wireless guest profile, set the required WLAN configuration parameters described in [Table 85](#).
7. Click **Next** to configure VLAN settings. The VLAN details are displayed.
8. Select any of the following options for **Client IP Assignment**:

Table 89: *VLAN Assignment*

| Parameter | Description |
|--------------------------------------|---|
| Instant AP assigned | <p>On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on Instant APs on page 384.</p> <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none">■ Default—Assigns IP address to the client in the same subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network.■ Custom —Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, enter the scope of VLAN that is allowed. |
| External DHCP server assigned | <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none">■ Static —Allows you to specify a VLAN id of single VLAN, or a comma separated list of VLANs, or a range of VLANs for all clients on this network. If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID.■ Dynamic—Assigns the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules by clicking the + sign. The New VLAN Assignment Rule page is displayed to enter details such as attribute, operator, string and VLAN ID.■ Native Vlan—Assigns the client VLAN is assigned to the native VLAN. |

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **WLANs > Security** page.

Table 90: Internal Captive Portal Configuration Parameters

| Parameter | Description |
|--------------------------------|---|
| Captive Portal Type | <p>Select any of the following:</p> <ul style="list-style-type: none"> ■ Internal - Authenticated—When Internal Authenticated is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ■ Internal - Acknowledged—When Internal Acknowledged is enabled, the guest users are required to accept the terms and conditions to access the Internet. ■ External—When External is enabled, the guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. Also enter the details in Walled Garden, and Advanced section. ■ Cloud Guest—When Cloud Guest is enabled, the guest users are required to select the Guest Captive Portal Profile. ■ None—Select this option if you do not want to set any splash page. |
| Captive Portal Location | Select Acknowledged or Authenticated from the drop-down list. |
| Splash Page Properties | <p>Under Splash Page Properties when Customize Captive Portal is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design.</p> <ul style="list-style-type: none"> ■ Top Banner Title—Enter a title for the banner. To preview the page with the new banner title, click Preview Splash Page. ■ Header fill color—Specify a background color for the header. ■ Welcome Text—To change the welcome text, click the first square box in the splash page, enter the required text in the Welcome Text box, and click OK. Ensure that the welcome text does not exceed 127 characters. ■ Policy Text—To change the policy text, click the second square in the splash page, enter the required text in the Policy Text box, and click OK. Ensure that the policy text does not exceed 255 characters. ■ Page Fill Color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL. ■ Logo Image—To upload a custom logo, click Upload, browse the image file, and click upload image. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete. ■ To preview the captive portal page, click Preview splash page. ■ Captive-portal proxy server IP and Port—If you want to configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the Captive-portal proxy server IP and Captive Portal Proxy Server Port fields. |
| Encryption | <p>By default, this field is disabled. Select Enabled and configure the following encryption parameters:</p> <ul style="list-style-type: none"> ■ Key Management—Specify an encryption and authentication key ■ Passphrase format—Specify a passphrase format. ■ Passphrase—Enter a passphrase and retype to confirm. |
| Authentication | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled. ■ Primary Server—Sets a primary authentication server. <ul style="list-style-type: none"> ● To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users. |

Table 90: *Internal Captive Portal Configuration Parameters*

| Parameter | Description |
|--|---|
| | <ul style="list-style-type: none">● To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs on page 356.■ Secondary Server—To add another server for authentication, configure another authentication server.■ Load Balancing—Set this to Enabled if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 390. |
| Advanced Settings > Captive Portal Proxy Server IP | Specify the Captive Portal Proxy Server IP . |
| Advanced Settings > Captive Portal Proxy Server Port | Specify the Captive Portal Proxy Server Port . |
| Advanced Settings > Reauth Interval | Specify a value for Reauth Interval . When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. |
| Advanced Settings > Accounting | Select an accounting mode for posting accounting information at the specified Accounting interval . When the accounting mode is set to Authentication , the accounting starts only after client authentication is successful and stops when the client logs out of the network. If the accounting mode is set to Association , the accounting starts when the client associates to the network successfully and stops when the client disconnects. This is applicable for WLAN SSIDs only. |
| Advanced Settings > Blacklisting | If you are configuring a wireless network profile, select Enabled to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only. |
| Advanced Settings > Disable If Uplink Type Is | To exclude uplink, select an uplink type. |

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security > External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Security** page.
2. Select the Splash Page type as **External**.

3. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
4. Select a captive portal profile. To add a new profile, click **+** and configure the following parameters:

Table 91: *External Captive Portal Profile Configuration Parameters*

| Data Pane Item | Description |
|-----------------------------------|--|
| Name | Enter a name for the profile. |
| Type | Select any one of the following types of authentication: <ul style="list-style-type: none"> ■ Radius Authentication—Select this option to enable user authentication against a RADIUS server. ■ Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication. |
| IP or Hostname | Enter the IP address or the host name of the external splash page server. |
| URL | Enter the URL of the external captive portal server. |
| Port | Enter the port number that is used for communicating with the external captive portal server. |
| Use HTTPS | Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected. |
| Captive Portal Failure | This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network. |
| Server Offload | Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server. |
| Prevent Frame Overlay | Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page. |
| Automatic URL Whitelisting | On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. |
| Auth Text | If the External Authentication splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected. |
| Redirect URL | Specify a redirect URL if you want to redirect the users to another URL. |

5. Click **Save**.
6. On the external captive portal splash page configuration page, specify encryption settings if required.
7. Specify the following authentication parameters under **Advanced Settings**:
 - **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
 - **Primary Server**—Sets a primary authentication server.
 - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.

- To add a new server, click +. For information on configuring external servers, see [Configuring External Authentication Servers for APs on page 356](#).
 - **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers.
8. If required, under **Walled Garden**, create a list of domains that are blacklisted and also a white list of websites that the users connected to this splash page profile can access.
 9. To exclude uplink, select an uplink type.
 10. If MAC authentication is enabled, you can configure the following parameters:
 - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
 - **Uppercase Support**—Set to **Enabled** to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
 11. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.
 12. If required, enable blacklisting. Set a threshold for blacklisting clients based on the number of failed authentication attempts.
 13. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

For information on how to create a cloud guest network profile, see [Configuring a Guest Access Splash Page Profile](#)

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Open the guest SSID to edit and click **Security**:
 - a. Select **Cloud Guest** from the **Splash Page Type** list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.
 - c. To enable encryption, set **Encryption** to **Enabled** and configure the encryption parameters.
 - d. To exclude uplink, select **3G/4G**, **Wi-Fi**, or **Ethernet** option from **Disable If Uplink Type Is** accordion.
 - e. Click **Next**.
2. Click **Save Settings**.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. Open the guest SSID that you want to edit.
2. Under **Access**, select any of the following types of access control:

- **Unrestricted** — Select this to set unrestricted access to the network.
- **Network Based** — Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule:
 - a. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. Click **Save**.
- **Role Based** — Select **Role Based** to enable access based on user roles.
For role-based access control:
 1. Create a user role:
 - a. Click **New** in **Role** pane.
 - b. Enter a name for the new role and click **OK**.
 2. Create access rules for a specific user role:
 - a. Click **(+)** icon and select appropriate options for **RuleType**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. Click **Save**.
 3. Create a role assignment rule.
 - a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.
 - b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.
 - c. Click **Save**.
- 3. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select the guest network profile for which you want to disable captive portal authentication.
2. Under **Security**, select **None** for **Splash Page Type**.
3. Click **Save Settings**.

Configuring Access Points Ports Networks on Guest Users on Instant APs

Instant APs support the captive portal authentication method in which a webpage is presented to the guest users, when they try to access the Internet in hotels, conference centres, or Wi-Fi hotspots. The webpage also prompts the guest users to authenticate or accept the usage policy and terms. Captive portals are used at Wi-Fi hotspots and can be used to control wired access as well.

The captive portal solution for an Instant AP cluster consists of the following:

- The captive portal web login page hosted by an internal or external server.
- The RADIUS authentication or user authentication against internal database of the AP.
- The SSID broadcast by the Instant AP.

The Instant AP administrators can create a wired or WLAN guest network based on captive portal authentication for guests, visitors, contractors, and any non-employee users who can use the enterprise Wi-Fi

network. Administrators can also create guest accounts and customize the captive portal page with organization-specific logo, terms, and usage policy. With captive portal authentication and guest profiles, the devices associating with the guest SSID are assigned an initial role and are assigned IP addresses. When a guest user tries to access a URL through HTTP or HTTPS, the captive portal webpage prompts the user to authenticate with a user name and password.

Splash Page Profiles

Instant APs support the following types of splash page profiles:

- **Internal Captive portal**— Select this splash page to use an internal server for hosting the captive portal service. Internal captive portal supports the following types of authentication:
 - **Internal Authenticated**— When **Internal Authenticated** is enabled, a guest user who is pre-provisioned in the user database has to provide the authentication details.
 - **Internal Acknowledged**—When **Internal Acknowledged** is enabled, a guest user has to accept the terms and conditions to access the Internet.
- **External Captive portal**—Select this splash page to use an external portal on the cloud or on a server outside the enterprise network for authentication.
- **Cloud Guest**—Select this splash page to use the cloud guest profile configured through the **Guest Management** tab.

Selecting **None** disables the captive portal authentication.

For information on how to create splash page profiles, see the following sections:

- [Configuring Access Points Ports Networks on Guest Users on Instant APs on page 319](#)
- [Configuring an Internal Captive Portal Splash Page Profile on page 321](#)
- [Configuring an External Captive Portal Splash Page Profile on page 323](#)
- [Configuring a Cloud Guest Splash Page Profile on page 325](#)
- [Disabling Captive Portal Authentication on page 326](#)

Creating a Wired Network Profile for Guest Users

To create an SSID for guest access, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Ports**.
6. To create a new SSID profile, click **Add Port Profile**. The **Create a New Network** pane is displayed.
7. Under the basic settings, enter a name that is used to identify the network in the **Port Profile Name** box.
8. Click **Next** to configure VLAN settings. The VLAN details are displayed.
9. Select any of the following options for **Client IP Assignment**:

Table 92: VLAN Assignment

| Parameter | Description |
|--------------------------------------|--|
| Instant AP assigned | <p>On selecting this option, the client obtains the IP address from the Virtual Controller. The Virtual Controller creates a private subnet and VLAN on the Instant AP for the wireless clients. The network address translation for all client traffic that goes out of this interface is carried out at the source. This setup eliminates the need for complex VLAN and IP address management for a multi-site wireless network. For more information on DHCP scopes and server configuration, see Configuring DHCP Pools and Client IP Assignment Modes on Instant APs on page 384.</p> <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none"> ■ Default—Assigns IP address to the client in the same subnet as the Instant APs. By default, the client VLAN is assigned to the native VLAN on the wired network. ■ Custom —Allows you to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. When this option is selected, enter the scope of VLAN that is allowed. |
| External DHCP server assigned | <p>If this option is selected, specify any of the following options:</p> <ul style="list-style-type: none"> ■ Static —Allows you to specify a VLAN id of single VLAN, or a comma separated list of VLANS, or a range of VLANs for all clients on this network. If a large number of clients need to be in the same subnet, you can select this option to configure VLAN pooling. VLAN pooling allows random assignment of VLANs from a pool of VLANs to each client connecting to the SSID. ■ Dynamic—Assigns the VLANs dynamically from a DHCP server. You can also create a new VLAN assignment rules by clicking the + sign. The New VLAN Assignment Rule page is displayed to enter details such as attribute, operator, string and VLAN ID. ■ Native Vlan—Assigns the client VLAN is assigned to the native VLAN. |

Configuring an Internal Captive Portal Splash Page Profile

To configure internal captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Ports > Security** page.

Table 93: Internal Captive Portal Configuration Parameters

| Parameter | Description |
|--------------------------------|--|
| Captive Portal Type | <p>Select any of the following:</p> <ul style="list-style-type: none"> ■ Internal - Authenticated—When Internal Authenticated is enabled, the guest users are required to authenticate in the captive portal page to access the Internet. The guest users who are required to authenticate must already be added to the user database. ■ Internal - Acknowledged—When Internal Acknowledged is enabled, the guest users are required to accept the terms and conditions to access the Internet. ■ External—When External is enabled, the guest users are required to enter the proxy server details such as IP address and captive portal proxy server port details. Also enter the details in Walled Garden, and Advanced section. ■ Cloud Guest—When Cloud Guest is enabled, the guest users are required to select the Guest Captive Portal Profile. ■ None—Select this option if you do not want to set any splash page. |
| Captive Portal Location | Select Acknowledged or Authenticated from the drop-down list. |
| Splash Page Properties | <p>Under Splash Page Properties when Customize Captive Portal is clicked, use the editor to specify text and colors for the initial page that is displayed to the users connecting to the network. The initial page asks for user credentials or email, depending on the splash page type (Internal - Authenticated or Internal - Acknowledged) for which you are customizing the splash page design. Perform the following steps to customize the splash page design.</p> <ul style="list-style-type: none"> ■ Top Banner Title—Enter a title for the banner. To preview the page with the new banner title, click Preview Splash Page. ■ Header fill color—Specify a background color for the header. ■ Welcome Text—To change the welcome text, click the first square box in the splash page, enter the required text in the Welcome Textbox, and click OK. Ensure that the welcome text does not exceed 127 characters. ■ Policy Text—To change the policy text, click the second square in the splash page, enter the required text in the Policy Text box, and click OK. Ensure that the policy text does not exceed 255 characters. ■ Page Fill Color—To change the color of the splash page, click the Splash page rectangle and select the required color from the color palette. ■ Redirect URL—To redirect users to another URL, specify a URL in Redirect URL. ■ Logo Image—To upload a custom logo, click Upload, browse the image file, and click upload image. Ensure that the image file size does not exceed 16 KB. To delete an image, click Delete. ■ To preview the captive portal page, click Preview splash page. ■ Captive-portal proxy server IP and Port—If you want to configure a captive portal proxy server or global proxy server to match your browser configuration, enter the IP address and port number in the Captive-portal proxy server IP and Captive Portal Proxy Server Port fields. |
| Encryption | <p>By default, this field is disabled. Select Enabled and configure the following encryption parameters:</p> <ul style="list-style-type: none"> ■ Key Management—Specify an encryption and authentication key ■ Passphrase format—Specify a passphrase format. ■ Passphrase—Enter a passphrase and retype to confirm. |
| Authentication | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ MAC Authentication—To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled. ■ Primary Server—Sets a primary authentication server. <ul style="list-style-type: none"> ● To use an internal server, select Internal server and add the clients that are required to authenticate with the internal RADIUS Server. Click Users to add the users. |

Table 93: *Internal Captive Portal Configuration Parameters*

| Parameter | Description |
|---|---|
| | <ul style="list-style-type: none"> ● To add a new server, click +. For information on configuring external servers, see Configuring External Authentication Servers for APs on page 356. ■ Secondary Server—To add another server for authentication, configure another authentication server. ■ Load Balancing—Set this to Enabled if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 390. |
| Users | Create and manage users in the captive portal network. Only registered users of type Guest Employee will be able to access this network. |
| Advanced Settings > MAC Authentication | To enable MAC address based authentication for Personal and Open security levels, set MAC Authentication to Enabled . |
| Advanced Settings > Reauth Interval | Specify a value for Reauth Interval . When set to a value greater than zero, APs periodically re-authenticate all associated and authenticated clients. |
| Advanced Settings > Blacklisting | If you are configuring a wireless network profile, select Enabled to enable blacklisting of the clients with a specific number of authentication failures. This is applicable for WLAN SSIDs only. |
| Advanced Settings > Disable If Uplink Type Is | To exclude uplink, select an uplink type. |

2. Click **Save Settings**.

Configuring an External Captive Portal Splash Page Profile

You can configure external captive portal profiles and associate these profiles to a user role or SSID. You can create a set of captive portal profiles in the **Security > External Captive Portal** data pane and associate these profiles with an SSID or a wired profile. You can also create a new captive portal profile under the **Security** tab of the WLAN wizard or a Wired Network pane. You can configure up to eight external captive portal profiles.

When the captive portal profile is associated to an SSID, it is used before user authentication. If the profile is associated to a role, it is used only after the user authentication. When a captive portal profile is applied to an SSID or wired profile, the users connecting to the SSID or wired network are assigned a role with the captive portal rule. The guest user role allows only DNS and DHCP traffic between the client and network, and directs all HTTP or HTTPS requests to the captive portal unless explicitly permitted.

To configure an external captive portal profile, complete the following steps:

1. Open the guest SSID to edit and configure the following parameters in the **Security** page.
2. Select the Splash Page type as **External**.
3. If required, configure a captive portal proxy server or a global proxy server to match your browser configuration by specifying the IP address and port number in the **Captive Portal Proxy Server IP** and **Captive Portal Proxy Server Port** fields.
4. Select a captive portal profile. To add a new profile, click + and configure the following parameters:

Table 94: *External Captive Portal Profile Configuration Parameters*

| Data Pane Item | Description |
|-----------------------------------|--|
| Name | Enter a name for the profile. |
| Type | Select any one of the following types of authentication: <ul style="list-style-type: none"> ■ Radius Authentication—Select this option to enable user authentication against a RADIUS server. ■ Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication. |
| IP or Hostname | Enter the IP address or the host name of the external splash page server. |
| URL | Enter the URL of the external captive portal server. |
| Port | Enter the port number that is used for communicating with the external captive portal server. |
| Use HTTPS | Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected. |
| Captive Portal Failure | This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network. |
| Server Offload | Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server. |
| Prevent Frame Overlay | Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page. |
| Automatic URL Whitelisting | On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. |
| Auth Text | If the External Authentication splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected. |
| Redirect URL | Specify a redirect URL if you want to redirect the users to another URL. |

5. Click **Save**.

6. On the external captive portal splash page configuration page, specify encryption settings if required.

7. Specify the following authentication parameters in **Advanced Settings**:

- **MAC Authentication**—To enable MAC address based authentication for **Personal** and **Open** security levels, set **MAC Authentication** to **Enabled**.
- **Primary Server**—Sets a primary authentication server.
 - To use an internal server, select **Internal server** and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users.
 - To add a new server, click +. For information on configuring external servers, see [Configuring External Authentication Servers for APs on page 356](#).
- **Secondary Server**—To add another server for authentication, configure another authentication server.
- **Load Balancing**—Set this to **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers.

8. If required, under **Walled Garden**, create a list of domains that are blacklisted and also a white list of websites that the users connected to this splash page profile can access.
9. To exclude uplink, select an uplink type.
10. If MAC authentication is enabled, you can configure the following parameters:
 - **Delimiter Character**—Specify a character (for example, colon or dash) as a delimiter for the MAC address string. When configured, the Instant AP uses the delimiter in the MAC authentication request. For example, if you specify the colon as a delimiter, MAC addresses in the xx:xx:xx:xx:xx:xx format are used. If the delimiter is not specified, the MAC address in the xxxxxxxxxxxx format is used. This option is available only when MAC authentication is enabled.
 - **Uppercase Support**—Set to **Enabled** to allow the Instant AP to use uppercase letters in MAC address string for MAC authentication. This option is available only if MAC authentication is enabled.
11. Configure the **Reauth Interval**. Specify a value for **Reauth Interval**. When set to a value greater than zero, Instant APs periodically re-authenticate all associated and authenticated clients.
12. If required, enable blacklisting. Set a threshold for blacklisting clients based on the number of failed authentication attempts.
13. Click **Save Settings**.

Configuring a Cloud Guest Splash Page Profile

For information on how to create a cloud guest network profile, see [Configuring a Guest Access Splash Page Profile](#)

Associating a Cloud Guest Splash Page Profile to a Guest SSID

To use the Cloud Guest Splash page profile for the guest SSID, ensure that the Cloud Guest Splash Page profile is configured through the **Guest Access** app.

To associate a Cloud Guest splash page profile to a guest SSID, complete the following steps:

1. Open the guest SSID to edit and click **Security**:
 - a. Select **Cloud Guest** from the **Splash Page Type** list.
 - b. Select the splash page profile name from the **Guest Captive Portal Profile** list and click **Next**.
 - c. To enable encryption, set **Encryption** to **Enabled** and configure the encryption parameters.
 - d. To exclude uplink, select **3G/4G**, **Wi-Fi**, or **Ethernet** option from **Disable If Uplink Type Is** accordion.
 - e. Click **Next**.
2. Click **Save Settings**.

Configuring ACLs for Guest User Access

To configure access rules for a guest network, complete the following steps:

1. Open the guest SSID that you want to edit.
2. Under **Access**, select any of the following types of access control:
 - **Unrestricted** — Select this to set unrestricted access to the network.
 - **Network Based** — Select **Network Based** to set common rules for all users in a network. By default, **Allow any to all destinations** access rule is enabled. This rule allows traffic to all destinations. To define an access rule:

- a. Click **(+)** icon and select appropriate options for **Rule Type**, **Service**, **Action**, **Destination**, and **Options** fields.
- b. Click **Save**.

■ **Role Based** — Select **Role Based** to enable access based on user roles.

For role-based access control:

1. Create a user role:
 - a. Click **New** in **Role** pane.
 - b. Enter a name for the new role and click **OK**.
2. Create access rules for a specific user role:
 - a. Click **(+)** icon and select appropriate options for **RuleType**, **Service**, **Action**, **Destination**, and **Options** fields.
 - b. Click **Save**.
3. Create a role assignment rule.
 - a. Under **Role Assignment Rule**, click **New**. The **New Role Assignment Rule** pane is displayed.
 - b. Select appropriate options in **Attribute**, **Operator**, **String**, and **Role** fields.
 - c. Click **Save**.
3. Click **Save Settings**.

Disabling Captive Portal Authentication

To disable captive portal authentication, perform the following steps:

1. Select the guest network profile for which you want to disable captive portal authentication.
2. Under **Security**, select **None** for **Splash Page Type**.
3. Click **Save Settings**.

Configuring Network Port Profile AssignmentDownloadable User Roles

Aruba Central allows you to download pre-existing user roles when you create network profiles.



The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

Aruba Instant and ClearPass Policy Manager include support for centralized policy definition and distribution.

When ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager. If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. In order to provide highly granular per-user level access, user roles can be created when a user has been successfully authenticated. During the configuration of a policy enforcement profile in ClearPass Policy Manager, the administrator can define a role that should be assigned to the user after successful authentication. In RADIUS authentication, when ClearPass Policy Manager successfully authenticates a user, the user is assigned a role by ClearPass Policy Manager.

If the role is not defined on the Instant AP, the role attributes can also be downloaded automatically. This feature supports roles obtained by the following authentication methods:


- 802.1X (WLAN and wired users)
- MAC authentication
- Captive Portal

ClearPass Policy Manager Certificate Validation for Downloadable User Roles (DUR)

When a ClearPass Policy Manager server is configured as the domain for RADIUS authentication for downloading user roles, in order to validate the ClearPass Policy Manager customized CA, Instant APs are required to publish the root CA for the HTTPS server to the well-known URI (**`http://<clearpass-fqdn>/wellknown/aruba/clearpass/https-root.pem`**). The Instant AP must ensure that an FQDN is defined in the above URI for the RADIUS server and then attempt to fetch the trust anchor by using the RADIUS FQDN. Upon configuring the domain of the ClearPass Policy Manager server for RADIUS authentication along with a username and password, the Instant AP tries to retrieve the CA from the above well-known URI and store it in flash memory. However, if there is more than one ClearPass Policy Manager server configured for authentication, the CA must be uploaded manually.

Enabling Downloadable User Roles Feature for Wireless Networks in Aruba Central

To enable the Downloadable User Roles feature, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. To create a new SSID profile, click the + icon. The **Create a New Network** pane is displayed.
5. Configure the WLAN settings and VLAN settings.
6. In the Security tab, select the radius server in **Primary Server** field.



At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

7. Click **Next**, the **Access** tab is displayed.
8. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed.



The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

9. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page is displayed.




The **Edit Server** page displays the name of the radius server name. The **Name** field is non-editable.

10. Enter the following details:
 - **CPPM Username**—Enter the ClearPass Policy Manager admin username.
 - **Password**—Enter the password.
 - **Retype**—Retype the password.

11. Click **OK**.

Enabling Downloadable User Roles Feature for Wired Networks in Aruba Central

To enable the Downloadable User Roles feature, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. To create a new SSID profile, click the + icon. The **Create a New Network** pane opens to create a wireless network.
5. Configure the WLAN settings and VLAN settings.
6. In the **Security** tab, select the radius server in **Primary Server** field.



At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

7. Click **Next**, the **Access** tab is displayed.
8. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The **CPPM Settings** table with **Name**, **CPPM Username**, and **Actions** columns related to the radius servers are displayed.



The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

9. Click the action corresponding to the radius server listed in the **CPPM Settings** table. The **Edit Server** page with the radius server name is displayed.



The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

10. Enter the following details:
 - **CPPM Username**—Enter the ClearPass Policy Manager admin username.
 - **Password**—Enter the password.
 - **Retype**—Retype the password.
11. Click **OK**.


Configuring Wired Port Profiles on Instant APs

If the wired clients must be supported on the Instant APs, configure wired port profiles and assign these profiles to the access point ports of an Instant AP.

The access point ports of an Instant AP allow third-party devices such as VoIP phones or printers (which support only wired port connections) to connect to the wireless network. You can also configure an ACL for additional security on the Ethernet downlink.

To configure wired port settings, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Ports**. The **Wired Port Profiles** page is displayed.
6. To create a new wired port profile, click the + **Add Port Profiles**. The **Create a New Network** pane is displayed.

Complete the configuration for each of the tabs in the **Create a New Network** page as described in the below sections:

Configuring General Network Profile Settings

To configure general network profile settings, complete the following steps in the **General** tab:

1. Enter a name that is used to identify the network in the **Port Profile Name** box.
2. Under **Advanced Settings** section, configure the following parameters:
 - a. **Speed/Duplex**—Ensure that appropriate values are selected for **Speed/Duplex**. Contact your network administrator if you need to assign speed and duplex parameters.
 - b. **PoE**—Set **PoE** to **Enabled** to enable Power over Ethernet.
 - c. **Admin Status**—The **Admin Status** indicates if the port is up or down.
 - d. **Content Filtering**—To ensure that all DNS requests to non-corporate domains on this wired port network are sent to OpenDNS, select **Enabled** for **Content Filtering**.
 - e. **Uplink**—Select **Enabled** to configure uplink on this wired port profile. If **Uplink** is set to **Enabled** and this network profile is assigned to a specific port, the port is enabled as an Uplink port.
 - f. **Spanning Tree**—Set the **Spanning Tree** to **Enabled** to enable STP on the wired port profile. STP ensures that there are no loops in any bridged Ethernet network and operates on all downlink ports, regardless of forwarding mode. STP does not operate on uplink ports and is supported only on Instant APs with three or more ports. By default, STP is disabled on wired port profiles.
 - g. **Inactivity Timeout**—Enter the time duration after which an inactive user needs to be disabled from the network. The user must undergo the authentication process to re-join the network.
 - h. **802.3az**—Select **Enabled** to support 802.3az Energy Efficient Ethernet (EEE) standard on the device. This option allows the device to consume less power during periods of low data activity. This setting can be enabled for provisioned APs or AP groups through the wired port network. If this feature is enabled for an AP group, APs in the group that do not support 802.3az ignore this setting. This option is available for Instant APs that support a minimum of Aruba Instant 8.4.0.0 firmware version.
3. Click **Next**. The **VLANs** pane is displayed.

Configuring VLAN Settings

To configure VLAN-specific settings, complete the following steps in the **VLAN** tab:

1. On the VLANs pane, configure VLANs for the wired port network:
 - a. **Mode**—Specify any of the following modes:
 - **Access**—Select this mode to allow the port to carry a single VLAN specified as the native VLAN.
 - **Trunk**—Select this mode to allow the port to carry packets for multiple VLANs specified as allowed VLANs.
 - b. Specify any of the following values for **Client IP Assignment**:
 - **Instant AP Assigned**—Select this option to allow the Virtual Controller to assign IP addresses to the wired clients. When the Virtual Controller assignment is used, the source IP address is translated for all client traffic that goes through this interface. The Virtual Controller can also assign a guest VLAN to a wired client. In the Client VLAN Assignment section, select **Default** when the client VLAN must be

assigned to the native VLAN on the network. Select **Custom** to customize the client VLAN assignment to a specific VLAN, or a range of VLANs. Click the **Show Named VLANs** section to view all the named VLANs mapped to VLAN ID. Click the + **Add Named VLAN** icon and enter the VLAN Name and VLAN ID that is required to be mapped. Clicking **OK** populates the named VLAN in the VLAN Name to VLAN ID Mapping table.

- **External DHCP server Assigned**—Select this option to allow the clients to receive an IP address from the network to which the Virtual Controller is connected. On selecting this option, the **New** button to create a VLAN is displayed. Create a new VLAN if required.
- c. If the **Trunk** mode is selected:
- Specify the **Allowed VLAN**, enter a list of comma separated digits or ranges, for example 1, 2, 5, or 1-4, or all. The Allowed VLAN refers to the VLANs carried by the port in Access mode.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Native VLAN**. A VLAN that does not have a VLAN ID tag in the frames is referred to as Native VLAN. You can specify a value within the range of 1-4093.
- d. If the **Access** mode is selected, perform one of the following options:
- If the **Client IP Assignment** is set to **Virtual Controller Assigned**, proceed to step 6.
 - If the **Client IP Assignment** is set to **Network Assigned**, specify a value for **Access VLAN** to indicate the VLAN carried by the port in the **Access** mode.

2. Click **Next**. The **Security** pane details are displayed.

Configuring Security Settings

To configure security-specific settings, complete the following steps in the **Security** tab:

1. On the **Security** pane, select the following security options as per your requirement:
 - **802.1X Authentication**—Select **Enabled** to enable 802.1X authentication. Configure the basic parameters such as the authentication server, and MAC Authentication Fail-Through. Select any of the following options for authentication server:
 - **New**—On selecting this option, an external RADIUS server must be configured to authenticate the users. For information on configuring an external server, see [Configuring External Authentication Servers for APs on page 356](#).
 - **Internal Server**— If an internal server is selected, add the clients that are required to authenticate with the internal RADIUS server. Click the **Users** link to add the users.
 - **Load Balancing**— Set this to **Enabled** if you are using two RADIUS authentication servers, so that the load across the two RADIUS servers is balanced. For more information on the dynamic load balancing mechanism, see [Dynamic Load Balancing between Authentication Servers on page 356](#).
 - **MAC Authentication**—To enable MAC authentication, select **Enabled**. The MAC authentication is disabled by default.
 - **Captive Portal**—Select **Enabled** captive portal authentication. For more information on configuring security on captive portal, see [Configuring Access Points Ports Networks on Guest Users on Instant APs](#).
 - **Open**—Select **Enabled** to set security for open network.
2. Enable the **Port Type Trusted** option to connect uplink and downlink to a trusted port only.
3. In the **Primary Server** field, perform one of the following steps:
 - **Internal Server**—To use an internal server, select Internal Server and add the clients that are required to authenticate with the internal RADIUS Server. Click **Users** to add the users. To add a new server, click +. For information on configuring external servers, see [Configuring External Servers for Authentication on page 1](#).

- **Secondary Server**—To add another server for authentication, configure another authentication server.
 - **Load Balancing**—Select **Enabled** if you are using two RADIUS authentication servers, to balance the load across these servers. For more information on the dynamic load balancing mechanism, see [Dynamic Load Balancing between Authentication Servers on page 356](#).
- 4. **MAC Authentication Fail-Thru**—Select **Enabled** to attempt 802.1X authentication is attempted when the MAC authentication fails.
- 5. Under the **Advance Settings** section, configure the following options:
 - **Use IP for Calling Station ID**—Select **Enabled** to configure client IP address as calling station ID.
 - **Called Station ID Type**— Select one of the following options:
 - **Access Point Group**—Uses the VC ID as the called station ID.
 - **Access Point Name**—Uses the host name of the Instant AP as the called station ID.
 - **VLAN ID**—Uses the VLAN ID of as the called station ID.
 - **IP Address**—Uses the IP address of the Instant AP as the called station ID.
 - **MAC address**—Uses the MAC address of the Instant AP as the called station ID.



The **Called Station ID Type** detail can be configured even if the **Use IP for Calling Station ID** is set to **Disable**.

- **Reauth Interval**—Specify the interval at which all associated and authenticated clients must be reauthenticated.
6. Click **Next**. The **Access** pane is displayed.

Configuring Access Settings

To configure access-specific settings, complete the following steps in the **Access** tab:

1. Enable the **Downloadable User** option to allow downloading of pre-existing user roles. The CPPM Settings table with **Name**, **CPPM Username** and **Actions** columns related to the radius servers are displayed.

The Downloadable User Role feature is optional.



The Downloadable User Roles feature is available only for networks that include APs that run a minimum of Aruba Instant 8.4.0.0 firmware version with a minimum of ClearPass server version 6.7.8.

At least one radius server must be configured to apply the Downloadable User Roles feature. For more information on configuring radius server, see [Authentication Servers for Instant APs](#)

2. Click the action corresponding to the server. The **Edit Server** page is displayed.



The **Edit Server** page displays the radius server name. The **Name** field is non-editable.

3. Enter the CPPM username along with the CPPM authentication credentials for the radius server.
4. Click **Ok**.
5. Under Access Rules, configure the following access rule parameters:
 - a. Select any of the following types of access control:
 - **Role-based**— Allows the users to obtain access based on the roles assigned to them.
 - **Unrestricted**— Allows the users to obtain unrestricted access on the port.

- **Network-based**— Allows the users to be authenticated based on access rules specified for a network.
- b. If the **Role-based** access control is selected:
 - Under **Role**, select an existing role for which you want to apply the access rules, or click **New** and add the required role. To add a new access rule, click **Add Rule** under **Access Rules For Selected Roles**.




The default role with the same name as the network is automatically defined for each network. The default roles cannot be modified or deleted.

- Configure role assignment rules. To add a new role assignment rule, click **New** under **Role Assignment Rules**. Under **New Role Assignment Rule**:
 - a. Select an attribute.
 - b. Specify an operator condition.
 - c. Select a role.
 - d. Click **Save**.

6. Click **Finish** to create the wired port profile successfully.

Configuring Network Port Profile Assignment

To map the wired ports profile to ethernet ports, perform the following:


1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - e. Under **Manage**, click **Devices > Access Points**.
 - f. Click the settings  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. Click **Show Advanced**.
5. Click **Ports**. The **Wired Port Profiles** page is displayed.
6. In the **Port Profiles Assignments** section, assign wired port profiles to Ethernet ports:
 - g. Select a profile from the **Ethernet 0/0** drop down list.
 - h. Select the profile from the **Ethernet 0/1** drop down list.
 - i. If the Instant AP supports Ethernet 2, Ethernet 3 and Ethernet 4 ports, assign profiles to these ports by selecting a profile from the **Ethernet 0/2**, **Ethernet 0/3**, and **Ethernet 0/4** drop-down list respectively.
7. Click **Save Settings**.

Viewing Wired Port Profile Summary Table

The **Network Summary** page now displays all the settings configured in the **General**, **Security**, **VLANs**, and **Access** tabs to create the wired port profiles. Click **Finish** to complete the network profile creation and save the settings.

Editing a WLAN Profile


To edit a network profile, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.

4. In the **Wireless SSIDs** table of **WLANS** page, select the network that you want to edit.
5. Click the **Edit** icon under the **Actions** column. The network details are displayed.
6. Modify the profile.
7. Click **Save Settings**.

Editing a Access Points Ports Profile

To edit a network profile, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.



When you click the **Show Advanced** option, the **Devices > Access Points** tab displays the **WLANS, Ports, Access Points, Radios, Security, VPN, Services, System, Configuration Audit** tabs.


5. Click **Ports**. The **Wired Port Profiles** page is displayed.
6. Select the network that you want to edit.
7. Click the **Edit** icon under the **Actions** column. The network details are displayed.
8. Modify the profile.
9. Click **Save Settings**.



When you click the **Hide Advanced** option, the **Devices > Access Points** tab displays only the **WLANS, Access Points, and Radio** tabs as the default configuration tabs.

Deleting a Network Profile

To delete a network profile, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **WLANS** to display the wireless networks.
5. Select the network that you want to delete.
6. To delete a wired network, click **Show Advanced** in **Device**.
7. Click the **Delete** icon.
8. Click **OK** to confirm deletion.

Aruba Mesh Network and Mesh Instant AP

Mesh Network Overview

The mesh solution effectively expands and configures network coverage for outdoor and indoor enterprises in a wireless environment. The mesh network automatically reconfigures broken or blocked paths when traffic traverses across mesh Instant AP. This feature provides increased reliability by allowing the network to continue operating even when an Instant AP is non-functional or if the device fails to connect to the network.



A mesh network requires at least one valid wired or 3G uplink connection.

The mesh network must be provisioned by plugging into the wired network for the first time.

Mesh Instant APs

The Instant APs that are configured for mesh can either operate as mesh portals or as mesh points based on the uplink type.

Instant AP as Mesh Portal

Any provisioned Instant AP that has a valid wired or 3G uplink connection functions as a mesh portal. A mesh portal acts as a gateway between the wireless mesh network and the enterprise wired LAN. The mesh roles are automatically assigned based on the Instant AP configuration. The mesh portal can also act as a virtual controller.



The mesh portal reboots after 5 minutes when it loses its uplink connectivity to a wired network.

Instant AP as Mesh Point

The Instant AP without an ethernet link functions as a mesh point. The mesh point establishes an all-wireless path to the mesh portal and provides traditional WLAN services such as client connectivity, IDS capabilities, user role association, and QoS for LAN-to-mesh communication to the clients, and performs mesh backhaul or network connectivity. The mesh points authenticate to the mesh portal and establish a secured link using AES encryption.



A mesh point also supports LAN bridging by connecting any wired device to the downlink port of the mesh point. In the case of single ethernet port platforms such as Instant AP-105, you can convert the Eth0 uplink port to a downlink port by enabling Eth0 Bridging.

Redundancy is observed in a mesh network when two Instant APs have valid uplink connections, and most mesh points try to mesh directly with one of the two portals.

There can be a maximum of eight mesh points per mesh portal in a mesh network. When mesh Instant APs boot up, they detect the environment to locate and associate with their nearest neighbor. The mesh Instant APs determine the best path to the mesh portal ensuring a reliable network connectivity.



In a dual-radio Instant AP, the 2.4 GHz radio is always used for client traffic, and the 5 GHz radio is always used for both mesh-backhaul and client traffic.

Automatic Mesh Role Assignment

Aruba Central supports enhanced role detection during Instant AP boot-up and Instant AP running time. When a mesh point discovers that the Ethernet 0 port link is up, it sends loop detection packets to check the availability of Ethernet 0 link. If the Ethernet 0 link is available, the mesh point reboots as a mesh portal. Else, the mesh point does not reboot.

Mesh Role Detection during System Boot-Up

If the ethernet link is down during Instant AP boot-up, the Instant AP acts as a mesh point. If the ethernet link is up, the Instant AP continues to detect if the network is reachable in the following scenarios:

- In a static IP address scenario, the Instant AP acts as a mesh portal if it successfully pings the gateway. Otherwise, it acts as a mesh point.

- In case of DHCP, the Instant AP acts as a mesh portal when it obtains the IP address successfully. Otherwise, it acts as a mesh point.
- In case of IPv6, Instant APs do not support the static IP address but only support DHCP for detection of network reachability.



If the Instant AP has a 3G or 4G USB modem plugged, it always acts as a mesh portal. If the Instant AP is set to Ethernet 0 bridging, it always acts as a mesh point.

Mesh Role Detection during System Running Time

The mesh point uses the Loop Protection for Secure Jack Port feature to detect the loop when the ethernet is up. If the loop is detected, the Instant AP reboots. Otherwise, the Instant AP does not reboot and the mesh role continues to act as a mesh point.


Setting up Instant Mesh Network

- To provision Instant APs as mesh Instant APs:
- Connect the Instant APs to a wired switch.
- Ensure that the virtual controller key is synchronized and the country code is configured.
- Ensure that a valid SSID is configured on the Instant AP.
- If the Instant AP has a factory default SSID (Instant SSID), delete the SSID.
- If an ESSID is enabled on the virtual controller, disable it and reboot the Instant AP cluster.
- Disconnect the Instant APs that you want to deploy as mesh points from the switch, and place the Instant APs at a remote location. The Instant APs come up without any wired uplink connection and function as mesh points. The Instant APs with valid uplink connections function as mesh portals.

Configuring Wired Bridging on Ethernet 0 for Mesh Point

Aruba Central supports wired bridging on the Ethernet 0 port of an Instant AP. You can configure wired bridging, if the Instant AP is configured to function as a mesh point.

Perform the following steps to configure support for wired bridging on the Ethernet 0 port of an Instant AP from Aruba Central UI:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Access Points**. The **Access Points** page is displayed.
5. To edit an Instant AP, click the edit icon corresponding to the AP. The edit pane to modify the Instant AP parameters is displayed.
6. Expand the **Uplink** section.
7. To configure a non-native uplink VLAN, specify the number of VLANs in the **Uplink Management VLAN** text box.
8. Enable the **Eth0 Bridging** toggle button.
9. Click **OK**.
10. Reboot the Instant AP.

Mesh Cluster Function

Aruba Central introduces the mesh cluster function for easy deployments of Instant APs. You can configure the ID, password, and also provision Instant APs to a specific mesh cluster.

In a cluster-based scenario, you can configure unlimited mesh profiles in a network. When an Instant AP boots up, it attempts to find a mesh cluster configuration. The Instant AP fetches a pre-existing mesh cluster configuration, if any. Otherwise, it uses the default mesh configuration in which the SSID, password, and cluster name are generated by the virtual controller key.



Instant APs that belong to the same mesh network can establish mesh links with each other. The Instant APs can establish a mesh link in a standalone scenario also. However, the network role election does not take place in a standalone environment. Users can set the same mesh cluster configuration to establish mesh links with other networks. For more information on mesh cluster configuration, refer to the *Mesh Instant AP Configuration* chapter of *Aruba Instant User Guide*.

Configuring Time-Based Services for Wireless Network Profiles

Aruba Central allows you to configure the availability of a WLAN SSID at a particular time of the day. You can now create a time range profile and assign it to a WLAN SSID, so that you can enable or disable access to the SSID and thus control user access to the network during a specific time period.

Instant APs support the configuration of both absolute and periodic time range profiles. You can configure an absolute time range profile to execute during a specific time frame, or create a periodic profile to execute at regular intervals based on the periodicity specified in the configuration.

Before You Begin

Before you configure time-based services, ensure that the NTP server connection is active.

Creating a Time Range Profile

To create a time range profile, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** page is displayed.
6. Click **Time-Based Services**.
7. Click **+** under the time range profiles in the Time-Based Profiles table. The **New profile** window for creating a time range profile is displayed. Configure the parameters that are listed in the following table:

Table 95: *Time Range Profile Configuration Parameters*

| Parameter | Description |
|-------------------------------------|--|
| Name | Specify a name for the time range profile. |
| Type | <p>Select the type of time range profile:</p> <ul style="list-style-type: none"> ■ Periodic—Allows you configure a specific periodicity and recurrence pattern for a time range profile. ■ Absolute—Allows you to configure an absolute day and time range. |
| Repeat | <p>Specify the frequency for the periodic time range profile:</p> <ul style="list-style-type: none"> ■ Daily—Enables daily recurrence. ■ Weekly—Allows you define a specific time range with specific start and end days in a week. |
| Day Range | <p>Absolute Time Range</p> <p>For an absolute time range profile, this field allows you to specify the start day and end day, both in mm/dd/yyyy format. You can also use the calendar to specify the start and end days.</p> <p>Periodic Time Range</p> <p>For a periodic time range profile, the following Day Range options are available:</p> <ul style="list-style-type: none"> ■ For daily recurrence—If the Repeat option is set to Daily, this field allows you to select the following time ranges: <ul style="list-style-type: none"> ● Monday—Sunday (All Days) ● Monday—Friday (Weekdays) ● Saturday—Sunday (Weekend) <p>For example, if you set the Repeat option to Daily and then select Monday –Friday (Weekday) for Day Range, and Start Time as 1 and End time as 2, the applied time range will be Monday to Friday from 1 am to 2 am; that is, on Monday at 3 am, the profile will not be applied or disabled.</p> ■ For weekly occurrence—If the Repeat option is set to Weekly, this field allows you to select the start and end days of a week and time range. <p>For example, if you set Start day as Monday and End day as Friday, and Start time as 1 and End time as 2, the applied time range profile is Monday 1 am to Friday 2 am every week; that is, on Monday at 3 am, the profile will be applied or enabled.</p> |
| Start Time | Select the start time for the time range profile from the Hours and Minutes drop-down lists, respectively. |
| End Time | Select the end time for the time range profile from the Hours and Minutes drop-down lists, respectively. |
| Visualization Graph for Time | The Visualization graph (approximated to the hour) provides a visual display of the selected time range (Day range, Start Time, and End Time) for periodic profiles. |

Associating a Time Range Profile to an SSID

To apply a time range profile to an SSID, complete the following steps:


1. Click the edit icon next to the SSID for which you want to apply the time range profile. You can also add a time range profile when configuring an SSID.
2. Click **Time Range Profiles**.
3. Select a time range profile from the list and select a value from the **Status** drop-down list.

- When a time range profile is enabled on SSID, the SSID is made available to the users for the configured time range. For example, if the specified time range is 12:00 to 13:00, the SSID becomes available only between 12 PM to 1 PM on a given day.
- If a time range is disabled, the SSID becomes unavailable for the configured time range. For example, if configured time-range is 14:00 to 17:00, the SSID is made unavailable from 2 PM to 5 PM on a given day.

4. Click **Save**.

Associating a Time Range Profile to ACL

Aruba Central allows you to configure time-based services for specific ACL. To apply a time range profile to an access rule, complete the following procedure:

5. In the **Network Operations** app, use the filter to select a group or a device.
6. Under **Manage**, click **Devices > Access Points**.
7. Click the  configuration icon to display the AP configuration dashboard.
8. Click **Show Advanced**.
9. Click **Security**. The **Security** page for the selected group or device is displayed.
10. In the Roles section, click the edit icon listed for access rules under **Access Rules For Selected Roles** to which you want to apply the time range profile.
11. The **Access Rule** page is displayed.
12. In the **Options** section, select the **Time Range** check box and select the time range profile from the drop-down list.
 - When a time range profile is associated with an ACL, the configured time range is applied on all the WLAN SSID with the specific ACL.
 - If a time range is disabled or if the time range profile is deleted for an ACL, all WLAN SSID with the specific ACL will be able to access the network without any time constraint.
13. Click **Save**.

For more information on time range configuration, see the *Aruba Instant User Guide*.

Configuring ARM and RF Parameters on Instant APs

This section provides the following information:

- [ARM Overview on page 338](#)
- [Configuring ARM Features on page 339](#)
- [Configuring Radio Parameters on page 342](#)

ARM Overview

ARM is a radio frequency management technology that optimizes WLAN performance even in the networks with highest traffic by dynamically and intelligently choosing the best 802.11 channel and transmitting power for each Instant AP in its current RF environment. ARM works with all standard clients, across all operating systems, while remaining in compliance with the IEEE 802.11 standards. It does not require any proprietary client software to achieve its performance goals. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. By ensuring the fair distribution of available Wi-Fi bandwidth to mobile devices, ARM ensures that data, voice, and video applications have sufficient network resources at all times. ARM allows mixed 802.11 a, b, g, n, and ac client types to inter operate at the highest performance levels.

When ARM is enabled, an Instant AP dynamically scans all 802.11 channels within its 802.11 regulatory domain at regular intervals and sends reports on WLAN coverage, interference, and intrusion detection to the Virtual Controller. ARM computes coverage and interference metrics for each valid channel, chooses the best performing channel, and transmit power settings for each Instant AP RF environment. Each Instant AP gathers other metrics on its ARM-assigned channel to provide a snapshot of the current RF health state.

Instant APs support the following ARM features:

- **Channel or Power Assignment**—Assigns channel and power settings for all the Instant APs in the network according to changes in the RF environment.
- **Voice Aware Scanning**—Improves voice quality by preventing an Instant AP from scanning for other channels in the RF spectrum during a voice call and by allowing an Instant AP to resume scanning when there are no active voice calls.
- **Load Aware Scanning**—Dynamically adjusts the scanning behavior to maintain uninterrupted data transfer on resource intensive systems when the network traffic exceeds a predefined threshold.
- **Bandsteering**—Assigns the dual-band capable clients to the 5 GHz band on dual-band Instant APs thereby reducing co-channel interference and increasing the available bandwidth for dual-band clients.
- **Client Match**—Continually monitors the RF neighborhood of the client to support the ongoing band steering and load balancing of channels, and enhanced Instant AP reassignment for roaming mobile clients.



When Client Match is enabled on 802.11n capable Instant APs, the Client Match feature overrides any settings configured for the legacy band steering, station hand-off assist or load balancing features. The 802.11ac capable Instant APs do not support the legacy band steering, station hand off or load balancing settings, so these Instant APs must be managed using Client Match.

- **Airtime Fairness**—Provides equal access to all clients on the wireless medium, regardless of client type, capability, or operating system to deliver uniform performance to all clients.

For more information on ARM features supported by the APs, see the *Aruba Instant User Guide*.

Configuring ARM Features

To configure ARM features such as band steering, and airtime fairness mode and Client Match, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Configuration**  icon to display the AP configuration dashboard.
4. Click the **Radios** tab.
5. Under **RF > Adaptive Radio Management (ARM)**, the **Client Control** section displays the following components:
 - **Band Steering Mode**
 - **Airtime Fairness Mode**
 - **ClientMatch**
 - **ClientMatch Calculating Interval**
 - **ClientMatch Neighbor Matching**
 - **ClientMatch Threshold**
 - **Spectrum Load Balancing Mode**
6. For **Band Steering Mode**, configure the following parameters:

Table 96: *Band Steering Mode Configuration Parameters*

| Data pane item | Description |
|----------------------|---|
| Prefer 5 GHz | Enables band steering in the 5 GHz mode. On selecting this, the Instant AP steers the client to the 5 GHz band (if the client is 5 GHz capable), but allows the client connection on the 2.4 GHz band if the client persistently attempts for 2.4 GHz association. |
| Force 5 GHz | Enforces 5 GHz band steering mode on the Instant APs. |
| Balance Bands | Allows the Instant AP to balance the clients across the two radios to best utilize the available 2.4 GHz bandwidth. This feature takes into account the fact that the 5 GHz band has more channels than the 2.4 GHz band, and that the 5 GHz channels operate in 40 MHz, while the 2.5 GHz band operates in 20 MHz. |
| Disable | Allows the clients to select the band to use. |

7. For **Airtime Fairness Mode**, specify any of the following values:

Table 97: *Airtime Fairness Mode Configuration Parameters*

| Data Pane Item | Description |
|-------------------------|--|
| Default Access | Allows access based on client requests. When Air Time Fairness is set to Default Access option, per user and per SSID bandwidth limits are not enforced. |
| Fair Access | Allocates air time evenly across all the clients. |
| Preferred Access | Sets a preference where 802.11n clients are assigned more air time than 802.11a/11g. The 802.11a/11g clients get more airtime than 802.11b. The ratio is 16:4:1. |

8. For **Client Match**, configure the following parameters:

Table 98: *Additional ARM Configuration Parameters*

| Data Pane Item | Description |
|---|--|
| Client Match | Enables the Client Match feature on APs. When enabled, client count is balanced among all the channels in the same band. When Client Match is enabled, ensure that the Scanning option is enabled. For more information, see AP Control Configuration Parameters . NOTE: When the Client Match is disabled, channels can be changed even when the clients are active on a BSSID. The Client Match option is disabled by default. |
| ClientMatch Calculating Interval | Configures a value for the calculating interval of Client Match. The interval is specified in seconds and the default value is 3 seconds. You can specify a value within the range of 10-600. |
| ClientMatch Neighbor Matching% | Configures the calculating interval of Client Match. This number takes into account the least similarity percentage to be considered as in the same virtual RF neighborhood of Client Match. You can specify a percentage value within the range of 20-100. The default value is 60%. |

| Data Pane Item | Description |
|-------------------------------------|---|
| ClientMatch Threshold | Configures a Client Match threshold value. This number takes acceptance client count difference among all the channels of Client Match. When the client load on an AP reaches or exceeds the threshold in comparison, Client Match is enabled on that AP. You can specify a value within range of 1-20. The default value is 5. |
| CM Key | Client match uses the wired layer 2 protocol to synchronize information exchanged between Instant APs. Users have an option to configure the client match keys. Instant APs verify if the frames that they broadcast contain a common client match key. Instant APs that receive these frames verify if the sender belongs to same network or if the sender and receiver both have the same client match key. |
| Spectrum Load Balancing Mode | Enables the Spectrum Load Balancing mode to determine the balancing strategy for Client Match. The following options are available: <ul style="list-style-type: none"> ■ Channel ■ Radio ■ Channel + Radio |

9. Click **Access Point Control**, and configure the following parameters:

Table 99: *AP Control Configuration Parameters*

| Data pane item | Description |
|---------------------------------|--|
| Customize Valid Channels | Allows you to select a custom list of valid 20 MHz and 40 MHz channels for 2.4 GHz and 5 GHz bands. By default, the AP uses valid channels as defined by the Country Code (regulatory domain). On selecting Customize Valid Channels , a list of valid channels for both 2.4GHz and 5 GHz are displayed. The valid channel customization feature is disabled by default. The valid channels automatically show in the Static Channel Assignment data pane. |
| Min Transmit Power | Allows you to configure a minimum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the minimum transmission EIRP setting configured on an AP is not supported by the AP model, this value is reduced to the highest supported power setting. The default value for minimum transmit power is 18 dBm. |
| Max Transmit Power | Allows you to configure the maximum transmission power within a range of 3 to 33 dBm in 3 dBm increments. If the maximum transmission EIRP configured on an AP is not supported by the local regulatory requirements or AP model, the value is reduced to the highest supported power settings. |
| Client Aware | Allows ARM to control channel assignments for the Instant APs with active clients. When the Client Match mode is set to Disabled , an Instant AP may change to a more optimal channel, which disrupts current client traffic. The Client Aware option is Enabled by default. |

| Data pane item | Description |
|---------------------------|---|
| Scanning | Allows the Instant AP to dynamically scan all 802.11 channels within its 802.11 regulatory domain at regular intervals. This scanning report includes WLAN coverage, interference, and intrusion detection data. NOTE: For Client Match configuration, ensure that scanning is enabled. |
| Wide Channel Bands | Allows the administrators to configure 40 MHz channels in the 2.4 GHz and 5.0 GHz bands. 40 MHz channels are two 20 MHz adjacent channels that are bonded together. The 40 MHz channel effectively doubles the frequency bandwidth available for data transmission. For high performance, you can select 5 GHz. If the AP density is low, enable in the 2.4 GHz band. |
| 80 MHz Support | Enables or disables the use of 80 MHz channels on APs. This feature allows ARM to assign 80 MHz channels on APs with 5 GHz radios, which support a very high throughput. This setting is enabled by default. NOTE: Only the APs that support 802.11ac can be configured with 80 MHz channels. |

10. Click **Save Settings**.

Configuring Radio Parameters

To configure RF parameters for the 2.4 GHz and 5 GHz radio bands on an Instant AP, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the **Configuration**  icon to display the AP configuration dashboard.
4. Click **Radios** and then expand the **Radio** accordion in the **RF** dashboard.
5. Under 2.4 GHz, 5 GHz, or both, configure the following parameters by clicking the + sign.

Table 100: *Radio Configuration Parameters*

| Data Pane Item | Description |
|------------------------------------|---|
| Zone | Allows you to configure a zone per radio band for Instant APs in a cluster. You can also configure an RF zone per Instant AP. NOTE: Aruba recommends that you configure RF zone for either individual AP or for the cluster. Any discrepancy in the RF zone names may lead to configuration errors. |
| Legacy Only | When set to ON , the Instant AP runs the radio in the non-802.11n mode. This option is set to OFF by default. |
| 802.11d / 802.11h | When set to ON , the radios advertise their 802.11d (Country Information) and 802.11h (Transmit Power Control) capabilities. This option is set to OFF by default. |
| Beacon Interval | Configures the beacon period for the Instant AP in milliseconds. This indicates how often the 802.11 beacon management frames are transmitted by the AP. You can specify a value within the range of 60–500. The default value is 100 milliseconds. |
| Interference Immunity Level | Configures the immunity level to improve performance in high-interference environments. The default immunity level is 2. ■ Level 0 — No ANI adaptation. |

Table 100: Radio Configuration Parameters

| Data Pane Item | Description |
|--|---|
| | <ul style="list-style-type: none"> ■ Level 1 — Noise immunity only. This level enables power-based packet detection by controlling the amount of power increase that makes a radio aware that it has received a packet. ■ Level 2 — Noise and spur immunity. This level also controls the detection of OFDM packets, and is the default setting for the Noise Immunity feature. ■ Level 3 — Level 2 settings and weak OFDM immunity. This level minimizes false detects on the radio due to interference, but may also reduce radio sensitivity. This level is recommended for environments with a high-level of interference related to 2.4 GHz appliances such as cordless phones. ■ Level 4 — Level 3 settings, and FIR immunity. At this level, the AP adjusts its sensitivity to in-band power, which can improve performance in environments with high and constant levels of noise interference. ■ Level 5 — The AP completely disables PHY error reporting, improving performance by eliminating the time the Instant AP spends on PHY processing. <p>NOTE: Increasing the immunity level makes the AP lose a small amount of range.</p> |
| Channel Switch Announcement Count | Configures the number of channel switching announcements to be sent before switching to a new channel. This allows the associated clients to recover gracefully from a channel change. |
| Background Spectrum Monitoring | When set to ON , the APs in the access mode continue with their normal access service to clients, while performing additional function of monitoring RF interference (from both neighboring APs and non Wi-Fi sources such as, microwaves and cordless phones) on the channel they are currently serving the clients. |
| Customize ARM Power Range | Configures a minimum (Min Power) and maximum (Max Power) power range value for the 2.4 GHz and 5 GHz band frequencies. The default value is 3 dBm. Unlike the configuration in the ARM profile, the transmit power of all radios in the Radio profile do not share the same configuration. |
| Enable 11ac | When set to ON , VHT is enabled on the 802.11ac devices for the 5 GHz radio band. If VHT is enabled for the 5 GHz radio profile on an Instant AP, it is automatically enabled for all SSIDs configured on an Instant AP. By default, VHT is enabled on all SSIDs. NOTE: If you want the 802.11ac Instant APs to function as 802.11n Instant APs, clear this check box to disable VHT on these devices. |
| Smart antenna | Set to Enabled to combine an antenna array with a digital signal-processing capability to transmit and receive in an adaptive, spatially sensitive manner. |
| ARM/WIDS Override | When ARM/WIDS Override is off, the Instant AP will always process frames for WIDS. WIDS is an application that detects the attacks on a wireless network or wireless system, purposes even when it is heavily loaded with client traffic. When ARM/WIDS Override is on, the Instant AP will stop processing frames for WIDS. |

6. Click **Save Settings**.

Configuring IDS Parameters on APs

Aruba Central supports the IDS feature that monitors the network for the presence of unauthorized APs and clients. It also logs information about the unauthorized APs and clients, and generates reports based on the logged information.


Rogue APs

The IDS feature in the Aruba Central network enables you to detect rogue APs, interfering APs, and other devices that can potentially disrupt network operations. A rogue AP is an unauthorized AP plugged into the wired side of the network. An interfering AP is an AP seen in the RF environment, but it is not connected to the wired network. While the interfering AP can potentially cause RF interference, it is not considered a direct security threat, because it is not connected to the wired network. However, an interfering AP may be reclassified as a rogue AP.

The built-in IDS scans for APs that are not controlled by the VC. These are listed and classified as either Interfering or Rogue, depending on whether they are on a foreign network or your network.

Configuring Wireless Intrusion Detection and Protection Policies

To configure a Wireless Intrusion Detection and Protection policy:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click the **Wireless IDS/IPS** accordion.

The following three sections are displayed:

- **Detection**
- **Protection**
- **Firewall Settings**

You can configure the following options in the above mentioned sections:

- **Infrastructure Detection Policies**—Specifies the policy for detecting wireless attacks on APs.
- **Client Detection Policies**—Specifies the policy for detecting wireless attacks on clients.
- **Infrastructure Protection Policies**—Specifies the policy for protecting APs from wireless attacks.
- **Client Protection Policies**—Specifies the policy for protecting clients from wireless attacks.
- **Firewall Policies**—Specifies the policies to set a firewall for a secured network access.
- **Containment Methods**—Prevents unauthorized stations from connecting to your Aruba Central network.

Each of these options contains several default levels that enable different sets of policies. An administrator can customize enable or disable these options accordingly.

Detection

The detection levels can be configured using the **Detection** section. The following levels of detection can be configured in the WIP Detection page:D

- **Off**
- **Low**
- **Medium**
- **High**

The following table describes the detection policies enabled in the Infrastructure Detection **Custom settings** field.

Table 101: *Infrastructure Detection Policies*

| Detection level | Detection policy |
|-----------------|--|
| Off | Rogue Classification |
| Low | <ul style="list-style-type: none"> ■ Detect AP Spoofing ■ Detect Windows Bridge ■ IDS Signature — Deauthentication Broadcast ■ IDS Signature — Deassociation Broadcast |
| Medium | <ul style="list-style-type: none"> ■ Detect ad hoc networks using VALID SSID ■ Detect Malformed Frame — Large Duration |
| High | <ul style="list-style-type: none"> ■ Detect AP Impersonation ■ Detect ad hoc Networks ■ Detect Valid SSID Misuse ■ Detect Wireless Bridge ■ Detect 802.11 40 MHz intolerance settings ■ Detect Active 802.11n Greenfield Mode ■ Detect AP Flood Attack ■ Detect Client Flood Attack ■ Detect Bad WEP ■ Detect CTS Rate Anomaly ■ Detect RTS Rate Anomaly ■ Detect Invalid Address Combination ■ Detect Malformed Frame — HT IE ■ Detect Malformed Frame — Association Request ■ Detect Malformed Frame — Auth. ■ Detect Overflow IE ■ Detect Overflow EAPOL Key ■ Detect Beacon Wrong Channel ■ Detect devices with invalid MAC OUI |

The following table describes the detection policies enabled in the Client Detection **Custom settings** field.

Table 102: *Client Detection Policies*

| Detection level | Detection policy |
|-----------------|--|
| Off | All detection policies are disabled. |
| Low | Detect Valid Station Misassociation |
| Medium | <ul style="list-style-type: none"> ■ Detect Disconnect Station Attack ■ Detect Omerta Attack ■ Detect FATA-Jack Attack ■ Detect Block ACK DOS ■ Detect Hotspotter Attack ■ Detect unencrypted Valid Client ■ Detect Power Save DOS Attack |
| High | <ul style="list-style-type: none"> ■ Detect EAP Rate Anomaly ■ Detect Rate Anomaly ■ Detect Chop Chop Attack ■ Detect TKIP Replay Attack |

| Detection level | Detection policy |
|-----------------|--|
| | <ul style="list-style-type: none"> ■ IDS Signature — Air Jack ■ IDS Signature — ASLEAP |

Protection

The following levels of detection can be configured in the WIP Protection page:

- Off
- Low
- High

The following table describes the protection policies that are enabled in the Infrastructure Protection **Custom settings** field.

Table 103: *Infrastructure Protection Policies*

| Protection level | Protection policy |
|------------------|---|
| Off | All protection policies are disabled |
| Low | <ul style="list-style-type: none"> ■ Protect SSID — Valid SSID list is auto derived from AP configuration ■ Rogue Containment |
| High | <ul style="list-style-type: none"> ■ Protect from Adhoc Networks ■ Protect AP Impersonation |

The following table describes the detection policies that are enabled in the Client Protection **Custom settings** field.

Table 104: *Client Protection Policies*

| Protection level | Protection policy |
|------------------|--------------------------------------|
| Off | All protection policies are disabled |
| Low | Protect Valid Station |
| High | Protect Windows Bridge |

Containment Methods

You can enable wired and wireless containment measures to prevent unauthorized stations from connecting to your Aruba Central network.

Aruba Central supports the following types of containment mechanisms:

- Wired containment — When enabled, APs generate ARP packets on the wired network to contain wireless attacks.
- Wireless containment — When enabled, the system attempts to disconnect all clients that are connected or attempting to connect to the identified AP.
 - None — Disables all the containment mechanisms.

- Deauthenticate only — With deauthentication containment, the AP or client is contained by disrupting the client association on the wireless interface.
- Tarpit containment — With tarpit containment, the AP is contained by luring clients that are attempting to associate with it to a tarpit. The tarpit can be on the same channel or a different channel as the AP being contained.



The FCC and some third parties have alleged that under certain circumstances, the use of containment functionality violates 47 U.S.C. §333. Before using any containment functionality, ensure that your intended use is allowed under the applicable rules, regulations, and policies. Aruba is not liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality.

Firewall Settings

To configure firewall settings by specifying the policies for a secured network access, see [Configuring Firewall Parameters for Wireless Network Protection](#).

Configuring Authentication and Security Profiles on Instant APs

This section describes the authentication and security parameters to configure on an Instant AP provisioned in:

- [Supported Authentication Methods on page 347](#)
- [Authentication Servers for Instant APs on page 354](#)
- [Configuring External Authentication Servers for APs on page 356](#)
- [Configuring Users Accounts for the Instant AP Management Interface on page 359](#)
- [Configuring Guest and Employee User Profiles on Instant APs on page 360](#)
- [Configuring Roles and Policies on Instant APs for User Access Control on page 361](#)
- [Enabling ALG Protocols on Instant APs on page 377](#)
- [Blacklisting Instant AP Clients on page 377](#)

Supported Authentication Methods

Authentication is a process of identifying a user through a valid username and password. Clients can also be authenticated based on their MAC addresses.

The authentication methods supported by the Instant APs managed through Aruba Central are described in the following sections.

802.1X Authentication

802.1X is a method for authenticating the identity of a user before providing network access to the user. The Aruba Central network supports internal RADIUS server and external RADIUS server for 802.1X authentication. For authentication purpose, the wireless client can associate to a NAS or RADIUS client such as a wireless Instant AP. The wireless client can pass data traffic only after successful 802.1X authentication.




The NAS acts as a gateway to guard access to a protected resource. A client connecting to the wireless network first connects to the NAS.

Configuring 802.1X Authentication for a Network Profile

To configure 802.1X authentication for a wireless network profile, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS**, from the **Wireless SSIDs** table, select a network profile for which you want to enable 802.1X authentication, and click **Edit**.
5. In **Edit <profile-name>**, ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab.
6. Under **Security**, for the **Enterprise** security level, select the preferred option from **Key Management**.
7. To terminate the EAP portion of 802.1X authentication on the Instant AP instead of the RADIUS server, set **Termination** to **Enabled**.
For 802.1X authorization, by default, the client conducts an EAP exchange with the RADIUS server, and the AP acts as a relay for this exchange. When **Termination** is enabled, the Instant AP itself acts as an authentication server, terminates the outer layers of the EAP protocol, and only relays the innermost layer to the external RADIUS server.
8. Specify the type of authentication server to use.
9. Click **Save Settings**.


MAC Authentication

MAC authentication is used for authenticating devices based on their physical MAC addresses. MAC authentication requires that the MAC address of a machine matches a manually defined list of addresses. This authentication method is not recommended for scalable networks and the networks that require stringent security settings.

MAC authentication can be used alone or it can be combined with other forms of authentication such as WEP authentication.

Configuring MAC Authentication for a Network Profile

To configure MAC authentication for a wireless profile, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS** tab, select a network profile for which you want to enable MAC authentication and click **Edit**.
5. In the **Edit <profile-name>**, ensure that all required WLAN and VLAN attributes are defined, and then click the **Security** tab.
6. In **Security**, for **MAC Authentication**, select **Enabled** for **Personal** or **Open** security level.
7. Specify the type of authentication server to use.
8. Click **Save Settings**.

MAC Authentication with 802.1X Authentication

The administrators can enable MAC authentication for 802.1X authentication. MAC authentication shares all the authentication server configurations with 802.1X authentication. If a wireless or wired client connects to the network, MAC authentication is performed first. If MAC authentication fails, 802.1X authentication does not trigger. If MAC authentication is successful, 802.1X authentication is attempted. If 802.1X authentication is successful, the client is assigned an 802.1X authentication role. If 802.1X authentication fails, the client is assigned a **deny-all** role or **mac-auth-only** role.

You can also configure the following authentication parameters for MAC+802.1X authentication:


- **MAC authentication only role**—Allows you to create a **mac-auth-only** role to allow role-based access rules when MAC authentication is enabled for 802.1X authentication. The **mac-auth-only** role is assigned to a

client when the MAC authentication is successful and 802.1X authentication fails. If 802.1X authentication is successful, the **mac-auth-only** role is overwritten by the final role. The **mac-auth-only** role is primarily used for wired clients.

- L2 authentication fall-through—Allows you to enable the **I2-authentication-fallthrough** mode. When this option is enabled, the 802.1X authentication is allowed even if the MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. The **I2-authentication-fallthrough** mode is disabled by default.

Configuring MAC Authentication with 802.1X Authentication

To configure MAC authentication with 802.1X authentication for wireless network profile, configure the following parameters:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. In the **WLANS** tab, select a network profile for which you want to enable MAC and 802.1X authentication and click **Edit**.
5. Click **Security**.
6. Select **Perform MAC Authentication Before 802.1X** to use 802.1X authentication only when the MAC authentication is successful.
7. Select **MAC Authentication Fail Through** to use 802.1X authentication even when the MAC authentication fails.
8. Click **Save Settings**.

Captive Portal Authentication

Captive portal authentication is used for authenticating guest users. For more information, see [Configuring Wireless Networks on Guest Users on Instant APs on page 313](#).

MAC Authentication with Captive Portal Authentication

The following conditions apply to a network profile with MAC authentication and Captive Portal authentication enabled:

- If the captive portal splash page type is **Internal-Authenticated** or **External-RADIUS Server**, MAC authentication reuses the server configurations.
- If the captive portal splash page type is **Internal-Acknowledged** or **External-Authentication Text** and MAC authentication is enabled, a server configuration page is displayed.
- If the captive portal splash page type is **none**, MAC authentication is disabled.

The MAC authentication with captive portal authentication supports the **mac-auth-only** role.

Configuring MAC Authentication with Captive Portal Authentication

To configure the MAC authentication with captive portal authentication for a network profile, complete the following steps:

1. Select an existing wireless profile for which you want to enable MAC with captive portal authentication.
2. Under **Access**, specify the following parameters for a network with **Role Based** rules:
 - a. Select **Enforce Machine Authentication** when MAC authentication is enabled for captive portal. If the MAC authentication fails, the captive portal authentication role is assigned to the client.

b. For wireless network profile, select **Enforce MAC Auth Only Role** when MAC authentication is enabled for captive portal. After successful MAC authentication, the **MAC auth only** role is assigned to the client.

3. Click **Next** and then click **Save Settings**.

802.1X Authentication with Captive Portal Authentication

This authentication method allows you to configure different captive portal settings for clients on the same SSID. For example, you can configure an 802.1X SSID and create a role for captive portal access, so that some of the clients using the SSID derive the captive portal role. You can configure rules to indicate access to external or internal Captive portal, or none.

For more information on configuring captive portal roles for an SSID with 802.1X authentication, see [Configuring Wireless Networks on Guest Users on Instant APs on page 313](#).

WISPr Authentication

WISPr authentication allows a smart client to authenticate on the network when they roam between wireless Internet service providers, even if the wireless hotspot uses an ISP with whom the client may not have an account.

If a hotspot is configured to use WISPr authentication in a specific ISP and a client attempts to access the Internet at that hotspot, the WISPr AAA server configured for the ISP authenticates the client directly and allows the client to access the network. If the client only has an account with a *partner* ISP, the WISPr AAA server forwards the client's credentials to the partner ISP's WISPr AAA server for authentication. When the client is authenticated on the partner ISP, it is also authenticated on your hotspot's own ISP as per their service agreements. The Instant AP assigns the default WISPr user role to the client when your ISP sends an authentication message to the Instant AP.


Instant APs support the following smart clients:

- iPass
- Boingo

These smart clients enable client authentication and roaming between hotspots by embedding iPass Generic Interface Specification (GIS) *redirect*, *authentication*, and *logoff* messages within HTML messages that are sent to the Instant AP.

Configuring WISPr Authentication

To configure WISPr authentication, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Under **WISPr**, configure the following parameters:
 - **ISO Country Code**—The ISO Country Code for the WISPr Location ID.
 - **E.164 Area Code**—The E.164 Area Code for the WISPr Location ID.
 - **Operator Name**—The operator name of the hotspot.
 - **E.164 Country Code**—The E.164 Country Code for the WISPr Location ID.
 - **SSID/Zone**—The SSID/Zone for the WISPr Location ID.
 - **Location Name**—Name of the hotspot location. If no name is defined, the name of the Instant AP, to which the user is associated, is used.

7. Click **Save Settings**.

The WISPr RADIUS attributes and configuration parameters are specific to the RADIUS server used by your ISP for the WISPr authentication. Contact your ISP to determine these values. You can find a list of ISO and ITU country and area codes at the ISO and ITU websites (www.iso.org and <http://www.itu.int>).



A Boingo smart client uses a NAS identifier in the format <CarrierID>_<VenueID> for location identification. To support Boingo clients, ensure that you configure the NAS identifier parameter in the RADIUS server profile for the WISPr server.

Walled Garden


On the Internet, a walled garden typically controls access to web content and services. The Walled garden access is required when an external captive portal is used. For example, a hotel environment where the unauthenticated users are allowed to navigate to a designated login page (for example, a hotel website) and all its contents.

The users who do not sign up for the Internet service can view the allowed websites (typically hotel property websites). The website names must be DNS-based and support the option to define wildcards. When a user attempts to navigate to other websites that are not in the whitelist of the walled garden profile, the user is redirected to the login page. Instant AP supports Walled Garden only for the HTTP requests. For example, if you add yahoo.com in Walled Garden whitelist and the client sends an HTTPS request (<https://yahoo.com>), the requested page is not displayed and the users are redirected to the captive portal login page.

In addition, a blacklisted walled garden profile can also be configured to explicitly block the unauthenticated users from accessing some websites.

Configuring Walled Garden Access

To configure walled garden access, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Walled Garden**.
7. To allow access to a specific set of websites, create a whitelist, click + and add the domain names. This allows access to a domain while the user remains unauthenticated. Specify a POSIX regular expression (regex(7)). For example:
 - yahoo.com matches various domains such as news.yahoo.com, travel.yahoo.com and finance.yahoo.com
 - www.apple.com/library/test is a subset of www.apple.com site corresponding to path /library/test/*
 - favicon.ico allows access to /favicon.ico from all domains.
8. To deny users access to a domain, click + under Blacklist, and enter the domain name in the window. This prevents the unauthenticated users from viewing specific websites. When a URL specified in the blacklist is accessed by an unauthenticated user, Instant AP sends an HTTP 403 response to the client with an error message.
9. Click **Save**.

Support for Multiple PSK in WLAN SSID

Aruba Central allows you to configure multiple PSK (MPSK) in WLAN network profiles that include APs running a minimum of Aruba Instant 8.4.0.0 firmware version and later. MPSK enhances the WPA2 PSK mode by allowing device-specific or group-specific passphrases, which are generated by ClearPass Policy Manager and sent to the Instant AP.

WPA2 PSK-based deployments generally consist of a single passphrase configured as part of the WLAN SSID profile. This single passphrase is applicable for all clients that associate with the SSID. Starting from Aruba Instant 8.4.0.0, multiple PSKs in conjunction with ClearPass Policy Manager are supported for WPA and WPA2 PSK-based deployments. Every client connected to the WLAN SSID can have its own unique PSK.

A MPSK passphrase requires MAC authentication against a ClearPass Policy Manager server. The MPSK passphrase works only with wpa2-psk-aes encryption and not with any other PSK-based encryption. The Aruba-MPSK-Passphrase radius VSA is added and the ClearPass Policy Manager server populates this VSA with the encrypted passphrase for the device.

The workflow is as follows:

1. A user registers the device on a ClearPass Policy Manager guest-registration or device-registration webpage and receives a device-specific or group-specific passphrase.
2. The device associates with the SSID using wpa2-psk-aes encryption and uses MPSK passphrase.
3. The Instant AP performs MAC authentication of the client against the ClearPass Policy Manager server. On successful MAC authentication, the ClearPass Policy Manager returns Access-Accept with the VSA containing the encrypted passphrase.
4. The Instant AP generates a PSK from the passphrase and performs 4-way key exchange.
5. If the device uses the correct per-device or per-group passphrase, authentication succeeds. If the ClearPass Policy Manager server returns Access-Reject or the client uses incorrect passphrase, authentication fails.
6. The Instant AP stores the MPSK passphrase in its local cache for client roaming. The cache is shared between all the Instant APs within a single cluster. The cache can also be shared with standalone Instant APs in a different cluster provided the APs belong to the same multicast VLAN. Each Instant AP first searches the local cache for the MPSK information. If the local cache has the corresponding MPSK passphrase, the Instant AP skips the MAC authentication procedure, and provides access to the client.



When multiple PSK is enabled on the wireless SSID profile, make sure that MAC authentication is not configured for RADIUS authentication. Multiple PSK and MAC authentication are mutually exclusive and follows a special procedure which does not require enabling MAC authentication in the WLAN SSID manually. Also, ensure that the RADIUS server configured for the wireless SSID profile is not an internal server.


Points to Remember

The following configurations are mutually exclusive with MPSK for the WLAN SSID profile and does not require to be configured manually:

- MPSK and MAC authentication
- MPSK and Blacklisting
- MPSK and internal RADIUS server

Configuring Multiple PSK for Wireless Networks

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.

3. Click the  configuration icon to display the AP configuration page.
1. Go to **WLANS > Add SSID**.
 2. To modify an existing profile, go to **WLANS** to select a wireless SSID from the list of networks that is required to be edited.
 3. Click the **Security** tab.
 4. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
 5. From the **Key Management** drop-down list, select the **MPSK-AES** option.
 6. From the **Primary Server** drop-down list, select a server. The radius server selected from the list is the CPPM server.
 7. Click **Next** to complete the encryption configuration.

WPA3 Encryption

Aruba Central supports WPA3 encryption for security profiles in SSID creation for networks that include APs running Aruba Instant 8.4.0.0 firmware version and above. The WPA3 security provides robust protection with unique encryption per user session thereby ensuring a highly secured connection even on a public Wi-Fi hotspot.

The following are the WPA3 encryptions based on the **Enterprise**, **Personal**, or **Open** network types:

- **WPA-3 Personal** when the security level is **Personal**.
- **Enhanced Open** when the security level is **Open**.

When you select WPA3 as the encryption option in the **Key Management**, the **WPA3 Transition** option is displayed in the **Advanced Settings** section. Enable this option to allow transition from WPA3 to WPA2 and vice versa.

WPA3-Enterprise

WPA3-Enterprise enforces top secret security standards for an enterprise Wi-Fi in comparison to secret security standards. Top secret security standards includes:

- Deriving at least 384-bit PMK/MSK using Suite B compatible EAP-TLS.
- Securing pairwise data between STA and authenticator using AES-GCM-256.
- Securing group addressed data between STA and authenticator using AES-GCM-256.
- Securing group addressed management frames using BIP-GMAC-256.




Aruba Instant supports WPA3-Enterprise only in non-termination 802.1X and tunnel-forward modes. WPA3-Enterprise compatible 802.1x authentication occurs between STA and CPPM.

WPA3-Enterprise advertises or negotiates the following capabilities in beacons, probes response, or 802.11 association:

- AKM Suite Selector as 00-0F-AC:12
- Pairwise Cipher Suite Selector as 00-0F-AC:9
- Group data cipher suite selector as 00-0F-AC:9
- Group management cipher suite (MFP) selector as 00-0F-AC:12

If WPA3-Enterprise is enabled, STA is successfully associated only if it uses one of the four suite selectors for AKM selection, pairwise data protection, group data protection, and group management protection. If a STA mismatches any one of the four suite selectors, the STA association fails.

Configuring WPA3 for Enterprise Security for Wireless Network

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
 1. Go to **WLANS > +Add SSID**.
 2. To modify an existing profile, go to **WLANS** to select a wireless SSID from the list of networks that is required to be edited.
 3. Click the **Security** tab.
 4. Select **Enterprise** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
 5. Select one of the following from the Key Management drop-down list:
 - **WPA-3 Enterprise(GCM 256)**—Select this option to use WPA-3 security employing GCM encryption operation mode limited to encrypting 256 bits of plain text.
 - **WPA-3 Enterprise(CCM 128)**—Select this option to use WPA-3 security employing CCM encryption operation mode limited to encrypting 128 bits of plain text.
 6. Click **Next**.

Configuring WPA3 for Personal Security

1. Go to the **WLANS** and click **+**.
2. To modify an existing profile, in the **WLANS** page, select a WLAN SSID from the list of networks to edit.
3. Click the **Security** tab.
4. Select **Personal** from the **Security Level**. The authentication options applicable to the Enterprise network are displayed.
5. Select **WPA-3 Personal** from the **Key Management** drop-down list.
6. Click **Next**.

Authentication Servers for Instant APs

Based on the security requirements, you can configure internal or external RADIUS servers. This section describes the types of authentication servers and authentication termination, that can be configured for a network profile:

External RADIUS Server

In the external RADIUS server, the IP address of the VC is configured as the NAS IP address. Aruba Central RADIUS is implemented on the VC, and this eliminates the need to configure multiple NAS clients for every Instant AP on the RADIUS server for client authentication. Aruba Central RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable an external RADIUS server for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Aruba Central supports the following external authentication servers:

- RADIUS
- LDAP

To use an LDAP server for user authentication, configure the LDAP server on the VC, and configure user IDs and passwords.

To use a RADIUS server for user authentication, configure the RADIUS server on the VC.

RADIUS Server Authentication with VSA

An external RADIUS server authenticates network users and returns to the Instant AP the VSA that contains the name of the network role for the user. The authenticated user is placed into the management role specified by the VSA.

Internal RADIUS Server

Each Instant AP has an instance of free RADIUS server operating locally. When you enable the internal RADIUS server option for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The internal RADIUS server listens and replies to the RADIUS packet.

The following authentication methods are supported in the Aruba Central network:

- **EAP-TLS**—The EAP-TLS method supports the termination of EAP-TLS security using the internal RADIUS server. The EAP-TLS requires both server and CA certificates installed on the Instant AP. The client certificate is verified on the virtual controller (the client certificate must be signed by a known CA), before the username is verified on the authentication server.
- **EAP-TTLS (MSCHAPv2)**—The EAP-TTLS method uses server-side certificates to set up authentication between clients and servers. However, the actual authentication is performed using passwords.
- **EAP-PEAP (MSCHAPv2)**—EAP-PEAP is an 802.1X authentication method that uses server-side public key certificates to authenticate clients with server. The PEAP authentication creates an encrypted SSL / TLS tunnel between the client and the authentication server. Exchange of information is encrypted and stored in the tunnel ensuring the user credentials are kept secure.
- **LEAP**—LEAP uses dynamic WEP keys for authentication between the client and authentication server.

To use the internal database of an AP for user authentication, add the names and passwords of the users to be authenticated.



Aruba does not recommend the use of LEAP authentication because it does not provide any resistance to network attacks.

Authentication Termination on Instant AP

Aruba Central allows EAP termination for PEAP-Generic Token Card (PEAP-GTC) and Protected Extensible Authentication Protocol-Microsoft Challenge Authentication Protocol version 2 (PEAP-MSCHAPv2). PEAP-GTC termination allows authorization against an LDAP server and external RADIUS server while PEAP-MSCHAPv2 allows authorization against an external RADIUS server.

This allows the users to run PEAP-GTC termination with their username and password to a local Microsoft Active Directory server with LDAP authentication.

- **EAP-GTC**—This EAP method permits the transfer of unencrypted usernames and passwords from client to server. The EAP-GTC is mainly used for one-time token cards such as SecureID and the use of LDAP or RADIUS as the user authentication server. You can also enable caching of user credentials on the Instant AP to an external authentication server for user data backup.
- **EAP-MSCHAPv2**—This EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the back-end authentication server.

Dynamic Load Balancing between Authentication Servers

You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the Instant APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP.

The load balancing in Instant AP is performed based on the outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across asymmetric capacity RADIUS servers without the need to obtain inputs about the server capabilities from the administrators.

Configuring External Authentication Servers for APs

You can configure an external RADIUS server, TACACS, and LDAP server for user authentication. You can configure guest network using External Captive Portal profile for external authentication.

To configure a server, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. In the **Authentication Server** panel, click + to create a new server.
7. Select any of the following server types and configure the parameters for your deployment scenario.
8. Click **Save**.

Table 105: Authentication Server Configuration

| Type of Server | Parameters |
|----------------|---|
| RADIUS | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ Name—Name of the external RADIUS server. ■ IP Address— IP address or the FQDN of the external RADIUS server. ■ Auth Port—Authorization port number of the external RADIUS server. The default port number is 1812. ■ Accounting Port—The accounting port number used for sending accounting records to the RADIUS server. The default port number is 1813. ■ Shared Key and Retype Shared Key—Shared key for communicating with the external RADIUS server. ■ Timeout—The timeout duration for one RADIUS request. The Instant AP retries sending the request several times (as configured in the Retry count) before the user is disconnected. For example, if the Timeout is 5 seconds, Retry counter is 3, user is disconnected after 20 seconds. The default value is 5 seconds. ■ Retry Count—The maximum number of authentication requests that can be sent to the server group by the Instant AP. You can specify a value within the range of 1–5. The default value is 3 requests. ■ Dynamic Authorization—To allow the APs to process RFC 3576-compliant CoA and disconnect messages from the RADIUS server, select this check box. Disconnect messages terminate the user session immediately, whereas the CoA messages modify session authorization attributes such as data filters. When you enable the Dynamic Authorization option, the AirGroup CoA Port field is displayed with the port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999. ■ NAS IP Address—Enter the IP address. <ul style="list-style-type: none"> ● For Instant AP-based cluster deployments, ensure that you enter the VC IP address as the NAS IP address. ■ NAS Identifier—Use this to configure strings for RADIUS attribute 32, NAS Identifier, to be sent with RADIUS requests to the RADIUS server. ■ Dead Time—Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the Instant AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable. ■ If Dynamic RADIUS Proxy (DRP) is enabled on the APs, configure the following parameters: <ul style="list-style-type: none"> ● DRP IP—IP address to be used as source IP for RADIUS packets. ● DRP MASK—Subnet mask of the DRP IP address. ● DRP VLAN—VLAN in which the RADIUS packets are sent. ● DRP GATEWAY—Gateway IP address of the DRP VLAN. ■ Service Type Framed User—Select any of the following check boxes to send the service type as Framed User in the access requests to the RADIUS server: <ul style="list-style-type: none"> ● 802.1X ● MAC ● Captive Portal ■ Query Status of RADIUS Servers (RFC 5997) <ul style="list-style-type: none"> ● Authentication ● Accounting ■ Accounting Port |
| LDAP | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ Name—Name of the LDAP server ■ IP Address—IP address of the LDAP server ■ Auth Port—Authorization port number of the LDAP server. The default port number is 389. ■ Admin-DN—A distinguished name for the admin user with read and search privileges across all the entries in the LDAP database (the admin user need not have write privileges, but the admin user must be able to search the database, and read attributes of other users in the database). ■ Admin Password and Retype Admin Password—Password for the admin user. ■ Base-DN— Distinguished name for the node that contains the entire user database. |

| Type of Server | Parameters |
|-------------------------|--|
| | <ul style="list-style-type: none"> ■ Filter—The filter to apply when searching for a user in the LDAP database. The default filter string is (objectclass=*). ■ Key Attribute—The attribute to use as a key while searching for the LDAP server. For Active Directory, the value is sAMAccountName. ■ Timeout—Timeout interval within a range of 1–30 seconds for one RADIUS request. The default value is 5. ■ Retry Count—The maximum number of authentication requests that can be sent to the server group. You can specify a value within the range of 1–5. The default value is 3. |
| TACACS | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ Name—Name of the server. ■ Shared Key and Retype Key—The secret key to authenticate communication between the TACACS client and server. ■ Auth Port—The TCP IP port used by the server. The default port number is 49. ■ Timeout—A number between 1 and 30 seconds to indicate the timeout period for TACACS+ requests. The default value is 20 seconds. ■ IP Address—IP address of the server. ■ Retry Count—The maximum number of authentication attempts to be allowed. The default value is 3. ■ Dead Time (in mins)—Specify a dead time for authentication server in minutes. When two or more authentication servers are configured on the AP and a server is unavailable, the dead time configuration determines the duration for which the authentication server is available if the server is marked as unavailable. ■ Session Authorization—Enable this option to allow the authorization of sessions. |
| External Captive Portal | <p>The external captive portal servers are used for authenticating guest users in a WLAN. To create a external captive portal splash page profile, configure the following parameters.</p> <ul style="list-style-type: none"> ■ Name—Enter a name for the profile. ■ Type—Select any one of the following types of authentication: <ul style="list-style-type: none"> ● Radius Authentication—Select this option to enable user authentication against a RADIUS server. ● Authentication Text—Select this option to specify an authentication text. The specified text will be returned by the external server after a successful user authentication. ■ IP or Hostname—Enter the IP address or the host name of the external splash page server. ■ URL—Enter the URL of the external captive portal server. ■ Port—Enter the port number that is used for communicating with the external captive portal server. ■ Use HTTPS—Select this to enforce clients to use HTTPS to communicate with the captive portal server. This option is available only if RADIUS Authentication is selected. ■ Captive Portal Failure—This field allows you to configure Internet access for the guest users when the external captive portal server is not available. Select Deny Internet to prevent guest users from using the network, or Allow Internet to access the network. ■ Server Offload—Select the check box to enable the server offload feature. The server offload feature ensures that the non-browser client applications are not unnecessarily redirected to the external captive portal server, thereby reducing the load on the external captive portal server. ■ Prevent Frame Overlay—Select this check box to prevent the overlay of frames. When enabled, the frames display only those pages that are in the same domain as the main page. ■ Automatic URL Whitelisting—On enabling this for the external captive portal authentication, the URLs that are allowed for the unauthenticated users to access are automatically whitelisted. ■ Auth Text—If the External Authentication splash page is selected, specify the authentication text that is returned by the external server after successful authentication. This option is available only if Authentication Text is selected. ■ Redirect URL—Specify a redirect URL if you want to redirect the users to another URL. |

| Type of Server | Parameters |
|-----------------------------------|--|
| Dynamic Authorization Only | <p>Configure the following parameters:</p> <ul style="list-style-type: none"> ■ Name—Name of the server. ■ IP Address—IP address of the server. ■ AirGroup CoA Port—A port number for sending Bonjour support CoA on a different port than on the standard CoA port. The default value is 5999. ■ Shared Key and Retype Key—A shared key for communicating with the external RADIUS server. <p>Change of Authorization(CoA) is a subset of Dynamic Authorization include disconnecting messages.</p> |

9. Click **Save Server**.

To assign the authentication server to a network profile, select the newly added server when configuring security settings for a wireless or wired network profile.



You can also add an external RADIUS server when configuring a WLAN SSID profile.

Configuring Users Accounts for the Instant AP Management Interface

You can configure RADIUS or TACACS authentication servers to authenticate and authorize the management users of an Instant AP. The authentication servers determine if the user has access to administrative interface. The privilege level for different types of management users is defined on the RADIUS or TACACS server. The Instant APs map the management users to the corresponding privilege level and provide access to the users based on the attributes returned by the RADIUS or TACACS server.



In Aruba Central, the Instant AP management user passwords are stored and displayed as hash instead of plain text. The **hash-mgmt-user** command is enabled by default on the Instant APs provisioned in the template and UI groups. If a pre-configured Instant AP joins Aruba Central and is moved to a new group, Aruba Central uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the Instant AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an Instant AP.

To configure authentication parameters for local admin, read-only, and guest management administrator account settings, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Under **Administrator**, configure the following parameters:

Table 106: *Configuration Parameters for the Instant AP Users*

| Type of the User | Authentication Options | Steps to Follow |
|--------------------------------|--|--|
| Client Control | Internal | Select Internal if you want to specify a single set of user credentials. If using an internal authentication server: 1. Enter a Username and Password . 2. Retype the password to confirm. |
| | Authentication server | Select the RADIUS or TACACS authentication servers. You can also create a new server by selecting New from the Authentication server drop-down list. |
| | Authentication server w/ fallback to internal | Select Authentication server w/ fallback to internal option if you want to use both internal and external servers. When enabled, the authentication switches to Internal if there is no response from the RADIUS server (RADIUS server timeout). To use this option, select the authentication servers and configure the user credentials (username and password) for internal server based authentication. |
| | Load Balancing | If two servers are configured, the users can use them in the primary or backup mode, or load balancing mode. To enable load balancing, select Enabled from the Load balancing drop-down list. For more information on load balancing, see Dynamic Load Balancing between Authentication Servers on page 356 . |
| | TACACS accounting | If a TACACS server is selected, enable TACACS accounting to report management commands if required. |
| View Only | | To configure a user account with the read-only privileges: 1. Specify a Username and Password . 2. Retype the password to confirm. |
| Guest Registration Only | | To configure a guest user account with the read-only privileges: 1. Specify the Username and Password . 2. Retype the password to confirm. |

3. Click **Save Settings**.

Configuring Guest and Employee User Profiles on Instant APs

The local database of an Instant AP consists of a list of guest and employee users. The addition of a user involves specifying a login credentials for a user. The login credentials for these users are provided outside the Aruba Central system.

A guest user can be a visitor who is temporarily using the enterprise network to access the Internet. However, if you do not want to allow access to the internal network and the Intranet, you can segregate the guest traffic from the enterprise traffic by creating a guest WLAN and specifying the required authentication, encryption, and access rules.


An employee user is the employee who is using the enterprise network for official tasks. You can create Employee WLANs, specify the required authentication, encryption and access rules and allow the employees to use the enterprise network.

The user database is also used when an Instant AP is configured as an internal RADIUS server.

The local user database of APs can support up to 512 user entries except IAP-92/93. IAP-92/93 supports only 256 user entries. If there are already 512 users, IAP-92/93 will not be able to join the cluster.



To configure users, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Users for Internal Server**.
7. Enter the username in the **Username** text box.
8. Enter the password in the **Password** text box and reconfirm.
9. Select a type of user from the **Type** drop-down list.
10. Click **Add** and click **OK**. The users are listed in the **Users** list.
11. To edit user settings:
 - a. Select the user to modify under **Users**
 - b. Click **Edit** to modify user settings.
 - c. Click **OK**.
12. To delete a user:
 - a. In the **Users** section, select the username to delete
 - b. Click **Delete**.
 - c. Click **OK**.
13. To delete all or multiple users at a time:
 - a. Select the user names that you want to delete
 - b. Click **Delete All**.
 - c. Click **OK**.



Deleting a user only removes the user record from the user database, and will not disconnect the online user associated with the username.

Configuring Roles and Policies on Instant APs for User Access Control

Instant APs support identity-based access control to enforce application-layer security, prioritization, traffic forwarding, and network performance policies for wired and wireless networks. Using the Instant AP firewall policies, you can enforce network access policies to define access to the network, areas of the network that the user may access, and the performance thresholds of various applications.

Instant APs supports a role-based stateful firewall. In other words, Instant firewall can recognize flows in a network and keep track of the state of sessions. The firewall logs on the Instant APs are generated as syslog messages. The firewall feature also supports ALG functions such as SIP, Vocera, Alcatel NOE, and Cisco Skinny protocols.

ACL Rules

You can use ACL rules to either permit or deny data packets passing through the Instant AP. You can also limit packets or bandwidth available to a set of user roles by defining access rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses.

You can create access rules to allow or block data packets that match the criteria defined in an access rule. You can create rules for either inbound traffic or outbound traffic. Inbound rules explicitly allow or block the inbound network traffic that matches the criteria in the rule. Outbound rules explicitly allow or block the

network traffic that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to an IP address through the firewall.

The Instant AP clients are associated with user roles, which determine the client's network privileges and the frequency at which clients re-authenticate. Instant AP supports the following types of ACLs:

- ACLs that permit or deny traffic based on the source IP address of the packet.
- ACLs that permit or deny traffic based on source or destination IP address, or source or destination port number.



You can configure up to 64 access control rules for a firewall policy.

Configuring Network Address Translation Rules

NAT is the process of modifying network address information when packets pass through a routing device. The routing device acts as an agent between the public (the Internet) and private (local network), which allows translation of private network IP addresses to a public address space.


Instant AP supports the NAT mechanism to allow a routing device to use the translation tables to map the private addresses into a single IP address and packets are sent from this address, so that they appear to originate from the routing device. Similarly, if the packets are sent to the private IP address, the destination address is translated as per the information stored in the translation tables of the routing device.

For more information on roles and policies, see the following topics:

- [Configuring Network Service ACLs on page 362](#)
- [Configuring ACLs for Deep Packet Inspection](#)
- [Configuring User Roles for AP Clients on page 364](#)
- [Configuring Role Derivation Rules for AP Clients on page 365](#)
- [Configuring Firewall Parameters for Inbound Traffic on page 374](#)

Configuring Network Service ACLs

To configure access rules for network services, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Roles**.
7. Under **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The new rule window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To configure access to applications or application categories, select a service category from the following list:
 - **Network**
 - **Application Category**
 - **Application**
 - **Web Category**
 - **Web Reputation**

10. Based on the selected service category, configure the following parameters:

Table 107: Access rule configuration parameters

| Data Pane Item | Description |
|-------------------------|---|
| Rule Type | Select a rule type from the list, for example Access Control . |
| Service | <p>Select a service from the list of available services. You can allow or deny access to any or all of the following services based on your requirement:</p> <ul style="list-style-type: none"> ■ any—Access is allowed or denied to all services. ■ custom—Available options are TCP, UDP, and Other. If you select the TCP or UDP options, enter appropriate port numbers. If you select the Other option, enter the appropriate ID. <p>NOTE: If TCP and UDP uses the same port, ensure that you configure separate access rules to permit or deny access.</p> |
| Action | <p>Select any of following attributes:</p> <ul style="list-style-type: none"> ■ Select Allow to allow access users based on the access rule. ■ Select Deny to deny access to users based on the access rule. ■ Select Destination-NAT to allow the changes to destination IP address. ■ Select Source-NAT to allow changes to the source IP address. |
| Destination | <p>Select a destination option. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations — Access is allowed or denied to all destinations. ■ To a particular server — Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server — Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network — Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network — Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain Name — Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box. |
| Log | Select Log to create a log entry when this rule is triggered. The Aruba Central firewall supports firewall based logging. Firewall logs on the Instant APs are generated as security logs. |
| Blacklist | Select Blacklist to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as Auth failure blacklist time on the BLACKLISTING tab of the Security window. |
| Classify Media | <p>Select Classify Media to prioritize video and voice traffic. When enabled, a packet inspection is performed on all non-NAT traffic and the traffic is marked as follows:</p> <ul style="list-style-type: none"> ■ Video: Priority 5 (Critical) ■ Voice: Priority 6 (Internetwork Control) |
| Disable Scanning | Select Disable Scanning to disable ARM scanning when this rule is triggered. The selection of the Disable Scanning applies only if ARM scanning is enabled. |
| DSCP Tag | Select DSCP Tag to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0 to 63. |
| 802.1 priority | Select 802.1 priority to specify an 802.1 priority. Specify a value between 0 and 7. |
| Time Range | Select this check box to allow a specific user to access the network for a specific time range. You can select the time range profile from the drop-down list that appears when the Time Range check box is selected. |

11. Click **Save Settings**.


Configuring User Roles for AP Clients

Every client in the Aruba Central network is associated with a user role, which determines the client's network privileges, the frequency of re-authentication, and the applicable bandwidth contracts. The user role configuration on an Instant AP involves the following procedures:

- [Creating a User Role on page 364](#)
- [Assigning Bandwidth Contracts to User Roles on page 364](#)

Creating a User Role

To create a user role, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Roles**. The **Roles** pane contents are displayed.
7. Under **Roles**, click **New**.
8. Enter a name for the new role and click **OK**.



You can also create a user role when configuring wireless profile. For more information, see [Configuring ACLs for User Access to a Wireless Network on page 311](#).

Assigning Bandwidth Contracts to User Roles

The administrators can manage bandwidth utilization by assigning maximum bandwidth rates, or bandwidth contracts to user roles. The administrator can assign a bandwidth contract configured in Kbps to upstream (client to the Instant AP) or downstream (Instant AP to clients) traffic for a user role. The bandwidth contract will not be applicable to the user traffic on the bridged out (same subnet) destinations. For example, if clients are connected to an SSID, you can restrict the upstream bandwidth rate allowed for each user to 512 Kbps.

By default, all users that belong to the same role share a configured bandwidth rate for upstream or downstream traffic. The assigned bandwidth will be served and shared among all the users. You can also assign bandwidth per user to provide every user a specific bandwidth within a range of 1 to 65535 Kbps. If there is no bandwidth contract specified for a traffic direction, unlimited bandwidth is allowed.

To assign bandwidth contracts to a user role:

1. Select **Configuration > Wireless > Security**. The **Security** pane contents are displayed.
2. Click **Roles**. The **Roles** pane contents are displayed.
3. [Create a new role](#) or select an existing role.
4. Under **Access Rules For Selected Roles**, click **(+)**.
5. Select **Bandwidth Contract** under **Rule-Type**.
6. Specify the downstream and upstream rates in Kbps. If the assignment is specific for each user, select **Peruser**.
7. Click **Save**.
8. Associate the user role to a WLAN SSID or wired profile.

You can also create a user role and assign bandwidth contracts while configuring an SSID.

Configuring Role Derivation Rules for AP Clients

Aruba Central allows you to configure role and VLAN derivation-rules. You can configure these rules to assign a user role or VLAN to the clients connecting to an SSID or a wired profile.


Creating a Role Derivation Rule

You can configure rules for determining the role that is assigned for each authenticated client.



When creating more than one role assignment rule, the first matching rule in the rule list is applied.


To create a role assignment rule, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  settings icon to display the AP configuration page.
4. In the **WLANS** tab, select a network profile and click **Edit**.
5. Under **Access**, set the slider to **Role Based**.
6. Under **Role Assignment Rules**, click **New**. In **New Role Assignment Rule**, define a match method by which the string in *Operand* is matched with the attribute value returned by the authentication server.
7. Select the attribute from the **Attribute** list that the rule it matches against. The list of supported attributes includes RADIUS attributes, dhcp-option, dot1x-authentication-type, mac-address, and mac-address-and-dhcp-options.
8. Select the operator from the **Operator** list. The following types of operators are supported:
 - **contains**— The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **Is the role**— The rule is applied if the attribute value is the role.
 - **equals**— The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**— The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**— The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**— The rule is applied only if the attribute value ends with string specified in *Operand*.
 - **matches-regular-expression**— The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for WLAN clients.
9. Enter the string to match in the **String** box.
10. Select the appropriate role from the **Role** list.
11. Click **Save**.

Configuring VLAN Assignment Rule

To configure VLAN assignment rules for an SSID profile:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:

- a. Under **Manage**, click **Devices > Access Points**.
- b. Click the configuration  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. In the **WLANS** tab, to create a new SSID profile, click **+ Add SSID**. The **Create a New Network** pane display.
5. Click **+Add SSID** to create a new network profile or click the edit icon corresponding to the network profile that is required to be modified.
6. Perform the configurations in the **General**, **VLAN**, and **Security** tab.
7. Click **Next**. The **Access** tab is displayed.
8. Select the access rule from **Access Rules**.
9. In the **Access Rules For Selected Roles**, click **+ Add Rule** to add a new rule. The **Access Rule** page is displayed.




The **VLAN Assignment** option is also listed in the **Access Rule** page when you create or edit a rule for wired port profiles in the **Ports > Create a New Network > Access** tab.

10. From the **Rule Type** drop-down list, select **VLAN Assignment** option.
11. Enter the VLAN ID in the **VLAN ID** field under **Service** section. Alternatively, you can select the VLAN ID or the VLAN name from the drop-down list provided next to the VLAN ID field.
12. Click **Save**.

Configuring VLAN Derivation Rules

The users are assigned to a VLAN based on the attributes returned by the RADIUS server after users authenticate.


To configure VLAN derivation rules for an SSID profile:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - c. Under **Manage**, click **Devices > Access Points**.
 - d. Click the settings  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. In the **WLANS** tab, select a network profile and click **Edit**.
5. Under **VLAN**, select **Dynamic** under **Client VLAN Assignment**.
6. Click **New** to create a VLAN assignment rule. The **New VLAN Assignment Rule** window is displayed. In this window, you can define a match method by which the string in *Operand* is matched with the attribute values returned by the authentication server.
7. Select an attribute from the **Attribute** list.
8. Select an operator from the **Operator** list. The following types of operators are supported:
 - **contains**—The rule is applied only if the attribute value contains the string specified in *Operand*.
 - **equals**—The rule is applied only if the attribute value is equal to the string specified in *Operand*.
 - **not-equals**—The rule is applied only if the attribute value is not equal to the string specified in *Operand*.
 - **starts-with**—The rule is applied only if the attribute value starts with the string specified in *Operand*.
 - **ends-with**—The rule is applied only if the attribute value ends with string specified in *Operand*.

- **matches-regular-expression** — The rule is applied only if the attribute value matches the regular expression pattern specified in *Operand*. This operator is available only if the **mac-address-and-dhcp-options** attribute is selected in the **Attribute** list. The **mac-address-and-dhcp-options** attribute and **matches-regular-expression** are applicable only for the WLAN clients.
9. Enter the string to match in the **String** field.
 10. Select the appropriate VLAN ID from **VLAN**.
 11. Ensure that all other required parameters are configured.
 12. Click **Save** to apply the changes.

Configuring Firewall Parameters for Wireless Network Protection

To configure firewall settings, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. In the **Application Layer Gateway (ALG) Algorithms** section, select **Enabled** from the corresponding drop-down lists to enable **SIP**, **VOCERA**, **Alcatel NOE**, and **Cisco Skinny** protocols.
9. In the **Protection Against Wired Attacks** section, set the following options to **Enabled** :
 - **Drop Bad ARP**—Drops the fake ARP packets.
 - **Fix Malformed DHCP**—Fixes the malformed DHCP packets.
 - **ARP Poison Check**—Triggers an alert on ARP poisoning caused by the rogue APs.

Configuring Firewall Parameters for Inbound Traffic

Instant APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an Instant AP. You can configure firewall rules for the inbound traffic in the **Security > Inbound Firewall** section.

To configure the firewall rules, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. In the **Access Rule** section, click the + icon. The **Inbound Firewall** page is displayed.
9. Perform the following in the **Inbound Firewall** page:

Table 108: Inbound Firewall Rule Configuration Parameters


| Parameter | Description |
|--------------------|--|
| Service | <p>Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement:</p> <ul style="list-style-type: none"> ■ Any—Access is allowed or denied to all services. ■ Custom—Customize the access based on available options such as TCP, UDP, and other options. If you select the TCP or UDP options, enter appropriate port numbers. If the Other option is selected, ensure that an appropriate ID is entered. |
| Action | <p>Select any of following actions:</p> <ul style="list-style-type: none"> ■ Select Allow to allow user access based on the access rule. ■ Select Deny to deny user access based on the access rule. ■ Select Destination-NAT to allow making changes to the destination IP address and the port. ■ Select Source-NAT to allow making changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules. |
| Source | <p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ From all sources—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ From a particular host—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. ■ From a network—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network. |
| Destination | <p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ To a particular server—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain name—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in |

| Parameter | Description |
|-------------------------|--|
| | the IP text box. |
| Log | Select the Log check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs. |
| Blacklist | Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the Auth failure blacklist time on the Blacklisting tab of the Security window. |
| Classify Media | Select the Classify Media check box to classify and tag media on https traffic as voice and video packets. |
| Disable scanning | Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of Disable scanning applies only if ARM scanning is enabled. |
| DSCP tag | Select the DSCP tag check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value. |
| 802.1p priority | Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value. |

Configuring Management Subnets

You can configure subnets to ensure that the Instant AP management is carried out only from these subnets. When the management subnets are configured, Telnet, SSH, and UI access is restricted to these subnets only.


To configure management subnets, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. To add a new management subnet, complete the following steps:
 - Enter the subnet address in **Subnet**.
 - Enter the subnet mask in **Mask**.
 - Click **Add**.
9. To add multiple subnets, repeat step 2.
10. Click **Save Settings**.

Configuring Restricted Access to Corporate Network

You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master Instant AP, including clients connected to a slave Instant AP.

To configure restricted corporate access, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click the **Wireless IDS/IPS** accordion.
7. Click **Firewall Settings**.
8. Enable **Restrict Corporate Access**.
9. Click **Save Settings**.

Disabling Auto Topology Rules

If the firewalls rules are configured, the **Auto Topology Rules** are enabled by default. When the inbound firewall settings are enabled:

- ACEs must be configured to block auto topology messages, as there is no default rule at the top of predefined ACLs.
- ACEs must be configured to override the guest VLAN auto-expanded ACEs. In other words, the user defined ACEs take higher precedence over guest VLAN ACEs.

To disable the auto topology rules, set **Auto Topology Rules** to **OFF**.

Configuring ACLs for Deep Packet Inspection

To configure ACL rules for a user role for Deep Packet Inspection (DPI), complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The **Access Rule** window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To configure access to applications or application categories, select a service category from the following list:
 - Network
 - App Category
 - Application
 - Web Category
 - Web Reputation
10. Based on the selected service category, configure the following parameters:

Table 109: Access Rule Configuration Parameters

| Service category | Description |
|-------------------------------|---|
| App Category | Select the application categories to which you want to allow or deny access. |
| Application | Select the applications to which you want to allow or deny access. |
| Application Throttling | <p>Application throttling allows you to set a bandwidth limit for an application and application categories. For example, you can limit the bandwidth rate for video streaming applications such as YouTube or Netflix, or assign a low bandwidth to high risk sites.</p> <p>To specify a bandwidth limit:</p> <ol style="list-style-type: none"> 1. Select the Application Throttling check box. 2. Specify the Downstream and Upstream rates in Kbps per user. |
| Action | <p>Select one of the following actions:</p> <ul style="list-style-type: none"> ■ Destination-NAT—Translation of the destination IP address of a packet entering the network. ■ Source-NAT—Used by internal users to access the internet. ■ Allow—Select Allow to allow access users based on the access rule. ■ Deny—Select Deny to deny access to users based on the access rule. |
| Destination | <p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations— Access is allowed or denied to all destinations. ■ To a particular server—Access is allowed or denied to a particular server. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Access is allowed or denied to a network. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain Name—Access is allowed or denied to the specified domains. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in the IP text box. |
| Log | Select this check box if you want a log entry to be created when this rule is triggered. Aruba Central supports firewall based logging. Firewall logs on the Instant APs are generated as security logs. |
| Blacklist | Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as Auth failure blacklist time on the Blacklisting tab of the Security window. . |
| Classify Media | Select the Classify Media check box to classify and tag media on https traffic as voice and video packets. |
| Disable Scanning | Select Disable Scanning check box to disable ARM scanning when this rule is triggered. The selection of the Disable Scanning applies only if ARM scanning is enabled. |

Table 109: Access Rule Configuration Parameters


| Service category | Description |
|------------------------|---|
| DSCP Tag | Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value. |
| 802.1p priority | Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value. |
| Time Range | Select this check box to enable user to access network for a specific time period. You can select the time range profile from the drop-down list that appears when the Time Range check box is selected.. |

3. Click **Save**.

Configuring ACLs on APs for Website Content Classification

You can configure web policy enforcement on an AP to block certain categories of websites based on your organization specifications by defining ACL rules.

To configure ACLs for website content classification, follow the below procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Roles**, select the role to modify.
7. Under **Access Rules For Selected Roles**, click **(+)** to add a new rule. The **Access Rule** window is displayed.
8. Under **Rule Type**, select **Access Control**.
9. To set an access policy based on web categories:
 - a. Under **Service**, select **Web Category**.
 - b. Select the categories to which you want to deny or allow access. You can also search for a web category and select the required option.
 - c. Under **Action**, select **Allow** or **Deny**.
 - d. Click **Save**.
10. To filter access based on the security ratings of the website:
 - a. Select **Web Reputation** under **Service**.
 - b. Move the slider to select a specific web reputation value to deny access to websites with a reputation value lower than or equal to the configured value or to permit access to websites with a reputation value higher than or equal to the configured value. The following options are available:
 - **Trustworthy WRI > 81**—These are well known sites with strong security practices and may not expose the user to security risks. There is a very low probability that the user will be exposed to malicious links or payloads.

- **Low Risk WRI 61-80**—These are benign sites and may not expose the user to security risks. There is a low probability that the user will be exposed to malicious links or payloads.
- **Moderate WRI 41-60**—These are generally benign sites, but may pose a security risk. There is some probability that the user will be exposed to malicious links or payloads.
- **Suspicious WRI 21-40**—These are suspicious sites. There is a higher than average probability that the user will be exposed to malicious links or payloads.
- **High Risk WRI < 20**—These are high risk sites. There is a high probability that the user will be exposed to malicious links or payloads.

c. Under **Action**, select **Allow** or **Deny** as required.

11. To set a bandwidth limit based on web category or web reputation score, select the **Application Throttling** check box and specify the downstream and upstream rates in Kbps. For example, you can set a higher bandwidth for trusted sites and a low bandwidth rate for high risk sites.

12. If required, select the following check boxes:

- **Log** — Select this check box if you want a log entry to be created when this rule is triggered. Aruba Central supports firewall based logging. Firewall logs on the Instant APs are generated as security logs.
- **Blacklist** — Select this check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified as **Auth Failure Blacklist Time** on the **Blacklisting** pane of the **Security** window. For more information, see [Blacklisting Instant AP Clients on page 377](#).
- **Disable Scanning**—Select **Disable scanning** check box to disable ARM scanning when this rule is triggered. The selection of the **Disable scanning** applies only if ARM scanning is enabled, For more information, see [Configuring Radio Parameters on page 342](#).
- **DSCP Tag**—Select this check box to add a DSCP tag to the rule. DSCP is an L3 mechanism for classifying and managing network traffic and providing QoS on the network. To assign a higher priority, specify a higher value.
- **802.1p priority**—Select this check box to enable 802.1p priority. 802.1p priority is an L2 protocol for traffic prioritization to manage QoS on the network. There are eight levels of priority, 0-7. To assign a higher priority, specify a higher value.

13. Click **Save** to save the rules.


14. Click **Save Settings** in the **Roles** pane to save the changes to the role for which you defined ACL rules.

Configuring Custom Redirection URLs for Instant AP Clients

You can create a list of URLs to redirect users to when they access blocked websites. You can define an access rule to use these redirect URLs and assign the rule to a user role in the WLAN network.


Creating a List of Error Page URLs

To create a list of error page URLs, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Custom Blocked Page URL**, click **+** and enter the URL to block.
7. Repeat the procedure to add more URLs. You can add up to 8 URLs to the list of blocked web pages.
8. Click **OK**.

Configuring ACL Rules to Redirect Users to a Specific URL

To configure ACL rules to redirect users to a specific URL, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click the **Security** tab.
6. Under **Roles**, select the role for which you want to configure access rules.
7. Click **+** in the Access Rules section. The **New Rule window** is displayed.
8. Select the rule type as **Blocked Page URL**.
9. Select the URLs from the existing list of custom redirect URLs. To add a new URL, click **+**.
10. Click **Save**.

Configuring Firewall Parameters for Inbound Traffic

Instant APs support an enhanced inbound firewall for the traffic that flows into the network through the uplink ports of an Instant AP. You can configure firewall rules for the inbound traffic in the **Security > Inbound Firewall** section.

To configure the firewall rules, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
 2. Under **Manage**, click **Devices > Access Points**.
 3. Click the  configuration icon to display the AP configuration page.
 4. Click **Show Advanced**.
 5. Click **Security**.
- The **Security** details for the selected group or the device are displayed.
6. Under **Wireless IDS/IPS**, click **Firewall Settings**.
 7. In the **Access Rule** section, click the **+** icon.
- The **Inbound Firewall** page is displayed.
8. Perform the following in the **Inbound Firewall** page:

Table 110: Inbound Firewall Rule Configuration Parameters

| Parameter | Description |
|--------------------|--|
| Service | <p>Select a service from the list of available services. You can allow or deny access to any or all of the services based on your requirement:</p> <ul style="list-style-type: none"> ■ Any—Access is allowed or denied to all services. ■ Custom—Customize the access based on available options such as TCP, UDP, and other options. If you select the TCP or UDP options, enter appropriate port numbers. If the Other option is selected, ensure that an appropriate ID is entered. |
| Action | <p>Select any of following actions:</p> <ul style="list-style-type: none"> ■ Select Allow to allow user access based on the access rule. ■ Select Deny to deny user access based on the access rule. ■ Select Destination-NAT to allow making changes to the destination IP address and the port. ■ Select Source-NAT to allow making changes to the source IP address. The destination NAT and source NAT actions apply only to the network services rules. |
| Source | <p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ From all sources—Traffic from all sources is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ From a particular host—Traffic from a particular host is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the host. ■ From a network—Traffic from a particular network is either allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask of the source network. |
| Destination | <p>Select a destination option for the access rules for network services, applications, and application categories. You can allow or deny access to any the following destinations based on your requirements.</p> <ul style="list-style-type: none"> ■ To all destinations—Traffic for all destinations is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. ■ To a particular server—Traffic to a specific server is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address of the destination server. ■ Except to a particular server—Access is allowed or denied to servers other than the specified server. After selecting this option, specify the IP address of the destination server. ■ To a network—Traffic to the specified network is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the IP address and netmask for the destination network. ■ Except to a network—Access is allowed or denied to networks other than the specified network. After selecting this option, specify the IP address and netmask of the destination network. ■ To a Domain name—Traffic to the specified domain is allowed, denied, or the IP address is translated at the source or the destination as defined in the rule. After selecting this option, specify the domain name in the Domain Name text box. ■ To AP IP—Traffic to the specified Instant AP is allowed. After selecting this option, specify the domain name in the IP text box. ■ To AP Network—Traffic to the specified Instant AP network is allowed. After selecting this option, specify the domain name in the IP text box. ■ To master IP—Traffic to the specified master Instant AP or virtual controller is allowed. After selecting this option, specify the domain name in |

| Parameter | Description |
|-------------------------|--|
| | the IP text box. |
| Log | Select the Log check box if you want a log entry to be created when this rule is triggered. Instant supports firewall-based logging function. Firewall logs on the Instant APs are generated as security logs. |
| Blacklist | Select the Blacklist check box to blacklist the client when this rule is triggered. The blacklisting lasts for the duration specified in the Auth failure blacklist time on the Blacklisting tab of the Security window. |
| Classify Media | Select the Classify Media check box to classify and tag media on https traffic as voice and video packets. |
| Disable scanning | Select Disable scanning check box to disable ARM scanning when this rule is triggered. The selection of Disable scanning applies only if ARM scanning is enabled. |
| DSCP tag | Select the DSCP tag check box to specify a DSCP value to prioritize traffic when this rule is triggered. Specify a value within the range of 0–63. To assign a higher priority, specify a higher value. |
| 802.1p priority | Select the 802.1p priority check box to specify an 802.1p priority. Specify a value between 0 and 7. To assign a higher priority, specify a higher value. |

9. Click **Ok**.

10. Click **Save Settings**.




For all subnets, a deny rule is created by default as the last rule. If at least one rule is configured, the deny all rule is applied to the upstream traffic by default..

The inbound firewall is not applied to traffic coming through the GRE tunnel.

Configuring Restricted Access to Corporate Network


You can configure restricted corporate access to block unauthorized users from accessing the corporate network. When restricted corporate access is enabled, corporate access is blocked from the uplink port of master Instant AP, including clients connected to a slave Instant AP.

To configure restricted corporate access, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Security**.
The **Security** page is displayed.
6. Under **Wireless IDS/IPS**, click **Firewall Settings**.
7. Enable **Restrict Corporate Access**.
8. Click **Save Settings**.

Enabling ALG Protocols on Instant APs

To configure protocols for ALG, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Firewall Settings**.
7. Under **Application Layer Gateway (ALG) Algorithms**, select **Enabled** against the corresponding protocol to enable SIP, VOCERA, ALCATEL NOE, and CISCO SKINNY protocols.
8. Click **Save Settings**.



When the protocols for the ALG are **Disabled** the changes do not take effect until the existing user sessions have expired. Reboot the Instant AP and the client, or wait a few minutes for changes to take effect.


Blacklisting Instant AP Clients

The client blacklisting denies connection to the blacklisted clients. When a client is blacklisted, it is not allowed to associate with an Instant AP in the network. If a client is connected to the network when it is blacklisted, a deauthentication message is sent to force client disconnection.

Blacklisting Clients Manually

Manual blacklisting adds the MAC address of a client to the blacklist. These clients are added into a permanent blacklist. These clients are not allowed to connect to the network unless they are removed from the blacklist.

To add a client to the blacklist manually:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Blacklisting**.
7. Click **+** and enter the MAC address of the client to be blacklisted.
8. Click **OK**.
9. Click **Save Settings**.



For the blacklisting to take effect, you must enable the blacklisting option when you create or edit the WLAN SSID profile. Go to **WLANs > Security > Advanced Settings** and enable the **Blacklisting** option. For more information, see [Configuring Wireless Network Profiles on Instant APs](#).

To delete a client from the manual blacklist, select the MAC Address of the client under the **Manual Blacklisting**, and then click **Delete**.


Blacklisting Clients Dynamically

The clients can be blacklisted dynamically when they exceed the authentication failure threshold or when a blacklisting rule is triggered as part of the authentication process.

When a client takes time to authenticate and exceeds the configured failure threshold, it is automatically blacklisted by an Instant AP.

In session firewall based blacklisting, an ACL rule automates blacklisting. When the ACL rule is triggered, it sends out blacklist information and the client is blacklisted.

To configure the blacklisting duration:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Blacklisting**.
7. Under **Dynamic Blacklisting**:
 - a. For **Auth Failure Blacklist Time**, enter the duration after which the clients that exceed the authentication failure threshold must be blacklisted.
 - b. For **PEF Rule Blacklisted Time**, enter the duration after which the clients can be blacklisted due to an ACL rule trigger.
8. Click **Save Settings**.

You can configure a maximum number of authentication failures by the clients, after which a client must be blacklisted. For more information on configuring maximum authentication failure attempts, see [Configuring Wireless Network Profiles on Instant APs on page 300](#).



To enable session-firewall-based blacklisting, select the **Blacklist** check box in the **Access Rule** page during the WLAN SSID profile creation. For more information, see [Configuring Network Service ACLs](#).

Configuring Instant APs for VPN Services

This section describes the following VPN configuration procedures:

- [Instant AP VPN Overview on page 378](#)
- [Configuring Instant APs for VPN Tunnel Creation on page 379](#)
- [Configuring Routing Profiles for Instant AP VPN on page 383](#)

Instant AP VPN Overview

As Instant APs use a Virtual Controller architecture, the Instant AP network does not require a physical controller to provide the configured WLAN services. However, a physical controller is required for terminating VPN tunnels from the Instant AP networks at branch locations or data centers, where the Aruba controller acts as a VPN Concentrator.

When the VPN is configured, the Instant AP acting as the Virtual Controller creates a VPN tunnel to Aruba Mobility Controller in your corporate office. The controller acts as a VPN endpoint and does not supply the Instant AP with any configuration.

The VPN features are recommended for:

- Enterprises with many branches that do not have a dedicated VPN connection to the corporate office.
- Branch offices that require multiple APs.
- Individuals working from home, connecting to the VPN.

Supported VPN Protocols

Instant APs support the following VPN protocols for remote access:

Table 111: *VPN Protocols*

| VPN Protocol | Description |
|-------------------------|--|
| Aruba IPsec | <p>IPsec is a protocol suite that secures IP communications by authenticating and encrypting each IP packet of a communication session.</p> <p>You can configure an IPsec tunnel to ensure that the data flow between the networks is encrypted. However, you can configure a split-tunnel to encrypt only the corporate traffic.</p> <p>When IPsec is configured, ensure that you add the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. IPsec supports Local, L2, and L3 modes of IAP-VPN operations.</p> <p>NOTE: The Instant APs support IPsec only with Aruba Controllers.</p> |
| Layer-2 (L2) GRE | <p>GRE is a tunnel protocol for encapsulating multicast, broadcast, and L2 packets between a GRE-capable device and an endpoint. Instant APs support the configuration of L2 GRE (Ethernet over GRE) tunnel with an Aruba Controller to encapsulate the packets sent and received by the Instant AP.</p> <p>You can use the GRE configuration for L2 deployments when there is no encryption requirement between the Instant AP and controller for client traffic.</p> <p>Instant APs support two types of GRE configuration:</p> <ul style="list-style-type: none">■ Manual GRE—The manual GRE configuration sends unencrypted client traffic with an additional GRE header and does not support failover. When manual GRE is configured on the Instant AP, ensure that the GRE tunnel settings are enabled on the controller.■ Aruba GRE—With Aruba GRE, no configuration on the controller is required except for adding the Instant AP MAC addresses to the whitelist database stored on the controller or an external server. Aruba GRE reduces manual configuration when Per-AP tunnel configuration is required and supports failover between two GRE endpoints. <p>NOTE: Instant APs support manual and Aruba GRE configuration only for L2 mode of operations. Aruba GRE configuration is supported only with Aruba Controllers.</p> |
| L2TP | <p>The L2TP version 3 feature allows Instant AP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with Instant AP gets the IP address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.</p> |

Configuring Instant APs for VPN Tunnel Creation


Instant AP supports the configuration of tunneling protocols such as GRE, IPsec, and L2TPv3. This section describes the procedure for configuring VPN host settings on an Instant AP to enable communication with a controller in a remote location:

- [Configuring IPsec VPN Tunnel](#)
- [Configuring Automatic GRE VPN Tunnel](#)
- [Configuring a GRE VPN Tunnel](#)
- [Configuring an L2TPv3 VPN Tunnel](#)

Configuring IPsec VPN Tunnel

An IPsec tunnel is configured to ensure that the data flow between the networks is encrypted. When configured, the IPsec tunnel to the controller secures corporate data. You can configure an IPsec tunnel from Virtual Controller using Aruba Central.

To configure a tunnel using the IPsec Protocol, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **VPN**. The **VPN** details for the selected group or the device are displayed.
6. Click **Controller**.
7. Select **Aruba IPSec** from the **Protocol** drop-down list.
8. Enter the IP address or FQDN for the main VPN/IPsec endpoint in the **Primary host** field.
9. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** field. This entry is optional. When you specify the primary and backup host details, the other fields are displayed.
10. Specify the following parameters.
 - a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select the **Preemption** check box. This step is optional.
 - b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold-time. The default value for **Hold time** is 600 seconds.
 - c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select the **Fast failover** check box. When fast failover is enabled and if the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - d. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
 - e. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.
 - f. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, select the **Reconnect user on failover** check box.
 - g. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within a range of 30-900 seconds. By default, the reconnection duration is set to 60 seconds. The **Reconnect time on failover** field is displayed only when **Reconnect user on failover** is enabled.
11. When the IPsec tunnel configuration is completed, the packets that are sent from and received by an Instant AP are encrypted.
12. Click **Save Settings**.



You will be unable to upload the self-signed certificate from Aruba Central. You must upload the self-signed certificate to Aruba Activate followed by the AP reboot procedure. When the AP contacts Aruba Activate, the Aruba Activate informs the AP about the self-signed AP certificate that is required to be downloaded. The AP then installs a new certificate before connecting to Aruba Central. For more information, see *Aruba Activate User Guide*.

Configuring Automatic GRE VPN Tunnel

You can configure an Instant AP to automatically set up a GRE tunnel from the Instant AP to controller in Aruba Central.

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **VPN**. The **VPN** details for the selected group or the device are displayed.
6. Click **Controller**.
7. Select **Aruba GRE** from the **Protocol** drop-down list.
8. Enter the IP address or FQDN for the main VPN/IPsec endpoint in the **Primary host** field.
9. Enter the IP address or FQDN for the backup VPN/IPsec endpoint in the **Backup host** field. This entry is optional. When you enter the primary host IP address and backup host IP address, other fields are displayed.
10. Specify the following parameters:
 - a. To allow the VPN tunnel to switch back to the primary host when it becomes available again, select the **Preemption** check box. This step is optional.
 - b. If **Preemption** is enabled, specify a value in seconds for **Hold time**. When preemption is enabled and the primary host comes up, the VPN tunnel switches to the primary host after the specified hold time. The default value for **Hold time** is 600 seconds.
 - c. To allow the Instant AP to create a backup VPN tunnel to the controller along with the primary tunnel, and maintain both the primary and backup tunnels separately, select the **Fast failover** check box. If the primary tunnel fails, the Instant AP can switch the data stream to the backup tunnel. This reduces the total failover time to less than one minute.
 - d. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, select the **Reconnect user on failover**.
 - e. To configure an interval for which wired and wireless users are disconnected during a VPN tunnel switch, specify a value in seconds for **Reconnect time on failover** within the range of 30—90 seconds. By default, the reconnection duration is set to 60 seconds.
 - f. Specify a value in seconds for **Secs between test packets**. Based on the configured frequency, the Instant AP can verify if an active VPN connection is available. The default value is 5 seconds, which means that the Instant AP sends one packet to the controller every 5 seconds.
 - g. Enter a value for **Max allowed test packet loss**, to define a number for lost packets, after which the Instant AP can determine that the VPN connection is unavailable. The default value is 2.
 - h. Select the **Per-AP tunnel** check box. The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN/GRE Endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.
11. Click **Save Settings**.


Configuring a GRE VPN Tunnel

You can also manually configure a GRE tunnel by configuring the GRE tunnel parameters on the Instant AP and controller. This procedure describes the steps involved in the manual configuration of a GRE tunnel from Virtual Controller by using Aruba Central.

During the manual GRE setup, you can either use the Virtual Controller IP or the Instant AP IP to create the GRE tunnel at the controller side depending upon the following Instant AP settings:

- If a Virtual Controller IP is configured and if Per-AP tunnel is disabled, the Virtual Controller IP is used to create the GRE tunnel.
- If a Virtual Controller IP is not configured or if Per-AP tunnel is enabled, the Instant AP IP is used to create the GRE tunnel.

To configure the GRE tunnel manually, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **VPN**. The **VPN** details for the selected group or the device are displayed.
6. Click **Controller**.
7. Select **Manual GRE** from the **Protocol** drop-down list.
8. Specify the following parameters:
 - a. **Host**—Enter the IPv4 or IPv6 address or FQDN for the main VPN/GRE tunnel.
 - b. **Backup Host**—(Optional) Enter the IPv4 or IPv6 address or FQDN for the backup VPN/GRE tunnel. You can edit this field only after you enter the IP address or FQDN in the **Host** field.
 - c. **Reconnect User On Failover**—When you enter the host IP address and backup host IP address, this field appears. Select this check box to disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary.
 - d. **Reconnect Time On Failover**—If you select the **Reconnect User On Failover** check box, this field appears. To configure an interval for which wired and wireless users must be disconnected during a VPN tunnel switch, specify a value within a range of 30-90 seconds. By default, the reconnection duration is set to 60 seconds.
 - e. **GRE Type**—Enter a value for the parameter.
 - f. **GRE MTU**—Specify a size for the **GRE MTU** within the range of 1024–1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1300.
 - g. **Per-AP-Tunnel**—The administrator can enable this option to create a GRE tunnel from each Instant AP to the VPN/GRE endpoint rather than the tunnels created just from the master Instant AP. When enabled, the traffic to the corporate network is sent through a Layer-2 GRE tunnel from the Instant AP itself and need not be forwarded through the master Instant AP.



By default, the **Per-AP tunnel** option is disabled.


- h. To disconnect all wired and wireless users when the system switches during VPN tunnel transition from primary to backup and backup to primary, select the **Reconnect user on failover**.
9. When the GRE tunnel configuration is completed on both the Instant AP and Controller, the packets sent from and received by an Instant AP are encapsulated, but not encrypted.

Configuring an L2TPv3 VPN Tunnel

The Layer 2 Tunneling Protocol version 3 (L2TPv3) feature allows Instant AP to act as L2TP Access Concentrator (LAC) and tunnel all wireless clients L2 traffic from AP to LNS. In a centralized L2 model, the VLAN on the corporate side are extended to remote branch sites. Wireless clients associated with Instant AP gets the IP

address from the DHCP server running on LNS. For this, AP has to transparently allow DHCP transactions through the L2TPv3 tunnel.


To configure an L2TPv3 tunnel by using Aruba Central, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **VPN**. The **VPN** details for the selected group or the device are displayed.
6. Click **Controller**.
7. Select **L2TPv3** from the Protocol drop-down list.
8. To configure a tunnel profile:
 - a. Turn on the **Enable Tunnel Profile** toggle switch.
 - b. Enter the profile name.
 - c. Enter the primary server IP address.
 - d. Enter the remote end backup tunnel IP address. This is an optional field and is required only when backup server is configured.
 - e. Enter the peer UDP and local UDP port numbers. The default value is 1701.
 - f. Enter the interval at which the hello packets are sent through the tunnel. The default value is 60 seconds.
 - g. Select the message digest as MD5 or SHA used for message authentication.
 - h. Enter a shared key for the message digest. This key should match with the tunnel end point shared key.
 - i. If required, set the failover mode. The following two failover modes are supported:
 - **Preemptive**—In this mode, if the primary comes up when the backup is active, the backup tunnel is deleted and the primary tunnel resumes as an active tunnel. If you configure the tunnel to be preemptive, and when the primary tunnel goes down, it starts the persistence timer which tries to bring up the primary tunnel.
 - **Non-Preemptive**—In this mode, when the backup tunnel is established after the primary tunnel goes down, it does not make the primary tunnel active again.
 - j. Set an interval between every failover retry. The default value is 60 seconds.
 - k. Configure a number of retries before the tunnel fails over.
 - l. Ensure that **Checksum** is disabled.
 - m. Specify a value for the tunnel MTU value if required. The default value is 1460.
 - n. Click **Save Settings**.

Configuring Routing Profiles for Instant AP VPN

Aruba Central can terminate a single VPN connection on Aruba Mobility Controller. The routing profile defines the corporate subnets which need to be tunneled through IPsec.

You can configure routing profiles to specify a policy based on routing into the VPN tunnel.

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.

5. Click **VPN**.

6. Click **Routing**.

7. Click + in the **Routing** table.

The **New Route** page with the route parameters is displayed.

8. Update the following parameters:

- **Destination**—Specify the destination network that is reachable through the VPN tunnel. This defines the IP or subnet that must reach through the IPsec tunnel. Traffic to the IP or subnet defined here will be forwarded through the IPsec tunnel.
- **Netmask**—Specify the subnet mask to the destination defined for **Destination**.
- **Gateway**—Specify the gateway to which traffic must be routed. In this field, enter one of the following based on the requirement:
 - The controller IP address on which the VPN connection will be terminated. If you have a primary and backup host, configure two routes with the same destination and netmask, but ensure that the gateway is the primary controller IP for one route and the backup controller IP for the second route.
 - The "tunnel" string if you are using the Instant AP in **Local** mode during local DHCP configuration.
- **Metric**—Specify the best optimal path for routing traffic. A value of 1 indicates the best path, 15 indicates the worst path, and 16 indicates that the destination is unreachable on the route.

9. Click **OK**.

10. Click **Finish**.

Configuring DHCP Pools and Client IP Assignment Modes on Instant APs

This section provides the following information:

- [Configuring DHCP Scopes on Instant APs on page 384](#)
- [Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients on page 390](#)

Configuring DHCP Scopes on Instant APs

The VC supports the following types different modes of DHCP address assignment:

- [Configuring Distributed DHCP Scopes on page 384](#)
- [Configuring a Centralized DHCP Scope on page 386](#)
- [Configuring Local DHCP Scopes on page 388](#)
- [Click DHCP For WLANs. on page 390](#)

Configuring Distributed DHCP Scopes

Aruba Central allows you to configure the DHCP address assignment for the branches connected to the corporate network through VPN. You can configure the range of DHCP IP addresses used in the branches and the number of client addresses allowed per branch. You can also specify the IP addresses that must be excluded from those assigned to clients, so that they are assigned statically.

Aruba Central supports the following distributed DHCP scopes:

- **Distributed, L2** — In this mode, the VC acts as the DHCP server, but the default gateway is in the data center. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC controls a scope

that is a subset of the complete IP Address range for the subnet distributed across all the branches. This DHCP Assignment mode is used with the L2 forwarding mode.

- **Distributed, L3** — In this mode, the VC acts as the DHCP server and the default gateway. Based on the number of clients specified for each branch, the range of IP addresses is divided. Based on the IP address range and client count configuration, the DHCP server in the VC is configured with a unique subnet and a corresponding scope.

To configure distributed DHCP scopes such as Distributed, L2 or Distributed, L3, complete the following procedure:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **DHCP**.
7. To configure a distributed DHCP mode, click + under **Distributed DHCP Scopes**. The **New DHCP Scope** pane is displayed.
8. Based on the type of distributed DHCP scope, configure the following parameters:

Table 112: *Distributed DHCP scope configuration parameters*

| Data pane item | Description |
|-------------------------|---|
| Name | Enter a name for the DHCP scope. |
| Type | Select any of the following options: <ul style="list-style-type: none"> ■ Distributed, L2— On selecting Distributed, L2, the VC acts as the DHCP Server but the default gateway is in the data center. Traffic is bridged into VPN tunnel. ■ Distributed, L3— On selecting Distributed, L3, the VC acts as both DHCP Server and default gateway. Traffic is routed into the VPN tunnel. |
| VLAN | Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. |
| Netmask | If Distributed, L2 is selected for type of DHCP scope, specify the subnet mask. The subnet mask and the network determine the size of subnet. |
| Default Router | If Distributed, L2 is selected for type of DHCP scope, specify the IP address of the default router. |
| DNS Server | If required, specify the IP address of a DNS server. |
| Domain Name | If required, specify the domain name. |
| Lease Time | Specify a lease time for the client in minutes. |
| IP Address Range | Specify a range of IP addresses to use. To add another range, click the + icon. You can specify up to four different ranges of IP addresses. <ul style="list-style-type: none"> ■ For Distributed, L2 mode, ensure that all IP ranges are in the same subnet as the default router. On specifying the IP address ranges, a subnet validation is performed to ensure that the specified ranges of IP address are in the same subnet as the default router and subnet mask. The configured IP range is divided into blocks based on the configured client count. ■ For Distributed, L3 mode, you can configure any discontinuous IP ranges. The configured IP |

Table 112: *Distributed DHCP scope configuration parameters*

| Data pane item | Description |
|-------------------------|--|
| | <p>range is divided into multiple IP subnets that are sufficient to accommodate the configured client count.</p> <p>NOTE: You can allocate multiple branch IDs (BID) per subnet. The Instant AP generates a subnet name from the DHCP IP configuration, which the controller can use as a subnet identifier. If static subnets are configured in each branch, all of them are assigned the with BID 0, which is mapped directly to the configured static subnet.</p> |
| DHCP Reservation | <p>Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations.</p> <p>NOTE: You can configure DHCP reservation only on virtual controllers.</p> <p>From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details:</p> <ul style="list-style-type: none">■ MAC—Specify the MAC address of the device for which the IP address has to be reserved.■ IP—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range. <p>NOTE: Aruba Central allows you to configure a maximum of 32 DHCP reservations.</p> <p>To delete a DHCP reservation, click the delete icon.</p> |
| Option | <p>Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. For example, 176, 242, 161, and so on. To add multiple DHCP options, click the + icon. You can add up to eight DHCP options.</p> |

9. Click **Next**.

10. Specify the number of clients to use per branch. The client count configured for a branch determines the use of IP addresses from the IP address range defined for a DHCP scope. For example, if 20 IP addresses are available in an IP address range configured for a DHCP scope and a client count of 9 is configured, only a few IP addresses (in this example, 9) from this range will be used and allocated to a branch. The Instant AP does not allow the administrators to assign the remaining IP addresses to another branch, although a lower value is configured for the client count.

11. Click **Next**. The **Static IP** tab is displayed. Specify the number of first and last IP addresses to reserve in the subnet.

12. Click **Finish**.

Configuring a Centralized DHCP Scope

The centralized DHCP scope supports L2 and L3 clients.

When a centralized DHCP scope is configured:

- The Virtual Controller does not assign an IP address to the client and the DHCP traffic is directly forwarded to the DHCP Server.
- For L2 clients, the Virtual Controller bridges the DHCP traffic to the controller over the VPN/GRE tunnel. The IP address is obtained from the DHCP server behind the controller serving the VLAN/GRE of the client. This DHCP assignment mode also allows you to add the DHCP option 82 to the DHCP traffic forwarded to the controller.
- For L3 clients, the Virtual Controller acts as a DHCP relay agent that forwards the DHCP traffic to the DHCP server located behind the controller in the corporate network and reachable through the IPsec tunnel. The centralized L3 VLAN IP is used as the source IP. The IP address is obtained from the DHCP server.

To configure a centralized DHCP scope:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **DHCP**.
7. To configure **Centralized** DHCP scopes, click + under **Centralized DHCP Scopes**. The **New DHCP Scope** data pane is displayed.
8. Based on type of DHCP scope, configure the following parameters:

Table 113: *DHCP mode configuration parameters*

| Data pane item | Description |
|-----------------------|--|
| Name | Enter a name for the DHCP scope. |
| Type | Select one of the following options: <ul style="list-style-type: none">■ Centralized ,Layer-2■ Centralized ,Layer-3 |
| VLAN | Specify a VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. |
| Split Tunnel | Enable the split tunnel function if you want allow a VPN user to access a public network and a local LAN or WAN network at the same time through the same physical network connection. For example, a user can use a remote access VPN software client connecting to a corporate network using a home wireless network. When the split tunnel function is enabled, the user can connect to file servers, database servers, mail servers, and other servers on the corporate network through the VPN connection. When the user connects to resources on the Internet (websites, FTP sites, and so on), the connection request goes directly to the gateway provided by the home network. The split DNS functionality intercepts DNS requests from clients for non-corporate domains (as configured in Enterprise Domains list) and forwards to the Instant AP's own DNS server. When split tunnel is disabled, all the traffic including the corporate and the Internet traffic is tunneled irrespective of the routing profile specifications. If the GRE tunnel is down and when the corporate network is not reachable, the client traffic is dropped. |
| DHCP Relay | Select Enabled to allow the Instant APs to intercept the broadcast packets and relay DHCP requests. |
| Helper Address | Enter the IP address of the DHCP server. |

Table 113: *DHCP mode configuration parameters*

| Data pane item | Description |
|------------------|---|
| VLAN IP | Field is applicable only if you select Centralized ,Layer-3 . Specify the VLAN IP address of the DHCP relay server. |
| VLAN Mask | Field is applicable only if you select Centralized ,Layer-3 . Specify the VLAN subnet mask of the DHCP relay server. |
| Option 82 | <p>Select one of the following options:</p> <ul style="list-style-type: none"> ■ None—If you have configured the DHCP Option 82 XML file, the ALU option scope is disabled in the drop-down list. To enable ALU, set the drop-down list to None and delete the DHCP Option 82 XML file. To enable the XML option, select None from the drop-down list and select the XML file from the DHCP Option 82 XML drop-down list. ■ ALU—ALU option is disabled if an XML file is selected from the DHCP Option 82 XML drop-down list in the System > General pane. Select ALU to enable DHCP Option 82 to allow clients to send DHCP packets with the Option 82 string. The Option 82 string is available only in the Alcatel (ALU) format. The ALU format for the Option 82 string consists of the following: <ul style="list-style-type: none"> ● Remote Circuit ID; X AP-MAC; SSID; SSID-Type ● Remote Agent; X IDUE-MAC ■ XML—XML option is enabled only if an XML file is selected from the DHCP Option 82 XML drop-down list in the System > General pane. Alternatively, to enable the XML option, select None from the drop-down list and select the XML file from the DHCP Option 82 XML drop-down list. <p>For information related to XML files, see DHCP Option 82 XML on page 296.</p> |

9. Click **Save Settings**.

The following table describes the behavior of the DHCP Relay Agent and Option 82 in the Instant AP.

Table 114: *DHCP Relay and Option 82*

| DHCP Relay | Option 82 | Behavior |
|------------|-----------|--|
| Enabled | Enabled | DHCP packet relayed with the ALU-specific Option 82 string |
| Enabled | Disabled | DHCP packet relayed without the ALU-specific Option 82 string |
| Disabled | Enabled | DHCP packet not relayed, but broadcast with the ALU-specific Option 82 string |
| Disabled | Disabled | DHCP packet not relayed, but broadcast without the ALU-specific Option 82 string |

Configuring Local DHCP Scopes

You can configure the following types of local DHCP scopes on an Instant AP:

- **Local**—In this mode, the VC acts as both the DHCP Server and default gateway. The configured subnet and the corresponding DHCP scope are independent of subnets configured in other Instant AP clusters. The VC assigns an IP address from a local subnet and forwards traffic to both **corporate** and **non-corporate** destinations. The network address is translated appropriately and the packet is forwarded through the IPsec tunnel or through the uplink. This DHCP assignment mode is used for the NAT forwarding mode.
- **Local, L2**—In this mode, the VC acts as a DHCP server and the gateway is located outside the Instant AP.

- **Local, L3**—In this mode, the VC acts as a DHCP server and default gateway, and assigns an IP address from the local subnet. The Instant AP routes the packets sent by clients on its uplink. This DHCP assignment mode is used with the L3 forwarding mode.

To configure a new local DHCP scope, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **DHCP**.
7. Click **Local DHCP Scopes**.
8. Click + to add new local DHCP scope. The **New DHCP Scope** pane is displayed.
9. Based on type of DHCP scope, configure the following parameters:

Table 115: *Local DHCP configuration parameters*

| Data pane item | Description |
|-------------------------|---|
| Name | Enter a name for the DHCP scope. |
| Type | <p>Select any of the following options:</p> <ul style="list-style-type: none"> ■ Local— On selecting Local, the DHCP server for local branch network is used for keeping the scope of the subnet local to the Instant AP. In the NAT mode, the traffic is forwarded through the uplink. ■ Local, L2—On selecting Local, L2, the VC acts as a DHCP server and a default gateway in the local network is used. ■ Local, L3—On selecting Local, L3, the VC acts as a DHCP server and gateway. |
| VLAN | Enter the VLAN ID. To use this subnet, ensure that the VLAN ID specified here is assigned to an SSID profile. |
| Network | Specify the network to use. |
| Netmask | Specify the subnet mask. The subnet mask and the network determine the size of subnet. |
| Excluded Address | Specify a range of IP addresses to exclude. You can add up to two exclusion ranges. Based on the size of the subnet and the value configured for Excluded address , the IP addresses either before or after the defined range are excluded. |
| DHCP Reservation | <p>Displays the total number of DHCP reservations. Click the number to view the list of DHCP reservations.</p> <p>NOTE: You can configure DHCP reservation only on virtual controllers.</p> <p>From the filter bar, select a virtual controller and click the + icon to configure DHCP reservation. Specify the following details:</p> <ul style="list-style-type: none"> ■ MAC—Specify the MAC address of the device for which the IP address has to be reserved. ■ IP—Specify the IP address that has to be reserved for the MAC address. The IP address should be in the IP address range. <p>NOTE: Aruba Central allows you to configure a maximum of 32 DHCP reservations.</p> <p>To delete a DHCP reservation, click the delete icon.</p> |
| Default Router | Enter the IP address of the default router. |

Table 115: *Local DHCP configuration parameters*


| Data pane item | Description |
|--------------------|--|
| DNS Server | Enter the IP address of a DNS server. |
| Domain Name | Enter the domain name. |
| Lease Time | Enter a lease time for the client in minutes. |
| Option | Specify the type and a value for the DHCP option. You can configure the organization-specific DHCP options supported by the DHCP server. To add multiple DHCP options, click the (+) icon. |

10. Click **Save Settings**.

Configuring DHCP for WLANs

You can configure the DHCP server to use for wireless LANs that have Client IP Assignment set to Virtual Controller Assigned. To configure the DHCP for WLANs, perform the following the following steps:

To configure a new local DHCP scope, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **DHCP**.
7. Click **DHCP For WLANs**.
8. Enter the **Domain Name**, **DNS Server**, **Lease Time**, **Network**, and **Mask** values.
9. Click **Save Settings**.

Configuring DHCP Server for Assigning IP Addresses to Instant AP Clients

The DHCP server is a built-in server, used for networks in which clients are assigned IP address by the VC. You can customize the DHCP pool subnet and address range to provide simultaneous access to more number of clients. The largest address pool supported is 2048. The default size of the IP address pool is 512.


When the DHCP server is configured and if the **Client IP assignment** parameter for an SSID profile is set to **Virtual Controller Assigned**, the Virtual Controller assigns the IP addresses to the WLAN or wired clients. By default, the Instant AP automatically determines a suitable DHCP pool for **Virtual Controller Assigned** networks.

The Instant AP typically selects the 172.31.98.0/23 subnet. If the IP address of the Instant AP is within the 172.31.98.0/23 subnet, the Instant AP selects the 10.254.98.0/23 subnet. However, this mechanism does not avoid all possible conflicts with the wired network. If your wired network uses either 172.31.98.0/23 or 10.254.98.0/23, and you experience problems with the **Virtual Controller Assigned** networks after upgrading to Aruba Central, manually configure the DHCP pool by following the steps described in this section.



To configure a domain name, DNS server, and DHCP server for client IP assignment.

1. In the **Network Operations** app, use the filter to select a group or a device.

2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **DHCP**.
7. Enter the domain name of the client in **Domain Name**.
8. Enter the IP addresses of the DNS servers in **DNS Server**. To add another DNS server, click the + icon.
9. Enter the duration of the DHCP lease in **Lease Time**.
10. Select **Minutes**, **Hours**, or **Days** for the lease time from the list next to **Lease Time**. The default lease time is 0.
11. Enter the network in the **Network** box.
12. Enter the mask in the **Mask** box.



To provide simultaneous access to more than 512 clients, use the Network and Mask fields to specify a larger range. While the network (or prefix) is the common part of the address range, the mask (suffix) specifies how long the variable part of the address range is.

13. Click **Save Settings**.

Configuring Services

This section describes how to configure AirGroup, location services, Lawful Intercept, OpenDNS, and Firewall services.

- [Configuring AirGroup Services on page 391](#)
- [Configuring an Instant AP for RTLS Support on page 394](#)
- [Configuring an Instant AP for ALE Support on page 395](#)
- [Managing BLE Beacons on page 395](#)
- [Configuring OpenDNS Credentials on Instant APs on page 396](#)
- [Configuring CALEA Server Support on Instant APs on page 397](#)
- [Configuring Instant APs for Palo Alto Networks Firewall Integration on page 398](#)
- [Configuring XML API Interface on page 399](#)
- [Application Visibility and Deep Packet Inspection on page 399](#)

Configuring AirGroup Services

AirGroup is a zero configuration networking protocol that enables service discovery, address assignment, and name resolution for desktop computers, mobile devices, and network services. It is designed for flat, single-subnet IP networks such as wireless networking at home.

Bonjour can be installed on computers running Microsoft Windows and is supported by the new network-capable printers. Bonjour uses multicast DNS (mDNS) to locate devices and the services offered by these devices. The AirGroup solution supports both wired and wireless devices. Wired devices that support Bonjour services are part of AirGroup when connected to a VLAN that is terminated on the Virtual Controller.

In addition to the mDNS protocol, Instant APs also support UPnP, and DLNA enabled devices. DLNA is a network standard derived from UPnP, which enables devices to discover the services available in a network.

DLNA also provides the ability to share data between the Windows or Android-based multimedia devices. All the features and policies applicable to mDNS are extended to DLNA to ensure full interoperability between compliant devices.

AirGroup Features

AirGroup provides the following features:

- Send unicast responses to mDNS queries and reduces mDNS traffic footprint.
- Ensure cross-VLAN visibility and availability of AirGroup devices and services.
- Allow or block AirGroup services for all users.
- Allow or block AirGroup services based on user roles.
- Allow or block AirGroup services based on VLANs.

For more information on AirGroup solution, see *Aruba Instant User Guide*.


AirGroup Services

Bonjour supports zero-configuration services. The services are pre-configured and are available as part of the factory default configuration. The administrator can also enable or disable any or all services.

The following services are available for Instant AP clients:

- AirPlay — Apple AirPlay allows wireless streaming of music, video, and slide shows from your iOS device to Apple TV and other devices that support the AirPlay feature.
- AirPrint — Apple AirPrint allows you to print from an iPad, iPhone, or iPod Touch directly to any AirPrint compatible printer.
- iTunes— The iTunes service is used by iTunes Wi-Fi sync and iTunes home-sharing applications across all Apple devices.
- RemoteMgmt— Use this service for remote login, remote management, and FTP utilities on Apple devices.
- Sharing— Applications such as disk sharing and file sharing, use the service ID that are part of this service on one or more Apple devices.
- Chat— The iChat® (Instant Messenger) application on Apple devices uses this service.
- ChromeCast—The ChromeCast service allows you to use a ChromeCast device to play audio or video content on a high-definition television by streaming content through Wi-Fi from the Internet or local network.
- DLNA Media—Applications such as Windows Media Player use this service to browse and play content on a remote device.
- DLNA Print—This service is used by printers that support DLNA.

To enable AirGroup services:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**.
6. Under the **AirGroup** accordion, select the **AirGroup** check-box.



The **mDNS (Bonjour)** and **SSDP (DLNA/UPNP)** check-boxes are selected by default.

Select at least **mDNS (Bonjour)** or **SSDP (DLNA/UPNP)** to proceed further.

Optionally, select the **Guest Bonjour Multicast** check-box to allow guest users to use the Bonjour services that are enabled in a guest VLAN. When **Guest Bonjour Multicast** is enabled, the Bonjour devices are visible only in the guest VLAN and AirGroup does not discover or enforce policies in guest VLAN.

7. Under the **AirGroup Settings** sub-accordion, select the check-box against one or more AirGroup services listed in [Table 116](#).

Table 116: *AirGroup Services*

| Mode | Description |
|----------------------------------|--|
| AirGroup Across Mobility Domains | AirGroup service availability in inter cluster domains. |
| AirPrint | Wireless printing between AirPrint capable devices and AirPrint compatible printers. |
| Enable AirPlay | Wireless streaming of music, video, or slide shows from AirPlay capable devices and AirPlay compatible devices. |
| iTunes | iTunes service for home-sharing applications. |
| Remote Management | Remote login, remote management, or FTP utilities on compatible devices. |
| Sharing | Applications like disk sharing or file sharing on compatible devices. |
| Chat | Instant messenger application between compatible devices. |
| Googlecast | Wireless streaming of audio or video content from the Internet or local network on a HDTV through a Chromecast device. |
| DIAL | Wireless streaming between DIAL compatible devices likes devices like Roku, Chromecast, or FireTV. |
| AmazonTV | Wireless playing of content from the Internet or local network on a HDTV through a FireTV device. |
| DLNA Print | Wireless printing between DLNA capable devices and DLNA compatible printers. |
| DLNA Media | Wireless browsing or playing audio or video content by applications like Windows Media Player on remote devices. |
| Allow All | All AirGroup services. |

- Optionally, when enabling an AirGroup service, define disallowed roles. The disallowed roles are not allowed to use the specific AirGroup service. To disallow roles:
 1. Click **Edit** against **Disallowed Roles**.
 2. Move the roles from the **Available** pool to the **Selected** pool.
 3. Click **Ok**.
- Optionally, when enabling an AirGroup service, define disallowed VLANs. The disallowed VLANs are not allowed to use the specific AirGroup service. To disallow VLANs:
 1. Click **Edit** against **Disallowed VLANs**.
 2. Type the VLANs in **Enter comma-separated list of VLAN IDs**. Separate multiple VLANs with a comma.
 3. Click **Ok**.

- Optionally, configure and enable a new AirGroup service. If defined, disallowed roles or VLANs are not allowed to use the new AirGroup service. To configure and enable a new AirGroup service:
 - Click **Add New Service**.
 - Type the service name in **Service Name**. Use alphanumeric characters.
 - Type a service ID in **Service ID**. Use + to add additional service IDs.
Sample service ID: **urn:schemas-upnp-org:service:RenderingControl:1** or **_sleep-proxy_udp**.
 - Click **Ok**.
 - Select the check-box against the new AirGroup service.
- Optionally, under **ClearPass Settings** sub-accordion, configure the parameters listed in [Table 117](#).

Table 117: ClearPass Settings


| Mode | Description |
|-----------------------------------|--|
| ClearPass Policy Manager Server 1 | Specify the ClearPass Policy Manager server to use. Select one from the drop-down or define a new ClearPass Policy Manager server. |
| Enforce ClearPass Registration | Specify if ClearPass registration should be enforced. |

- Click **Save Settings**.

Configuring an Instant AP for RTLS Support

Aruba Central supports the real time tracking of devices. With the help of the RTLS, the devices can be monitored in real time or through history.

To configure RTLS, complete the following steps:

- In the **Network Operations** app, use the filter to select a group or a device.
- Under **Manage**, click **Devices > Access Points**.
- Click the  configuration icon to display the AP configuration page.
- Click **Show Advanced**.
- Click **Services**. The Services page is displayed.
- Click **Real Time Locating System > Aruba**.
- Select **Aruba RTLS** to send the RFID tag information to the Aruba RTLS server.
- Click **3rd Party** and select **Aeroscout** to send reports on the stations to a third-party server.
- In the **IP/FQDN** and **Port** field, specify the IP address and port number of the RTLS server, to which location reports must be sent.
- In the **Passphrase** field, enter the passphrase required for connecting to the RTLS server.
- Retype the passphrase in the **Retype Passprahrse** field.
- Specify the update interval within the range of 6–60 seconds in the **Update every** field. The default interval is 30 seconds.
- If **3rd Party** is selected, specify the IP address and port number of the 3rd party server.
- Select **Include Unassociated Stations** to send reports on the stations that are not associated to any Instant AP.
- Click **Save Settings**.

Configuring an Instant AP for ALE Support

ALE is designed to gather client information from the network, process it and share it through a standard API. The client information gathered by ALE can be used for analyzing a client's Internet behavior for business such as shopping preferences.

ALE includes a location engine that calculates the associated and unassociated device location every 30 seconds by default. For every device on the network, ALE provides the following information through the Northbound API:

- Client user name
- IP address
- MAC address
- Device type
- Application firewall data, showing the destinations and applications used by associated devices.
- Current location
- Historical location

ALE requires the AP placement data to be able to calculate location for the devices in a network.


ALE with Aruba Central

Aruba Central supports Analytics and Location Engine (ALE). The ALE server acts as a primary interface to all third-party applications and the Instant AP sends client information and all status information to the ALE server.

To integrate Instant AP with ALE, the ALE server address must be configured on an Instant AP. If the ALE server is configured with a host name, the Virtual Controller performs a mutual certificated-based authentication with ALE server, before sending any information.

Enabling ALE support on an Instant AP

To configure an Instant AP for ALE support:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The **Services** page is displayed.
6. Under **Real Time Locating System**, click **Aruba**, and then select **Analytics & Location**.
7. Specify the ALE server name or IP address.
8. Specify the reporting interval within the range of 6–60 seconds. The Instant AP sends messages to the ALE server at the specified interval. The default interval is 30 seconds.
9. Click **Save Settings**.

Managing BLE Beacons

Instant APs support Aruba BLE devices, such as BT-100 and BT-105, which are used for location tracking and proximity detection. The BLE devices can be connected to an Instant AP and are managed by a cloud-based Beacon Management Console. The BLE Beacon Management feature allows you to configure parameters for managing the BLE beacons and establishing secure communication with the Beacon Management Console.

Support for BLE Asset Tracking

Instant AP assets can be tracked using BLE tags, Instant AP beacons scan the network. When a tag is detected, the Instant AP sends a beacon with information about the tag including the MAC address and RSSI of the tag to the Virtual Controller.

To manage beacons and configure BLE operation mode, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The Services page is displayed.
6. Click **Real Time Locating System > Aruba**.
7. To manage the BLE devices using BMC, select the **Manage BLE Beacons** check box.
8. Enter the authorization token. The authorization token is a text string of 1–255 characters used by the BLE devices in the HTTPS header when communicating with the BMC. This token is unique for each deployment.
9. In **Endpoint URL**, enter the URL of the server to which the BLE sends the monitoring data.
10. Select any of the following options from **BLE Operation Mode** drop-down list:

Table 118: *BLE Operation Modes*

| Mode | Description |
|---------------------------|---|
| beaconing | The built-in BLE chip in the Instant AP functions as an iBeacon combined with the beacon management functionality. |
| disabled | The built-in BLE chip of the Instant AP is turned off. The BLE operation mode is set to Disabled by default. |
| dynamic-console | The built-in BLE chip of the Instant AP functions in the beaconing mode and dynamically enables access to Instant AP console over BLE when the link to LMS is lost. |
| persistent-console | The built-in BLE chip of the Instant AP provides access to the Instant AP console over BLE and also operates in the Beaconing mode. |


11. To configure BLE web socket management server, click **BLE Asset Tag Mgmt Server(wss)** field and enter the URL of BLE web socket management server.
12. To configure BLE HTTPS management server, select the **BLE Asset Tag Mgmt Server(https)** check box to enter the BLE HTTPS management server URL.
13. Enter the URL of BLE HTTPS management server corresponding to the **Server URL** field.
14. Enter the authorization token and the location ID in the **Authorization token** and **Location ID** field respectively.
15. Click **Save Settings**.

Configuring OpenDNS Credentials on Instant APs

Instant APs use the OpenDNS credentials to provide enterprise-level content filtering.

To configure OpenDNS credentials:

1. In the **Network Operations** app, use the filter to select a group or a device.

2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The Services page is displayed.
6. Click **OpenDNS**. The OpenDNS page is displayed.
7. Enter the **Username** and **Password**.
8. Click **Save Settings**.

Configuring CALEA Server Support on Instant APs

LI allows the Law Enforcement Agencies to perform an authorized electronic surveillance. Depending on the country of operation, the ISPs are required to support LI in their respective networks.

In the United States, Service Providers are required to ensure LI compliance based on CALEA specifications.

Aruba Central supports CALEA integration with an Instant AP in a hierarchical and flat topology, mesh Instant AP network, the wired and wireless networks.



Enable this feature only if lawful interception is authorized by a law enforcement agency.


For more information on the communication and traffic flow from an Instant AP to CALEA server, see *Aruba Instant User Guide*.

To enable an Instant AP to communicate with the CALEA server, complete the following steps:

- [Creating a CALEA Profile](#)
- [Creating ACLs for CALEA Server Support](#)


Creating a CALEA Profile

To create a CALEA profile, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The Services page is displayed.
6. Click **CALEA**. The **CALEA** tab details are displayed.
7. Specify the following parameters:
 - **IP address**— Specify the IP address of the CALEA server.
 - **Encapsulation type**— Specify the encapsulation type. The current release of Aruba Central supports GRE only.
 - **GRE type**— Specify the GRE type.
 - **MTU**— Specify a size for the MTU within the range of 68—1500. After GRE encapsulation, if packet length exceeds the configured MTU, IP fragmentation occurs. The default MTU size is 1500.
8. Click **OK**.

Creating ACLs for CALEA Server Support

To create an access rule for CALEA, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - a. Under **Manage**, click **Devices > Access Points**.
 - b. Click the **Settings** () icon to display the AP configuration page.
3. If you select the device, click **Devices** under **Manage**.
4. Click **Show Advanced**.
5. Click **Security**. The Security page is displayed.
6. Click **Roles**.
7. Under **Access Rules for Selected Roles**, click + icon. The **New Rule** window is displayed.
8. Set the **Rule Type** to **CALEA**.
9. Click **Save**.
10. Create a role assignment rule if required.
11. Click **Save Settings**.


Configuring Instant APs for Palo Alto Networks Firewall Integration

Instant APs maintains the network (such as mapping IP address) and user information for its clients in the network. To integrate the Instant AP network with a third-party network, you can enable an Instant AP to provide this information to the third-party servers.

To integrate an Instant AP with a third-party network, you must add a global profile. This profile can be configured on an Instant AP with information such as IP address, port, user name, password, firewall enabled or disabled status.

Configuring an Instant AP for Network Integration

To configure an Instant AP for network integration:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The Services page is displayed.
6. Click **Network Integration**. The PAN firewall configuration options are displayed.
7. Select **Enable** to enable PAN firewall.
8. Specify the **User Name** and **Password**. Ensure that you provide user credentials of the PAN firewall administrator.
9. Re-enter the password in the **Retype** box.
10. Enter the PAN firewall **IP Address**.
11. Enter the port number within the range of 1—65535. The default port is 443.
12. Click **Save Settings**.

Configuring XML API Interface

The XML API interface allows Instant APs to communicate with an external server. The communication between Instant AP and an external server through XML API Interface includes the following steps:

- An API command is issued in the XML format from the server to the virtual controller.
- The virtual controller processes the XML request and identifies where the client is and sends the command to the correct slave Instant AP.
- Once the operation is completed, the virtual controller sends the XML response to the XML server.
- The administrators can use the response and take appropriate action to suit their requirements. The response from the virtual controller is returned using the predefined formats.

To configure XML API for servers, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **Services**. The **Services** page is displayed.
6. Go to **Network Integration > XML API Server Configuration**.
7. Click + to add a new XML API server.
8. Enter a name for the XML API server in the **Name** text box.
9. Enter the IP address of the XML API server in the **IP Address** text box.
10. Enter the subnet mask of the XML API server in the **Mask** text box.
11. Enter a passcode in the **Passphrase** text box, to enable authorized access to the XML API Server.
12. Re-enter the passcode in the **Retype Passphrase** box.
13. To add multiple entries, repeat the procedure.
14. Click **Add**.
15. Click **Save Settings**.
16. To edit or delete the server entries, use the **Edit** and **Delete** buttons, respectively.

For information on adding an XML API request, see *Aruba Instant User Guide*.

Application Visibility and Deep Packet Inspection

AppRF is a custom built Layer 7 firewall capability supported for Instant APs managed by Aruba Central. It consists of an on-board deep packet inspection and a cloud-based Web Policy Enforcement service that allows creating firewall policies based on types of application.

Instant APs with DPI capability analyze data packets to identify applications in use and allow you to create access rules to determine client access to applications, application categories, web categories and website URLs based on security ratings. You can also define traffic shaping policies such as bandwidth control and QoS per application for client roles. For example, you can block bandwidth monopolizing applications on a guest role within an enterprise.



The Deep Packet Inspection feature is supported on Instant AP running 6.4.3.x-4.1.x.x or later releases. The AppRF feature is not supported on IAP-104/105 and IAP-134/135 devices.

You can configure InstantInstant APs to send URL information for the blocked HTTP and HTTPS sessions to ALE. The URL information can be extracted for the associated clients for DPI, analytics, and data mining through the Northbound APIs. To enable URL information logging and extraction, enable the URL Visibility parameter in the InstantInstant AP UI or CLI. For more information, see *Aruba Instant User Guide*.


For more information on DPI and application analytics, see the following topics:

- [Application Visibility on page 251](#)
- [Enabling Application Visibility Service on APs](#)
- [Configuring ACLs for Deep Packet Inspection on page 370](#)
- [Configuring ACLs on APs for Website Content Classification on page 372](#)
- [Configuring Custom Redirection URLs for Instant AP Clients on page 373](#)

Enabling Application Visibility Service on APs

To view application usage metrics for WLAN clients, enable the Application Visibility service on APs.

To enable the Application Visibility feature, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the settings  icon to display the AP configuration page.
4. If you select the device, click **Device** under **Manage**.
5. Click **Show Advanced**.
6. Click **Services**. The **Services** page opens.
7. Click **AppRF**.
8. Select any of the following options for **Deep Packet Inspection**:
 - **All**—Performs deep packet inspection on client traffic to application, application categories, website categories, and websites with a specific reputation score.
 - **App**—Performs deep packet inspection on client traffic to applications and application categories.
 - **WebCC**—Performs deep packet inspection on client traffic to specific website categories and websites with specific reputation ratings.
 - **None**—Disables deep packet inspection.
9. Click **Save Settings**.

Configuring Uplink Interfaces on Instant APs

This section provides the following information:

- [Uplink Interfaces on page 400](#)
- [Uplink Preferences and Switching on page 404](#)

Uplink Interfaces

Aruba Central supports 3G and 4G USB modems, and the Wi-Fi uplink to provide access to the corporate network.



By default, the AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and

8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

The following types of uplinks are supported on Aruba Central:

- [3G/4G Uplink](#)
- [Ethernet Uplink on page 402](#)
- [Wi-Fi Uplink on page 403](#)

3G/4G Uplink

Aruba Central supports the use of 3G/4G USB modems to provide the Internet backhaul to Aruba Central. The 3G/4G USB modems can be used to extend client connectivity to places where an Ethernet uplink cannot be configured. This enables the Instant APs to automatically choose the available network in a specific region.

Types of Modems

Aruba Central supports the following three types of 3G modems:

- **True Auto Detect** — Modems of this type can be used only in one country and for a specific ISP. The parameters are configured automatically and hence no configuration is necessary.
- **Auto-detect + ISP/country** — Modems of this type require the user to specify the Country and ISP. The same modem is used for different ISPs with different parameters configured for each of them.
- **No Auto-detect** — Modems of this type are used only if they share the same Device-ID, Country, and ISP details. You need to configure different parameters for each of them. These modems work with Aruba Central when the appropriate parameters are configured.

Table 119: 4G supported modem


| Modem Type | Supported 4G Modem |
|------------------|--|
| True Auto Detect | <ul style="list-style-type: none">■ Pantech UML290■ Ether-lte |



When UML290 runs in auto detect mode, the modem can switch from 4G network to 3G network or vice-versa based on the signal strength. To configure the UML290 for the 3G network only, manually set the USB type to **pantech-3g**. To configure the UML290 for the 4G network only, manually set the 4G USB type to **pantech-lte**.

Configuring Cellular Uplink Profiles

You can configure 3G or 4G uplinks using Aruba Central.

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Uplink** and perform any of the following steps:

- To configure a 3G or 4G uplink automatically, select the **Country** and **ISP**. The parameters are automatically populated.
- To configure a 3G or 4G uplink manually, perform the following steps:
 - a. Obtain the modem configuration parameters from the local IT administrator or the modem manufacturer.
 - b. Enter the type of the 3G/4G modem driver type:
 - For 3G — Enter the type of 3G modem in the **USB type** text box.
 - For 4G — Enter the type of 4G modem in the **4G USB type** text box.
 - c. Enter the device ID of modem in the **USB dev** text box.
 - d. Enter the TTY port of the modem in the **USB tty** text box.
 - e. Enter the parameter to initialize the modem in the **USB init** text box.
 - f. Select the service protocol from the **ISP** drop-down list.
 - g. Enter the parameter to dial the cell tower in the **USB dial** text box.
 - h. Enter the username used to dial the ISP in the **USB user** text box.
 - i. Enter the password used to dial the ISP in the **USB password** text box.
 - j. Enter the parameter used to switch a modem from the storage mode to modem mode in the **USB mode switch** text box.
- 7. Select the USB authentication type from the **USB Auth Type** drop-down list.
- 8. Click **Save Settings**.
- 9. Reboot the Instant AP for changes to affect.

Ethernet Uplink

The Ethernet 0 port on an Instant AP is enabled as an uplink port by default. The Ethernet uplink supports the following:

- PPPoE
- DHCP
- Static IP

You can use PPPoE for your uplink connectivity in a single AP deployment.



Uplink redundancy with the PPPoE link is not supported.

When the Ethernet link is up, it is used as a PPPoE or DHCP uplink. After the PPPoE settings are configured, PPPoE has the highest priority for the uplink connections. The Instant AP can establish a PPPoE session with a PPPoE server at the ISP and get authenticated using PAP or the CHAP. Depending upon the request from the PPPoE server, either the PAP or the CHAP credentials are used for authentication. After configuring PPPoE, reboot the Instant AP for the configuration to take effect. The PPPoE connection is dialed after the AP comes up. The PPPoE configuration is checked during Instant AP boot and if the configuration is correct, Ethernet is used for the uplink connection.




When PPPoE is used, do not configure Dynamic RADIUS Proxy and IP address of the VC. An SSID created with default VLAN is not supported with PPPoE uplink.

You can also configure an alternate Ethernet uplink to enable uplink failover when an Ethernet port fails.

Configuring PPPoE uplink profile

To configure PPPoE settings:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Uplink**. Under **PPPoE**, configure the following parameters:
 - a. Enter the **PPPoE service name** provided by your service provider in **Service Name**.
 - b. In the **Chap Secret** and **Retype CHAP Secret** fields, enter the secret key used for CHAP authentication. You can use a maximum of 34 characters for the CHAP secret key.
 - c. Enter the user name for the PPPoE connection in the **USER** field.
 - d. In the **Password** and **Retype Password** fields, enter a password for the PPPoE connection and confirm it.
7. To set a local interface for the PPPoE uplink connections, select a value from **Local Interface**. The selected DHCP scope is used as a local interface on the PPPoE interface and the Local, L3 DHCP gateway IP address as its local IP address. When configured, the local interface acts as an unnumbered PPPoE interface and allocated the entire Local, L3 DHCP subnet to the clients.



The options in **Local Interface** are displayed only if a Local, L3 DHCP scope is configured on the Instant AP.

8. Click **Save Settings**.
9. Reboot the Instant AP.

Wi-Fi Uplink

The Wi-Fi uplink is supported for all Instant AP models, except 802.11ac APs. Only the master Instant AP uses the Wi-Fi uplink. The Wi-Fi allows uplink to open, PSK-CCMP, and PSK-TKIP SSIDs.

- For single radio Instant APs, the radio serves wireless clients and Wi-Fi uplink.
- For dual radio Instant APs, both radios can be used to serve clients but only one of them can be used for Wi-Fi uplink.



When Wi-Fi uplink is in use, the client IP is assigned by the internal DHCP server.

Configuring a Wi-Fi Uplink Profile


The following configuration conditions apply to the Wi-Fi uplink:

- To bind or unbind the Wi-Fi uplink on the 5 GHz band, reboot the Instant AP.
- If Wi-Fi uplink is used on the 5 GHz band, mesh is disabled. The two links are mutually exclusive.

To provision an Instant AP with Wi-Fi Uplink, complete the following steps:

1. If you are configuring a Wi-Fi uplink after restoring factory settings on an Instant AP, connect the Instant AP to an Ethernet cable to allow the Instant AP to get the IP address. Otherwise, go to step 2.
2. In the **Network Operations** app, use the filter to select a group or a device.

3. Under **Manage**, click **Devices > Access Points**.

4. Click the  configuration icon to display the AP configuration dashboard.

5. Click **Show Advanced**.

6. Click **System**. The **System** details for the selected group or the device are displayed.

7. Click **Uplink**, under **WiFi**, enter the name of the wireless network that is used for Wi-Fi uplink in the **Name (SSID)** box.

8. From **Management**, select the type of key for uplink encryption and authentication. If the uplink wireless router uses mixed encryption, WPA-2 is recommended for Wi-Fi uplink.

9. From **Band**, select the band in which the VC currently operates. The following options are available:

- 2.4 GHz (default)
- 5 GHz

10. From **Passphrase Format**, select a **Passphrase format**. The following options are available:

- 8 - 63 alphanumeric characters
- 64 hexadecimal characters



Ensure that the hexadecimal password string is exactly 64 digits in length.

11. Enter a PSK passphrase in **Passphrase** and click **OK**.

12. Click **Save Settings**.

Uplink Preferences and Switching

This topic describes the following procedures:

- [Enforcing Uplinks on page 404](#)
- [Setting an Uplink Priority on page 405](#)
- [Enabling Uplink Pre-emption on page 405](#)

Enforcing Uplinks


The following conditions apply to the uplink enforcement:

- When an uplink is enforced, the Instant AP uses the specified uplink regardless of uplink pre-emption configuration and the current uplink status.
- When an uplink is enforced and multiple Ethernet ports are configured and uplink is enabled on the wired profiles, the Instant AP tries to find an alternate Ethernet link based on the priority configured.
- When no uplink is enforced and pre-emption is not enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured.
- When no uplink is enforced and pre-emption is enabled, and if the current uplink fails, the Instant AP tries to find an available uplink based on the priority configured. If current uplink is active, the Instant AP periodically tries to use a higher priority uplink and switches to the higher priority uplink even if the current uplink is active.

To enforce a specific uplink on an Instant AP, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.

2. Under **Manage**, click **Devices > Access Points**.


3. Click the  configuration icon to display the AP configuration page.

4. Click **Show Advanced**.

5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Uplink**.
7. Under **Management**, select the type of uplink from **Enforce Uplink**. If Ethernet uplink is selected, the **Port** field is displayed.
8. Specify the Ethernet interface port number.
9. Click **Save Settings**. The selected uplink is enforced on the Instant AP.

Setting an Uplink Priority

To set an uplink priority:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Uplink**.
7. Under **Uplink Priority List**, select the uplink, and increase or decrease the priority. By default, the Eth0 uplink is set as a high priority uplink.
8. Click **Save Settings**. The selected uplink is prioritized over other uplinks.

Enabling Uplink Pre-emption

The following configuration conditions apply to uplink pre-emption:

- Pre-emption can be enabled only when no uplink is enforced.
- When pre-emption is disabled and the current uplink fails, the Instant AP tries to find an available uplink based on the uplink priority configuration.
- When pre-emption is enabled and if the current uplink is active, the Instant AP periodically tries to use a higher priority uplink, and switches to a higher priority uplink even if the current uplink is active.

To enable uplink pre-emption:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration page.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Uplink**.
7. Under **Management**, ensure that the **Enforce Uplink** is set to **None**.
8. Set **Pre-Emption** to **ON**.
9. Click **Save Settings**.

Switching Uplinks based on the Internet Availability

You can configure Aruba Central to switch uplinks based on the Internet availability.

When the uplink switchover based on Internet availability is enabled, the Instant AP continuously sends ICMP packets to some well-known Internet servers. If the request is timed out due to a bad uplink connection or uplink interface failure, and the Internet is not reachable from the current uplink, the Instant AP switches to a different connection.

To configure uplink switching, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
 2. Under **Manage**, click **Devices > Access Points**.
 3. Click the  configuration icon to display the AP configuration page.
 4. Click **Show Advanced**.
 5. Click **System**.
- The **System** details for the selected group or the device are displayed.
6. Click **Uplink** and expand the **Management** accordion.
 7. Specify a value for **Failover Internet IP**.
 8. Enable **Internet Failover**.
 9. Specify values for **Failover Internet Packet Send Frequency**, **Failover Internet Packet Lost Count**, and **Internet Check Count**.
 10. Click **Save Settings**.



By default, the master AP sends the ICMP packets to 8.8.8.8 IP address only if the out-of-service operation based on Internet availability (internet-down state) is configured on the SSID. You can use **Failover Internet IP** as an alternative to the default option to configure an IP address to which the AP must send AP packets, and verify if the Internet is reachable when the uplink is down.



When **Internet failover** is enabled, the Instant AP ignores the VPN status, although uplink switching based on VPN status is enabled.

Configuring Preferred Uplink on AP-318 and 370 Series APs

The AP-318 and 370 Series APs have an ethernet port for eth0 and a fibreport for eth1. Either of these ports can be configured as the uplink port as required. By default, eth1 port is configured as the uplink for these AP platforms. All functionalities of the eth0 port is supported by eth1 port with exception to the following:

- Eth0 bridging feature is not supported when the eth1 port is configured as preferred uplink.
- If LACP is enabled, the eth1 port cannot be configured as the preferred uplink.




By default, the AP-318, AP-374, AP-375, and AP-377 access points have Eth1 as the uplink port and Eth0 as the downlink port. Aruba recommends you not to upgrade the mentioned access points to 8.5.0.0 and 8.5.0.1 firmware versions as the upgrade process changes the uplink from Eth1 to Eth0 port thereby making the devices non-reachable.

Configuring Enterprise Domains

The enterprise domain names list displays the DNS domain names that are valid on the enterprise network. This list is used to determine how client DNS requests are routed. When **Content Filtering** is enabled, the DNS request of the clients is verified and the domain names that do not match the names in the list are sent to the OpenDNS server.

To configure an enterprise domain, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.

5. Click **System**.
6. Click **Enterprise Domains**.
7. Click **+** and enter a name in the **New Domain Name**.
8. Click **OK**.

To delete a domain, select the domain and click **Delete**.

Configuring SNMP Parameters

This section provides the following information:

- [SNMP Configuration Parameters on page 407](#)
- [Configuring Community String for SNMP on page 408](#)
- [Configuring SNMP Traps on page 408](#)

SNMP Configuration Parameters

Aruba Central supports SNMPv1, SNMPv2c, and SNMPv3 for reporting purposes only. An Instant AP cannot use SNMP to set values in an Aruba system.

You can configure the following parameters for an Instant AP:

Table 120: *SNMP parameters*


| Data Pane Item | Description |
|---|--|
| Community Strings for SNMPV1 and SNMPV2 | An SNMP Community string is a text string that acts as a password, and is used to authenticate messages sent between the Virtual Controller and the SNMP agent. |
| If you are using SNMPv3 to obtain values from the Instant AP, you can configure the following parameters: | |
| Name | A string representing the name of the user. |
| Authentication Protocol | An indication of whether messages sent on behalf of this user can be authenticated, and if so, the type of authentication protocol used. This can take one of the two values: <ul style="list-style-type: none"> ■ MD5—HMAC-MD5-96 Digest Authentication Protocol ■ SHA—HMAC-SHA-96 Digest Authentication Protocol |
| Authentication protocol password | If messages sent on behalf of this user can be authenticated, the (private) authentication key for use with the authentication protocol. This is a string password for MD5 or SHA depending on the choice above. |
| Privacy protocol | An indication of whether messages sent on behalf of this user can be protected from disclosure, and if so, the type of privacy protocol which is used. This takes the value DES (CBC-DES Symmetric Encryption). |
| Privacy protocol password | If messages sent on behalf of this user can be encrypted/decrypted with DES, the (private) privacy key for use with the privacy protocol. |

Configuring Community String for SNMP

This section describes the procedure for configuring SNMPv1, SNMPv2, and SNMPv3 community strings using the Aruba Central.


Creating Community strings for SNMPv1 and SNMPv2 using Aruba Central

To create community strings for SNMPv1 and SNMPv2, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **SNMP**.
7. To add a new community string, click + and enter the string in the **New Community String** text box.
8. Click **OK**.
9. To delete a community string, select the string, and click **Delete**.

Creating community strings for SNMPv3 using Aruba Central


To create community strings for SNMPv3, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - a. Under **Manage**, click **Devices > Access Points**.
 - b. Click the configuration  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **SNMP**.
7. Select the type of authentication protocol from the **Auth protocol** drop-down list.
8. Enter the authentication password in the **Password** text box and retype the password in the **Retype** text box.
9. Select the type of privacy protocol from the **Privacy protocol** drop-down list.
10. Enter the privacy protocol password in the **Password** text box and retype the password in the **Retype** text box.
11. Click **OK**.
12. To edit the details for a particular user, select the user and click **Edit**.
13. To delete a particular user, select the user and click **Delete**.

Configuring SNMP Traps

Aruba Central supports the configuration of external trap receivers. Only the Instant AP acting as the VC generates traps. The OID of the traps is 1.3.6.1.4.1.14823.2.3.3.1.200.2.X.

To configure SNMP traps, complete the following steps.

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - c. Under **Manage**, click **Devices > Access Points**.
 - d. Click the settings  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **SNMP**.
7. Under **SNMP Traps**, enter a name in the **SNMP Engine ID** text box. It indicates the name of the SNMP agent on the access point. The SNMPV3 agent has an engine ID that uniquely identifies the agent in the device and is unique to that internal network.
8. Click **+** and update the following fields:
 - **IP Address**— Enter the **IP Address** of the new SNMP Trap receiver.
 - **Version**— Select the SNMP version— **v1**, **v2c**, **v3** from the drop-down list. The version specifies the format of traps generated by the access point.
 - **Community/Username**— Specify the community string for SNMPv1 and SNMPv2c traps and a username for SNMPv3 traps.
 - **Port**— Enter the port to which the traps are sent. The default value is 162.
 - **Inform**— When enabled, traps are sent as SNMP INFORM messages. It is applicable to SNMPv3 only. The default value is **Yes**.
9. Click **OK** to view the trap receiver information in the **SNMP Trap Receivers** window.


Configuring Syslog and TFTP Servers for Logging Events

This section provides the following information:

- [Configuring Syslog Server on Instant APs on page 409](#)
- [Configuring TFTP Dump Server Instant APs on page 410](#)

Configuring Syslog Server on Instant APs

To specify a syslog server for sending syslog messages to the external servers, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Logging**.
7. Under **Servers**, enter the IP address of the server to which you want to send system logs in the **Syslog Server** box.
8. Select the required values to configure Syslog Facility Levels. Syslog facility is an information field associated with a syslog message. It is an application or operating system component that generates a log message. The Instant AP supports the following syslog facilities:

- **AP-Debug**—Detailed log about the AP device.
- **Network**—Log about change of network, for example, when a new Instant AP is added to a network.
- **Security**—Log about network security, for example, when a client connects using wrong password.
- **System**—Log about configuration and system status.
- **User**—Important logs about client.
- **User-Debug**—Detailed log about client.
- **Wireless**—Log about radio.

[Table 121](#) describes the logging levels in order of severity, from the most severe to the least.


Table 121: *Logging levels*

| Logging level | Description |
|--------------------|---|
| Emergency | Panic conditions that occur when the system becomes unusable. |
| Alert | Any condition requiring immediate attention and correction. |
| Critical | Any critical condition such as a hard drive error. |
| Error | Error conditions. |
| Warning | Warning messages. |
| Notice | Significant events of a non-critical nature. The default value for all syslog facilities. |
| Information | Messages of general interest to system users. |
| Debug | Messages containing information useful for debugging. |

9. Click **Save Settings**.

Configuring TFTP Dump Server Instant APs

To configure a TFTP server for storing core dump files, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. If you select a group, perform the following steps:
 - a. Under **Manage**, click **Devices > Access Points**.
 - b. Click the configuration  icon to display the AP configuration page.
3. If you select the device, click **Device** under **Manage**.
4. Click **Show Advanced**.
5. Click **System**. The **System** page for the selected group or device is displayed.
6. Click **Logging**.
7. Under **Servers**, enter the IP address of the TFTP server in the **TFTP Dump Server** box.
8. Click **Save Settings**.

Resetting an AP

You can reset the system configuration of an Instant AP by erasing the existing configuration on the Instant AP. To erase the existing configuration on an Instant AP, perform any of the following procedures:


Clearing Instant AP Configuration Using Groups

To reset an Instant AP using groups, complete the following steps:

1. Create a new group. Ensure that the group has no additional configuration.
2. Move the Instant AP that you want to reset, under the new group. After the Instant AP is moved to a new group, the configuration on the Instant AP is erased and the default group configuration is pushed to the Instant AP. However, in this procedure, only the system configuration is cleared and the **Per AP Settings** on the Instant AP are retained.

Resetting an AP through the Console

To reset an Instant AP from the console, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group.
2. Under **Manage**, click **Devices > Access Points** to view the AP monitoring dashboard.
3. Click the  list icon to display the AP list page.
4. Select the AP to reset.
5. From the **Actions** drop-down, click **Console**.
6. Execute the **write erase all** command at the command prompt.
7. Reboot the Instant AP. With this procedure, the complete configuration including the **Per AP Settings** on the Instant AP is reset.

After the reboot, the Instant AP is moved to default group and will not be present in the group to which it was previously attached.

For information on resetting an Instant AP to factory default configuration by using the reset button on the device, see *Aruba Instant User Guide*.


Rebooting APs

You can reboot an Instant AP or an Instant AP cluster using the Aruba Central UI.

Perform any of the following procedures:

Reboot an Instant AP

To reboot an Instant AP, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group.
2. Under **Manage**, click **Devices > Access Points** to view the AP monitoring dashboard.
3. Click the  list icon to display the AP list page.
4. Click **Up** to display a table with the list of online APs in the group.
5. In the table, click the Instant AP to reboot. The **Access Point Details** page corresponding to the AP is displayed.


6. In the **Actions** drop-down list, click **Reboot AP**.
7. In the **Reboot** dialog box, click **Continue**.



The **Access Points Details** page takes less than a minute to update the interface status after the AP is rebooted and reconnected to Aruba Central.

Reboot an Instant AP cluster

To reboot an Instant AP cluster:

1. In the **Network Operations** app, use the filter to select a group.
2. Under **Manage**, click **Devices > Access Points** to view the AP monitoring dashboard.
3. Click the  list icon to display the AP list page.
4. Click **Up** to display a table with the list of online APs in the group.
5. In the table, select the master Instant AP to reboot.
6. In the **Actions** drop-down list, click **Reboot Swarm**.
7. In the **Reboot** dialog box, click **Continue**.




The **Access Points Details** page takes less than a minute to update the interface status after the VC is rebooted and reconnected to Aruba Central.

Mapping Instant AP Certificates

When an Instant AP joins a group that does not have a certificate, the Instant AP's existing certificate is retained. When an Instant AP joins a group that already has a certificate, the Instant AP's certificate is overwritten by the group's certificate.

To map an Instant AP certificate name to a specific certificate type or category, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **Security**. The **Security** details for the selected group or the device are displayed.
6. Click **Certificate**.
7. To map a certificate to a specific certificate category, click **Certificate Usage**.
8. Select the required certificate from the corresponding drop-down list. Aruba Central supports the following types of certificates:
 - Server certificates for RADIUS, Captive Portal, and RadSec (for cloud guest networks) authentication.
 - CA certificates—To validate the identity of a client.
 - Authentication Server—To verify the identity of the server to a client.
 - Captive portal server—To verify the identity of internal captive portal server.
 - RadSec—To verify the identity of the TLS server.
 - RadSec CA—For mutual authentication between the Instant AP and the TLS server.
9. Click **Save Settings**. Aruba Central pushes the certificate to all Instant APs in that group.




To enable certificates for the Cloud Guest Service, contact the Aruba Central support team.

Configuring HTTP Proxy on Instant AP

If your network requires a proxy server for Internet access, ensure that you configure the HTTP proxy on the Instant AP to download the image from the cloud server. After setting up the HTTP proxy settings, the Instant AP connects to the Activate server, Aruba Central, or OpenDNS server through a secure HTTP connection. You can also exempt certain applications from using the HTTP proxy (configured on an Instant AP) by providing their host name or IP address under exceptions. Aruba Central allows the user to configuring HTTP proxy on an Instant AP.

To configure HTTP proxy on Instant AP through Aruba Central, complete the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Devices > Access Points**.
3. Click the  configuration icon to display the AP configuration dashboard.
4. Click **Show Advanced**.
5. Click **System**. The **System** details for the selected group or the device are displayed.
6. Click **Proxy** and specify the following:
 - a. Enter the HTTP proxy server IP address in the **Server** box.
 - b. Enter the port number in the **Port** box.
7. Click **Save Settings**.



Aruba Central displays the **Username**, **Password**, and **Retype Password** fields under **System > Proxy** for Instant AP running Aruba Instant 8.3.0.0. The Instant APs with the Aruba Instant 8.3.0.0 firmware require user credentials for proxy server authentication.

Configuring APs Using Templates

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple devices in a group and thus automate AP deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba APs.

For template-based provisioning, APs must be assigned to a group with template-based configuration method enabled.

To create a template for the devices in a template group, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a template group.
2. Under **Templates**, click **+** to add a new template.
The **Add Template** window is displayed.
3. Add the template name.
4. Set the model and firmware version parameters to **ALL**.
5. Add the CLI script content. Check the following guidelines before adding content to the template:
 - Ensure that the command text indentation matches the indentation in the running configuration.

- The template allows multiple **per-ap-settings** blocks. The template must include the **per-ap-settings %sys_lan_mac%** variable. The **per-ap-settings** block uses the variables for each AP. The general VC configuration uses variables for master AP to generate the final configuration from the provided template. Hence, Aruba recommends that you upload all variables for all devices in a cluster and change values as required for individual AP variables.

You can obtain the list of variables for **per-ap-settings** by using the **show amp-audit** command. The following example shows the list of variables for **per-ap-settings**:

```
(Instant AP)# show amp-audit | begin per-ap
per-ap-settings 70:3a:0e:cc:ee:60
hostname EE:60-335-24
rf-zone bj-qa
ip-address 10.65.127.24 255.255.255.0 10.65.127.1 10.65.6.15 ""
swarm-mode standalone
wifi0-mode access
wifi1-mode access
g-channel 6+ 21
a-channel 140 26
uplink-vlan 0
g-external-antenna 0
a-external-antenna 0
aplx-peap-user peap22 282eaf1077b8d898b91ec41b5da19895
```

- The commands in the template are case-sensitive.
- IF ELSE ENDIF conditions are supported in the template. If the template text includes the if condition, % sign is required at the beginning and the end of the text. For example, %if guest%. The following example shows the template text with the IF ELSE ENDIF condition.

```
wlan ssid-profile %ssid_name%
%if disable_ssid=true%
disable-ssid
%endif%
%if ssid_security=wpa2%
opmode wpa2-aes
%else%
opmode opensystem
%endif%
```

- Templates also support nesting of the IF ELSE END IF condition blocks. The following example shows how to nest such blocks:

```
%if condition1=true%
routing-profile
route 10.10.0.0 255.255.255.0 10.10.0.255
%if condition2=true%
routing-profile
route 10.20.0.0 255.255.255.0 10.20.0.255
%else%
routing-profile
route 10.30.0.0 255.255.255.0 10.30.0.255
%endif%
%else%
routing-profile
route 10.40.0.0 255.255.255.0 10.40.0.255
%if condition3=true%
routing-profile
route 10.50.0.0 255.255.255.0 10.50.0.255
%else%
routing-profile
route 10.60.0.0 255.255.255.0 10.60.0.255
```



```
%endif%
%endif%
```

- To comment out a line in the template text, use the pound sign (#). Any template text preceded by # is ignored when processing the template.
- To allow or restrict APs from joining the Instant AP cluster, Aruba Central uses the **_sys_allowed_ap_** system-defined variable. Use this variable only when allowed APs configuration is enabled. For example, **_sys_allowed_ap: "a_mac, b_mac, c_mac"**. Use this variable only once in the template.

6. Click **OK**.

The variables configured for the Instant AP devices functioning as the VCs are replaced with the values configured at the template level.



If any device in the cluster has any missing variables, the configuration push to those AP devices in the cluster fails. The audit trail for such instances shows the missing variables.

You can configure the RF zone for an AP by adding the **rf-zone %rfzone%** variable in the template. Similarly, you can add the **wifi0-mode %wifi0-mode%** variable to configure a Wi-Fi0 interface of an AP to function in the access, monitor, or spectrum monitor mode. For information on managing template variables, see [Managing Variable Files](#).

Sample Template

The following example shows the typical contents allowed in a template file for APs:

```
virtual-controller-country %countrycode%
virtual-controller-key d2d8c79e010af35667dae85f950cf144b476ab4beba9ce5696
organization %org%
name %VCname%
virtual-controller-ip %vcip%
terminal-access
clock timezone none 00 00
rf-band all

allow-new-aps
allowed-ap 38:17:c3:cd:34:ca

hash-mgmt-password
hash-mgmt-user admin password cleartext public

syslog-level debug
syslog-level warn ap-debug

arm
wide-bands none
a-channels 44,44+,40,36
g-channels 13,1+
min-tx-power 15
max-tx-power 127
band-steering-mode prefer-5ghz
air-time-fairness-mode fair-access
channel-quality-aware-arm-disable
client-match
client-match nb-matching 55
client-match calc-interval 5
client-match slb-mode 2

wlan access-rule default_wired_port_profile
index 0
rule any any match any any any permit
```



```

wlan access-rule wired-SetMeUp
  index 1
  rule masterip 0.0.0.0 match tcp 80 80 permit
  rule masterip 0.0.0.0 match tcp 4343 4343 permit
  rule any any match udp 67 68 permit
  rule any any match udp 53 53 permit

wlan access-rule %ssid_name%
  index 2
  rule any any match any any any permit

wlan ssid-profile %ssid_name%
  %if disable_ssid=true%
  disable-ssid
  %endif%
  %if ssid_security=wpa2%
  opmode wpa2-aes
  %else%
  opmode opensystem
  %endif%
  type employee
  essid %ssid_name%
  wpa-passphrase %pw%
  max-authentication-failures 0
  auth-server InternalServer
  rf-band all
  captive-portal disable
  dtim-period 1
  broadcast-filter arp
  blacklist
  dmo-channel-utilization-threshold 90
  local-probe-req-thresh 0
  max-clients-threshold 64
  okc
  %if condition1=true%
  routing-profile
    route 10.10.0.0 255.255.255.0 10.10.0.255
  %if condition2=true%
  routing-profile
    route 10.20.0.0 255.255.255.0 10.20.0.255
  %else%
  routing-profile
    route 10.30.0.0 255.255.255.0 10.30.0.255
  %endif%
  %else%
  routing-profile
    route 10.40.0.0 255.255.255.0 10.40.0.255
  %if condition3=true%
  routing-profile
    route 10.50.0.0 255.255.255.0 10.50.0.255
  %else%
  routing-profile
    route 10.60.0.0 255.255.255.0 10.60.0.255
  %endif%
  %endif%

wired-port-profile wired-SetMeUp
  switchport-mode access
  allowed-vlan all
  native-vlan guest
  no shutdown
  access-rule-name wired-SetMeUp
  speed auto
  duplex auto
  no poe
  type guest

```



```

captive-portal disable
no dot1x

wired-port-profile default_wired_port_profile
switchport-mode trunk
allowed-vlan all
native-vlan 1
shutdown
access-rule-name default_wired_port_profile
speed auto
duplex full
no poe
type employee
captive-portal disable
no dot1x

enet0-port-profile default_wired_port_profile
enet1-port-profile wired-SetMeUp

uplink
preemption
enforce none
failover-internet-pkt-lost-cnt 10
failover-internet-pkt-send-freq 30
failover-vpn-timeout 180

cluster-security
allow-low-assurance-devices

per-ap-settings %_sys_lan_mac%
hostname %hostname%
rf-zone %rfname%
swarm-mode %mode%
wifi0-mode %wifi0mode%
wifil-mode %wifilmode%
g-channel %gch% %gtx%
a-channel %ach% %gtx%

```

Password Management in Configuration Templates for AP

In Aruba Central, the AP management user passwords are stored and displayed as hash instead of plain text. Password for AP can be set using the following commands:

```

mgmt-user <user-name> <password>

mgmt-user <user-name> <password> read-only

mgmt-user <user-name> <password> guest-mgmt

```



The **mgmt-user** commands are used for APs running below Aruba Instant 4.3 firmware version.

The **hash-mgmt-user** command is enabled by default on the APs provisioned in the template and UI groups. If a pre-configured AP joins Aruba Central and is moved to a new group, Aruba Central uses the **hash-mgmt-user** configuration settings and discards **mgmt-user** configuration settings, if any, on the AP. In other words, Aruba Central hashes management user passwords irrespective of the management user configuration settings running on an AP.



The **hash-mgmt** commands can only be used for APs running firmware versions equal to or above Aruba Instant 4.3.

Password for AP can be set using the following **hash-mgmt-user** commands:

```
hash-mgmt-user <user-name> password hash <hash-password>
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password>
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype read-only
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype read-only
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype guest-mgmt
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype guest-mgmt
```

```
hash-mgmt-user <user-name> password hash <hash-password> usertype local
```

```
hash-mgmt-user <user-name> password cleartext <cleartext-password> usertype local
```

Aruba Central supports the use of hash commands with clear text, however, Aruba recommends you to use hash passwords instead of clear text passwords to avoid password disclosures.

Aruba Central allows you to re-use the hash from one AP on another AP.



All AP templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

Aruba switches enable secure, role-based network access for wired users and devices, independent of their location or application. With Aruba switches, enterprises can deploy a consistent and secure access to network resources based on the type of users, client devices, and connection methods.

Aruba Central offers a cloud-based management platform for managing Aruba switch infrastructure. It simplifies switch management with flexible configuration options, monitoring dashboards, and troubleshooting tools.

- [Getting Started with Aruba Switch Deployments on page 421](#)
- [Provisioning Factory Default Switches on page 423](#)
- [Provisioning Pre-Configured Switches on page 426](#)
- [Using Configuration Templates for Switch Management on page 435](#)
- [Configuring or Viewing Switch Properties in UI Groups on page 437](#)
- [Aruba Switch Stack on page 459](#)
- [Monitoring Switches and Switch Stacks on page 162](#)

Supported Switch Platforms



To manage your Aruba switches using Aruba Central, ensure that the switch software is upgraded to 16.05.0007 or a later version. However, if you already have switches running lower software versions in your account, you can continue to manage these devices from Aruba Central.

The following tables list the switch platforms, corresponding software versions supported in Aruba Central, and switch stacking details.

Table 122: *Supported Aruba Switch Series, Software Versions, and Switch Stacking*

| Switch Platform | Supported Software Versions | Recommended Software Versions | Switch Stacking Support | Supported Stack Type (Frontplane (VSF) / Backplane (BPS)) |
|--------------------------|-----------------------------|-------------------------------|---|---|
| Aruba 2530 Switch Series | YA/YB.16.05.0008 or later | YA/YB.16.10.0003 | N/A | N/A |
| Aruba 2540 Switch Series | YC.16.03.0004 or later | YC.16.10.0003 | N/A | N/A |
| Aruba 2920 Switch Series | WB.16.03.0004 or later | WB.16.10.0003 | Yes Switch Software Dependency: WB.16.04.0008 or later | BPS |

| Switch Platform | Supported Software Versions | Recommended Software Versions | Switch Stacking Support | Supported Stack Type (Frontplane (VSF) / Backplane (BPS)) |
|---------------------------|-----------------------------|-------------------------------|--|---|
| Aruba 2930F Switch Series | WC.16.03.0004 or later | WC.16.10.0003 | Yes Switch Software Dependency: WC.16.07.0002 | VSF |
| Aruba 2930M Switch Series | WC.16.04.0008 or later | WC.16.10.0003 | Yes Switch Software Dependency: WC.16.06.0006 | BPS |
| Aruba 3810 Switch Series | KB.16.03.0004 or later | KB.16.10.0003 | Yes Switch Software Dependency: KB.16.07.0002 | BPS |
| Aruba 5400R Switch Series | KB.16.04.0008 or later | KB.16.10.0003 | Yes Switch Software Dependency: KB.16.06.0008 | VSF |



Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins.

Table 123: *Supported Aruba Mobility Access Switch Series and Software Versions*

| Mobility Access Switch Series | Supported Software Versions |
|--|---|
| <ul style="list-style-type: none"> ■ S1500-12P ■ S1500-24P ■ S2500-24P ■ S3500-24T | ArubaOS 7.3.2.6 ArubaOS 7.4.0.3 ArubaOS 7.4.0.4 ArubaOS 7.4.0.5 ArubaOS 7.4.0.6 |

Data sheets and technical specifications for the supported switch platforms are available at:
<https://www.arubanetworks.com/products/networking/switches/>

Getting Started with Aruba Switch Deployments

Before you get started with your onboarding and provisioning operations, browse through the list of [Aruba switches supported](#) in Aruba Central.

Provisioning Workflow

The following sections list the steps required for provisioning switches in Aruba Central.

Provisioning a Factory Default Switch

Like most Aruba devices, Aruba Switches support ZTP. Switches with factory default configuration have very basic configuration for all ports in VLAN-1. When a new switch (factory default) is powered on, it automatically obtains IP address, connects to Aruba Activate and downloads the provisioning parameters. When the switch identifies Aruba Central as its management entity, it connects to Aruba Central.

To manage switches from Aruba Central, you must onboard the switches to the device inventory and assign a valid subscription.

For step-by-step instructions, see [Provisioning Factory Default Switches on page 423](#).

Provisioning a Pre-configured or Locally-Managed Switch

Pre-configured switches have customized configuration; for example, an additional VLAN or static IP address configured on the default.

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central as their management platform, therefore you must manually enable the Aruba Central management service on these switches to allow them to connect to Aruba Central.

For step-by-step instructions, see [Provisioning Pre-Configured Switches](#).

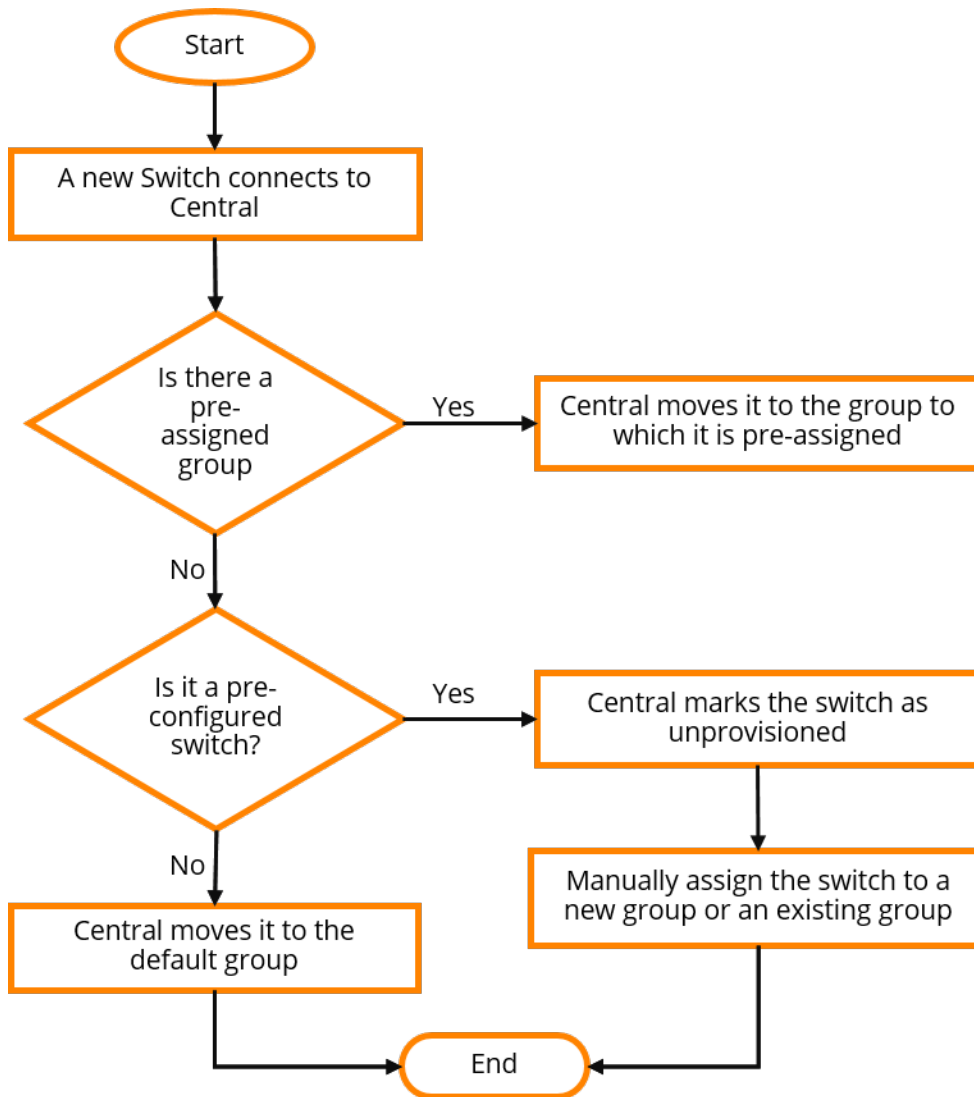
Group Assignment

Aruba Central supports provisioning switches in one of the following types of groups:

- UI group—Allows you to customize and manage device parameters using the UI workflows, that is, the menu options and tabs available under **Network Operations**.
- Template Group—Allows you to configure devices using CLI-based configuration templates.

The following figure illustrates the group assignment workflow in Aruba Central:

Figure 96 *Group Assignment-Switches*



Configuration and Management

Aruba Central supports managing switch configuration using UI workflows or configuration templates. Based on your configuration requirements, ensure that you assign switches to either UI group or template group.

For more information on managing switches in Aruba Central, see the following topics:

- [Using Configuration Templates for Switch Management on page 435](#)
- [Configuring or Viewing Switch Properties in UI Groups on page 437](#)

Switch Monitoring

To view the operation status of switches and health of wired access network:

- In the **Network Operations** app, use the filter to select a group that has switches.
- Under **Manage**, click **Devices** > **Switches**.

For more information, see [Monitoring Your Network on page 145](#).

Troubleshooting and Diagnostics

The **Configuration Audit** page under **Network Operations > Device(s) > Switches** in the Aruba Central UI displays errors in configuration sync, templates, and a list of configuration overrides. For more information, see [Viewing Configuration Status on page 107](#).

To troubleshoot switches remotely, use the tools available under **Network Operations > Analyze > Tools**. For more information, see [Using Troubleshooting Tools](#).

Provisioning Factory Default Switches

Switches that run default configuration either after shipped from a factory or a factory reset are referred to as factory default switches. This topic describes the steps for provisioning factory default switches in Aruba Central.

- [Step 1: Onboard the Switch to Aruba Central](#)
- [Step 2: Assign the Switch to a Group](#)
- [Step 3: Connect the Switch to Aruba Central](#)
- [Step 4: Provision the Switch to a Group](#)
- [Step 5: Verify the configuration Status](#)

Step 1: Onboard the Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- [Log in to Aruba Central](#)
- [Add switches to Aruba Central](#)
- [Assign Subscriptions](#)

Step 2: Assign the Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. By default, Aruba Central assigns the factory default switches to default group. You can create a new group and assign switch to the new group.

For more information on creating a group, see [Creating a Group on page 91](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**. The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Maintain**, click **Organization > Groups**. The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Connect the Switch to Aruba Central

Switches with factory default configuration have very basic configuration for all ports in VLAN-1 that is required for obtaining an IP address and automatic provisioning (ZTP). For ZTP, switches must have a valid IP address, DNS, and NTP configuration.

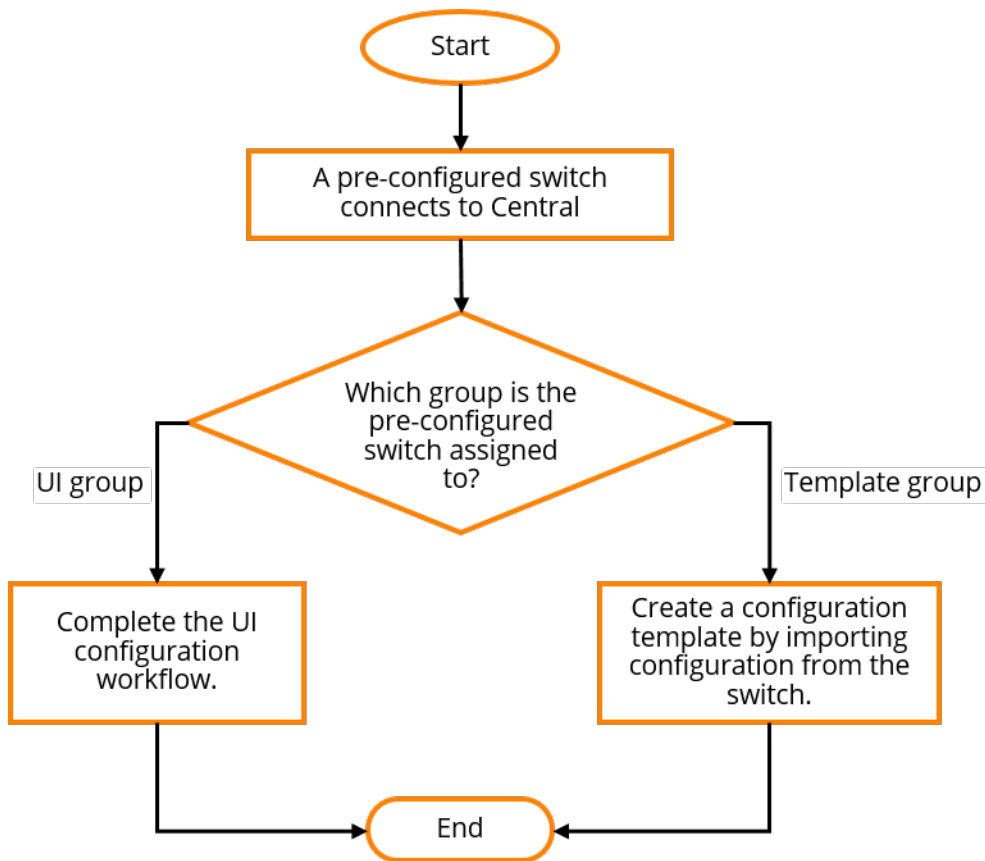
When a factory default switch is powered on and connected to the Internet, it establishes connection with Aruba Activate and downloads the provisioning parameters. If the switch is already added and assigned a subscription, it connects to Aruba Central.

Step 4: Provision the Switch to a Group

When the switch connects to Central, if it is already added to the device inventory and is assigned a subscription in Aruba Central, Aruba Central assigns it to a pre-assigned group. If there is no pre-assigned group, Aruba Central moves the device to the **default** group. Based on your configuration requirements, you create a UI group or template group and assign the switch.

The following figure illustrates the provisioning step required for each group type.


Figure 97 Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, Aruba Central uses the current configuration of switch as base configuration and applies it to the other switches that join this group later. You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Device(s)** > **Switches**. For more information, see [Configuring or Viewing Switch Properties in UI Groups](#).

Provisioning Switches in Template Groups

If you have assigned the switch to a template group, create a new configuration template. To create a configuration template:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Templates**. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. Enter a name for the template in the **Template Name** field.
7. Ensure that **Aruba Switch** is selected in the **Device** drop-down.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
 - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
 - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.



If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.

If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Build a new template or import configuration information from a switch that is already provisioned in the template group.
 - To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in [Using Configuration Templates for Switch Management on page 435](#).
 - To import configuration text from a switch that is already provisioned in the template group:
 - a. Select the switch from which you want to import the configuration.
 - b. Click **Import Template**. The imported configuration is displayed in the **Template** text box.

Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements. For more information see [Managing Variable Files](#).




All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *HPE ArubaOS-Switch Access Security Guide*.

11. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the configuration Status

To verify the configuration status:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
 - To verify the configuration status for the template group, click **configuration Audit**. The **configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **Failed / Pending config changes**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Provisioning Pre-Configured Switches

Unlike factory default switches, locally managed switches and the switches with custom configuration require one touch provisioning. These switches do not automatically identify Aruba Central as their management platform, therefore you must manually enable the Aruba Central management service on these switches to allow them to connect to Aruba Central.

To onboard a locally-managed or a pre-configured switch to Aruba Central, follow one of the following options:

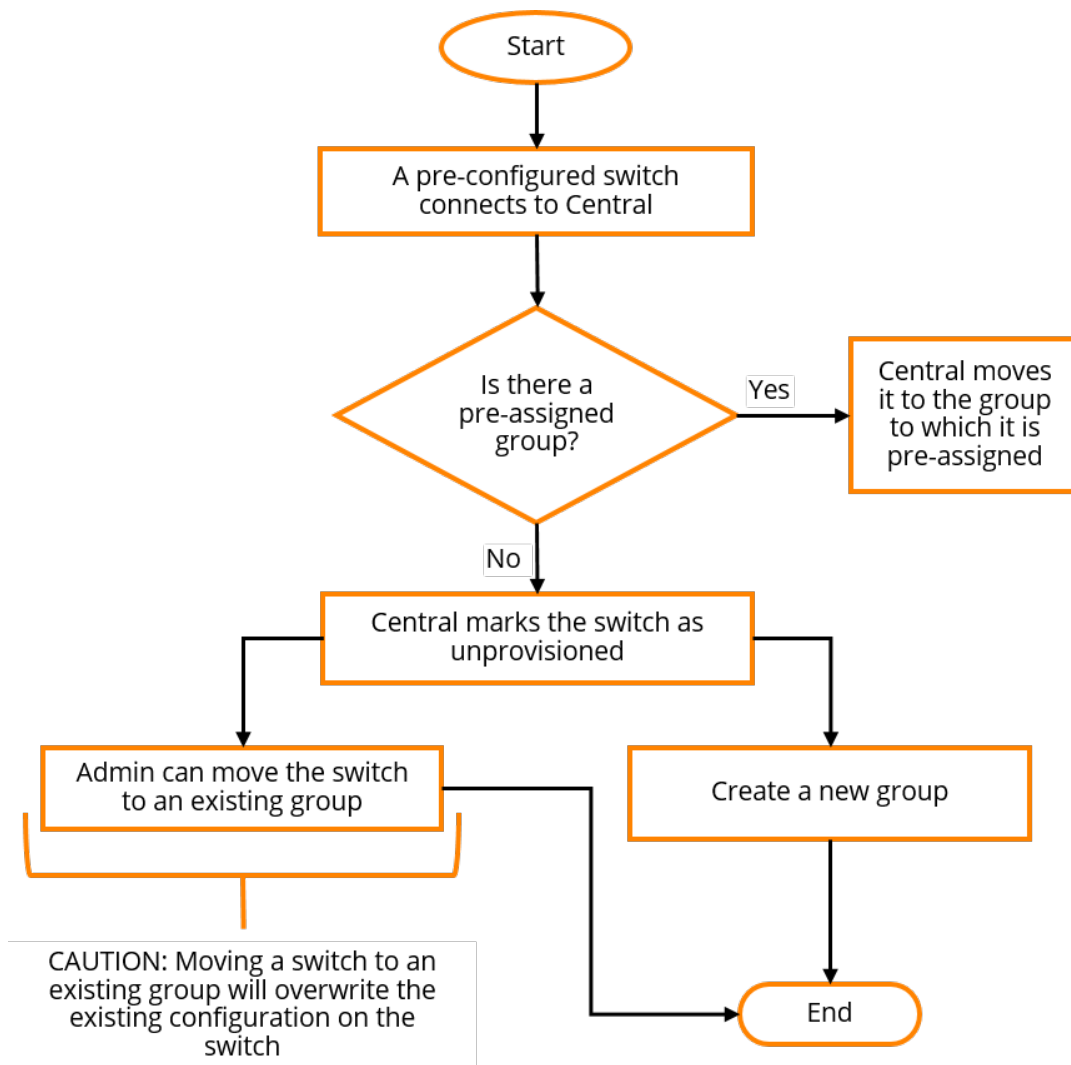
- Manually enable Aruba Central management service on the switch and connect it to Aruba Central. Aruba recommends that you use this option if you want to preserve the current configuration running on the switch. For more information on this procedure, see the workflows described in this topic.
- Reset the switch configuration to factory default and use ZTP to provision the switch. For information on provisioning factory default switches, see [Provisioning Factory Default Switches on page 423](#).

Aruba Central supports provisioning switches using one of the following methods:

- Pre-provisioning—In this workflow, a switch is added to the device inventory and assigned a group in Aruba Central before it connects to Aruba Central.
- Onboarding connected switches—In this workflow, Aruba Central onboards the switch that attempts to connect and then assigns a group.

The following figure illustrates provisioning procedure for a pre-configured switch.

Figure 98 *Provisioning Workflow for Pre-Configured Switches*



Workflow 1—Pre-Provisioning a Switch

The pre-provisioning workflow includes the following steps:

- [Step 1: Onboard the Switch to Aruba Central](#)
- [Step 2: Assign the Switch to a Group](#)
- [Step 3: Enable Aruba Central Management Service on the Switch](#)
- [Step 4: Provision the Switch to a Group](#)
- [Step 5: Verify the configuration Status](#)

Step 1: Onboard the Switch to Aruba Central

To onboard switches to the device inventory in Aruba Central, complete the following steps:

- [Log in to Aruba Central](#)
- [Add switches to Aruba Central](#)
- [Assign Subscriptions](#)

Step 2: Assign the Switch to a Group

Before assigning a group, determine if the switch must be provisioned in a UI or template group. If you want to preserve the existing configuration on the switch, Aruba recommends that you create a new group for the switch.

For more information on creating a group, see [Creating a Group](#).

To assign a device to a group from the **Account Home** page:

1. In the **Account Home** page, under **Global Settings**, click **Device Inventory**. The Device Inventory page is displayed
2. Select the device that you want to assign to a group.
3. Click **Assign Group**. The **Assign a Group to the Selected Devices** window is displayed.
4. Select the group to which you want to assign.
5. Click **Assign Device(s)**.

To assign a device to a group from the **Network Operations** app:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Maintain**, click **Organization > Groups**. The Groups page is displayed.
3. From the devices table on the right, select the device that you want to assign to a new group.
4. Drag and drop the device to the group to which you want to assign the device.

Step 3: Enable Aruba Central Management Service on the Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
configuration and Status - Activate Provision Service
Activate Provision Service      : Enabled
Activate Server Address         : device.arubanetworks.com
```

2. If the Activate provision service is not enabled, execute the following command at the switch CLI:

```
(switch)# activate provision enable
```

3. To enable switches to automatically connect to Aruba Central, enforce ZTP on the switch:

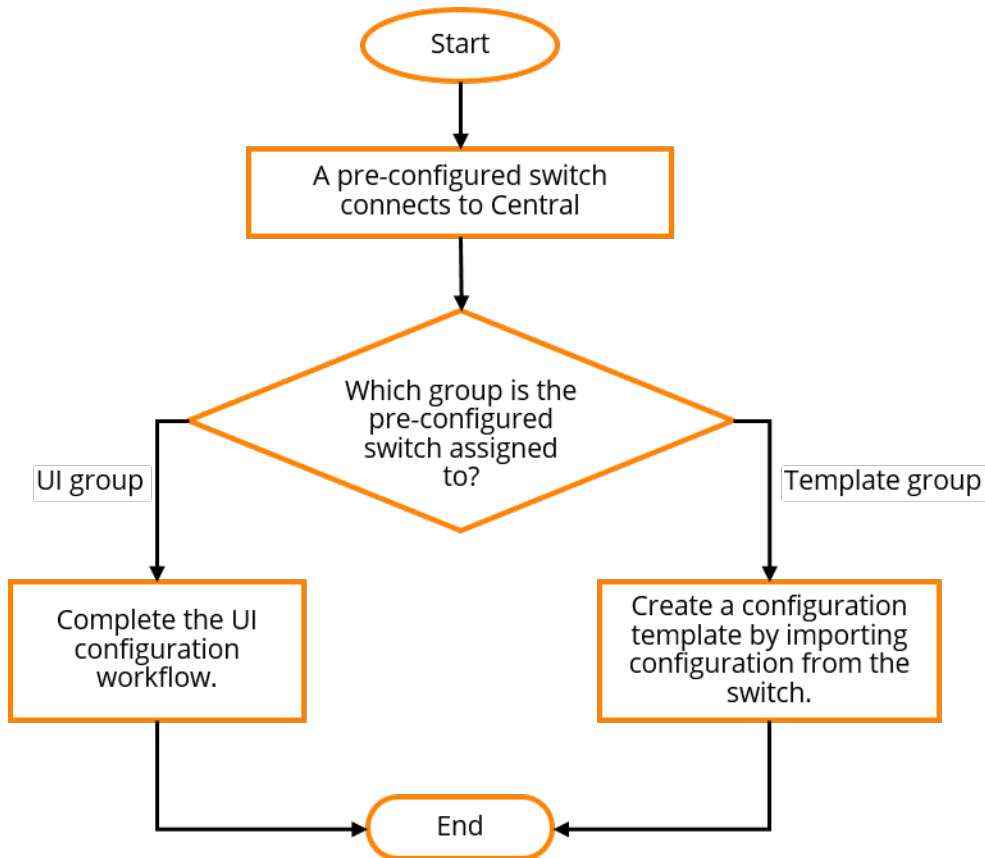
```
(switch)# activate provision force
```

The switch establishes connection with Activate and is directed to Aruba Central. If the switch is already added to the device inventory and is assigned a subscription, Aruba Central assigns it to a pre-assigned group.

Step 4: Provision the Switch to a Group


When the switch connects to Aruba Central, Aruba Central automatically assigns it to the pre-assigned group. The following figure illustrates the provisioning steps for each group type.

Figure 99 Switch Provisioning Steps Per Group Type



If the switch is assigned to a new UI group, you can modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage** > **Device(s)** > **Switches**. For more information, see [Configuring or Viewing Switch Properties in UI Groups](#).

If you have assigned the switch to a template group, you can import the existing configuration to a new configuration template and apply this template to other devices in the group. To create a configuration template using the existing configuration on the switch:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Device(s)** > **Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Templates**. The Templates page is displayed.
5. Click + to add a new template. The **Add Template** window is displayed.
6. Enter a name for the template in the **Template Name** field.
7. Ensure that **Aruba Switch** is selected in the **Device** drop-down.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
 - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.

- A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.



If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.

If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Import configuration from the switch.

Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration templates and variable definitions, see [Using Configuration Templates for Switch Management](#) and [Managing Variable Files](#).




All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information about using password commands, see the Configuring Username and Password Security chapter in the *HPE ArubaOS-Switch Access Security Guide*.

11. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the configuration Status

To verify the configuration status:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
 - To verify the configuration status for a template group, select the template group and click **configuration Audit**. The **configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **Failed / Pending config change**.
6. To compare running configuration and pending changes, click **View** under **Config Comparsion Tool**.

Workflow 2—Provisioning a Switch On-Demand

To dynamically provision switches on-demand, complete the following steps:

- [Step 1: Enable Aruba Central Management Service on the Switch](#)

- [Step 2: Add the Switch to Aruba Central](#)
- [Step 3: Assign a Subscription](#)
- [Step 4: Provision the Switch to a Group](#)
- [Step 5: Verify the configuration Status](#)

Step 1: Enable Aruba Central Management Service on the Switch

A locally-managed or pre-configured switch cannot connect to Aruba Central, unless it is configured to identify Aruba Central as its management entity. To manage such a device from Aruba Central, you must manually enable the provisioning and management service on the switch.

1. Verify if the Activate provisioning service is enabled by executing the following command at the switch CLI:

```
switch)# show activate provision
configuration and Status - Activate Provision Service
Activate Provision Service      : Enabled
Activate Server Address         : device.arubanetworks.com
```

2. If the Activate provision service is not enabled, execute the following command at the switch CLI:

```
(switch)# activate provision enable
```

3. To enable switches to automatically connect to Aruba Central, enforce ZTP on the switch:

```
(switch)# activate provision force
```

The switch establishes connection with Activate. Activate directs the switch to Aruba Central.

Step 2: Add the Switch to Aruba Central

Add the switch to the Aruba Central device inventory. For more information, see [Onboarding Devices on page 72](#)

Step 3: Assign a Subscription

To allow Aruba Central to manage the switch, ensure that a valid subscription is assigned to the switch. For more information, see [Managing Subscriptions on page 78](#).

Step 4: Provision the Switch to a Group

If the switch has a valid subscription assigned, Aruba Central marks the switch as **unprovisioned**. To preserve the switch configuration, move it to a new group.


To move the device to a UI group:

1. In the **Network Operations** app, use the filter to select **All Devices**.
2. Under **Maintain**, click **Organization > Groups**. The Groups page is displayed.
3. Select the device.
4. Click **Import configuration to New Group**. The **Import configuration** window is displayed.
5. Enter a name for the group.
6. Configure a password for the group.
7. Click **Import configuration**. Aruba Central imports the switch configuration to the new group.

You can also modify the configuration of switches in a group using the UI menu options under the **Network Operations** app > **Manage > Device(s) > Switches**. For more information, see [Configuring or Viewing Switch Properties in UI Groups](#).

To move the device to a template group:

1. [Create a template group](#).
2. On the **Groups** page, select the switch.

3. Drag and drop the switch to the new template group that you just created. Aruba Central adds the switch to the new template group.
4. To import switch configuration to a new configuration template:
 - a. In the **Network Operations** app, use the filter to select a template group.
 - b. Under **Manage**, click **Device(s) > Switches**.
 - c. Click the  configuration icon to display the switch configuration dashboard.
 - d. Click **Templates**. The Templates page is displayed.
 - e. Click + to add a new template. The **Add Template** window is displayed.
 - f. Enter a name for the template in the **Template Name** field.
 - g. Ensure that **Aruba Switch** is selected in the **Device** drop-down.
 - h. Select the switch model and the software version to which you want to apply the new template. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
 - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
 - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
 - i. Select the manufacturing part number of the switch in the **Part Number** drop-down.

The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.



If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.

If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

j. Import configuration from the switch.

Importing configuration from the switch allows you to quickly create a basic configuration template that you can apply for all devices in a template group. Before applying the template to other switches in the group, ensure that the template text is variabilized based on the deployment requirements. For more information on configuration templates and variable definitions, see [Using Configuration Templates for Switch Management](#) and [Managing Variable Files](#).




All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *HPE ArubaOS-Switch Access Security Guide*.

k. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Step 5: Verify the configuration Status

To verify the configuration status:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
 - To verify the configuration status for a template group, click **configuration Audit**. The **configuration Audit** dashboard displays the number of devices with template and configuration synchronization errors.
 - To view configuration errors for a specific device, select a switch from the filter bar. The **configuration Audit** dashboard displays the number of template and configuration synchronization errors for the device.
4. To view template errors, click **View Template Errors**.
5. To view configuration synchronization errors, click **Failed / Pending config changes**.
6. To compare running configuration and pending changes, click **View** under **Config Comparison Tool**.

Managing Password in Configuration Templates

All IAP and switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.



When configuring a password, you can add the `include-credentials` command in the template. This command stores the password in the **running-config** file associated with the switch. Aruba Central automatically executes this command while reading the switch configuration.

Password for Switches

The following format of the passwords can be set on the Switches:

```
password manager plaintext <string>
password manager sha1 <string>
password manager sha256 <string>
password manager user-name <string> plaintext <string>
password manager user-name <string> sha1 <string>
password manager user-name <string> sha256 <string>
```

Password for APs

The following format of the passwords can be set on the APs:

```
mgmt-user <STRING:username:User_name> { <STRING:password:Password> }
hash-mgmt-user <STRING:username:User_name> password cleartext <STRING:cleartext_
password:Password>
hash-mgmt-user <STRING:username:User_name> password hash <STRING:hash_password:Password>
```

Setting Password using Variables

User cannot enter the entire password line in a variable. The following examples show the valid and invalid format for entering password using a variable.

Valid format where the variable contains only the password (for example, %pass_var% = Aruba@123) for the device:

```
hostname "Aruba-2930M-24G"
password manager plaintext "%pass_var%"
include-credentials
no cwmp enable
```

Invalid format where the variable contains the password command (for example, %pass_var% = password manager plaintext Aruba@123) for the device:

```
hostname "Aruba-2930M-24G"
%pass_var%
include-credentials
no cwmp enable
```

Configuring Aruba Switches

Aruba Central supports provisioning switches in UI and template groups. Aruba Central supports basic configuration options in the UI.

The users can also assign switches to template groups and use configuration templates and variables to manage switches from Aruba Central.

See the following topics for more information on managing switches in Aruba Central:

- [Using Configuration Templates for Switch Management on page 435](#)
- [Configuring or Viewing Switch Properties in UI Groups on page 437](#)

CA Certificate Installation using API and Templates

This feature is supported for switches with a minimum firmware version of 16.09.

Aruba Central supports the installation of CA certificates through templates and APIs. Typically, an administrator uses an NB API to push the CA certificate to the Aruba Central certificate store. The certificates must be pushed to the certificate store of the same tenant. After that, use the ArubaOS-Switch CLI commands in an Aruba Central template to push the certificate as part of the configuration audit.

If the certificate push or install process is not successful, the Aruba Central audit logs display the specific failure. Only those certificates that are installed through Aruba Central are monitored by Aruba Central. Other switch certificates are not supported for monitoring.

Use the following command to push the CA certificate: `cert-prof name "<name of cert>"`

For example, if the certificate name is `ca_cert_1`, the following is the format of the command: `cert-prof name "ca_cert_1"`.

Points to Note

- Unlike IAPs and Gateways, where a certificate cannot be deleted if it is referenced in a template or a variable, in switches, users can delete a certificate even if it is referenced in a template or a variable.
- Deleting an existing certificate and creating a new certificate with the same name but with different certificate data does not guarantee that the new certificate is installed for switches. Re-apply the template or variable to ensure that the change is propagated.

Using Configuration Templates for Switch Management

Templates in Aruba Central refer to a set of configuration commands that can be used by the administrators for provisioning devices in a group. Configuration templates enable administrators to apply a set of configuration parameters simultaneously to multiple switches in a group and thus automate switch deployments.



To minimize configuration errors and troubleshoot device-specific configuration issues, Aruba recommends that the device administrators familiarize themselves with the CLI configuration commands available on Aruba switches.


Creating a Group for Template-Based Configuration

For template-based provisioning, switches must be assigned to a group with template-based configuration method enabled.

For more information, see [Managing Groups on page 91](#) and [Assigning Devices to Groups on page 92](#).

Creating a Configuration Template

To create a configuration template for switches:

1. In the **Network Operations** app, use the filter to select a template group.
2. Under **Manage**, click **Devices > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Templates**. The Templates page is displayed.
5. Click **+** to add a new template. The **Add Template** window is displayed.
6. Enter a name for the template in the **Template Name** field.
7. Ensure that **Aruba Switch** is selected in the **Device** drop-down.
8. Select the switch model and software version. You can specify any of the following combinations:
 - **ALL** for both **Model** and **Version**—To apply the template to all switch models and all supported switch software versions.
 - **ALL** for **Model** and a specific software version for **Version**—To apply the template to all switch models running the specified software version.
 - **ALL** for **Version** and a specific switch model for **Model**—To apply the template to a specific switch model and all software versions supported by the selected switch model.
 - A specific switch model and a software version—To apply the template to a specific switch model and the software version. The template created for a specific switch model and a firmware version takes precedence over the template that is created for all platforms and versions.
9. Select the manufacturing part number of the switch in the **Part Number** drop-down.

The **Part Number** drop-down is displayed only if you select a switch model in the **Model** drop-down.



If you select a specific switch model and part number, you can apply the template to a standalone switch and not to a stack.

If you select **All** in the **Model** drop-down, or if you select a switch model and **All** in the **Part Number** drop-down, you can apply a template to both a standalone switch and stack.

10. Build a new template or import configuration information from a switch that is already provisioned in the template group.

- To build a new template, add the switch command information in the **Template** text box. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note on page 436](#).
- To import configuration text from a switch that is already provisioned in the template group:
 - a. Select the switch from which you want to import the configuration.
 - b. Click **Import Template**. The imported configuration is displayed in the **Template** text box.
 - c. If required, modify the configuration parameters. Ensure that the template text adheres to the guidelines listed in the [Important Points to Note on page 436](#).

Importing configuration from an existing device in the template group allows you to quickly create a basic template. However, before applying the template to other switches in the group, ensure that the template text is variabilized as per your deployment requirements.



All switch templates must include a password command to set a password for the device. The template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command. For more information, see [Managing Password in Configuration Templates](#).

For more information about using password commands, see the Configuring Username and Password Security chapter in the *HPE ArubaOS-Switch Access Security Guide*.

11. Click **Save**. After you apply the configuration template, switches reboot and reconnect to Aruba Central with the new configuration.

Important Points to Note

Note the following points when adding configuration text to a template:

- The CLI syntax in the switch template must be accurate. Aruba recommends that you validate the configuration syntax on the switch before adding it to the template text.
- Ensure that the command text indentation matches the indentation in the running configuration.
- The commands in the template are case-sensitive.



When configuring a password, you can add the `include-credentials` command in the template. This command stores the password in the **running-config** file associated with the switch. Aruba Central automatically executes this command while reading the switch configuration.

The following example illustrates the case discrepancies that the users must avoid in the template text:

```
trunk E1-E4 trk1 trunk
interface Trk1
  dhcp-snooping trust
  exit

trunk E1-E4 trk1 trunk
switch-interconnect trk1

trunk E5-E6 trk2 trunk
vlan 5
  name "VLAN5"
  untagged Trk2
  tagged Trk1
  isolate-list Trk1
  ip igmp forcedfastleave Trk1
  ip igmp blocked Trk1
  ip igmp forward Trk1
```



```

    forbid Trk1

loop-protect Trk2

trunk E1-E4 trk1 trunk
trunk E4-E5 trk2 trunk
spanning-tree Trk1 priority 4
spanning-tree Trk2 admin-edge-port

trunk A2-A4 trk1 trunk
igmp fastlearn Trk1

trunk E4-E5 trk2 trunk
ip source-binding 2 4.5.6.7 b05ada-96a4a0 Trk2

[no] ip source-binding trap OutOfResources

snmp-server mib hpSwitchAuthMIB ..

snmp-server mib hpicfMACsec unsecured-access ..

[no] lldp config <P-PORT-LIST> dot1TlvEnable ..

[no] lldp config <P-PORT-LIST> medTlvEnable ..

no lldp config <P-PORT-LIST> medPortLocation..

[no] lldp config <P-PORT-LIST> dot3TlvEnable ..

[no] lldp config <P-PORT-LIST> basicTlvEnable ..

[no] lldp config <P-PORT-LIST> ipAddrEnable <lldp-ip>

trunk-load-balance L4-based
trunk-load-balance L3-based

```

Best Practices

Aruba recommends you to follow the below steps to use configuration templates in managing switches:

1. Configure the switch.
2. Add the switch to Aruba Central.
3. Create the template, You can use **Import template** option to import an existing template created for switches.
4. Modify the template based on the user requirement. For example, addition or removal of variables.
5. Save the edited template.

Configuring or Viewing Switch Properties in UI Groups

This section describes the configuration and viewing procedures for the switches in the UI groups.



Aruba Central does not support pre-configured switches in a UI group. If you want to move a switch from a template group to a UI group, you must clear the switch configuration, delete the device from Aruba Central, and then provision the switch as a new device in a UI group.

To configure or view properties of the switches provisioned in UI groups, perform the following procedure:

1. In the **Network Operations** app, use the filter to select a group or a device.


2. Under **Manage**, click **Device(s) > Switches** to display the switch dashboard.
 3. Click the  configuration icon to edit the switch properties. Tabs to access different configuration pages are displayed.
- The following table describes the different configuration pages and their functions.

Table 124: *Tabs for Configuring Switches Provisioned in a UI Group*

| Tab | Function |
|------------------------|---|
| Switches | Configure or view general switch properties, such as, hostname, type of IP addressing, and so on. See Configuring or Viewing the Switch Properties . |
| Stacks | Create stacks, add members, or view stacking details such as stack type, stack id, topology, and so on. See Configuring Switch Stacks using UI Groups |
| Ports | Assign or view port properties, such as, PoE, access policies, and trunk groups. See Configuring Switch Ports on Aruba Switches |
| PoE | Configure or view PoE settings for each port. See Configuring PoE Settings on Aruba Switch Ports . |
| Trunk Groups | Configure or view trunk groups and their associated properties, such as, members of the trunk group, type of trunk group, and so on. See Configuring Trunk Groups on Aruba Switches in UI Groups . |
| VLANs | Configure or view VLANs and the associated ports and access policies. See Configuring VLANs on Switches |
| Spanning Tree | Configure or view spanning tree protocol and its associated properties. See Enabling Spanning Tree Protocol on Aruba Switches in UI Groups |
| Loop Protection | Configure or view loop protection and its associated properties. See Configuring Loop Protection on Aruba Switch Ports . |
| Access Policy | Add or view access policies. See Configuring Access Policies on Aruba Switches . |
| DHCP Snooping | Configure or view DHCP snooping, authorized DHCP servers IP addresses, and their associated properties. See Configuring DHCP Snooping . |
| Port Rate Limit | View or specify bandwidth to be used for inbound or outbound traffic for each port. See Configuring Port Rate Limit on Aruba Switches in UI Groups . |
| Access/DNS | Configure or view the administrator and operator logins. See Configuring System Parameters for a Switch . |
| SNMP | Add or view SNMP community and its trap destination. See Configuring SNMP on Aruba Switches . |
| CDP | Configure CDP and its associated properties. See Configuring CDP . |
| Routing | Configure or view a specific routing path to a gateway. See Configuring Routing on Aruba Switches . |

| Tab | Function |
|----------------------------|--|
| DHCP Pools | Add or view a DHCP pool and its associated properties. See Configuring DHCP Pools on Aruba Switches . |
| IGMP | Configure IGMP and its associated properties. See Configuring IGMP . |
| Time | Configure time synchronization in switches. See Configuring Time Synchronization . |
| Configuration Audit | View configuration sync errors and overrides. See Viewing Configuration Status . |

Configuring or Viewing the Switch Properties

When you add a switch to a group, the switch inherits the configuration of the group.

It is not recommended to add a switch with an existing configuration to a group that already has a defined configuration. Aruba Central permits device-level overrides, however the overrides are resolved or preserved based on the requirements.

You can create a new group and add a pre-configured switch to that group so that the group inherits the configuration of the switch. If the switch inherits the group configuration, the configuration parameters are already defined. If required, you can edit these parameters. All factory default switches are provisioned in a new group and these parameters can also be defined at the group level.

To edit the configuration parameters for the switch in an UI group, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon. The **Switches** page is displayed with the following information:

Table 125: Switches Parameters

| Name | Description | Value |
|------------------------|--|---|
| MAC Address | MAC address of the switch. | Property inherited from the switch. |
| Hostname | Name of the host. | A string. |
| IP Assignment | Method of IP assignment as static or DHCP. | Static or DHCP . |
| IP Address | IP address for static IP assignment. | IPv4 address. |
| Netmask | Netmask for static IP assignment. | Netmask address. |
| Default Gateway | Default gateway for static IP assignment. | IPv4 address. |
| Location | Location of the switch. | For example: Portland, Oregon. |
| Contact | Email address or phone number. | For example: admin@xyzcompany.com . |

4. To edit the switch configuration parameters, click the edit icon.
5. Click **OK**.
6. Click **Save Settings**.

Configuring Switch Ports on Aruba Switches

To view the port details of a switch, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
 2. Under **Manage**, click **Device(s) > Switches**.
 3. Click the  configuration icon to display the switch configuration dashboard.
 4. Click **Interface > Ports**. The Ports page is displayed with the list of ports configured on the switch.
- For the Aruba Mobility Access Switches, the Ports page displays the following information:

Table 126: *Ports Page—Mobility Access Switches*

| Name | Description | Value |
|-------------------------|--|---|
| Port Number | Indicates the number assigned to the switch port. | Dependent on the type of switch. |
| Admin Status | Indicates the operational status of the port. | Up or Down . |
| Port Mode | Indicates the mode of operation. The port can be configured to function in Trunk or Access mode. | Trunk Mode or Access Mode . By default, a port is in Access mode and carries traffic only for the VLAN to which it is assigned. In Trunk mode, a port can carry traffic for multiple VLANs. |
| VLAN | Shows the VLAN to which the port is assigned. Based on the port mode, you can assign different types of VLAN. | <ul style="list-style-type: none">■ For Access mode, an Access VLAN can be specified.■ For Trunk mode, the Native VLAN and Allowed VLAN can be configured. |
| Auto Negotiation | Indicates the status of the Auto Negotiation. | <ul style="list-style-type: none">■ If auto negotiation is enabled, the Speed and Duplex fields are automatically set to Auto.■ If auto negotiation is disabled, the speed can be set to 10 Mbps, 100 Mbps, or 1 Gbps and the duplex mode can be set to half or full. |
| Speed/Duplex | Displays the speed and duplex configuration settings for the client traffic. | |
| Trusted | Indicates if the port is trusted. | |

For Aruba switches, the Ports page displays the following information:

Table 127: Ports Page—Aruba Switches

| Name | Description | Value |
|----------------------------|--|---|
| Port Number | Indicates the number assigned to the switch port. | Dependent on the switch type. |
| Name | Name of the port for easy identification. You can add or edit port names. However, do not delete port names as it may cause config push to fail. The config push failure may also arise if you move a switch from a group configured with port names to a new group. This issue is only applicable to switch firmware versions earlier than 16.08.0002. | For example: UPLINK-SRVR-ROOM. |
| Admin Status | Allows you to set the operational status of the port. | Up or Down |
| Speed-Duplex (Mbps) | Allows you to set the maximum bandwidth of the port traffic. | Select from drop-down menu. Default is Auto . |
| Access Policy (In) | Allows you to apply an existing access policy for the inbound traffic on the port. | Select from drop-down menu. See Configuring Access Policies on Aruba Switches . |
| Access Policy (Out) | Allows you to apply an existing access policy for the outbound traffic on the port. | Select from drop-down menu. See Configuring Access Policies on Aruba Switches . |
| Trunk Group | Displays the name of the trunk group to which the port is assigned. | To configure a Trunk Group, see Configuring Trunk Groups on Aruba Switches in UI Groups . |
| DHCP Snooping | Status of port to filter DHCP messages received at the port. | Trust or Untrust |


5. Select the port row, click **Edit**.

6. Click **Save**.

Configuring PoE Settings on Aruba Switch Ports

Power over Ethernet (PoE) is a technology that allows the switches to deliver power to the powered devices (PD). If you have switches provisioned in UI groups, you can enable or disable PoE operation on switch ports. The PoE page displays the configuration details of all PoE enabled ports.

To configure the PoE settings of a switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > PoE**. The PoE page is displayed.
5. Select the port(s) you want to edit and click **Edit**.

The **Edit Power Over Ethernet Settings** window is displayed.

6. Configure the following parameters:

Table 128: *PoE Parameters*

| Name | Description | Value |
|-----------------------------|---|----------------------------|
| Port | The number assigned to the switch port. The port number is auto-generated and cannot be changed in the settings. | Auto-generated port number |
| PoE | The status of the PoE operation on the port. When PoE is enabled, the switch sends power to the powered device (PD). | Enabled or Disabled |
| Priority | The PoE priority level of the port. If there is not enough power available to provision all active PoE ports, then PoE ports at priority level as critical are powered first, then high and low priority at the last. | Low, High or Critical |
| LLDP MED TLV (PoE) | The status of the LLDP MED TLV configuration. Switches use LLDP to repeatedly query the PD to discover the power requirement and send the exact power required. | Enabled or Disabled |
| LLDP Dot3 TLV (PoE+) | The status of the LLDP Dot3 TLV configuration. | Enabled or Disabled |
| Allocation By | The PoE power allocation method used for the port. If usage is selected, then the allocation is made based on the automatic allocation by the PD. If class is selected, then the allocation is made based on class of the PD. | Usage or Class |
| Pre Std Detect | The status of support for pre-standard devices. When this option is enabled, switch supports some pre-802.3af devices. | Enabled or Disabled |
| Configured type | The user-defined identifier for the port to identify its intended use. | A string |



The status of LLDP in PoE page is displayed as Enabled only if one or both LLDP settings (LLDP MED TLV (PoE) and LLDP Dot3 TLV (PoE+)) are enabled for the port.

7. Click **OK**.

8. Click **Save Settings**.

Configuring VLANs on Switches

The Aruba switches support the following types of VLANs:

- Port-based VLANs—In the case of trusted interfaces, all untagged traffic is assigned a VLAN based on the incoming port.
- Tag-based VLANs—In the case of trusted interfaces, all tagged traffic is assigned a VLAN based on the incoming tag.

The Aruba Mobility Access Switch also supports the following types of VLANs:

- Voice VLANs—You can use voice VLANs to separate voice traffic from data traffic when the voice and data traffic are carried over the same Ethernet link.

- **MAC-based VLANs**—In the case of untrusted interfaces, you can associate a client to a VLAN based on the source MAC of the packet. Based on the MAC, you can assign a role to the user after authentication.

Adding VLAN Details

By default, all ports in the Switches are assigned to VLAN 1. However, if the ports are assigned to different VLANs, the VLANs page displays their details.

To add a VLAN, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > VLANs**. The VLANs page is displayed.
5. In the **VLANs Settings** accordion, click **+** to add a VLAN and configure the following parameters.

Table 129: *Configuring and Viewing VLAN Parameters*

| Name | Description | Value |
|-----------------------|--|---|
| Name | The name of the VLAN. | A string |
| IP Assignment | The method of IP assignment. | Static, DHCP, or Disabled |
| IP Address | The IP address for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down. | IPv4 address |
| Netmask | The netmask for static IP assignment. This field is enabled only when you select Static from the IP Assignment drop-down. | IPv4 address |
| DHCP Server | Indicates whether the switch is configured as the DHCP server on the VLAN. <ul style="list-style-type: none"> ■ This field is enabled only when you select Static from the IP Assignment drop-down. ■ You can enable DHCP Server option only when there are no DHCP Helper IP addresses configured. | Toggle switch to the on or off position |
| DHCP Helper IP | IP address of the DHCP helper server for that VLAN. <ul style="list-style-type: none"> ■ You can configure a maximum of 16 DHCP helper IP addresses for each VLAN. ■ You can configure DHCP Helper IP addresses only when DHCP Server option is disabled. | IPv4 address |
| Voice | Indicates whether support for voice VLANs are enabled for the VLAN interface. | Toggle switch to the on or off position |
| Jumbo | Indicates whether jumbo packet handling is enabled for the VLAN interface. | Toggle switch to the on or off position |

| Name | Description | Value |
|---------------------------------|---|---|
| Access Policy (In) | The security policy that you want to apply for the inbound traffic. | See Configuring Access Policies on Aruba Switches . |
| Access Policy (Out) | The security policy that you want to apply for the outbound traffic. | |
| VLAN Access Policy (In) | The security policy that you want to apply for the bridged and routed inbound packets on the VLAN. | |
| VLAN Access Policy (Out) | The security policy that you want to apply for the bridged and routed outbound packets on the VLAN. | |

6. To configure the VLAN ports, complete the following steps:
 - a. In the **Ports** table, select the port number(s).
 - b. Select any of the following port modes:
 - **Tagged Ports**
 - **Untagged Ports**
 - **None**
7. To assign the VLAN to a trunk group, select the trunk group in the **Trunk Groups** table.
8. Click **OK**.
9. Click **Save Settings**.

Editing the VLAN Details

To edit the details of a VLAN, point to the row for the VLAN, and click the edit icon in the **Actions** column, and configure the parameters.

Deleting VLAN Details

To delete the VLAN details, complete the following steps:

1. Ensure that the VLANs are not tagged to any ports.
2. Point to the row for the VLAN, and click the edit icon in the **Actions** column.




VLAN 1 is the primary VLAN and cannot be deleted.

Configuring DHCP Relay Settings

You can configure a switch as a DHCP relay agent for transmitting DHCP messages between the DHCP server and client. You can also configure the option-82 feature for the switch to include DHCP relay information in the forwarded DHCP request messages.

To configure a switch as a DHCP relay agent, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > VLANs**. The VLANs page is displayed.
5. Expand the **DHCP Relay Settings** accordion.
6. To enable DHCP relay, move the **DHCP Relay** toggle switch to the on position.



DHCP Relay option is enabled by default.

7. To enable option-82 feature, move the **DHCP Relay Option 82** toggle switch to the on position.
8. Click **Save Settings**.

Configuring Trunk Groups on Aruba Switches in UI Groups

If you have switches provisioned in an UI group, Aruba Central enables you to configure port trunking on these switches using the UI workflows. The network administrator can configure a trunk group on switches to create one logical link or a trunk by aggregating multiple links. The trunk link functions as a high-speed link to provide increased bandwidth.

A trunk group is a set of up to eight ports configured as members of the same port trunk.

Table 130: *Trunk Group configuration Support Per Switch Platform*

| Aruba Switch Platform | Valid Trunk Groups |
|--|--------------------|
| Aruba 2540 Switch Series | Trk1-Trk26 |
| Aruba 2920 Switch Series Aruba 2930F Switch Series Aruba 2930M Switch Series | Trk1-Trk60 |
| Aruba 2530 Switch Series | Trk1-Trk24 |
| Aruba 3810 Switch Series | Trk1-Trk144 |

The following are some guidelines:

- All ports in the same trunk group must be of the same trunk type (LACP or trunk.)
- The names of the trunk groups include the prefix **Trk** followed by the numbers in a sequential order. For example, Trk1, Trk2 and so on.
- When STP is enabled on the switch, the STP configuration is applied for all ports at the trunk group level. Individual ports cannot be configured for STP or VLAN operation.

Adding Trunk Groups on Switches

To configure a trunk group on switches:

Ensure that the switches are onboarded and provisioned to a UI group in Aruba Central.


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > Trunk Groups**. The Trunk Groups page is displayed.
5. In the **Trunk Group** table, click **+** to add a trunk group and configure the following parameters:

Table 131: *Ports Page—Aruba Switches*

| Name | Description | Value |
|-----------------------|--|-------------------------------|
| Name | Indicates the number assigned to the switch port. | String. |
| Type | A name of the port for easy identification. | Trunk or LACP . |
| Untagged VLANs | If the switch ports are untagged, select a VLAN from the Untagged VLAN list. | Select from drop-down menu. |
| Tagged VLANs | If the switch ports are tagged, select the VLANs from the Tagged VLAN list. | Select from drop-down menu. |
| Ports | Select the ports for trunking. You can use up to eight ports for link aggregation. The ports in a trunk group need not be consecutive. | Select from drop-down menu. |

6. Click **OK**.
7. Click **Save Settings**.
8. To verify the configuration, click **configuration Audit**.

Editing Trunk Groups on Switches

To edit details of a trunk group, point to the row for the trunk group, and click the edit icon in the **Actions** column, and configure the parameters.

Deleting Trunk Groups on Switches

To delete a trunk group, point to the row for the trunk group, and click the delete icon in the **Actions** column.

Enabling Spanning Tree Protocol on Aruba Switches in UI Groups

The Spanning Tree Protocol (STP) eliminates Layer 2 loops in networks, by selectively blocking some ports and allowing other ports to forward traffic, based on global (bridge) and local (port) parameters you can configure.

STP is always disabled by default on Aruba switches. To configure STP for switches provisioned in the UI groups:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > Spanning Tree**. The Spanning Tree page is displayed.
5. Enable MSTP if you want to avoid bridge loops between network nodes and to maintain a single active path between the network nodes. MSTP will be enabled for all VLANs assigned to switch ports. If you have a trunk group configured for the switches in the group, MSTP is enabled at the trunk level.
6. Set the priority of the UI group.
7. To configure MSTP parameters for ports, select the port row(s) in **Port Settings**, click **Edit**.
8. To configure MSTP parameters for trunks, select the trunk group row(s) in **Trunk Group Settings**, click **Edit**.
9. Configure the following MSTP parameters for ports or trunks of individual switches:

Table 132: *Viewing or Configuring Port and Trunk Settings*

| Name | Description | Value |
|------------------------|---|--|
| Priority | <p>A number used to identify the root bridge in an STP instance. The switch with the lowest value has the highest priority and is the root bridge. A higher numerical value means a lower priority; thus, the highest priority is 0.</p> <p>When the switches in a network select their root bridge, two parameters are considered, the STP priority and the MAC address of the switch. All Aruba switches have a default STP priority of 8. So the switch with the lowest MAC automatically gets selected as a root bridge. This is not a recommended process as it randomizes the selection of the root bridge.</p> | 0 – 8 Default: 8 |
| BPDU Protection | A security feature used to protect the active STP topology by preventing spoofed BPDU packets from entering the STP domain. In a typical implementation, BPDU protection is applied to the edge ports and access ports connected to end-user devices that do not run STP. If STP BPDU packets are received on a protected port, the port is disabled and the network manager is alerted via SNMP traps. | Enable or Disable Default: Disable |
| BPDU Filter | <p>Enables control of STP participation for each port. The feature can be used to exclude specific ports from becoming part of STP operations. A port with the BPDU filter enabled ignores incoming BPDU packets and stays locked in the STP forwarding state. All other ports maintain their role.</p> <p>Recommended ports for BPDU filter: Ports or trunks connected to client devices.</p> | Enable or Disable Default: Disable |
| Admin-Edge | <p>When set, the port directly goes into forwarding state.</p> <p>This configuration is not recommended for ports which connect to infrastructure devices. A BPDU guard also assists when a port inadvertently goes into a forwarding state.</p> | Enable or Disable Default: Disable |
| Root Guard | Sets the port to ignore superior BPDUs to prevent the switch from becoming the Root Port. | Enable or Disable Default: Disable |
| Trunk Group | Sets the trunk group to which the port is assigned. | Enable or Disable Default: Disable |


Configuring Loop Protection on Aruba Switch Ports



Enabling Loop Protection consumes CPU resources.

Loop protection provides protection against loops by transmitting loop protocol packets out of ports. For switches provisioned in UI groups, administrators can enable or disable loop protection on the switch ports or trunks by using the menu options available under the Network Operations app.

Loop protection is always disabled by default on Aruba switches. To configure loop protection for switches provisioned in the UI groups:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Interface > Loop Protection**. The Loop Protection page is displayed.

5. Depending on whether you want to configure a port or trunk, complete one of the following steps:

- In the **Port Settings** tab, select the port(s), click **Edit**.
- In the **Trunk Settings** tab, select the trunk(s), click **Edit**.

Table 133: *Viewing or Configuring Port Settings*

| Name | Description | Value |
|------------------------|--|--|
| Port | The number assigned to the switch port. | 0 – 65535 |
| Loop Protection | Enables or disables loop protection. | Enable or Disable Default: Disable |
| Trunk Group | Name of the trunk group to which the port belongs. | Dependent on the switch type. |

Table 134: *Viewing or Configuring Trunk Settings*

| Name | Description | Value |
|------------------------|--|--|
| Trunk Group | Name of the trunk group to which the port belongs. | Dependent on the switch type. |
| Loop Protection | Enables or disables loop protection. | Enable or Disable Default: Disable |

6. Set loop protection to **Enable** in the Loop Protection drop-down.


7. Click **OK**.

8. Click **Save Settings**.

Configuring Port Rate Limit on Aruba Switches in UI Groups

Rate limiting allows allocating a specific bandwidth for the incoming and outgoing traffic from each port. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

Port rate limit is always disabled by default on Aruba switches. To configure port rate limit for switches provisioned in the UI groups:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Security > Port Rate Limit**. The Port Rate Limit page is displayed.
5. Under **Port Rate Limit**, select the port or ports you want to modify and click **Edit**.
6. Set the value of **Limit** to **Traffic by Category** if you prefer to set individual limitations.
Else, set the value of **Limit** to **All Traffic** to set a collective limitation.

Percentage limits are based on link speed. For example, if a 100 Mbps port negotiates a link at 100 Mbps and the inbound rate-limit is configured at 50%, then the traffic flow through that port is limited to no more than 50 Mbps. Similarly, if the same port negotiates a 10 Mbps link, then it allows no more than 5 Mbps of inbound traffic. Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, disable the port instead of configuring a rate limit of 0.



- a. If you select **All Traffic**, rate limit is placed on all packets received from unknown sources. Move the slider to **Enable** and then enter the values for **IN** and **OUT** in percentage values.
- b. If you select **Traffic by Category**, refer to the following table to set the correct parameters.


Table 135: *Traffic by Category Parameters*

| Name | Description | Value |
|------------------------|--|---|
| Broadcast | Sets a rate limit on broadcast traffic. | Expressed as percentage of the total bandwidth. |
| Multicast | Indicates the operational status of the port. | |
| Unknown Unicast | Indicates the mode of operation. The port can be configured to function in Trunk or Access mode. | |
| ICMP | Sets a rate limit on ICMP traffic. | |

Configuring CDP

Cisco Discovery Protocol (CDP) is used to share information about connected network devices. It is used to share information such as device type, model, interfaces, IP addresses, operating system versions, and VLANs. You can configure CDP modes for the switch.

To enable CDP for the switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **System > CDP**. The CDP page is displayed.
5. To enable CDP for the switch, move the **CDP** toggle switch to the on position.
6. Select any of the following modes from the **Mode** drop-down:
 - **rx-only**—Switch only receives CDP information from other connected devices and stores this information in the database. However, it does not send its own information to other devices.
 - **pass-through**—CDP information passes through the switch to other connected devices.
 - **pre-standard-voice**—Enables CDP-compatible voice VLAN discovery with pre-standard VoIP phones.
7. Click **Save Settings**.


Configuring Access Policies on Aruba Switches



Aruba Central does not support access policy configuration on Aruba Mobility Access Switches.

To restrict certain types of traffic on physical ports of Aruba switches, you can configure ACLs from the Aruba Central UI.

To create an access policy, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Security > Access Policy**. The Access Policy page is displayed.
5. Click **+** to add a new access policy. The **New Access Policy** page is displayed.
6. Enter a name for the policy.

7. Click **Add**.

8. To add a rule to the access policy, click + under **Rules for test**, and configure the following parameters:

Table 136: *Configuring Rules for Access Policies*

| Name | Description | Value |
|--------------------|--|---|
| Source | Select a source of the traffic for which you want to an access rule. | <ul style="list-style-type: none">■ Any, Network, or Host■ For Network, specify IP address and mask■ For Host, specify IP address |
| Destination | Select a destination. | <ul style="list-style-type: none">■ Any, Network, or Host■ For Network, specify IP address and mask■ For Host, specify IP address |
| Protocol | Select the type of protocol. Some protocols also require source and destination ports. | Select from drop-down. |
| Action | The action that the switch must perform on the traffic received at a port. | Permit or Deny |

9. Click **OK**.

10. Click **Save Settings**.

The access policies must be applied to a switch port and the VLAN assigned to a port. For more information on access policy assignment to ports and VLANs, see the following topics:

- [Configuring Switch Ports on Aruba Switches](#)
- [Configuring VLANs on Switches](#)


Configuring SNMP on Aruba Switches

You can configure SNMP community settings and trap settings through the UI.



SNMP settings can be configured only when switch is installed with the minimum supported firmware version of 16.09 or later.

To enable SNMP on a switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches** to display the switch dashboard.
3. Click the  configuration icon to edit switch properties and configure options.
4. Click **System > SNMP**. The SNMP page is displayed.
5. Move the **SNMP** toggle switch to the on position.

Configuring community settings

You can add or delete SNMP communities to restrict access to the switch.

Adding a read community

To add an SNMP community, complete the following steps:

1. In the **SNMP** page, expand the **Community Settings** accordion.
The **Read Community** table displays the list of communities that have read-only access.
2. To add a read community, click +. The **Add Community** window is displayed.
3. Enter the name of the community in the **Community** text box and click **OK**.

Deleting a read community

To delete a read community, click the delete icon for the community you want to delete.

Configuring trap settings

You can configure authentication, trap destination, and trap categories using trap settings.

Adding a trap destination

To add a trap destination, complete the following steps:

1. In the **SNMP** page, expand the **Trap Settings** accordion.
The **Trap Destination** table displays the following information:
Destination IP—The destination IP address for sending the trap.
Community—The community name used for sending the trap.
2. To add a read destination, click +. The **Add Trap Destination** window is displayed.
3. Configure the parameters listed in step 1.
4. Click **OK**

Deleting a trap destination

To delete a trap destination, point to the row for the trap destination, and click the delete icon in the **Actions** column.

Enabling trap categories

To enable trap categories, complete the following steps:


1. In the **Trap Settings** accordion, select the authentication type used to connect to the SNMP server from the **Authentication** drop-down.
2. In the **Trap Category** table, select the checkbox for the trap category you want to enable.
3. Click **Save Settings**.



The availability of trap categories differs based on the device model.

Configuring DHCP Pools on Aruba Switches

To configure a new DHCP pool on a switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Security > DHCP Pools**. The DHCP Pools page is displayed.



Aruba 2530 Switch Series do not support DHCP server on the device platform. Hence, Aruba Central pushes the

group-level configuration for DHCP to all applicable devices in the group except the Aruba 2530 Switch Series.

If any of the devices is running a lower version, a warning message is displayed, and the DHCP configuration changes are pushed only to the devices that support the DHCP. If the devices are upgraded to a supported version or moved out of the group, the warning message will not be displayed.

5. To activate the DHCP service, move the **Enable DHCP service** toggle switch to the on position.

The DHCP service can be enabled only if there is a valid DHCP pool.

6. To add a new DHCP pool, click + and configure the following parameters:

Table 137: *Configuring a DHCP Pool*

| Name | Description | Value |
|------------------------------|---|---|
| Name | Name of the pool. | A string. |
| Network | A valid network IP address to assigned to the DHCP pool. | IPv4 address |
| Netmask | Netmask of the DHCP pool. | Subnet mask |
| Lease Time | The lease time for the DHCP pool in days-hours-minutes format. | You can set a maximum value of 365 days 23 hours and 59 minutes in the DD-HH-MM format. |
| Default Router | IP address of the default router in the subnet. | You can add up to 8 IP addresses. |
| DNS Server | Address of the DNS server. To add multiple DNS servers, click +. | You can add up to 8 DNS servers. |
| Netbios Server | Address of the Netbios server. The Netbios server address configuration is not required for Mobility Access Switches. To add multiple Netbios servers, click +. | You can add up to 8 Netbios servers. For Mobility Access Switches, an option called WINS Server is available. |
| IP Address Range | IP address range within the network and network mask combination. To add multiple IP address range, click +. | You can add up to 64 IP address range. |
| Exclude Address Range | IP address range to exclude. This field is available only for the Mobility Access Switches. To add multiple excluded address range, click +. | You can add up to 64 IP address range. |
| Option | The code type, and ASCII or HEX value of the DHCP option to configure. To add multiple options, click +. | You can add up to 8 options. A value within the range of 2-254 with type as hexadecimal and ASCII is valid. |

7. Click **Add**.

8. Click **Save Settings**.

9. To edit the details of a DHCP pool, point to the row for the DHCP pool, and click the edit icon in the **Edit** column, and configure the parameters.

10. To delete a DHCP pool, point to the row for the DHCP pool, and click the delete icon in the **Delete** column. When the **Do you want to delete <DHCP Pool Name>?** pop-up window prompts you, click **Yes**.

Configuring DHCP Snooping

DHCP snooping provides network security by filtering untrusted DHCP messages. Filtering is performed by distinguishing trusted ports connected to a DHCP server or switch and untrusted ports connected to end-users.


When you enable DHCP snooping, DHCP packets received at untrusted ports will be dropped, because all ports are configured as untrusted by default. You must configure the ports to be trusted in the **Switches > Interface > Ports** page.

You must also configure authorized DHCP servers for the network to have a functional DHCP server that serves clients on this switch.

By default, DHCP snooping is disabled for the switch.

Enabling DHCP Snooping on a Switch

To enable DHCP snooping on a switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Security > DHCP Snooping**. The DHCP Snooping page is displayed.
5. To enable DHCP snooping for the switch, move the **DHCP Snooping** toggle switch to the on position.
6. To enable option-82 for the switch, move the **DHCP Snooping Option-82** toggle switch to the on position.

When you enable both DHCP snooping and option-82, the switch drops the option-82 information from the DHCP packets.

7. Click **Save Settings**.

Adding Authorized DHCP Servers for a Switch

To add the list of IP addresses of authorized DHCP servers for a switch, complete the following steps:

1. In the DHCP Snooping page, click + in the **Authorized DHCP Servers IP** table. The Add Authorized DHCP Server IP window is displayed.
2. Enter the IP address in the **Authorized DHCP Servers IP** field.
3. Click **OK**.
4. Click **Save Settings**.

Deleting Authorized DHCP Servers for a Switch

To delete the authorized DHCP servers IP addresses, in the **Authorized DHCP Servers IP** table, point to IP address, and click the delete icon for the DHCP server IP you want to delete.

Enabling DHCP Snooping for a VLAN

To enable DHCP snooping for a VLAN, complete the following steps:


1. In the **DHCP Snooping Settings** table, select the VLAN row(s) for which you want to configure DHCP snooping, and click **Edit**.
2. Select **Enable** or **Disable** from the **DHCP Snooping** drop-down.
3. Click **OK**.
4. Click **Save Settings**.

Configuring IGMP

In a network where IP multicast traffic is transmitted for various multimedia applications, Internet Group Management Protocol (IGMP) helps reduce bandwidth usage on a per-port basis on a switch. Enabling IGMP for a VLAN allows the ports to detect IGMP queries and report packets, and manage IP multicast traffic through the switch.

By default, IGMP is disabled for all VLANs.

To enable IGMP for a VLAN, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **IGMP**. The IGMP page is displayed with the list of existing VLANs.
5. Select the VLAN row(s) for which you want to configure IGMP, and click **Edit**.
6. Select **Enable** or **Disable** from the **IGMP** drop-down.
7. Click **OK**.
8. To configure the switch to filter unknown multicast messages, move the **Filter Unknown Multicast** toggle switch to the on position.
9. Click **Save Settings**.

Configuring Time Synchronization

Time synchronization in a switch ensures maintaining a uniform time among all interoperating devices. Aruba Central offers the Simple Network Time Protocol (SNTP) time synchronization protocol for switches. In SNTP, Aruba Central supports broadcast, unicast, and DHCP modes.

To configure time synchronization in a switch, complete the following steps:


1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **System > Time**. The Time page is displayed.
5. Configure the following parameters.

Table 138: *Configuring Time Synchronization Parameters*

| Name | Description | Value |
|----------------------------|---|---|
| Time Sync Method | The synchronization method or protocol to use for synchronizing the time on the switch. | SNTP |
| Mode | <p>The operating mode for connecting to a time server. The following modes are supported:</p> <ul style="list-style-type: none"> ■ Broadcast—The switch acquires time updates from the data that any time server broadcasts to the network. The switch uses the time data from the first server detected and ignores others. If the poll interval expires thrice without the switch acquiring a time update from the first server detected, the switch accepts a time update from the next server broadcast. Note: To use the Broadcast mode, the switch and the time server must be in the same subnet. Also, the time server must be configured to broadcast time updates to the network broadcast address. ■ Unicast—The switch acquires time updates from a specific server for time synchronization. This mode requires at least one server address to be configured in the Server Address field. ■ DHCP—The switch attempts to acquire a time server IP address from the DHCP server. If the switch receives a server address, it polls the server for time updates according to the poll interval. If the switch does not receive a time server IP address, it cannot perform time synchronization updates. ■ Disabled—Time synchronization is disabled. | Broadcast, Unicast, DHCP, and Disabled Default: DHCP |
| Server Address | <p>IP address of the time server that the switch accesses for obtaining time synchronization updates. This field is applicable only when you select the Unicast mode for synchronization.</p> <p>You can configure a maximum of three time server IP addresses. When you add more than one IP address, the priority that the switch considers in selecting the IP address is the order in which you add the IP address. Therefore, the first IP address that you add will be priority 1, second IP address will be priority 2, and so on.</p> <p>You can delete the IP addresses by clicking the delete icon corresponding to the address. When more than one IP addresses are added, you must first delete the IP address you added last.</p> | IPv4 address |
| Timezone | The time zone corresponding to the location of the switch. | Time zone selected from the drop-down. |
| Daylight Time Rule | <p>The rule that the switch uses to adjust the time for Daylight Saving Time (DST). For information about the predefined and user-defined times, see Predefined DST Rules on page 456.</p> <p>When you select the User-defined option, you must configure the beginning and ending months and dates for DST changes in the Begin Month and Day and End Month and Day fields. All DST rules begin and end at 2 a.m. on the configured dates.</p> | Alaska, Canada and Continental US, Middle Europe and Portugal, Southern Hemisphere, Western Europe, and User-defined. |
| Begin Month and Day | The beginning month and date for the user-defined DST changes. This field appears only when you select User-defined in the Daylight Time Rule field. | Month and date selected from the drop-down. |
| End Month and Day | The ending month and date for the user-defined DST changes. This field appears only when you select User-defined in the Daylight Time Rule field. | Month and date selected from the drop-down. |

6. Click **Save Settings**.

Predefined DST Rules

Following are the details of the beginning and ending days for the predefined DST rules:

| Predefined DST Rule Name | Description |
|----------------------------|---|
| Alaska | <ul style="list-style-type: none">■ Begin DST at 2 a.m. on March 8.■ End DST at 2 a.m. on November 1. |
| Canada and Continental US | |
| Middle Europe and Portugal | <ul style="list-style-type: none">■ Begin DST at 2 a.m. on March 25.■ End DST at 2 a.m. on September 24. |
| Southern Hemisphere | <ul style="list-style-type: none">■ Begin DST at 2 a.m. on October 25.■ End DST at 2 a.m. on March 1. |
| Western Europe | <ul style="list-style-type: none">■ Begin DST at 2 a.m. on March 25.■ End DST at 2 a.m. on October 25. |

Configuring Routing on Aruba Switches




This is a beta feature and not recommended for a production environment.

Central does not support routing on Aruba Mobility Access Switches.

Static routes provide a means for restricting and troubleshooting routed traffic flows and in small networks can provide the simplest and most reliable configuration for routing. Static routes are manually configured in the routing table.

You can enable routing on Aruba switches in Aruba Central.

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **IP Settings > Routing**. The Routing page is displayed.
5. You can toggle routing to **enabled** on the slider menu.

Before enabling routing, you must already have configured a path to the gateway.

6. In the **Routes** table, click + to add a VLAN and configure the following parameters:

Table 139: *Routing Path Parameters*

| Name | Description | Value |
|-----------------|---|--|
| Network | A valid network IP address for the destination network or host. | IPv4 address. |
| Netmask | Netmask of the IP address. | Netmask address. |
| Gateway | Default gateway IP address. | IPv4 address. |
| Metric | A parameter used by the routers to determine the best optimal path for routing traffic. | This is a fixed metric for static IP routes, and is set to "1". |
| Distance | The administrative distance helps routers determine the best route when there are multiple routes to the destination. A lower value is recommended. | The default administrative distance for static IP routes is 1, but can be configured to any value in the range of 1 - 255. |

If the routing metric and administrative distance are set to a lower value for static routes, switches use the static IP routes as the best route for routing traffic.


7. Click **Save**.

Configuring System Parameters for a Switch

The **System** menu under **Switches-MAS** and **Switches** allows you to configure administrator credentials and enable mode for the switch users.


Configuring Administrator Credentials for Mobility Access Switch

To configure administrator credentials for a Mobility Access Switch, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches-MAS**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **System > Access/DNS**. The **Access/DNS** page is displayed.
5. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
6. Enter the password for enable mode in the **Enable Mode Password** text box and confirm the password.
7. Click **Save Settings**.

Configuring Administrator and Operator Credentials for Other Aruba Switches


To configure administrator credentials for other Aruba switches, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **System > Access/DNS**. The **Access/DNS** page is displayed.
5. Enter the username for the administrator user in the **Admin Username** text box.
6. Enter the password for admin in the **Admin Password** text box and confirm the administrator password.
7. To configure the operator user credentials, complete the following steps:
 - a. Select the **Set Operator Username** check box.

- b. Enter a username and password for the operator user.
 - c. Confirm the password.
8. Click **Save Settings**.

Configuring a Name Server

To set a static IP switches, you must configure a name server. To configure a name server, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s)** and perform one of the following steps:
 - To configure Aruba Mobility Access Switches, click **Switches-MAS**.
 - To configure Aruba switches, click **Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **System** > **Access/DNS**. The **Access/DNS** page is displayed.
5. Select **DHCP** or **Static** from the **Name Server** drop-down.
6. If you selected **Static** in the drop-down, enter the IP address of the name server obtained from the DNS server in the text box.
7. Click **Save Settings**.

Aruba Switch Stack

A switch stack is a set of switches that are interconnected through stacking ports. The switches in a stack elect a primary switch called Commander and a backup switch as Standby. The remaining switches become Members of the stack. The following table lists the switches that support stacking:

Table 140: *Switch Stacking Support*

| Switch Platform | Maximum Number of Stack Members | Minimum Supported Version | Supported Stack Type (VSF) / Backplane (BPS)) |
|---------------------------|---------------------------------|---------------------------|---|
| Aruba 2920 Switch Series | 4 | WB.16.04.0008 | BPS |
| Aruba 2930M Switch Series | 10 | WC.16.06.0006 | BPS |
| Aruba 2930F Switch Series | 8 | WC.16.07.0002 | VSF |
| Aruba 5400R Switch Series | 2 | KB.16.06.0008 | VSF |
| Aruba 3810 Switch Series | 10 | KB.16.07.0002 | BPS |



Provisioning and configuring of Aruba 5400R switch series and switch stacks is supported only through configuration templates. Aruba Central does not support moving Aruba 5400R switches from the template group to a UI group. If an Aruba 5400R switch is pre-assigned to a UI group, then the device is moved to an unprovisioned group after it joins Aruba Central.

For more information on topology and configuration of switch stacks, see the *HPE ArubaOS-Switch Management and configuration Guide* for the respective switch series.

Provisioning Switch Stacks in Aruba Central

The switch elected as the commander establishes a WebSocket connection to Aruba Central. The following criteria apply to provisioning and management of switch stacks in Aruba Central:

- Switch stacks can be added only to a template group and cannot be moved to a UI group.
- If the standalone switches in a group join to form a switch stack, the switch is moved to the Unprovisioned state.

- If a switch stack is moved from a pre-provisioned group to an existing group in the UI, it will be moved to Unprovisioned state.
- After forming a switch stack, you can remove a member and erase its stacking configuration. However, the member can join Aruba Central as a standalone switch only after it is deleted from the switch stack.
- When a stack is removed, the stack members cannot join Aruba Central until the stack entry is deleted. For more information on deleting the stack, see [Configuring Switch Stacks using UI Groups](#). When a stack entry is not deleted and the member tries to rejoin Aruba Central, an event is triggered in the Audit Trail page stating that the stack association is detected.

Assigning Labels and Sites

Aruba Central supports organizing your devices into sites for ease of monitoring. Sites refer to physical locations in which the devices are installed. Administrators can assign switch stacks to a single site for ease of managing installations and monitoring the overall site health. For more information on assigning devices to sites, see [Managing Sites on page 84](#).

Similarly, switch stacks can also be tagged using labels. Labels allow you to identify or tag devices installed in a specific site for ease of monitoring. For more information on assigning labels, see [Managing Labels on page 86](#).

If any one member of the switch stack is assigned to a site, Aruba Central automatically assigns all other members in a switch stack to the same site. Similarly, if a label is assigned to an individual member in a stack, the same label is applied to all other members of the stack.



Because all members of a switch stack must be assigned to the same site and label, Aruba Central automatically corrects the site and label assignment for switch stacks that were earlier assigned to different labels or sites. If you have such switch stacks in your account, you will notice that all stack members are migrated to the same site or label to which the commander was assigned. Aruba recommends that you review the sites and labels assigned by Aruba Central to verify that the switch stacks in your account are assigned to sites and labels that you intended to use, and if required, assign all members of stack to a common site or label of your choice.

Configuring Switch Stacks

For information on configuring switch stacks using template groups, see [Configuring Switch Stacks using Template Groups](#).

For information on configuring switch stacks using UI groups, see [Configuring Switch Stacks using UI Groups](#).

Monitoring Switch Stacks

See [Monitoring Switches and Switch Stacks on page 162](#).

Viewing Switch Stacks in Site Topology

See [Topology on page 262](#).


Configuring Switch Stacks using Template Groups

The switch stacks are provisioned under template groups in Aruba Central. The template groups allow you to configure and modify the settings of a switch stack using configuration templates.

When uploading a configuring template, ensure that the variables are uploaded for all the members of the stack. The template is applied with the variables of the member that is elected as the commander.

To create a configuration template for switch stack, complete the following steps:

1. In the **Network Operations** app, use the filter to select a template group.

2. Under **Manage**, click **Devices > Switches**.
3. Click the  configuration icon to display the switch configuration dashboard.
4. Click **Templates**. The Templates page is displayed.
5. Click **+** to create a template for the Aruba switch stack.
6. Specify a name for the template.
7. Select Aruba Switch from the **Device** drop-down list.
8. Select the Aruba Switch model in the **Model** drop-down list.
9. Select the Aruba Switch software version in the **Version** drop-down list.
10. Enter the template text in the **Template** box.



All switch templates must include a password command to set a password for the device. The switch template cannot be saved without adding a password command. If the configuration that is pushed from Aruba Central to the device does not contain a password command, the configuration push is aborted for the device and a log is added to the audit trail. For example, if you add the password command in a condition block and the condition evaluates to false, the configuration that is pushed will not contain the password command.

11. Click **Save**.



Aruba Central does not support the use of part number (J-number) in place of Switch model number in configuration templates for the Aruba switch stack.

The following pre-defined variables are refreshed and re-imported from a switch stack when a new stack member is added or removed, or when a failover occurs.

- `_sys_template_header`
- `_sys_module_command`
- `_sys_stack_command`
- `_sys_oobm_command`
- `_sys_vlan_1_untag_command`
- `_sys_vlan_1_tag_command`

For information about deploying VSF stacks of ArubaOS Switches using Zero Touch Provisioning (ZTP) in Aruba Central, see the [VSF Stacking Guide](#).

For information about switch stacks using UI groups, see [Configuring Switch Stacks using UI Groups](#).

Configuring Switch Stacks using UI Groups

Aruba Central supports both Backplane stacking (BPS) and Virtual Switching Framework (VSF) switch stacking. You can create switch stacks and add stack members through the UI. The stack configuration is possible only when the switches are online.



Stacks created using UI groups can only be managed in a UI group. If a device is moved to a template group, then the device cannot be managed in a UI group without rebuilding the stack.

Onboarding commander and members to Aruba Central

The following is a high-level process flow for configuring switch stacks:

1. Add the switches to the device inventory and assign a valid subscription. All the switch members must be set to factory default and powered off.

2. Power on the switch you intend to add as a commander. The switch comes up online in Central as a standalone switch.
3. Create a stack with the standalone switch. After stack creation, the switch will reboot and comes up as a stack commander. For more information, see [Creating a switch stack on page 462](#).
4. Add members to the stack when the commander is active. For more information, see the section [Adding a stack member on page 463](#).
5. After adding members, connect the stacking modules and stacking cables to all switches and power on the members in a sequence as mentioned in the [Recommended deployment workflow on page 462](#).



If the stack members are connected and powered on before adding to a stack, then the members might not join the stack.


Recommended deployment workflow

The following procedure provides the recommended deployment workflow for deploying three-member VSF stack (Commander, Standby and a Member switch).

1. Connect a staging port on the first switch in the VSF stack to a DHCP enabled network or a device that has access to the internet. After rebooting and initialization, the switch assumes its role as commander and the LED on the VSF stack ports of the switch will turn amber.
2. Connect a VSF port of the next switch to the VSF port of the commander switch. During initialization, the switch will act as standby and the LED on the VSF port will turn amber.
3. Connect a VSF port of the next switch to the VSF port of the standby switch. During initialization, the new switch acts as a member and the LED on the VSF port of the switch will turn amber.
4. Connect the VSF port of the commander switch to the VSF port of the member to complete the loop.

Creating a switch stack

To create a switch stack, complete the following steps:

1. In the **Network Operations** app, use the filter to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the  configuration icon to display the switches configuration dashboard.
4. Click **Stacks**.

The Stacks table displays the following information:

Table 141: *Stacks table*

| Name | Description | Value |
|--------------------|---|--------------------------|
| Name | The name of the switch stack. | A string |
| Type | The type of switch stacking. | BPS or VFS |
| Stack ID | The ID of the switch stack. The stack ID is auto-generated and cannot be changed in the settings. | Auto-generated String |
| Members | The number of members on the switch stack. | Integer |
| MAC Address | The MAC address of the switch stack. | Alphanumeric MAC address |

| Name | Description | Value |
|-----------------------|---|---|
| Topology | The type of switch stack topology. | Chain, Ring, or unknown |
| Status | The status of the stack formation. | Pending, In-progress, Active, or Failed |
| VSF Port Speed | The port speed in the case of VSF stacking. This column is hidden by default. You must select the column from the columns list. | 1G or 10G |

5. In the **Stacks** table, click + to add a stack.

The **Create New Stack** window is displayed.

6. Select a commander switch from the **Select Commander Switch** drop-down list. The model number and serial number of switches are displayed in the drop-down list.



The commander switch must be installed with the minimum supported firmware version of 16.06 or later.

- If the selected switch supports VSF Stacking, configure the following parameters:
 - **Link 1 Name and Port(s)**—The name of the link 1 and its corresponding ports.
 - **Link 2 Name and Port(s)**—The name of the link 2 and its corresponding ports.
 - **Domain ID**—The domain ID of the switch stack.
 - **Port Speed**—The VSF port speed from the drop-down.
 - If the selected switch supports BPS stacking, insert the stacking module in switch and continue to step 7.
7. Click **Save & Reboot Stack**. When the stack reboots, the status of the stack formation is displayed in the **Stacks** table. Do not make any changes to the stack until the status changes from In Progress to Active or Failed. If stack creation fails due to some issues, delete the stack entry and retry.

Editing a Stack

To edit a stack, select the stack row you want to edit and click the edit icon.



You can edit a stack only when its status is **Active**.

Removing a stack

To remove a stack, select the stack row that you want to remove and click the delete icon.



You can remove a stack only when its status is **Failed**.

Adding a stack member

Stacking allows you to add switches to the stack only when the commander is active.

To add a switch to stack as a new member, complete the following steps:

1. In the **Network Operations** app, use the filter bar to select a group or a device.
2. Under **Manage**, click **Device(s) > Switches**.
3. Click the configuration icon to display the Switches configuration dashboard.
4. Click **Stacks**.

5. In the **Stacks** table, select the stack row for which you want to add a member. The **Members** table displays the list of members for that particular stack. The **Members** table displays the following information:

Table 142: *Members table*

| Name | Description | Value |
|---------------------|--|---------------------------------|
| Name | The name of the switch stack member. | A string |
| MAC Address | The MAC address of the stack member. | Alphanumeric MAC address |
| Model | The hardware model of the switch. | A String |
| Priority | The priority level of the stack member. | 1 to 255 |
| Role | The role of a stack member. | Commander, member, or standby |
| Status | The status of the switch stack member. | Active, Inactive, or Not Joined |
| Link1 Port | The name of the link and its corresponding port of the stack member. | A String |
| Link2 Port | | |

6. In the **Members** table, click **+** to add a stack member.

The **Add Stack Member For <stack name>** window is displayed. The following information is auto-generated:

- **Member ID**—Member identification number of the member.
- **Priority**—Priority of the member.

7. Select the member using one of the following options:

- **Same as Commander**—Use this option when your commander and member have the same model number.
- **Select Model** —Use this option when your commander and member have different model numbers. Select the switch model from the model drop-down list.

8. If the selected switch supports VSF Stacking, configure the following parameters:

- **Link1 Name and Port(s)**—Specify the name of the link 1 and its corresponding port.
- **Link2 Name and Port(s)**—Specify the name of the link 2 and its corresponding port.

9. To add another stack member, click **Save & Add Another**.



A message is displayed above the **Members** table when the maximum number of switches in a stack has been added.

10. Click **Save**. After the stack members appear in **Members** table, connect the stacking modules and stacking cables to all switches and power on the switches.

Editing a stack member

To edit a stack member, select the member row you want to edit and click the edit icon.

Removing a stack member

To delete a stack member, select the member row that you want to delete and click the delete icon.

After removing a member, disconnect the switch from the stack. To disconnect the switch from the stack, do one of the followings:

- Turn off the power from the switch.
- Restart the switch.



You can remove only the stack member that has the lowest priority. For example, if there are three stack members with priority 254, 253 and 252 respectively and if you want to remove a stack member with priority 253, then first you need to remove the member with priority 252.

Priority cannot be assigned manually. Commander switch is always assigned with priority 255. The priority of other subsequent members is decremented by 1.

The Aruba SD Branch solution offers the best-in-class wireless and wired infrastructure and management orchestration features with the SD-WAN capabilities. The SD Branch solution extends the SD-WAN concept to all elements in the branch to deliver a full stack solution that addresses the business challenges of distributed enterprises. Coupled with Aruba Central, the solution provides a cloud-hosted environment for simplified operations and improved agility.

Why SD-WAN?

A traditional branch setup supports client connectivity requirements across different geographical locations for various types of business operations. The sites in remote geographical locations serve as branch offices, while the headquarters or main office serves as a data center that hosts network resources to store, manage, and distribute data. The main office also hosts a centralized Virtual Private Network (VPN) management system to aggregate traffic from the remote branch sites. A Wide Area Network (WAN) —with Multiprotocol Label Switching (MPLS), T1, T3, Broadband, or Cellular links—is used for connecting multiple local area networks to a central corporate network or data centers separated by distance.

Due to an increase in the number of client devices at the remote sites and the new bandwidth requirements, branch office networks are expected rapidly scale to provide uninterrupted user experience. A traditional branch infrastructure with multiple appliances, different operating systems, and management tools only adds to the cost, involves a maintenance overhead, and demands skilled IT personnel.

The Aruba SD-WAN solution simplifies your branch deployments with a single management interface for administering, managing, and monitoring your branch networks. It also provides a unified policy enforcement framework with operational ease.

Key Features and Benefits

The SD-WAN solution comes with the following key capabilities:

- Zero Touch Provisioning of devices— Ability to self-provision without operator's intervention.
- Centralized overlay management and control— A single cloud-based network management interface for managing and monitoring SD Branch devices. Aruba Central, the cloud based network management system, supports unified management of SD branch devices with ZTP and hierarchical configuration.
- IPsec based Automatic VPN Tunnels—Support for high-performance and automatic IPsec VPN for secure overlay networking.
- Unified security policy for wired, wireless, and WAN—Support for a common security policy framework based on user roles for WAN, WLAN, and LAN users.
- Dynamic path selection—Support for dynamically steering traffic or a service request to the best available path. For example, you can configure a policy to dynamically route the real-time voice and video traffic on the link with the lowest latency and jitter, and the bulk file traffic on the link with the maximum bandwidth.
- Deep Packet Inspection and Web Content Classification—Support for monitoring and analyzing application usage by clients.
- Visibility, analytics, and troubleshooting—Dashboards for monitoring branch health, device performance, and client connectivity metrics. Alerts, reports, and audit trails for monitoring and troubleshooting network performance issues.
- Policy-based Routing—In addition to the traditional destination-based routing, the SD Branch devices

support routing client traffic based on user role or type of application, For example, traffic generated from the guest devices can be routed directly to the internet, while traffic from the employees can be routed to the MPLS network.

How It Works

The SD-WAN solution includes a new set of devices called Aruba Gateways that inter-operate Aruba Switches and Instant APs to provide a full-fledged WAN architecture.

Based on the size of your branch setup, you can choose device combination that best suits your requirement:

- Medium to large branches—For branches that require more than 24 ports, you can use a combination of Branch Gateways and one or more Aruba switches at the branch site, with Aruba 7200 Series Mobility Controller as VPN Concentrator at the data center.
- Small to medium branches—For branches that require less than 24 ports (including all WAN and LAN ports), you can deploy Branch Gateways at the branch sites, with Aruba 7200 Series Mobility Controller as VPN Concentrator at the data center.
- Micro branches—For micro branches, you can deploy an Instant AP cluster at the branch site, with Aruba 7200 Series Mobility Controller as the VPN Concentrator at the data center.

[Figure 100](#) shows a typical deployment topology of an SD Branch with Branch Gateways and a micro branch with Instant APs:

Figure 100 SD Branch Topology

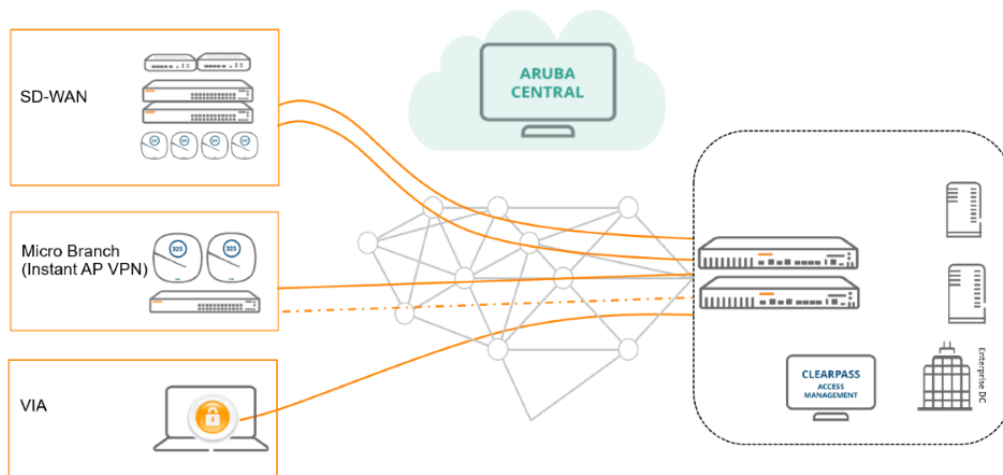


Figure 101 illustrates the communication flow between Aruba Central, branch sites, and data center.

Figure 101 *Aruba Central and Cloud Communication*

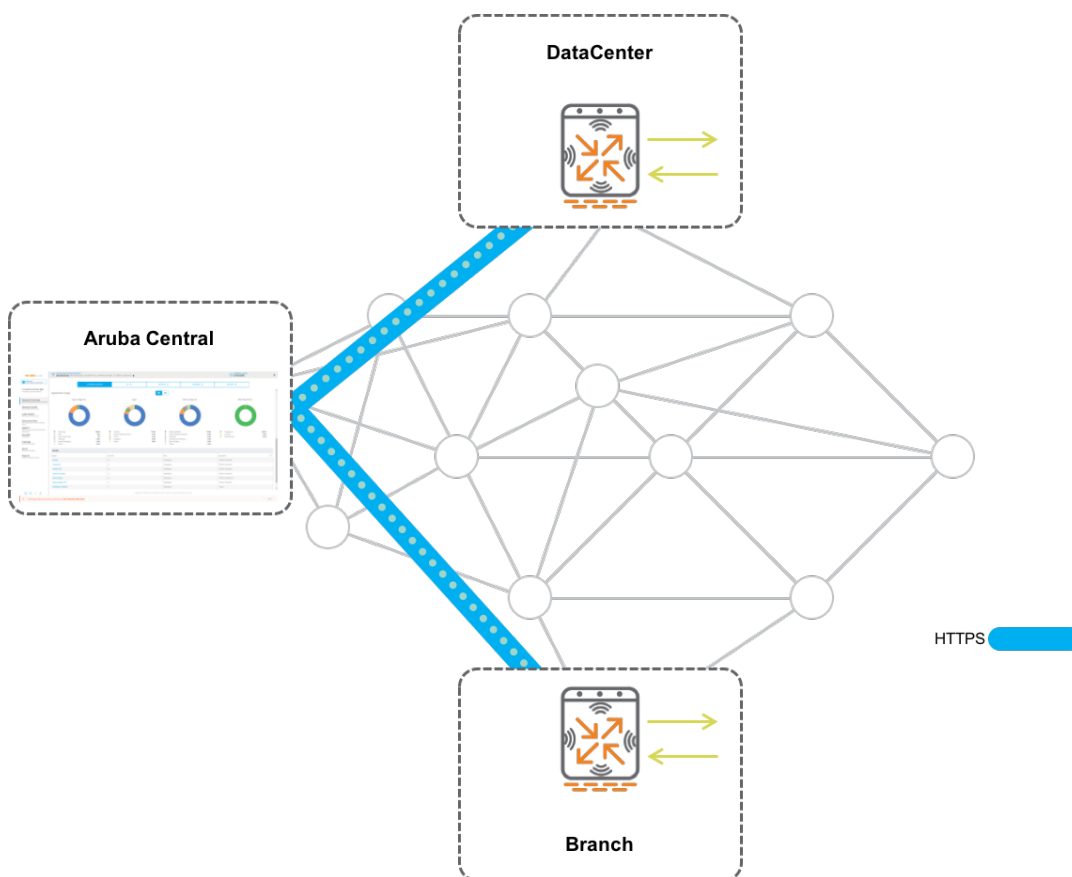
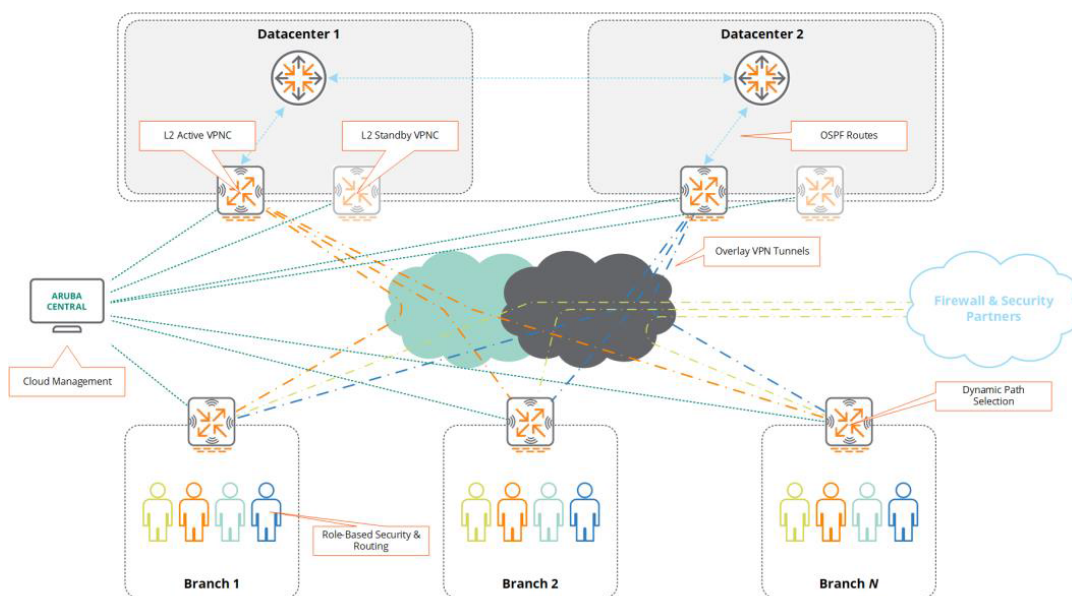


Figure 102 shows all elements in an SD Branch and the SD-WAN data flow.

Figure 102 *Aruba SD-WAN Data Flow*



What are the Solution Requirements?

The Aruba Gateways are the most important components of the Aruba SD-Branch Solution. The SD-WAN Gateway portfolio includes Aruba 7000 Series and Aruba 7200 Series Mobility Controllers that function as Branch Gateways and VPN Concentrators respectively.

The following sections list the supported hardware platforms and minimum software versions required for setting up an SD-Branch.

At the Branch Site

[Table 143](#) shows the list of hardware and software requirements for a branch site:

Table 143: *SD Branch Site Devices*

| SD Branch Component | Hardware Platforms | Minimum Software Version |
|---|---|---|
| Branch Gateways | Aruba 7000 Series Mobility Controller | ArubaOS 8.1.0.0-1.0.0.0 |
| Aruba Switches function with Branch Gateways to detect and isolate rogue APs, and blacklist rogue devices. | Aruba 3810 Switch Series | KB.16.05.0007 or later |
| | Aruba 5400R Switch Series | KB.16.05.0007 or later |
| | Aruba 2920 Switch Series | WB.16.05.0007 or later |
| | Aruba 2930F Switch Series | WC.16.05.0007 or later |
| Instant APs function as VPN clients at branch sites. The client data traffic from these APs are aggregated by the VPN Concentrator located at the data center | Aruba 310 Series and 300 Series Instant APs | Aruba Instant 6.5.3.x Aruba Instant 8.3.0.0 or later |

At the Data Center

At the data center, you can deploy Aruba 7200 Series Mobility Controller as VPN Concentrator. For data center redundancy, you can deploy two VPN concentrators in the active-standby or active-active mode.

Table 144: *Data Center*

| SD-Branch Component | Hardware Platform | Minimum Software Version |
|---|--|--------------------------|
| VPNC—A VPN Concentrator functions as a VPN management system that aggregates data traffic from the branches and terminates IPsec VPN tunnels. | Aruba 7200 Series Mobility Controllers | ArubaOS 8.1.0.0-1.0.0.0 |
| Virtual Gateway—The headend gateway at the enterprise data center can be hosted as a virtual appliance. The virtualised instance enterprise data center gateway in public or private cloud is referred to as Virtual Gateway. Aruba Virtual Gateways function as VPN Concentrators. | Aruba Virtual Mobility Controller | ArubaOS 8.1.0.0-1.0.4.1 |

In the Cloud

A valid Aruba Central subscription is required to avail cloud-based administration, management, configuration and monitoring of SD branch components such as Branch Gateways, VPN Concentrators, Instant APs, and Aruba Switches.

How Do I Get Started?

To start using the SD-WAN solution, complete the steps described in the [Getting Started](#) section.

Aruba Central supports a robust set of REST APIs to enable users to build custom applications and integrate the APIs with their applications. The Aruba Central API framework uses OAuth protocol to authenticate and authorize third-party applications, and allows them to obtain secure and limited access to an Aruba Central service.

This section includes the following topics:

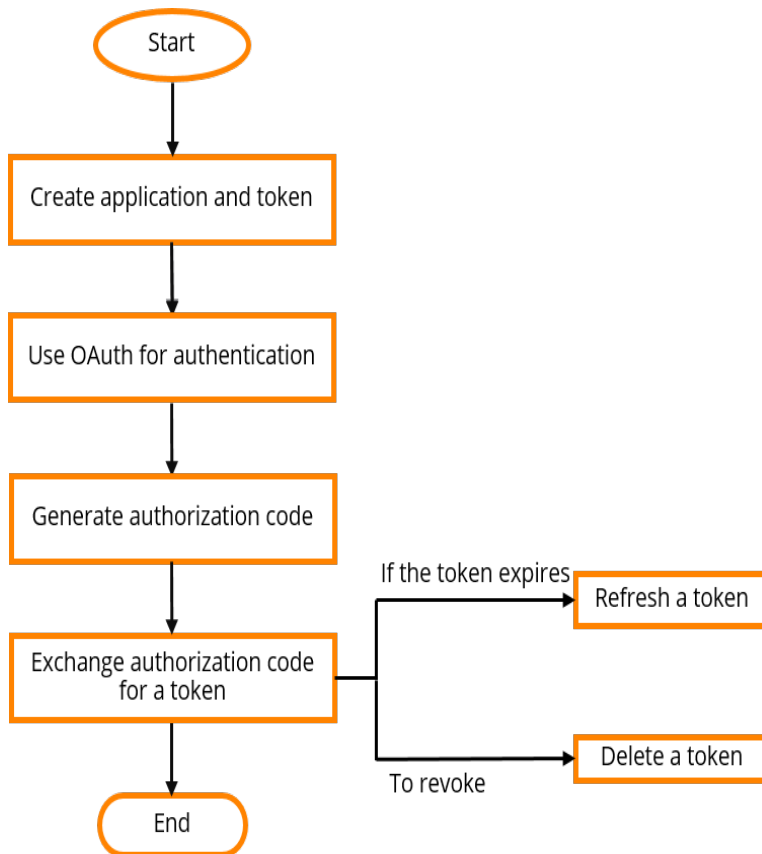
- [API Gateway and NB APIs on page 471](#)
- [Accessing API Gateway on page 472](#)
- [Viewing Swagger Interface on page 473](#)
- [List of Supported APIs on page 474](#)

API Gateway and NB APIs

The **API Gateway** feature in Aruba Central supports the REST API for all Aruba Central services. This feature allows Aruba Central users to write custom applications, embed, or integrate the APIs with their own applications. The REST APIs support HTTP GET and POST operations by providing a specific URL for each query. The output for these operations is returned in the JSON format.

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. The access tokens provide a temporary and secure access to the APIs. The access tokens have a limited lifetime for security reasons and the applications should use the refresh API to obtain new tokens periodically (every 2 hours).

The following figure illustrates the API gateway workflow for the users:

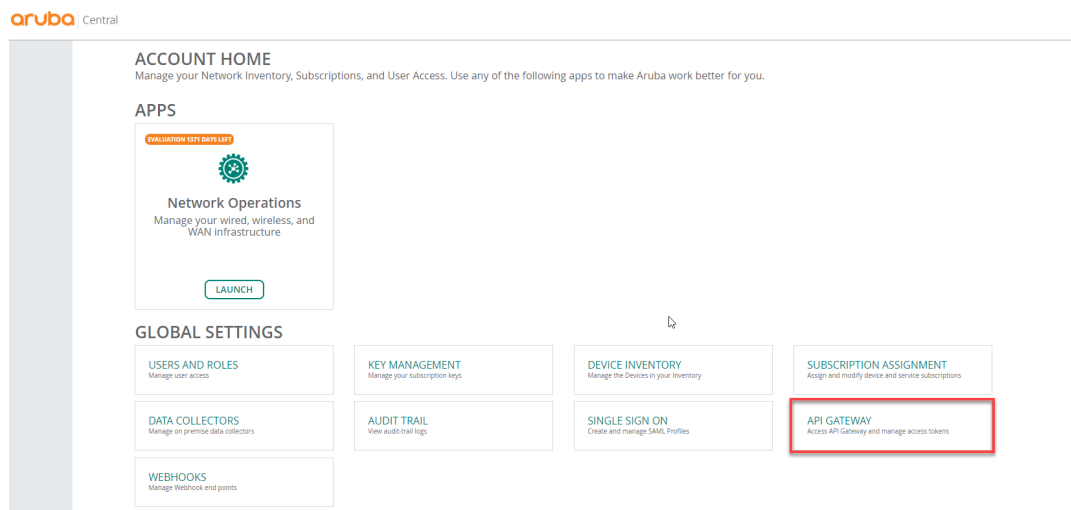


Accessing API Gateway

To access the API Gateway:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

The **API Gateway** page is displayed. You can get new tokens and refresh old tokens. To obtain a new token application, you must set authentication parameters for a user session.



Important Points to Note

- The admin user profile of MSP has **System Apps & Tokens** tab which displays all the apps and tokens generated locally in the admin user profile. This tab also displays all the apps created in the non-admin user

profiles. Clicking these apps lists out all the associated tokens created for the non-admin user profile.

- Administrator role is specific to an app and hence the administrator account related RBAC library APIs and decorators must contain the application name as one of the parameters in the access verification query.
- The decorators associated with **Account Home**, **Network Operations**, or **ClearPass Device Insight** must contain **account_setting**, **central**, or **optik** as app names respectively, as one of the parameters.

Domain URLs

The following table shows the region-specific domain URLs for accessing API Gateway:

Table 145: Domain URLs for API Gateway Access

| Region | Domain Name |
|-------------|---|
| US-1 | app1-apigw.central.arubanetworks.com |
| US-2 | apigw-prod2.central.arubanetworks.com |
| EU-1 | eu-apigw.central.arubanetworks.com |
| Canada-1 | apigw-ca.central.arubanetworks.com |
| China-1 | apigw.central.arubanetworks.com.cn |
| APAC-1 | api-ap.central.arubanetworks.com |
| APAC-EAST1 | apigw-apaceast.central.arubanetworks.com |
| APAC-SOUTH1 | apigw-apacsouth.central.arubanetworks.com |



The procedures described in this article use app1-apigw.central.arubanetworks.com as an example. Ensure that you use the appropriate domain URL when accessing API Gateway or generating tokens.

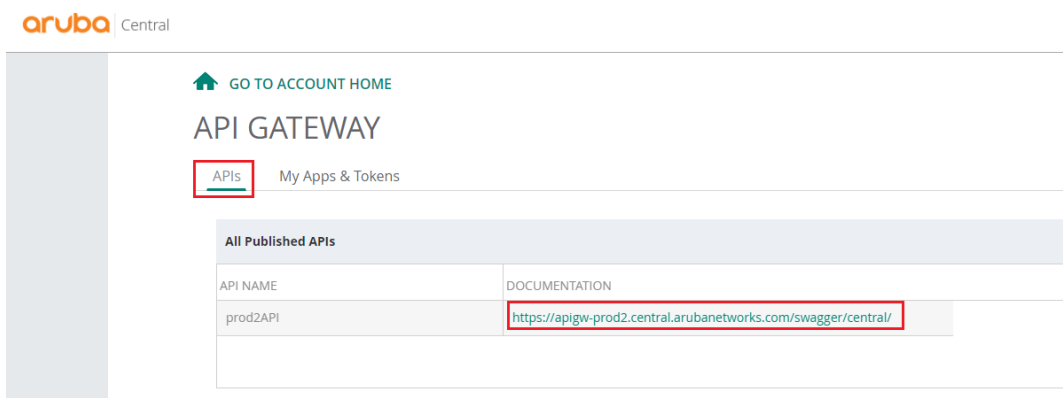
Viewing Swagger Interface

To view the APIs managed through Aruba Central, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

The **API Gateway** page with the list of published APIs is displayed.

2. To view the Swagger interface, click the link in the **Documentation** column next to the specific published API name. The documentation is displayed in a new window.



List of Supported APIs

Aruba Central supports the following APIs for the managed devices.

Table 146: *APIs and Description*

| API | Description |
|-------------------------------|--|
| Monitoring | Gets network, client, and event details. It also allows you to manage labels and switches. |
| Configuration | Allows you to configure and retrieve the following: <ul style="list-style-type: none">■ Groups■ Templates■ Devices |
| AppRF | Gets Top N AppRF statistics. |
| Guest | Gets visitor and session details of the portal. |
| MSP | <p>Allows you to manage and retrieve the following:</p> <ul style="list-style-type: none">■ Customers■ Users■ Resources■ Devices <p>Aruba has enforced a request limit for the following APIs:</p> <ul style="list-style-type: none">■ GET /msp_api/v1/customers■ GET /msp_api/v1/customers/{customer_id}/devices■ GET /msp_api/v1/devices■ PUT /msp_api/v1/customers/{customer_id}/devices <p>The maximum limit is set to 50 per API call. If you exceed this limit, the API call returns the HTTP error code 400 and the following error message: LIMIT_REQUEST_EXCEEDED.</p> |
| User Management | Allows you to manage users and also allows you to configure various types of users with a specific level of access control. |
| Audit Event Logs | Gets a list of audit events and the details of an audit event. |
| Device Inventory | Gets device details and device statistics. |
| Licensing | Allows you to manage and retrieve subscription keys. |
| Presence Analytics | Allows you to configure the Presence Analytics application. It also retrieves site and loyalty data. |
| Device Management | Allows you to manage devices. |
| Firmware | Allows you to manage firmware. |
| Troubleshooting | Gets a list of troubleshooting commands for a specific type of device. |
| Notification | Gets notification alerts generated for events pertaining to device provisioning, configuration, and user management. |
| Unified Communications | Retrieves data for all sessions for a specific period of time. It also retrieves the total number of clients who made calls in the given time range and gets the Lync/Skype for Business URL for the Aruba Central cluster that you are using. |

Table 146: APIs and Description

| API | Description |
|--------------------------|---|
| Refresh API Token | Allows you to refresh the API token. |
| Reporting | Gets the list of configured reports for the given customer ID. |
| WAN Health | Allows you to the following: <ul style="list-style-type: none"> ■ Get list of configured WAN health policies. ■ Create a new WAN health policy. ■ Delete an existing WAN health policy. ■ Get the details of any specific WAN health policy. ■ Update an existing WAN health policy. ■ Get policy schedule details. ■ Create a schedule for a WAN health policy. ■ Get statistics for WAN health cookie generated for a site. ■ Get WAN health test results. ■ Get WAN health test results for a specific site. |
| Network Health | Allows you to get data for all the labels and sites. |
| Webhook | Allows you to add, or delete Webhooks, and get or refresh Webhook tokens. See Webhooks on page 487 for further details on Webhook. |
| VisualRF | Allows you retrieve information on floor plans, location of APs, clients and rogue devices. |
| DPS Monitoring | Gets DPS compliance and session statistics for all the links of a device belonging to a specific policy. |

For a complete list of APIs and the corresponding documentation, see <https://app1-apigw.central.arubanetworks.com/swagger/central>.

Creating Application and Token

To create an application, complete the following steps:

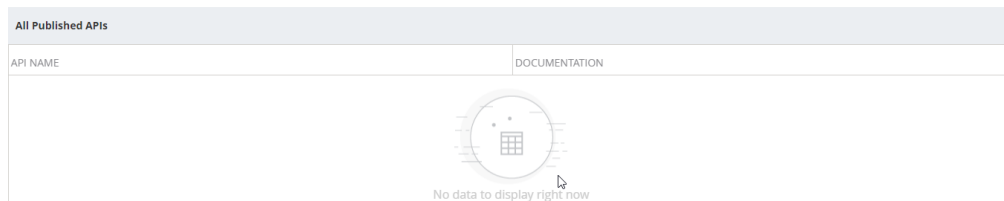
1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

The **API Gateway** page is displayed.

[GO TO ACCOUNT HOME](#)

API GATEWAY

APIs My Apps & Tokens Usage





2. Click the **My Apps & Tokens** tab.



The admin user will be able to create new apps for all the non-admin user by clicking **+ Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click **+ Add Apps & Tokens**.


| My Apps & Tokens | | | | | |
|---|-----------|---------------|--------------|-------------|------------|
| NAME | CLIENT ID | CLIENT SECRET | REDIRECT URI | APPLICATION | CREATED AT |
|  <p>No data to display right now</p> | | | | | |

| Token List | | | | | |
|---|-----------|-------------|--------------|--------------|----------------|
| TOKEN ID | USER NAME | APPLICATION | GENERATED AT | REVOKE TOKEN | DOWNLOAD TOKEN |
|  <p>No data to display right now</p> | | | | | |

4. In the **New Token** pop-up window, do the following:

- Enter the application name. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable.
- In the **Redirect URI** field, enter the redirect URL.
- From the Application drop-down list, select the application.
- Click **Generate**. A new application is created and added to the **My Apps & Tokens** table. The **My Apps & Tokens** table displays the following details:

- **Name**—Name of the application. In non-admin user profile, the **Application Name** field contains the logged-in user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name.
- **Client ID**—Unique ID for each application.
- **Client Secret**—Unique secret ID for each application.
- **Redirect URI**—Redirect URL.
- **Application**—Name of the application. For example, Network Operations.
- **Tokens**—Token created for the application. The option is available to admin user profile only.
- **Created At**—Date on which the application was created.

5. To delete the added application, click delete  icon on the row corresponding to an application and click **Yes** to delete that application.



Only admin users will be able to generate tokens with multiple application names. In non-admin user profile, the **Application Name** field contains the user name and is non-editable. Any new tokens generated in non-admin user profile is associated with the same application name. However, all the multiple application names and the associated tokens in non-admin user profiles from the earlier versions is retained in the **Token List** table.

Using OAuth 2.0 for Authentication

For secure access to the APIs, the Aruba Central API Framework plug-in supports OAuth protocol for authentication and authorization. OAuth 2.0 is a simple and secure authorization framework. It allows

applications to acquire an access token for Aruba Central through a variety of work flows supported within the OAuth 2.0 specification.

All OAuth 2.0 requests must use the SSL endpoint available at <https://app1-apigw.central.arubanetworks.com>.

Access and Refresh Tokens

The access token is a string that identifies a user, app, or web page and is used by the app to access an API. The access tokens provide a temporary and secure access to the APIs.

The access tokens have a limited lifetime. If the application uses web server or user-agent OAuth authentication flows, a refresh token is provided during authorization that can be used to get a new access token.

If you are writing a long running applications (web app) or native mobile application you should refresh the token periodically. For more information, see [Refreshing a token](#).

This section includes the following topics:

- [Obtaining Access Token](#)
- [Accessing APIs](#)
- [Viewing and Revoking Tokens](#)
- [Adding a New Token](#)

Obtaining Access Token

Users can generate the OAuth token using one of the following methods:

- [Obtaining Token Using Offline Token Mechanism](#)
- [Obtaining Token Using OAuth Grant Mechanism](#)

Accessing APIs

To access the API, use the following URL:

<https://app1-apigw.central.arubanetworks.com/>.

This endpoint is accessible over SSL and the HTTP (non-SSL) connections are redirected to the SSL port.

Table 147: *Accessing the API*

| URL | Description |
|---|--|
| https://app1-apigw.central.arubanetworks.com/ | The API gateway URL. All APIs can be accessed from this URL by providing a correct access token. |

The query parameters for the API are as follows:

Table 148: *Query Parameters for the API*

| Parameter | Value | Description |
|--------------|--------------|--|
| request_path | URL Path | URL path of an API, for example, to access monitoring APIs, use the path <i>/monitoring/v1/aps</i> . |
| access_token | access_token | Pass the token string in URL parameter that is obtained in step 2. |

Example

Request Method: GET

https://app1-apigw.central.arubanetworks.com/monitoring/v1/aps?access_token=e325c0fb3f1547b5b735de3221690c2f

Response:

```
{
  "aps": [
    {
      "firmware_version": "6.4.4.4-4.2.3.1_54637",
      "group_name": "00TestVRK",
      "ip_address": "10.29.18.195",
      "labels": [
        "Filter_242",
        "Ziaomof",
        "roster",
        "242455",
        "Diegso"
      ],
      "macaddr": "6c:f3:7f:c3:5d:92",
      "model": "AP-134",
      "name": "6c:f3:7f:c3:5d:92",
      "radios": [
        {
          "band": 0,
          "index": 1,
          "macaddr": "6c:f3:7f:b5:d9:20",
          "status": "Down"
        },
        {
          "band": 1,
          "index": 0,
          "macaddr": "6c:f3:7f:b5:d9:30",
          "status": "Down"
        }
      ],
      "serial": "AX0140586",
      "status": "Down",
      "swarm_id": "e3bf1ba201a6f85f4b5eaedeed5e502d85a9aef58d8e1d8a0",
      "swarm_master": true
    }
  ],
  "count": 1
}
```

Viewing and Revoking Tokens

To view or revoke tokens, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**. The **Token List** table displays the following:
 - **Token ID**—Token ID of the application.
 - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.
 - **Application**—Name of the application to which this token is associated to. For example, Network Operations.
 - **Generated At**—Date on which the token was generated.

- **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
- **Download Token**—Click **Download Token** to download the token.



In MSP mode, the admin user profile has **System Apps & Tokens** tab which displays all the apps and tokens generated in all non-admin user profiles in addition to the apps and tokens created in the admin user profile. To view all the tokens of admin and non-admin user, go to **Account Home > Global Settings > API Gateway > System Apps & Tokens**.

Adding a New Token

To add a new token, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**.



The admin user can create new tokens for all non-admin users by clicking + **Add Apps & Tokens** in the **System Apps & Tokens** tab.

3. Click + **Add Apps & Tokens** to add a new token.
4. Enter the application name in the **Application Name** box and click **Generate**.



If you have registered a custom URI when creating a new app under **System Apps and Tokens**, the **Redirect URI** option is disabled for you in the **My Apps and Tokens** tab > **Add Apps and Tokens > New Token**. In such cases, the **Redirect URI** option in **Add Apps and Tokens > New Token** under **My Apps and Tokens** populates your already registered URI.

Obtaining Token Using Offline Token Mechanism

To obtain tokens using the offline token method, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **My Apps & Tokens**.



In the MSP mode, the admin user profile can view the **System Apps & Tokens** tab which displays all the apps and tokens generated in all the non-admin user profiles in addition to the apps and tokens created in the admin user profile.

3. Click + **Add Apps & Tokens**. The **New Token** pane is displayed.
4. Enter the application name and redirect URI in the **Application Name** and **Redirect URI** fields respectively.
5. Choose the application from the **Application** drop-down list and click **Generate** to generate a new token.
6. The **Token List** table displays the following:
 - **Token ID**—Token ID of the application.
 - **User Name**—Name of the user to whom this token is associated to. An application can be associated to multiple users.

- **Application**—Name of the application to which this token is associated to. For example, Network Operations.
- **Generated At**—Date on which the token was generated.
- **Revoke Token**—Click **Revoke Token** and click **Yes** to revoke the token associated to a particular user. For example, if two users are associated to an application and if you want to remove access to a particular user, revoke the token associated to that user.
- **Download Token**—Click **Download Token** to download the token.

Obtaining Token Using OAuth Grant Mechanism

The following section describes the steps for obtaining the access token and refresh token using the authorization code grant mechanism:

- [Step 1: Authenticating a User and Creating a User Session](#)
- [Step 2: \[Optional\] Generating Client Credentials](#)
- [Step 3: Generating Authorization Code](#)
- [Step 4: Exchanging Auth Code for a Token](#)
- [Step 5: Refreshing a Token](#)
- [Step 6: Deleting a Token](#)

Step 1: Authenticating a User and Creating a User Session

The following API authenticates a user and returns a user session value that can be used to create future requests for a client with the specified username and password. It is assumed that you already have a client ID for your application. For more information on how to create an application and obtain tokens, see [Creating Application and Token](#).

Log in to the API gateway server and establish the user session. This endpoint is accessible over SSL, and HTTP (non-SSL) connections are redirected to SSL port. For region-specific domain URLs for accessing the API gateway, see [Domain URLs](#).

If user authentication is successful, the request will return HTTP code 200 and the response header will include the following attributes.

Table 149: Authentication and User session Response Codes

| Header Key | Values | Description |
|---|---------------------------------|---|
| https://app1-apigw.central.arubanetworks.com/oauth2/token | csrftoken=xxxx; session=xxxx | The server returns a CSRF token and identifies the user session, which must be used for all subsequent HTTP requests. |

Example

Request Method: POST

URL: https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/login?client_id=<client_id> HTTP/1.1

Host: app1-apigw.central.arubanetworks.com

Request Header:

Accept: application/json

Content -Type: application/json

POST Request Body(JSON):

```
{
  "username": "xxxxx",
  "password": "xxxxx"
}
```

Error Response:

400: Bad Request

Response Body (JSON):

```
{
  "extra": {},
  "message": "<error string>"
}
```

401: Auth failure

Response Body (JSON):

```
{
  "message": "Auth failure",
  "status": false
}
```

Success Response:

200: OK

Response Body (JSON):

```
{
  "status": true
}
```

Response Header:

Set-Cookie: csrftoken=xxxx;session=xxxx;



The **csrf token** value received in the successful response message must be used as a parameter for all subsequent POST/PUT requests. The **session** value must also be used for all subsequent requests to maintain the user session context.

Step 2: [Optional] Generating Client Credentials

The following API can be used to generate client credentials for a specific tenant using your Managed Service Provider (MSP) Client ID.

Table 150: URL to Generate Client Credentials

| URL | Description |
|---|--|
| <a href="https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>">https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id> | The <msp_client_id> variable is the client ID given from Central to that a Managed Service Provider that user registered the application. |

Example

Request Method: POST

URI—https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/client_credentials?client_id=<msp_client_id>

POST Request Body(JSON):

```
{
  "customer_id": "<tenant_id>"
}
```

Request Header: (Values from login API request)


```
Set-Cookie: csrftoken=xxxx;session=xxxx;
```

Response Body(JSON):

```
{
  "client_id": "<new-client-id>",
  "client_secret": "<new-client-secret>"
}
```

Step 3: Generating Authorization Code

After the user is authenticated and you have a valid session for that user, use this API to get authorization code. The authorization code is valid only for 5 minutes and must be exchanged for a token within that time.

Table 151: URL for to Generate an Authorization Code

| URL | Description |
|---|---|
| https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api | The endpoint is a POST call to get an authorization code. |

Query parameters for this API are as follows:

Table 152: Query Parameters for the Auth Code API

| Parameter | Values | Description |
|---------------|---|--|
| client_id | client_id is a unique hexadecimal string | The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin. |
| response_type | code | Use code as the response type to get the authorization code that can be exchanged for token |
| scope | all or read | Requested API permissions may be either all (for both read and write access) or read for read-only access. |

Example

Request Method: POST

URL: https://app1-apigw.central.arubanetworks.com/oauth2/authorize/central/api/?client_id=<client_id>&response_type=code&scope=all HTTP/1.1

Host: app1-apigw.central.arubanetworks.com

Request Header:

Accept: application/json Cookie: "session=xxxx" X-CSRF-Token: xxxx

Content -Type: application/json

POST Request Body(JSON):

```
{
  "customer_id": "xxxxxx"
}
```

Error Response:

400: Bad Request

Response Body (JSON):

```
{
  "extra": {},
  "message": "<error string>"
}
```


401: Auth failure

Response Body (JSON):

```
{
  "message": "Auth failure",
  "status": false
}
```

Success Response:

200: OK

Response Body (JSON):

```
{
  "auth_code": "xxxx"
}
```



Pass the **csrf-token** value you obtained in step one in the request header, otherwise the request will be rejected. Note the **auth_code** value in the response, as you will use this code to obtain an OAuth token.

Response Header:

Set-Cookie: csrf-token=xxxx;session=xxxx;

Step 4: Exchanging Auth Code for a Token

Once you have an authorization code, you just use that code to request an access from the server. The exchanges should be done within 300 seconds of obtaining the auth code from the previous step, or the API will return an error.

Table 153: *URL for to Generate an Auth Token*

| URL | Description |
|---|---|
| https:// app1- apigw.central.arubanetworks.com/oauth2/token | The endpoint is a POST call to get an access token using the authorization code obtained from the server. |

Query parameters for this API are as follows:

Table 154: *Query Parameters for the Auth Code API*

| Parameter | Values | Description |
|---------------|---|--|
| client_id | client_id is a unique hexadecimal string | The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin. |
| client_secret | client_secret is a unique hexadecimal string | The client_secret is a unique identifier provided to each developer at the time of registration. Application developers can obtain a client ID and client secret when they register with the API gateway admin. |
| grant_type | authorization_code | Use code to get the authorization code that can be exchanged for the token. |
| code | auth_code received from step 1 | The authorization code received from the authorization server. |
| redirect_uri | string | The redirect URI must be the same as the one given at the time of registration. This is an optional parameter. |

The response to this API query is a JSON dictionary with following values:

Table 155: *Auth Token Values*

| Parameter | Values | Description |
|---------------|---------|--|
| token_type | bearer | Identifies the token type. Central supports only the bearer token type (See https://tools.ietf.org/html/rfc6750) |
| refresh_token | string | Refresh tokens are credentials used to renew or refresh the access_token when it expires without repeating the complete authentication flow. A refresh token is a string representing the authorization granted to the client by the resource owner. |
| expires_in | seconds | The lifetime, in seconds, of the access token. |
| access_token | string | Access tokens are credentials used to access protected resources. An access token is a string representing an authorization issued to the client. |

Example

Request Method: POST

URL: https://apigw-prod2.central.arubanetworks.com/oauth2/token?client_id=<Ccentral-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx \

Content -Type: application/json

Response:

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```

Step 5: Refreshing a Token

You can use the refresh token obtained in the previous step to update the access token without repeating the entire authentication process.

Table 156: *URL to Refresh a Token*

| URL | Description |
|---|--|
| https://app1-apigw.central.arubanetworks.com/oauth2/token | The endpoint is a POST call to refresh the access token using the refresh token obtained from the server |

Query parameters for this API are as follows:

Table 157: *Query Parameters for Refresh Tokens*

| Parameter | Value | Description |
|---------------|---|--|
| client_id | client_id is a unique hexadecimal string | The client_id is a unique identifier that identifies the caller. Application developers obtain a client ID and a client secret when they register with the API gateway admin. |
| client_secret | client_secret is a unique hexadecimal string | The client_secret is a unique identifier provided to each developer at the time of registration. Application developers obtain a client ID and a client secret when they register with the API gateway admin. |
| grant_type | refresh_token | Specify refresh_token as the grant type to request that an authorization code be exchanged for a token |
| refresh_token | string | A string representing the authorization granted to the client by the resource owner. |

The response to this API query is a JSON dictionary with following values:

| Parameter | Value | Description |
|---------------|---------|---|
| token_type | bearer | Identifies the token type. Only the bearer token type is supported. For more information, see https://tools.ietf.org/html/rfc6750 . |
| refresh_token | string | Refresh tokens are credentials used to renew or refresh the access token when it expires without going through the complete authorization flow. A refresh token is a string representing the authorization granted to the client by the resource owner. |
| expires_in | seconds | The expiration duration of the access tokens in seconds. |
| access_token | string | Access tokens are credentials used to access the protected resources. An access token is a string representing an authorization issued to the client. |

Example

Method: POST

https://apigw-prod2.central.arubanetworks.com/oauth2/token?client_id=<Ccentral-API-app-clientid>&client_secret=xxxx&grant_type=authorization_code&code=xxxx \

Response

```
{
  "refresh_token": "xxxx",
  "token_type": "bearer",
  "access_token": "xxxx",
  "expires_in": 7200
}
```


Step 6: Deleting a Token

To delete the access token, access the following URL:

Table 158: *URL to Delete a Token*

| URL | Description |
|---|---|
| https://app1-apigw.central.arubanetworks.com/oauth2/token | This endpoint is accessible over SSL. The HTTP (non-SSL) connections are redirected to SSL port. Customer ID is a string. |

Example

Method : DELETE

URL:<https://app1-apigw.central.arubanetworks.com/oauth2/api/tokens>

JSON Body:

```
{
  "access_token": "<access_token_to_be_deleted>",
  "customer_id": "<customer_id_to_whom_token_belongs_to>"
}
```

Headers:

Content-Type: application/json

X-CSRF-Token: <CSRF_token_obatained_from_login_API>

Cookie: "session=<session_obatained_from_login_API>"

Viewing Usage Statistics

The **API Gateway** page includes the **Usage** tab that displays the API usage. The **Usage** tab is available only for administrators and the usage data is stored only for the previous 30 days. The following details are displayed:

- Assigned rate limit.
- Total usage.
- Per user usage.
- MSP and tenant usage if you are in MSP mode.

The administrator receives an alert through text message or email when the API usage reaches a threshold. You can set the threshold to 75% of the rate limit value.

To view the usage statistics for users of API Gateway, complete the following steps:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.
The **API Gateway** page is displayed.
2. Click **Usage**. The following details are displayed:

API GATEWAY

[APIs](#)


[My Apps & Tokens](#)

[Usage](#)


Please note that network stats / telemetry data is stored only for the last one month

Rate Limit:10000000

Total Usage

| DATE | USAGE PER DAY | USAGE PERCENTAGE |
|---|---------------|------------------|
|  <p>No data to display right now</p> | | |

Per User Usage

| USER | DATE | USAGE PER DAY |
|---|------|---------------|
|  <p>No data to display right now</p> | | |

- **Rate Limit**—The total rate limit assigned for API calls for a month.
- **Total Usage:**
 - **Date**—The date of usage.
 - **Usage Per Day**—Usage per day.
 - **Usage Percentage**—Usage percentage for a specific date.
- **Per User Usage:**
 - **User**—The name of the user.
 - **Date**—The date on which the application was accessed.
 - **Usage Per Day**—The total usage by the user per day. This is derived based on the total number of API calls made on a per day basis. This is an aggregate across all customers.
- If you are in MSP mode, the **MSP & Tenant Usage** table is displayed:
 - **Tenant ID**: ID of the tenant account.
 - **Date**: The date on which the application was accessed.
 - **Usage Per Day**: The total usage by the tenant account per day. This is derived based on the total number of API calls made on a per day basis.



The **Usage** tab is only available for administrators and the usage data is stored only for the previous 30 days.

Webhooks

Webhooks allow you to implement event reactions by providing real-time information or notifications to other applications. Aruba Central allows you to create Webhooks and select Webhooks as the notification delivery option for all alerts.

Using Aruba Central, you can integrate Webhooks with other third-party applications such as ServiceNow, Zapier, IFTTT, and so on.

You can access the Webhooks service either through the Aruba Central UI or API Gateway. Aruba Central supports creating up to 10 Webhooks. To enable redundancy, Aruba Central allows you to add up to three URLs per Webhook.

From Aruba Central, you can add, list, or delete Webhooks; get or refresh Webhooks token; get or update Webhooks settings for a specific item; and test Webhooks notification.

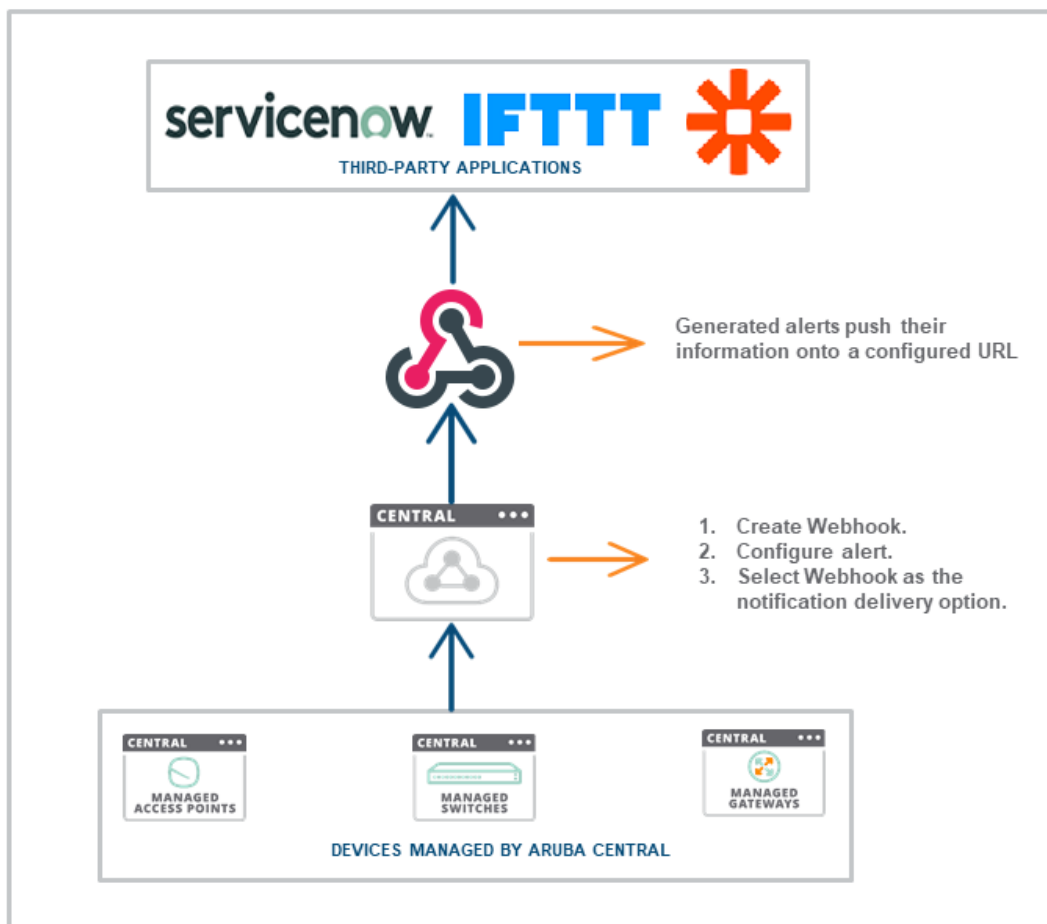
This section includes the following topics:

- [Creating and Updating Webhooks Through the UI on page 488](#)
- [Refreshing Webhooks Token Through the UI on page 489](#)
- [Creating and Updating Webhooks Through the API Gateway on page 489](#)
- [List of Webhooks APIs on page 490](#)
- [Sample Webhooks Payload Format for Alerts on page 491](#)

In the **Alerts & Events** page, click the **Configuration**  icon to configure and enable an alert. In the **Notification Options**, select **Webhooks** as the notification delivery option.

The following figure illustrates how Aruba Central integrates with third-party applications using Webhooks.

Figure 103 *Webhooks Integration*



Creating and Updating Webhooks Through the UI

To access the Webhooks service from the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.
The **Webhooks** page is displayed.
2. In the **Webhook** tab, click **+Webhook**.

WEBHOOKS

Webhook



| | | | | | + Webhook |
|---------|----------------|------------|------------|-------|---------------------------|
| Webhook | | | | | |
| NAME | NUMBER OF U... | UPDATED AT | WEBHOOK ID | TOKEN | |
| | | | | | |

a. **Webhook Name**—Enter a name for the Webhook

b. **URLs**—Enter the URL. Click + to enter another URL. You can add up to three URLs.

3. Click **Save**. The Webhooks is created and listed in the **Webhook** table.

The **Webhook** table displays the following information and also allows you to edit or delete Webhooks:

- **Name**—Name of the Webhooks.
- **Number of URL Entries**—Number of URLs in Webhooks. Click the number to view the list of URLs.
- **Updated At**—Date and time at which Webhooks was updated.
- **Webhook ID**—Webhooks ID.
- **Token**—Webhooks token. Webhooks token enables header authentication and the third-party receiving service must validate the token to ensure authenticity.
- **Edit**—In the **Webhook** table, select the Webhook from the list and click  icon to edit the Webhook. You can refresh the token and add URLs. Click **Save** to save the changes.
- **Delete**—In the **Webhook** table, select the Webhook from the list and click  icon and click **Yes** to delete the Webhook.

Refreshing Webhooks Token Through the UI

To refresh Webhooks token through the UI:

1. In the **Account Home** page, under **Global Settings**, click **Webhooks**.

The **Webhooks** page is displayed.

2. In the **Webhook** table, select the Webhook from the list and click  icon to edit.

3. In the pop-up window, click the refresh icon next to the token. The token is refreshed.

Creating and Updating Webhooks Through the API Gateway

The following HTTP methods are defined for Aruba Central API Webhooks resource:

- **GET**
- **POST**
- **PUT**
- **DELETE**

You can perform CRUD operation on the Webhooks URL configuration. The key configuration elements that are required to use API Webhooks service are Webhooks URL and a shared secret.

A shared secret token is generated for the Webhooks URL when you register for Webhooks. A hash key is generated using SHA256 algorithm by using the payload and the shared secret token. The API required to refresh the shared secret token is provided for a specific Webhooks configuration. You can choose the frequency at which you want to refresh the secret token.

To access and use the API Webhooks service:

1. In the **Account Home** page, under **Global Settings**, click **API Gateway**.

The **API Gateway** page is displayed.

2. In the **APIs** tab, click the **Swagger** link under the **Documentation** header. The Swagger website opens.
3. In the Swagger website, from the **URL** drop-down list, select **Webhook**. All available Webhooks APIs are listed under **API Reference**.



For more information on Webhooks APIs, refer to <https://app1-apigw.central.arubanetworks.com/swagger/central>.

List of Webhooks APIs

Aruba Central supports the following Webhooks APIs:

- **GET /central/v1/webhooks**—Gets a list of Webhooks.

The following is a sample response:

```
{
  "count": 1,
  "settings": [
    {
      "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
      "name": "AAA",
      "updated_ts": 1523956927,
      "urls": [
        "https://example.org/webhook1",
        "https://example.org/webhook1"
      ],
      "secure_token": "KEu5ZPTi44UO4MnMiOqz"
    }
  ]
}
```

- **POST /central/v1/webhooks**—Creates Webhooks.

The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **DELETE /central/v1/webhooks/{wid}**—Deletes Webhooks.

The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8"
}
```

- **GET /central/v1/webhooks/{wid}**—Gets Webhooks settings for a specific item.

The following is a sample response:

```
{
  "wid": "e26450be-4dac-435b-ac01-15d8f9667eb8",
  "name": "AAA",
  "updated_ts": 1523956927,
  "urls": [
    "https://example.org/webhook1",
    "https://example.org/webhook1"
  ],
  "secure_token": "KEu5ZPTi44UO4MnMiOqz"
}
```

- **PUT /central/v1/webhooks/{wid}**—Updates Webhooks settings for a specific item.

The following is a sample response:

```
{
  "name": "AAA",
  "wid": "e829a0f6-1e36-42fe-bafd-631443cbd581"
}
```

- **GET /central/v1/webhooks/{wid}/token**—Gets the Webhooks token for the Webhooks ID.

The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{"token": "zSMrzuYrblgBfByy2JrM", "ts": 1523957233}]"
}
```

- **PUT /central/v1/webhooks/{wid}/token**—Refreshes the Webhooks token for the Webhooks ID.

The following is a sample response:

```
{
  "name": "AAA",
  "secure_token": "[{"token": "zSMrzuYrblgBfByy2JrM", "ts": 1523957233}]"
}
```

- **GET /central/v1/webhooks/{wid}/ping**—Tests the Webhooks notification and returns whether success or failure.

The following is a sample response:

```
"Ping Response [{"url": "https://example.org", "status": 404}]"
```

Sample Webhooks Payload Format for Alerts

URL POST <webhook-url>

Custom Headers

```
Content-Type: application/json
X-Central-Service: Alerts
X-Central-Event: Radio-Channel-Utilization
X-Central-Delivery-ID: 72d3162e-cc78-11e3-81ab-4c9367dc0958
X-Central-Delivery-Timestamp: 2016-07-12T13:14:19-07:00
X-Central-Customer-ID: <#####>
```

Refer to the following topics to view sample JSON content:

- [Access Point Alerts—Sample JSON](#)
- [Switch Alerts—Sample JSON](#)
- [Gateway Alerts—Sample JSON](#)
- [Miscellaneous Alerts—Sample JSON](#)

Access Point Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

AP Disconnected

```
{
  "alert_type": "AP disconnected",
  "description": "AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c"
}
```



```

disconnected, Group:unprovisioned",
  "timestamp": 1564326129,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-4",
  "state": "Open",
  "nid": 4,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:09 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm2zVQ01ZtiGF20e",
  "severity": "Critical"
}

```

AP Connected Clients

```

{
  "alert_type": "AP_CONNECTED_CLIENTS",
  "description": "Number of Clients connected to AP with name 84:d4:7e:c5:c8:8c has been above 1 for about 5 minutes since 2019-07-29 12:26:00 UTC.",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1255",
  "state": "Open",
  "nid": 1255,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "name": "84:d4:7e:c5:c8:8c",
    "duration": "5",
    "threshold": "1",
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVGH9ZtiGF20d",
  "severity": "Major"
}

```

AP CPU Over Utilization

```

{
  "alert_type": "AP_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for AP 84:d4:7e:c5:c8:8c with serial CT0779239 has been above 10% for about 5 minutes since 2019-07-28 14:21:00 UTC.",
  "timestamp": 1564323960,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1250",
  "state": "Open",
  "nid": 1250,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "84:d4:7e:c5:c8:8c",
    "duration": "5",

```



```

    "time": "2019-07-28 14:21:00 UTC",
    "threshold": "10",
    "ds_key": "201804170291.CT0779239.cpu_utilization.5m",
    "serial": "CT0779239",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw4-VVrVQ01ZtiGFkZ3",
  "severity": "Critical"
}

```

AP Memory Over Utilization

```

{
  "alert_type": "AP_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for AP iap-303-iphone456-offline with serial CNGHKGX004
has been above 40% for about 5 minutes
since 2019-07-24 07:11:00 UTC.",
  "timestamp": 1563952560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1251",
  "state": "Open",
  "nid": 1251,
  "details": {
    "_rule_number": "1",
    "group": "3",
    "name": "iap-303-iphone456-offline",
    "labels": "3,118",
    "duration": "5",
    "time": "2019-07-24 07:11:00 UTC",
    "threshold": "40",
    "ds_key": "201804170291.CNGHKGX004.memory_utilization.5m",
    "serial": "CNGHKGX004",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWwiljihVQ01ZtiGThDA",
  "severity": "Major"
}

```

AP Radio Noise Floor

```

{
  "alert_type": "AP_RADIO_NOISE_FLOOR",
  "description": "Noise floor on AP iap-303-iphone456-offline operating on Channel 10 and
serving 0 clients has been above -110 dBm
for about 10 minutes since 2019-07-24 07:06:00 UTC.",
  "timestamp": 1563952560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1253",
  "state": "Open",
  "nid": 1253,
  "details": {
    "_rule_number": "0",
    "group": "3",
    "name": "iap-303-iphone456-offline",
    "_radio_num": "1",
    "client_count": "0",
    "labels": "3,118",
    "_band": "0",
    "duration": "10",
    "time": "2019-07-24 07:06:00 UTC",
    "threshold": "110",
    "ds_key": "201804170291.CNGHKGX004.radio.noisefloor",
    "serial": "CNGHKGX004",

```



```

    "channel": "10"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWwiljjgVQ01ZtiGThDB",
  "severity": "Critical"
}

```

AP Radio Over Utilization

```

{
  "alert_type": "AP_RADIO_OVER_UTILIZATION",
  "description": "Radio utilization on AP 84:d4:7e:c5:c8:8c operating on Channel 36E and serving 0 clients has been above 1% for about 5 minutes since 2019-07-28 14:31:00 UTC.",
  "timestamp": 1564324560,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1252",
  "state": "Open",
  "nid": 1252,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "84:d4:7e:c5:c8:8c",
    "_radio_num": "0",
    "client_count": "0",
    "_band": "1",
    "duration": "5",
    "unit": "%",
    "time": "2019-07-28 14:31:00 UTC",
    "threshold": "1",
    "ds_key": "201804170291.CT0779239.radio.busy64",
    "serial": "CT0779239",
    "channel": "36E"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5An08VQ01ZtiGFpgm",
  "severity": "Critical"
}

```

Client Attack detected

```

{
  "alert_type": "Client attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1) detected an unencrypted frame between a valid client (88:63:df:bb:2a:9d) and access point (BSSID 90:4c:81:72:77:55) with source 88:63:df:bb:2a:9d and receiver ff:ff:ff:ff:ff:ff SNR value is 55",
  "timestamp": 1564392710,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-13",
  "state": "Open",
  "nid": 13,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
    "time": "2019-07-29 09:31:50 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9EmBxVQ01ZtiG01Q8",
  "severity": "Critical"
}

```


Connected Clients

```
{
  "alert_type": "CONNECTED_CLIENTS",
  "description": "Number of Clients connected to swarm with name SetMeUp-CA:35:56 has been
above 1 for about 5 minutes
    since 2019-07-29 12:26:00 UTC.",
  "timestamp": 1564403460,
  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-1254",
  "state": "Open",
  "nid": 1254,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "SetMeUp-CA:35:56",
    "duration": "5",
    "aggr_context": "swarm",
    "time": "2019-07-29 12:26:00 UTC",
    "threshold": "1",
    "ds_key": "b8be21720dc04a8e9f0028374b6a9bbd.cluster.156.device.clients.5m",
    "serial": "156"
  },
  "operation": "create",
  "device_id": "156",
  "id": "AWw9tmhNVQ01ZtiGQR5U",
  "severity": "Critical"
}
```

Infrastructure Attack Detected

```
{
  "alert_type": "Infrastructure attack detected",
  "description": "An AP (NAME iap-303-iphone456-o and MAC 90:4c:81:cf:27:74 on RADIO 1)
detected that the Access Point with
    MAC f0:5c:19:23:56:10 and BSSID f0:5c:19:23:56:10 has sent a beacon for SSID tan This
beacon advertizes channel 149
    but was received on channel 161 with SNR 50 ",
  "timestamp": 1564400165,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-12",
  "state": "Open",
  "nid": 12,
  "details": {
    "group": "3",
    "labels": "3,142,141",
    "params": "None",
    "_rule_number": "0",
    "time": "2019-07-29 11:36:05 UTC"
  },
  "operation": "create",
  "device_id": "CNGHKGX004",
  "id": "AWw9hCLAVQ01ZtiGPlig",
  "severity": "Critical"
}
```

Insufficient Power Alert

```
{
  "alert_type": "INSUFFICIENT_POWER_ALERT",
  "description": "Insufficient inline power supplied to AP-205 with name 04:bd:88:c3:b6:f0",
  "timestamp": 1564403450,
  "webhook": "68612ee3-3ee9-4da4-b07b-13977a350344",
  "setting_id": "b8be21720dc04a8e9f0028374b6a9bbd-21",
  "state": "Open",
  "nid": 21,
  "details": {
    "group": "0",

```



```

    "name": "04:bd:88:c3:b6:f0",
    "labels": [],
    "label_site_desc": "",
    "time": "2019-07-29 12:30:50 UTC",
    "serial": "CM0381143",
    "group_name": "default",
    "ap_model": "AP-205"
  },
  "operation": "create",
  "device_id": "CM0381143",
  "id": "AWw9tkNGVQO1ZtiGQRz-",
  "severity": "Major"
}

```

Modem Plugged

```

{
  "alert_type": "Modem Plugged",
  "description": "Modem plugged to ap with name 84:d4:7e:c5:c8:8c'and MAC address 84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-18",
  "state": "Open",
  "nid": 18,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzJKL90tiGF20d",
  "severity": "Critical"
}

```

Modem Unplugged

```

{
  "alert_type": "Modem Unplugged",
  "description": "Modem unplugged from ap with name 84:d4:7e:c5:c8:8c'and MAC address 84:d4:7e:c5:c8:8c",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-19",
  "state": "Open",
  "nid": 19,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVQO1ZtiGF20d",
  "severity": "Critical"
}

```


New AP Detected

```
{
  "alert_type": "New AP detected",
  "description": "New AP with Name 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8c
detected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-3",
  "state": "Open",
  "nid": 3,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVQO1ZtiJH56e",
  "severity": "Major"
}
```

New Virtual Controller Detected

```
{
  "alert_type": "New Virtual Controller detected",
  "description": "New Virtual Controller with Name SetMeUp-CA:51:D6, Version 8.4.0.0_69847
and IP address 10.29.43.70
detected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-1",
  "state": "Open",
  "nid": 1,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "SetMeUp-CA:51:D6",
      "8.4.0.0_69847",
      "10.29.43.70"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVQO1ZtiJH56j",
  "severity": "Critical"
}
```

Rogue AP Detected

```
{
  "alert_type": "Rogue AP detected",
  "description": "An AP (NAME 84:d4:7e:c5:c8:8c and MAC address 84:d4:7e:c5:c8:8con RADIO 1)
detected an access point
(BSSID 0c:00:01:34:69:62 and SSID ssid1 on CHANNEL 52) as rogue",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-10",
  "state": "Open",
}
```



```

"nid": 10,
"details": {
  "_rule_number": "0",
  "group": "1",
  "labels": "",
  "params": [
    "84:d4:7e:c5:c8:8c",
    "84:d4:7e:c5:c8:8c",
    "1",
    "0c:00:01:34:69:62",
    "ssid1",
    "52"
  ],
  "time": "2019-07-28 15:02:08 UTC"
},
"operation": "create",
"device_id": "CT0779239",
"id": "AWw5GmlzVQ01ZtiJK891",
"severity": "Critical"
}

```

Uplink Changed

```

{
  "alert_type": "Uplink Changed",
  "description": "Uplink changed from 0 to 1 for ap'with name {params[2]} and MAC address {params[3]}",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-17",
  "state": "Open",
  "nid": 17,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "params": [
      "0",
      "1",
      "84:d4:7e:c5:c8:8c",
      "84:d4:7e:c5:c8:8c"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5GmlzVQ01ZtiGF20d",
  "severity": "Critical"
}

```

Virtual Controller Disconnected

```

{
  "alert_type": "Virtual controller disconnected",
  "description": "Virtual Controller with Name SetMeUp-CA:51:D6, Version 8.4.0.0_69847 and IP address 10.29.43.70 disconnected, Group:unprovisioned",
  "timestamp": 1564326128,
  "webhook": "780c65a0-10b6-4eb1-b725-21b0d52aa432",
  "setting_id": "201804170291-2",
  "state": "Open",
  "nid": 2,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",

```



```

    "params": [
      "SetMeUp-CA:51:D6",
      "8.4.0.0_69847",
      "10.29.43.70"
    ],
    "time": "2019-07-28 15:02:08 UTC"
  },
  "operation": "create",
  "device_id": "CT0779239",
  "id": "AWw5Gm1zVQ01ZtiGF20d",
  "severity": "Critical"
}

```

Switch Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

Switch Disconnected

```

{
  "alert_type": "Switch Disconnected",
  "description": "Switch with serial CN8AHKW095, MAC address 54:80:28:b8:f6:20 IP address 10.22.41.3 and Hostname Aruba-2930F-24G-PoEP-4SFPP disconnected, Group:unprovisioned",
  "timestamp": 1569475139,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-203",
  "state": "Open",
  "nid": 203,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "labels": "",
    "conn_status": "disconnected",
    "params": [
      "CN8AHKW095",
      "54:80:28:b8:f6:20",
      "10.22.41.3",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "time": "2019-09-26 05:18:59 UTC"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1sAhfAYu0OgJ2anzUD",
  "severity": "Major"
}

```

New Switch Connected

```

{
  "alert_type": "New Switch Connected",
  "description": "New Switch with serial CN8AHKW095, MAC address 54:80:28:b8:f6:20 IP address 10.22.41.3 and Hostname Aruba-2930F-24G-PoEP-4SFPP connected, Group:unprovisioned",
  "timestamp": 1569476559,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-201",
  "state": "Open",
  "nid": 201,
  "details": {
    "group": "1",
    "labels": "",

```



```

    "params": [
      "CN8AHKW095",
      "54:80:28:b8:f6:20",
      "10.22.41.3",
      "Aruba-2930F-24G-PoEP-4SFPP"
    ],
    "_rule_number": "0",
    "time": "2019-09-26 05:42:39 UTC"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AWlsF8IGYu0OgJ2an0Aq",
  "severity": "Major"
}

```

Switch Memory Over Utilization

```

{
  "alert_type": "SWITCH_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial CN8AHKW095 has been above 10% for about 5 minutes since 2019-09-26 05:48:00 UTC",
  "timestamp": 1569477180,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1301",
  "state": "Open",
  "nid": 1301,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "duration": "5",
    "time": "2019-09-26 05:48:00 UTC",
    "threshold": "10",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.memory_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AWlsITrfYu0OgJ2an0UP",
  "severity": "Critical"
}

```

Switch CPU Over Utilization

```

{
  "alert_type": "SWITCH_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for Switch Aruba-2930F-48G-PoEP-4SFPP with serial CN88HKX1CR has been above 5% for about 5 minutes since 2019-09-26 06:07:00 UTC.",
  "timestamp": 1569478320,
  "webhook": "f8b021a2-8127-4c28-a755-8ee6e01ada66",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1300",
  "state": "Open",
  "nid": 1300,
  "details": {
    "_rule_number": "0",
    "group": "41",
    "name": "Aruba-2930F-48G-PoEP-4SFPP",
    "duration": "5",
    "time": "2019-09-26 06:07:00 UTC",
    "threshold": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN88HKX1CR.cpu_utilization.5m",
    "serial": "CN88HKX1CR",
    "unit": "%"
  },
  "operation": "create",

```



```

    "device_id": "CN88HKX1CR",
    "id": "AW1sMqB4Yu0OgJ2an055",
    "severity": "Critical"
}

```

Switch Interface Rx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_RX_RATE",
  "description": "Receive rate for Interface 15 on Switch Aruba-2930F-24G-PoEP-4SFPP has been above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1303",
  "state": "Open",
  "nid": 1303,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "15",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.rx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2 aoCgl",
  "severity": "Critical"
}

```

Switch Interface Tx Rate

```

{
  "alert_type": "SWITCH_INTERFACE_TX_RATE",
  "description": "Transfer rate for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has been above 1 % for about 5 minutes since 2019-09-26 13:18:00 UTC.",
  "timestamp": 1569504180,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1302",
  "state": "Open",
  "nid": 1302,
  "details": {
    "_rule_number": "0",
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "max_value_for_percentage": "1000.0",
    "threshold": "1",
    "intf_name": "19",
    "time": "2019-09-26 13:18:00 UTC",
    "duration": "5",
    "ds_key": "e344d961bccd411dbd279bf92f61b989.CN8AHKW095.intf.tx_utilization.5m",
    "serial": "CN8AHKW095",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW1tvTgBYu0OgJ2aoCgk",
  "severity": "Critical"
}

```

Switch POE Utilization


```
{
  "alert_type": "SWITCH_POE_UTILIZATION",
  "description": "PoE utilization for Switch Aruba-2930F-24G-PoEP-4SFPP with serial
CN69HKW05T MAC address e0:07:1b:c4:8d:80
    and IP address 10.22.182.78 has been above 1%",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```

Switch Interface Input Errors

```
{
  "alert_type": "SWITCH_INTERFACE_INPUT_ERRORS",
  "description": "Input errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has been
above 90% for about
    30 minutes since 2019-09-26 06:07:00 UTC .",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}
```

Switch Interface Output Errors

```
{
  "alert_type": "SWITCH_INTERFACE_OUTPUT_ERRORS",
  "description": "Output errors for Interface 19 on Switch Aruba-2930F-24G-PoEP-4SFPP has
been above 90% for about
    30 minutes since 2019-09-26 06:07:00 UTC.",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
```



```

    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

Switch Mismatch Config

```

{
  "alert_type": "Switch Mismatch Config",
  "description": "Config mismatch occurred in switch with serial CN69HKW05T MAC address e0:07:1b:c4:8d:80 and IP address 10.22.182.78 and Hostname Aruba-2930F-48G-PoEP-4SFPP ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```

Switch Hardware Failure

```

{
  "alert_type": "SWITCH_HARDWARE_FAILURE",
  "description": "Switch with serial CN8AHKW095 : Fan 1 failed ",
  "timestamp": 1569505920,
  "webhook": "4d588353-3355-487d-81af-c97f62b0abb0",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1307",
  "state": "Open",
  "nid": 1307,
  "details": {
    "group": "0",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "ip": "10.22.182.78",
    "labels": [],
    "mac": "e0:07:1b:c4:8d:80",
    "time": "2019-09-26 13:52:00 UTC",
    "threshold": "1",
    "serial": "CN69HKW05T"
  },
  "operation": "create",
  "device_id": "CN69HKW05T",
  "id": "AW1t18ccYu0OgJ2aoDYw",
  "severity": "Critical"
}

```


Switch Interface Duplex Mode

```
{
  "alert_type": "SWITCH_INTERFACE_DUPLEX_MODE",
  "description": "Interface 19 on switch Aruba-2930F-24G-PoEP-4SFPP with serial CN8AHKW095 is operating at Half-Duplex mode",
  "timestamp": 1569901561,
  "webhook": "c71404f4-00c1-4241-8bf4-c8d3f981caa2",
  "setting_id": "e344d961bccd411dbd279bf92f61b989-1306",
  "state": "Open",
  "nid": 1306,
  "details": {
    "group": "1",
    "name": "Aruba-2930F-24G-PoEP-4SFPP",
    "labels": "",
    "mode": "Half",
    "intf_name": "19",
    "time": "2019-10-01 03:46:01 UTC",
    "serial": "CN8AHKW095"
  },
  "operation": "create",
  "device_id": "CN8AHKW095",
  "id": "AW2FbMiOYu0OgJ2asaWh",
  "severity": "Critical"
}
```

Gateway Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

WAN Uplink Flap

```
{
  "alert_type": "WAN_UPLINK_FLAP",
  "description": "Uplink link1_inet link status flapped 1% on device with CNHHKLB031 for about 15 minutes since 2019-07-25 12:36:00 UTC.",
  "timestamp": 1564059060,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1600",
  "state": "Open",
  "nid": 1600,
  "details": {
    "status": "DOWN",
    "_rule_number": "0",
    "group": "77",
    "labels": "8,661",
    "current_status": "UP",
    "duration": "15",
    "intf_name": "link1_inet",
    "time": "2019-07-25 12:36:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.flap.5m",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpL0fvVQ01ZtiGh-2_",
  "severity": "Critical"
}
```

WAN Tunnel Flap


```
{
  "alert_type": "WAN_TUNNEL_FLAP",
  "description": "Tunnel data-vpnc-00:1a:1e:03:83:30-link1_inet status flapped 1%
    on device CNHHKLB031 for about 15 minutes since 2019-07-25 12:26:00 UTC.",
  "timestamp": 1564058460,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1601",
  "state": "Open",
  "nid": 1601,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "_rule_number": "0",
    "group": "77",
    "dst_ip": "172.168.101.9",
    "labels": "8,661",
    "src_ip": "192.168.51.254",
    "duration": "15",
    "time": "2019-07-25 12:26:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.tunnel.flap.5m",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpJiAiVQO1ZtiGh5tw",
  "severity": "Critical"
}
```

WAN Auto Negotiation Flap

```
{
  "alert_type": "WAN_AUTO_NEGOTIATION_FLAP",
  "description": "Uplink GE0/0/1 speed flapped 1% on device CNHHKLB031 for about
    15 minutes since 2019-07-25 12:32:00 UTC.",
  "timestamp": 1564058820,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1602",
  "state": "Open",
  "nid": 1602,
  "details": {
    "new_speed": "Auto",
    "group": "77",
    "labels": "8,661",
    "duration": "15",
    "_rule_number": "0",
    "intf_name": "GE0/0/1",
    "time": "2019-07-25 12:32:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.uplink.speed.flap.5m",
    "serial": "CNHHKLB031",
    "speed": "1000",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpK55sVQO1ZtiGh8zr",
  "severity": "Minor"
}
```

WAN IPsec SA Establishment Failed

```
{
  "alert_type": "WAN_IPSEC_SA_ESTABLISHMENT_FAILED",
  "description": "IPsec Tunnel Establishment from 192.168.51.254 to 172.168.101.9 failed"
```



```

    on device CNHHKLB031 at 2019-07-25 12:49:56 UTC",
    "timestamp": 1564058996,
    "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
    "setting_id": "abce082bef4a428bb31366f6d6fff223f-1550",
    "state": "Open",
    "nid": 1550,
    "details": {
      "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
      "group": "77",
      "name": "None",
      "labels": [
        "8",
        "661"
      ],
      "src_ip": "192.168.51.254",
      "link_tag": "link1_inet",
      "time": "2019-07-25 12:49:56 UTC",
      "dst_ip": "172.168.101.9",
      "serial": "CNHHKLB031"
    },
    "operation": "create",
    "device_id": "CNHHKLB031",
    "id": "AWwpLlB0VQ01ZtiGh-WS",
    "severity": "Minor"
  }
}

```

WAN IPsec SA Down

```

{
  "alert_type": "WAN_IPSEC_SA_DOWN",
  "description": "IPSec tunnel from 192.168.52.254 to 172.168.101.9 is DOWN on device CNHHKLB031. Reason: Administrator cleared IPSEC SA at 2019-07-25 12:40:22 UTC",
  "timestamp": 1564058422,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6fff223f-1551",
  "state": "Open",
  "nid": 1551,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link2_mpls",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "src_ip": "192.168.52.254",
    "reason": "Administrator cleared IPSEC SA",
    "time": "2019-07-25 12:40:22 UTC",
    "dst_ip": "172.168.101.9",
    "serial": "CNHHKLB031",
    "uplink_tag": "link2_mpls"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpJY4aVQ01ZtiGh5c-",
  "severity": "Minor"
}

```

WAN IPsec SA All Down

```

{
  "alert_type": "WAN_IPSEC_SA_ALL_DOWN",
  "description": "All IPSec SAs down for device CNHHKLB031 at 2019-07-25 12:40:22 UTC",
  "timestamp": 1564058446,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6fff223f-1552",

```



```

"state": "Close",
"nid": 1552,
"details": {
  "serial": "CNHHKLB031",
  "labels": [
    "8",
    "661"
  ],
  "group": "77",
  "name": "None",
  "time": "2019-07-25 12:40:22 UTC"
},
"operation": "update",
"device_id": "CNHHKLB031",
"id": "AWwpJY3NVQO1ZtiGh5c9",
"severity": "Critical"
}

```

CFG Set Advertisement Failure

```

{
  "alert_type": "CFG_SET_ADVERTISEMENT_FAILURE",
  "description": "CFG-Set advertisement failure for Gateway with CNHHKLB031 on tunnel data-
vpnc-00:1a:1e:03:83:30-link1_inet
    from 192.168.51.254 to 172.168.101.9",
  "timestamp": 1564059635,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1554",
  "state": "Open",
  "nid": 1554,
  "details": {
    "alias_map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "src_ip": "192.168.51.254",
    "time": "2019-07-25 13:00:35 UTC",
    "map_name": "data-vpnc-00:1a:1e:03:83:30-link1_inet",
    "dst_ip": "172.168.101.9",
    "serial": "CNHHKLB031"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpOBCVVQO1ZtiGiD0f",
  "severity": "Major"
}

```

Controller CPU Over Utilization

```

{
  "alert_type": "CONTROLLER_CPU_OVER_UTILIZATION",
  "description": "CPU utilization for Gateway Aruba9004_40_OC_28 with serial CNHHKLB031 has
been above 1% for about 15 minutes
    since 2019-07-25 09:30:00 UTC.",
  "timestamp": 1564047900,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1351",
  "state": "Open",
  "nid": 1351,
  "details": {
    "_rule_number": "0",
    "group": "77",
    "name": "Aruba9004_40_OC_28",
    "labels": "8,661",

```



```

    "duration": "15",
    "time": "2019-07-25 09:30:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.cpu_utilization.5m",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwohP4LVQ01ZtiGgfbQ",
  "severity": "Critical"
}

```

Controller Memory Over Utilization

```

{
  "alert_type": "CONTROLLER_MEMORY_OVER_UTILIZATION",
  "description": "Memory utilization for Gateway Aruba9004_40_OC_28 with serial CNHHKLB031
has been above 1% for about 10 minutes
since 2019-07-25 09:30:00 UTC.",
  "timestamp": 1564047600,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1352",
  "state": "Open",
  "nid": 1352,
  "details": {
    "_rule_number": "0",
    "group": "77",
    "name": "Aruba9004_40_OC_28",
    "labels": "8,661",
    "duration": "10",
    "time": "2019-07-25 09:30:00 UTC",
    "threshold": "1",
    "ds_key": "abce082bef4a428bb31366f6d6ff223f.CNHHKLB031.memory_utilization.5m",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwogGqYVQ01ZtiGgc2L",
  "severity": "Major"
}

```

Controller OSPF Session Error

```

{
  "alert_type": "CONTROLLER OSPF SESSION ERROR",
  "description": "OSPF session state change for Gateway with hostname GSK_VPNC2 and serial
CW0003307 from Init State to Down State
for neighbor 1.0.0.2 on interface 100 with reason No hello packets received from
neighbour.Inactivity timer fired",
  "timestamp": 1564121712,
  "webhook": "60785e88-9513-4352-94d6-ec25fedbeddc",
  "setting_id": "b27f67fa44234c51a890fccea7c9b83e-1354",
  "state": "Open",
  "nid": 1354,
  "details": {
    "dst_state": "Down State",
    "neighbour_ip": "1.0.0.2",
    "group": "4",
    "uniq_identifier": "100-16777218",
    "labels": [
      "2",
      "11",
      "12",
      "15",
      "13",

```



```

    "8"
  ],
  "src_state": "Init State",
  "reason": "No hello packets received from neighbour.Inactivity timer fired",
  "time": "2019-07-26 06:15:12 UTC",
  "interface": "100",
  "serial": "CW0003307",
  "hostname": "GSK_VPNC2"
},
"operation": "create",
"device_id": "CW0003307",
"id": "AWws60Yxon2R5PyMmUU4",
"severity": "Major"
}

```

Gateway Base License Capacity Exceeded

```

{
  "alert_type": "GATEWAY_BASE_LICENSE_CAPACITY_EXCEEDED",
  "description": "Base license capacity limit exceeded for Gateway with name: Dev-BR1-GW-Kafka, serial: CP0015859",
  "timestamp": 1564141290,
  "webhook": "1348bcc4-ce00-4180-b314-32849c3638a1",
  "setting_id": "2fb4b8a7e77c496395950510a1d270bc-1356",
  "state": "Open",
  "nid": 1356,
  "details": {
    "serial": "CP0015859",
    "labels": [],
    "group": "1",
    "name": "Dev-BR1-GW-Kafka",
    "time": "2019-07-26 11:41:30 UTC"
  },
  "operation": "create",
  "device_id": "CP0015859",
  "id": "AWwuFgZqnGtA5yFV0hCr",
  "severity": "Critical"
}

```

DHCP Pool Consumption Alert

```

{
  "alert_type": "DHCP_POOL_CONSUMPTION_ALERT",
  "description": "DHCP Pool Consumption on Gateway CNHHKLB031 is 12% at 2019-07-25 13:02:39 UTC for 192.168.53.0/24",
  "timestamp": 1564059759,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1510",
  "state": "Open",
  "nid": 1510,
  "details": {
    "subnet": "192.168.53.0/24",
    "group": "77",
    "name": "None",
    "labels": "8,661",
    "time": "2019-07-25 13:02:39 UTC",
    "threshold": "12",
    "serial": "CNHHKLB031",
    "unit": "%"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpOfQAVQO1ZtiGiE2H",
  "severity": "Critical"
}

```

WAN Auto Negotiation


```
{
  "alert_type": "WAN_UPLINK_AUTONEGOTIATION_STATE_CHANGE",
  "description": "WAN ports autonegotiaton speed changed from 1000 Mbps to Auto Mbps for
device with CNHHKLB031 for
  uplink GE0/0/1 at 2019-07-25 12:46:36 UTC",
  "timestamp": 1564058796,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1506",
  "state": "Open",
  "nid": 1506,
  "details": {
    "new_speed": "Auto",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "intf_name": "GE0/0/1",
    "time": "2019-07-25 12:46:36 UTC",
    "serial": "CNHHKLB031",
    "speed": "1000"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwpK0IxVQ01ZtiGh8oh",
  "severity": "Minor"
}
```

WAN Uplink Status Change

```
{
  "alert_type": "WAN_UPLINK_STATUS_CHANGE",
  "description": "Uplink port link1_inet status change UP -&gt; DOWN for device with
CNHHKLB031 at 2019-07-25 09:22:31 UTC",
  "timestamp": 1564046551,
  "webhook": "394c7a3c-ca41-4476-8afc-857e54aa4b3b",
  "setting_id": "abce082bef4a428bb31366f6d6ff223f-1505",
  "state": "Open",
  "nid": 1505,
  "details": {
    "status": "UP",
    "group": "77",
    "name": "None",
    "labels": [
      "8",
      "661"
    ],
    "current_status": "DOWN",
    "intf_name": "link1_inet",
    "time": "2019-07-25 09:22:31 UTC",
    "serial": "CNHHKLB031",
    "uplink_tag": "link1_inet"
  },
  "operation": "create",
  "device_id": "CNHHKLB031",
  "id": "AWwocGtYVQ01ZtiGgT03",
  "severity": "Major"
}
```


Miscellaneous Alerts—Sample JSON

This section includes sample JSON content for the following alerts:

Device Config Change Detected

```
{
  "alert_type": "DEVICE_CONFIG_CHANGE_DETECTED",
  "description": "Config change detected on group nbapi_test for device type Switch by user
    example@hpe.com.\n\nSerial: None, \nMacAddress: None,
    \nConfig Content: Template Updated
    \nmodel: ALL\nversion: ALL\ndevice_type: HPPC\ntemplate changes: \n @@ -18,6 +18,6
@@\n\n\n
    ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+ name \"vlan_
44\"\n\n no ip address\n\n exit ",
  "timestamp": 1564383294,
  "webhook": "272eda1a-f79b-4192-ad6f-b35da11515bc",
  "setting_id": "715e45fe3ff8453da355cd34aff2afa5-2000",
  "state": "Open",
  "nid": 2000,
  "details": {
    "config_change": "Template Updated\nmodel: ALL\nversion: ALL\ndevice_type: HPPC\ntemplate
changes: \n @@ -18,6 +18,
    6 @@\n\n\n ip address dhcp-bootp\n\n exit\n\n vlan 13\n\n- name \"vlan_8888\"\n\n+ name
\"vlan_44\"\n\n no ip address\n\n exit ",
    "macaddr": "None",
    "group": "8",
    "dev_type": "Switch",
    "labels": "None",
    "group_name": "nbapi_test",
    "_rule_number": "0",
    "params": "None",
    "user": "example@hpe.com",
    "time": "2019-07-29 06:54:54 UTC",
    "serial": "None"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWw8grSBz6A6PlBvMk4",
  "severity": "Warning"
}
```

User Account Deleted

```
{
  "alert_type": "User account deleted",
  "description": "User with name v@gmail.com deleted.",
  "timestamp": 1569234480,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-15",
  "state": "Open",
  "nid": 15,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [
      "v@gmail.com"
    ],
    "_rule_number": "0",
    "time": "2019-09-23 10:28:00 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWldqe6rYu0OgJ2alXzT",
  "severity": "Major"
}
```


New User Account Added

```
{
  "alert_type": "New User account added",
  "description": "User account setting updated for user: newuser@gmail.com with language:en_US and idle timeout: 1800",
  "timestamp": 1569234534,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-14",
  "state": "Open",
  "nid": 14,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [],
    "_rule_number": "0",
    "time": "2019-09-23 10:28:54 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWldqr6nYu0OgJ2alX1l",
  "severity": "Major"
}
```

User Account Edited

```
{
  "alert_type": "User account edited",
  "description": "User with Name newuser@gmail.com, role readwrite and access [] updated.",
  "timestamp": 1569235100,
  "webhook": "057b0a95-9f06-4a0f-b4bf-149a28d749b3",
  "setting_id": "573b0412517a41c8a73a80f3e74ff0d2-16",
  "state": "Open",
  "nid": 16,
  "details": {
    "group": "-1",
    "labels": "None",
    "params": [
      "newuser@gmail.com",
      "readwrite",
      "[]"
    ],
    "_rule_number": "0",
    "time": "2019-09-23 10:38:20 UTC"
  },
  "operation": "create",
  "device_id": "",
  "id": "AWlds2LcYu0OgJ2alYM2",
  "severity": "Major"
}
```


The guest management feature allows guest users to connect to the network and at the same time, allows the administrator to control guest user access to the network.

Aruba Central allows administrators to create a splash page profile for guest users. Guest users can access the Internet by providing either the credentials configured by the guest operators or their respective social networking login credentials. For example, you can create a splash page that displays a corporate logo, color scheme and the terms of service, and enable logging in from a social networking service such as Facebook, Google, Twitter, and LinkedIn.

Businesses can also pair their network with the Facebook Wi-Fi service, so that the users logging into Wi-Fi hotspots are presented with a business page, before gaining access to the network.


To enable logging using Facebook, Google, Twitter, and LinkedIn credentials, ensure that you create an application (app) on the social networking service provider site and enable authentication for that app. The social networking service provider will then issue a client ID and client secret key that are required for configuring guest profiles based on social logins.

Guest operators can also create guest user accounts. For example, a network administrator can create a guest operator account for a receptionist. The receptionist creates user accounts for guests who require temporary access to the wireless network. Guest operators can create and set an expiration time for user accounts. For example, the expiration time can be set to 1 day.

For more information, see the following topics:

- [Guest Access Dashboard on page 513](#)
- [Creating Apps for Social Login on page 514](#)
- [Configuring a Guest Access Splash Page Profile on page 516](#)
- [Configuring Visitor Accounts on page 525](#)

Guest Access Dashboard

The  **Summary** page in the **Manage > Guest Access** application provides a dashboard displaying the number of guests, guest SSID, client count, type of clients, and guest connection for the selected group.

[Table 159](#) describes the contents of the **Guest Access Overview** page:

Table 159: *Guest Access Overview Page*

| Data Pane Item | Description |
|----------------------|--|
| Time Range | Time range for the graphs and charts displayed on the Overview pane. You can choose to view graphs for a time period of 1 day, 1 week, and 1 month. |
| Guests | Number of guests connected to the SSIDs with Guest splash page profiles. |
| Guest SSID | Number of guest SSIDs that are configured to use the Guest splash page profiles. |
| Avg. Duration | The average duration of client connection on the SSIDs with Guest splash page profiles. |

| Data Pane Item | Description |
|--------------------------------------|--|
| Max Concurrent Connections | Maximum number of client devices connected concurrently on the guest SSIDs. |
| Guest Connection (graph) | Time stamp for the client connections on the guest for the selected time range. |
| Guest Count by Authentication | Number of client devices based on the authentication type configured on the guest SSIDs. |
| Guest Count by SSID | Number of guest connections per SSID. |
| Client Type | Type of the client devices connected on the guest SSIDs. |

Creating Apps for Social Login

The following topics describe the procedures for creating applications to enable the social login feature:

- [Creating a Facebook App](#)
- [Creating a Google App](#)
- [Creating a Twitter App](#)
- [Creating a LinkedIn App](#)

Creating a Facebook App

Before creating a Facebook app, ensure that you have a valid Facebook account and you are registered as a Facebook developer with that account.

To create a Facebook app, perform the following steps:

1. Visit the Facebook app setup URL at <https://developers.facebook.com/apps>.
2. From **My Apps**, select **Add a New App**.
3. Enter the app name and your email address in the **Display Name** and **Contact Email** text boxes, respectively.
4. Click **Create App ID**.
5. Hover the mouse on **Facebook Login** and select **Setup**.
6. Click **Web** (that is, the WWW platform).
7. Enter the website URL in the **Site URL** box.
This URL is the same as the server URL mapped in the splash page configuration.
8. Click **Save**.
9. Read through the Next Steps section for further information on including Login Dialog, Access Tokens, Permissions, and App Review.
10. Go to **PRODUCTS > Facebook Login > Settings** from the left navigation menu.
11. Click the **Client OAuth Login** toggle switch to turn to **Yes**.
12. Enter the OAuth URI in the **Valid OAuth redirect URIs** box.

The URI is the server URL mapped in the splash configuration with **/oauth/reply** appended to it. To get the valid OAuth redirect URL, go to the **Guest Access > Splash Pages** path and click the eye (👁) icon available against the specific splash page name in the **Splash Pages** table.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, <https://example1.cloudguest.arubanetworks.com/oauth/reply>.

13. From the left navigation menu, select **App Review**.
14. Select the **Make <App Name> Public** toggle switch to make your app available to public.
15. Click **Category**.
16. In the **Choose a Category** pop-up window, select a category.
17. Click **Confirm**.
18. Select other extra permissions you want to provide for the users of your app.
There are 41 permissions available for you to select from.
19. Click **Add xx Items**, where x represents the number of permissions you selected.
20. Enter the reason for providing specific permissions and click **Save**.
21. Click **Submit for Review**.
22. On the left navigation pane, click the **Settings** icon.
Note the app ID and app secret key. Use the app ID and secret key when configuring Facebook login in the Aruba Central UI.
23. Under **App Domains**, enter the server URL.

Creating a Google App

Before creating an app for Google based login, ensure that you have a valid Google account.

To create a Google app, perform the following steps:

1. Access the Google Developer site at <https://code.google.com/apis/console>.
2. To select an existing project, click **Select a project** and select the desired project.
3. If the project is not created, click **Create a project**, enter the project name and click **Create**.
4. Click **Enable APIs and Services**.
5. Navigate to **Social** category, and then click **Google API**. The **Google API** window opens.
6. To enable the API, click **Enable**.
7. Click **Create Credentials**. If the credentials are already created, click **Go to credentials**.
8. In the **Credentials** pane, perform the following actions:
 - Under the **Where will you be calling the API from** section, select **Web Browser**.
 - Under the **What data you will be accessing** section, select **User Data**.
 - Click **What Credentials do I need**.
9. Under **Create an OAuth 2.0 client ID**. Enter the **OAuth 2.0 Client ID Name**.
10. Under **Authorized JavaScript Origins**, enter the base URL with FQDN of the guest instance that will be hosting the captive portal. For example, <https://%hostname%/>.
11. Under **Authorized Redirect URIs**, enter the cloud server OAuth reply URL that includes the FQDN of the cloud server instance with /oauth/reply appended at the end of the URL.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, <https://example1.cloudguest.exemplenetworks.com/oauth/reply>.

12. Click **Create Client ID**.
Under **Set up the OAuth 2.0 consent screen**, provide your **Email Address** and product name, and then click **Continue**. The client ID is displayed.

13. Click **Done**. A page showing the OAuth Client IDs opens.
14. Click the **OAuth client ID** to view the client ID and client secret key.
Use this client ID and client secret key when configuring Google login in the Aruba Central UI.

Creating a Twitter App

Before creating a Twitter app, ensure that you have a valid Twitter account.

To create a Twitter app, perform the following steps:

1. Visit the Twitter app setup URL at <https://apps.twitter.com>.
2. Click **Create New App**. The **Create an application** web page is displayed.
3. Enter the application name and description.
4. For OAuth 2.0 Redirect URLs, enter the HTTPS URL of the guest server to which you want to connect this social authentication source, and append /oauth/reply at the end of the URL.



Ensure that the URL is an HTTPS URL with a domain name and not the IP address. For example, <https://exa.example.com/oauth/reply>.

5. Select **Yes, I agree** to accept the Developer Agreement terms.
6. Click **Create a Twitter application**.
7. Click **Manage Keys and Access Tokens**.
The **Keys and Access Tokens** tab opens. The consumer key (API key) and consumer secret (API key) are displayed.
8. Note the ID and the secret key. The consumer key and consumer secret key when configuring Twitter login in Aruba Central UI.

Creating a LinkedIn App

Before creating a LinkedIn app, ensure that you have a valid LinkedIn account.

To create a LinkedIn app, complete the following steps:

1. Visit the LinkedIn app setup URL at <https://developer.linkedin.com>.
2. Click **My Apps**. You will be redirected to <https://www.linkedin.com/secure/developer/apps>.
3. Click **Create Application**. The **Create a New Application** web page is displayed.
4. Enter your company name, application name, description, website URL, application logo with the specification mentioned, application use, and contact information.
5. Click **Submit**. The **Authentication** page is displayed.
6. Note the client ID and client secret key displayed on the **Authentication** page.
7. For **OAuth 2.0 Redirect URLs**, enter the HTTPS URL of the guest server to which you want to connect this social authentication source and append /oauth/reply at the end of the URL.
8. Click **Add** and then click **Update**. The API and secret keys are displayed.
9. Note the API and secret key details. Use the API ID and secret key when configuring LinkedIn login in the Aruba Central UI.

Configuring a Guest Access Splash Page Profile

This topic describes the following procedures:

- [Adding a Guest Access Splash Page Profile](#)
- [Customizing a Splash Page Design](#)

- [Configuring a Guest Access Splash Page Profile](#)
- [Localizing a Guest Portal](#)
- [Associating a Splash Page Profile to an SSID](#)

Adding a Guest Access Splash Page Profile

To create a splash page profile:

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new Splash page, click the + icon.
The **New Splash Page** pane is displayed.
4. On the **Configuration** tab, configure the parameters described in the following table:

Table 160: *Splash Page Configuration*

| Data Pane Content | Description |
|--------------------------|--|
| Name | Enter a unique name to identify the splash profile. NOTE: If you attempt to enter an existing splash profile's name, Aruba Central displays a message stating that Splash page with this name already exists . |
| Type | Configure any of the following authentication methods to provide a secure network access to the guest users and visitors. <ul style="list-style-type: none"> ■ Anonymous ■ Authenticated ■ Facebook Wi-Fi |
| Anonymous | Configure the Anonymous login method if you want to allow guest users to log in to the Splash page without providing any credentials. For anonymous user authentication, you can also enable a pre-shared key to allow access. To enable a pre-shared key based authentication, set the Guest Key to ON and specify a password. |
| Authenticated | Configure authentication and authorization attributes, and login credentials that enable users to access the Internet as guests. You can configure an authentication method based on sponsored access and social networking login profiles. The authenticated options available for configuring the guest splash page are described in the following rows. |
| Username/Password | The Username/Password based authentication method allows pre-configured visitors to obtain access to wireless connection and the Internet. The visitors or guest users can register themselves by using the splash page when trying to access the network. The password is delivered to the users through print, SMS or email depending on the options selected during registration. To allow the guest users to register by themselves: <ol style="list-style-type: none"> 1. Enable Self-Registration. 2. Set the Verification Required to ON if the guest user account must be verified. 3. Specify a verification criteria to allow the self-registered users to verify through email or phone. <ul style="list-style-type: none"> ■ If email-based verification is enabled and the Send Verification Link is selected, a verification link is sent to the email address of the user. The guest users can click the link to obtain access to the Internet. ■ If phone-based verification is enabled, the guest users will receive an SMS. The administrators can also customize the content of the SMS by clicking on Customize |

Table 160: *Splash Page Configuration*

| Data Pane Content | Description |
|------------------------------------|---|
| | <p>SMS.</p> <p>4. Specify the duration within the range of 1-60 minutes, during which the users can access free Wi-Fi to verify the link. The users can log in to the network for the specified duration and click the verification link to obtain access to the Internet.</p> <p>By default, the expiration date for the accounts of self-registered guest users is set to infinite during registration. The administrator or the guest operator can set the expiration date after registration.</p> |
| Social Login | <p>Social Login—Enable this option to allow guest users to use their existing login credentials from social networking profiles such as Facebook, Twitter, Google, or LinkedIn and sign into a third-party website. When a social login based profile is configured, a new login account to access the guest network or third-party websites is not required.</p> <ul style="list-style-type: none"> ■ Facebook—Allows guest users to use their Facebook credentials to log in to the splash page. To enable Facebook integration, you must create a Facebook app and obtain the app ID and secret key. For more information on app creation, see Creating a Facebook App. Enter the app ID and secret key for client ID and client Secret respectively to complete the integration. ■ Twitter—Allows guest users to use their Twitter credentials to log in to the splash page. To enable Twitter integration, you must create a Twitter app and obtain the app ID and secret key. For more information, see Creating a Twitter App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. ■ Google—Allows guest users to use their Google credentials to log in to the splash page. To enable Google integration, you must create a Google app and obtain the app ID and secret key. For more information, see Creating a Twitter App. <ol style="list-style-type: none"> 1. Enter the app ID and secret key for client ID and client secret respectively. 2. To restrict authentication attempts to only the members of a Google hosted domain, enter the domain name in the Gmail for Work Domain text box. Ensure that you have a valid domain account licensed by Google Domains or Google Apps. For more information see: <ul style="list-style-type: none"> ■ https://apps.google.com/intx/en_in/ ■ https://domains.google.com/about/ 3. Specify a text for the Sign-In button. <ul style="list-style-type: none"> ■ LinkedIn—Allows guest user to use their LinkedIn credentials to log in to the splash page. To enable LinkedIn integration, you must create a LinkedIn app and obtain the app ID and secret key. For more information, see Creating a LinkedIn App. Enter the app ID and secret key for client ID and client secret respectively to complete the integration. |
| Facebook Wi-Fi | <p>If you want to enable network access through the free Wi-Fi service offered by Facebook. Select the Facebook Wi-Fi option. The Facebook Wi-Fi feature allows you to pair your network with a Facebook business page, thereby allowing the guest users to log in from Wi-Fi hotspots using their Facebook credentials.</p> <p>If the Facebook Wi-Fi business page is set up, when the users try to access the Internet, the browser redirects the user to the Facebook page. The user can log in with their Facebook account credentials and can either check in to access free Internet or skip checking in and then continue.</p> |
| Facebook Wifi Configuration | <p>After selecting the Facebook Wi-Fi option, complete the following steps to continue with the Facebook Wi-Fi configuration.</p> <ol style="list-style-type: none"> 1. Click the Configure Now link. 2. Sign in to your Facebook account. 3. If you do not have a business page, click Create Page. For more information on setting Facebook Wi-Fi service, see Setting up Facebook Wi-Fi for Your Business at https://www.facebook.com/help/126760650808045. |

Table 160: *Splash Page Configuration*

| Data Pane Content | Description |
|--|--|
| | <p>NOTE: Instant AP devices support Facebook Wi-Fi services on their own, without Aruba Central. However, for enabling social login based authentication, the guest splash pages must be configured in Aruba Central. For more information on Facebook Wi-Fi configuration on an Instant AP, see the <i>Aruba Instant User Guide</i>.</p> |
| Allow Internet In Failure | To allow users access the Internet when the external captive portal server is not available, click the Allow Internet In Failure toggle switch. By default, this option is disabled. |
| Override Common Name | <p>To override the default common name, click the Override Common Name toggle switch and specify a common name. The common name is the web page URL of the guest access portal. By default, the common name is set to securelogin.arubanetworks.com. The guest users can override this default name by adding their own common name.</p> <p>If your devices are managed by AirWave and you want to use your own certificate for the captive portal service, ensure that the captive portal certificate is pushed to the Instant AP from the AirWave management system. When the appropriate certificate is loaded on the AP, perform the following actions:</p> <ol style="list-style-type: none"> 1. Run the show captive-portal-domains command at the Instant AP command prompt. 2. Note the common name or the internal captive portal domain name. 3. Add this domain name in the Override Common Name field on the Splash Page configuration page. 4. Save the changes. |
| Guest Key | To set password for anonymous users, enable the Guest Key and enter a password. |
| Sponsored Guest | Enable the Sponsored Guest option to provide authorization control to a guest sponsor for allowing and denying a guest from accessing the network. |
| Allowed Sponsor Domains | Enter accepted company domain names. The domain name must match the suffix of the sponsor's email address. The domain names must be company names and not any public domain names such as gmail, yahoo, and so on. To add more domain names, click the add icon and enter the domain name. This is a mandatory field. |
| Allowed Sponsor Emails | Enter the allowed email addresses. If you leave this field empty, all emails that correspond to the allowed domains list are permitted to sponsor guests. To add more sponsor emails, click the add icon and enter the sponsor's email address. This is an optional field. |
| Authentication Success Behavior | <p>If Anonymous or Authenticated option is selected as the guest user authentication method, specify a method for redirecting the users after a successful authentication. Select one of the following options:</p> <ul style="list-style-type: none"> ■ Redirect to Original URL— When selected, upon successful authentication, the user is redirected to the URL that was originally requested. ■ Redirect URL— Specify a redirect URL if you want to override the original request of users and redirect them to another URL. |
| Authentication Failure Message | If the Authenticated option is selected as the guest user authentication method, enter the authentication failure message text string returned by the server when the user authentication fails. |
| Session Timeout | <p>Enter the maximum time in Day(s): Hour(s): Minute(s) format for which a client session remains active. The default value is 0:8:00. When the session expires, the users must re-authenticate.</p> <p>If MAC caching is enabled, the users are allowed or denied access based on the MAC address of the connective device.</p> |

Table 160: *Splash Page Configuration*

| Data Pane Content | Description |
|---------------------------|--|
| Share This Profile | Select this check box if you want to allow the users to share the Splash Page profile. The Splash Page profiles under All Devices can be shared across all the groups. |
| Daily Usage Limit | <p>Use this option to set a data usage limit for authenticated guest users, anonymous profiles, and Facebook Wi-Fi logins. By default, no daily usage limit is applied.</p> <p>To set a daily usage limit, use one of the following options:</p> <ul style="list-style-type: none"> ■ By Time— Specify the time limit in hours and minutes for data usage during a day. When a user exceeds the configured time limit, the device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified timezone. ■ By Data— Specify a limit for data usage in MB. You can set this limit to either Per User, Per Session, or Per Device. When the data usage exceeds the configured limit, the user device is disconnected from the network until the next day begins; that is, until 00.00 hours in the specified time zone. <ul style="list-style-type: none"> ● Per User— This option applies the data usage limit based on authenticated user credentials. ● Per Session—This option applies the data usage limit based on user sessions. ● Per Device—This option applies the data usage limit based on the MAC address of the client device connected to the network. <p>Important Points to Note</p> <ul style="list-style-type: none"> ■ The values configured for this feature do not serve as hard limits. There might be a slight delay in enforcing daily usage limits due to the time required for processing information. ■ For anonymous and Facebook Wi-Fi logins, the daily usage limit is applied per MAC address of the client device connected to the network. |
| Whitelist URL | To allow a URL, click + and add the URL to the whitelist. For example, if the terms and conditions configured for the guest portal include URLs, you can add these URLs to the whitelist, so that the users can access the required web pages. |

Customizing a Splash Page Design

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the + icon.
The **New Splash Page** pane is displayed.

To customize a splash page design, on the **Guest Access > Splash Page > New Splash Page > Customization** pane, configure the parameters described in the following table:

Table 161: *Splash page customization*

| Data Pane Content | Description |
|--------------------------|--|
| Background color | To change the color of the splash page, select a color from the Background Color palette. |
| Button color | To change the color of the sign in button, select a color from the Button Color palette. |
| Header fill color | Select the fill color for the splash page header from the Header fill color palette. |

| Data Pane Content | Description |
|-------------------------------|---|
| Page font color | To change the font color of the text on the splash page, select a color from the Page font color palette. |
| Page font Color | Select the font color of the splash page from the palette. |
| Logo | To upload a logo, click Browse , and browse the image file. Ensure that the image file size does not exceed 256 KB. |
| Background Image | Click Browse to upload a background image. Ensure that the background image file size does not exceed 512 KB. |
| Page Title | Add a suitable title for the splash page. |
| Welcome Text | Enter the welcome text to be displayed on the splash page. Ensure that the welcome text does not exceed 20,000 characters. |
| Terms & Conditions | <p>Enter the terms and conditions to be displayed on the splash page. Ensure that the terms and conditions text does not exceed 20000 characters.</p> <p>The text box also allows you to use HTML tags for formatting text. For example, to highlight text with italics, you can wrap the text with the <code><i> </i></code> HTML tag.</p> <p>Specify an acceptance criteria for terms and condition by selecting any of the following options from the Display "I Accept" Checkbox:</p> <ul style="list-style-type: none"> ■ No, Accept by default ■ Yes, Display Checkbox <p>If the I ACCEPT check box must be displayed on the Splash page, select the display format for terms and conditions.</p> <p>Ensure that Display Option For Terms & Conditions has the Inline Text option auto-selected and displayed as an uneditable text.</p> |
| Ad Settings | <p>If you want to display advertisements on the splash page, enter the URL in the Advertisement URL.</p> <p>For Advertisement Image, click Browse and upload the image.</p> |

Localizing a Guest Portal

1. From the **Network Operations** app, filter a group.
2. Under **Manage**, click **Guests** to display the **Splash Page**.
You can create splash page profiles only for the individual groups.
3. To create a new splash page, click the + icon.
The **New Splash Page** pane is displayed.

To localize or translate the Guest portal content, on the **Guest Access > Splash Page > New Splash Page > Localization** pane, configure the parameters described in the following table:



These are optional settings unless specified as a required parameter explicitly.

Table 162: *Guest Portal Localization*

| Data Pane Content | Description | Allowed Length of Text |
|---|---|------------------------|
| Login Section | | |
| Login button title | Enter the custom label text to be localized for the Login button. | 1-255 characters |
| Network login title | Enter the custom title text that you want to localize for the Network Login page. | 1-255 characters |
| Login page title | Enter the custom text for title in the Login page. | 1-255 characters |
| Access denied page title | Enter the custom title text for the Access Denied page. | 1-255 characters |
| Logged in title | Enter the custom Logged in title text for the page that allows access. | 1-255 characters |
| Username label | Enter the custom text for Username lable. | 1-255 characters |
| Username placeholder | Enter the custom text to show in in the Username placeholder. | 1-255 characters |
| Password placeholder | Enter the custom text to show in in the Password placeholder. | 1-255 characters |
| Email address placeholder | Enter the custom text to show in in the Email Address placeholder. | 1-255 characters |
| Register button title | Enter the custom title text for Register button. | 1-255 characters |
| Network login button title | Enter the custom title text for Network Login button. | 1-255 characters |
| Terms and Conditions title | Enter the custom text to show in the Terms and Conditions title. | 1-255 characters |
| 'I accept the Terms and Conditions' text | Enter the custom text to show for the 'I accept the Terms and Conditions' text adjacent to the check box. | Up to 20000 characters |
| Welcome Text | Enter a custom Welcome text to the guest portal user. | Up to 20000 characters |
| Login failed message | Enter a custom text to show for the Login Failed message when a user's login attempt gets denied or fails. | Up to 20000 characters |
| Logged in message | Enter a custom text to show for the Logged in message in the access allowed page. | Up to 20000 characters |
| Register Section | | |

Table 162: *Guest Portal Localization*

| Data Pane Content | Description | Allowed Length of Text |
|--|---|------------------------|
| Phone help message | Enter a custom help message to show for the Phone help field. | Up to 20000 characters |
| Phone number placeholder | Enter the custom placeholder text for the Phone Number input UI control. | 1-255 characters |
| 'Back' button text | Enter the custom text label to show for the Back button control. | 1-255 characters |
| 'Continue' button text | Enter the custom text label to show for the Continue button control. | 1-255 characters |
| Email radio button | Enter a custom text label for the Email option. | — |
| Phone radio button | Enter a custom label text for the Phone option. | — |
| Register page title | Enter a custom title text for the Register page. | 1-255 characters |
| Accept button title | Enter a custom title text for the Accept button. | 1-255 characters |
| Register Page instructions | Enter a custom message to show in the Register page. | Up to 20000 characters |
| Verification Section | | |
| Verification code label | Enter a custom text to show for the Verification code label. | 1-255 characters |
| Verification code placeholder | Enter a custom text to show for the Verification code placeholder. | 1-255 characters |
| Verification email check message | Enter a custom text for the Verification Email Check message. This is shown in the verification pending page. | Up to 20000 characters |
| Verification email notice message | Enter a custom text for the Verification Email Notice message. This is the message notifying the user when the email will be sent. | Up to 20000 characters |
| Verification email sent message | Enter a custom text for the Verification Email Sent message. | Up to 20000 characters |
| Verification phone notice message | Enter a custom text for the Verification Phone Notice message. This is the message notifying the user that an SMS has been sent. | Up to 20000 characters |
| Verified account message | Enter a custom text for the Verified Account message. This is the message that will be shown in the Verified page. | Up to 20000 characters |
| Verify account message | Enter a custom text for the Verify Account message. This is the message that will be shown in the Verify page. | Up to 20000 characters |

Table 162: *Guest Portal Localization*

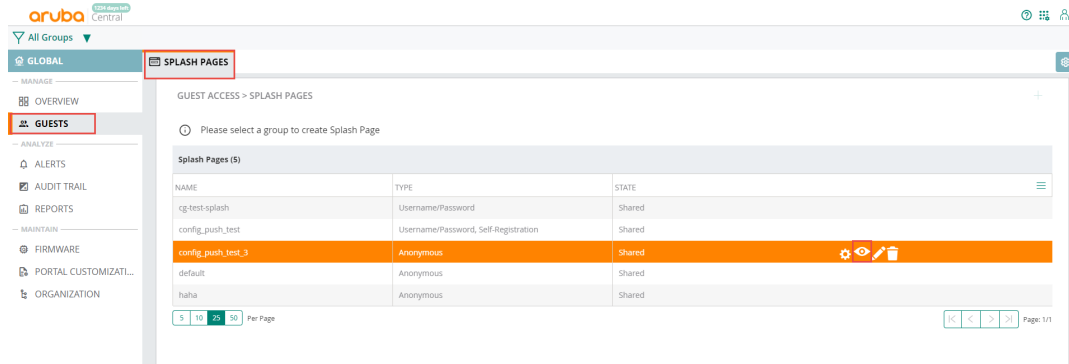
| Data Pane Content | Description | Allowed Length of Text |
|------------------------------|---|------------------------|
| Verify button title | Enter a custom label text for the Verify button. | 1–255 characters |
| Verify title | Enter a custom text for Verify title. | 1–255 characters |
| Network login message | Enter a custom text message to show in the Network Login page. | Up to 20000 characters |

- Click **Preview** to preview the localized guest portal page or click **Finish**.

Previewing and Modifying a Splash Page Profile

To preview a splash page profile, complete the following steps:

- From the **Network Operations** app, filter a group.
- Under **Manage**, click **Guests** to display the **Splash Page**.
A list of splash page profiles is displayed.
- Ensure that the pop-up blocker on your browser window is disabled.
- Hover over the splash profile you want to preview and click the preview icon. The Splash Page is displayed in a new window.




The **Splash Pages** page also allows you to perform any of the following actions:

- To view the Splash Page configuration text in an overlay window, click the settings icon next to the profile. You can copy the configuration text and apply it to AirWave managed APs using configuration templates.
- To modify a splash page profile, click the edit icon ext to the profile form list of profiles displayed in the Splash Page Profiles pane.
- To delete a profile, select the profile and click the delete icon next to the profile.

Associating a Splash Page Profile to an SSID

To associate a splash page profile with an SSID, complete the following steps:

- From the **Network Operations** app, filter a group.
- Under **Manage**, click **Device > Access Points**.
- Click the configuration icon  to open the configuration window.

4. Under **WLANs**, click **+Add SSID**.
5. The **Create a New Network** pane is displayed.
6. Refer to the AP configuration page for Aruba Central Online Help for more detailed information on how to create the network .

Configuring Visitor Accounts

The **Visitors** pane displays information on the session and account details of the visitors who access the splash page. It helps you monitor the guest sessions.

The MSP does not support creating or modifying guest visitor accounts. To configure visitors for WLAN networks and view visitor connection details, the administrators must drill down to the customer account and access it.

Adding a visitor

To add a new visitor:

1. From the MSP view, drill down to a customer account.
2. In the **Network Operations** app, navigate to **Manage > Guests > Visitors**.

The **Guest Access > Visitors** page is displayed.

3. Click on the **Account** tab, and then click **Add Visitor**.

The **Add Visitor** pane is displayed.

4. Configure the parameters described in the following table:

Table 163: *Adding Visitors*

| Data Pane Content | Description |
|-------------------|--|
| Name | Enter a unique name to identify the visitor. |
| Company | Enter the company name of the visitor. |
| Email | Enter the email ID of the visitor. |
| Phone | Enter the phone number of the visitor. |
| Password | <ul style="list-style-type: none"> ■ Click Generate. The automatically generated password is displayed in the PASSWORD text box. ■ Select Send Access Code to send the access code by email or SMS. |
| Valid Till | Specify the duration for the visitor account to expire in Day(S): Hour(s): Minute(s) format. To allow users to access the network for unlimited period of time, select Unlimited . |
| Enable | Select this check box to activate the user account. |

5. Click **Save**.
6. Click **Save and Print** to print the details of the visitor.

To view the guest or visitor sessions:

1. From the MSP view, drill down to a customer account.
2. In the **Network Operations** app, navigate to **Manage > Guests > Visitors**.

The **Guest Access > Visitors** page is displayed.

3. From the **Show visitors for network** drop-down list, select a network.

The following table displays the session details of the visitor:

Table 164: *Visitor Sessions Pane*

| Parameter | Description |
|----------------------------|---|
| Visitors | Displays the name of the visitor. |
| Login Type | Displays the login type of the client (Anonymous, Username/Password, Self-Registration, Facebook Wi-Fi). |
| Browser | Displays the type of browser that the client is connected. |
| MAC Address | Displays the MAC address of the connected client device. |
| Device Type | Displays the type of the device. |
| OS Name | Displays the OS on the client device. |
| Login Time | Displays the login time of the client. |
| Session Time (Secs) | Displays the duration for which the client is connected. |

The following table displays the account details of a visitor:

Table 165: *Visitor Accounts Pane*

| Parameter | Description |
|-------------------|---|
| Name | Displays the name of the visitor. |
| Email | Displays the email ID of the visitor. |
| Phone | Displays the contact number of the visitor. |
| Company | Displays the company name of the visitor. |
| Status | Indicates if the user account is in active or inactive state. |
| Creation | Displays the date and time on which the visitor account is created. |
| Expiration | Displays the date and time on which the visitor account expired. |
| Actions | Allows you to edit a specific visitor account. |



You can filter the visitors displayed in the **Account List** by visitor status. Select **Active**, **Inactive**, or **Show All** from the drop-down list.

Deleting Visitors

To delete one or more visitors:

1. Select the visitor or visitors you want to delete using the **Multiselect** box option.
2. Click **Delete**. The selected visitors get deleted.

Downloading Visitor Account Details

To download the visitor account details:

1. Click **Download** to download the visitor account details available in the **Accounts** tab.

The Presence Analytics service available on Aruba Central enables businesses to collect and analyze user presence data in public venues, enterprise environments, and retail hubs. The Presence Analytics service enables businesses to collect real-time data on user footprints within the wireless network range of Aruba Instant APs that are managed using Aruba Central. Using the Presence Analytics statistics, businesses can analyze user behavior and improve customer engagement, and thus maximize revenue opportunities, optimize workspace, and increase market presence.



Aruba Central supports Presence Analytics only on the APs running Aruba Instant 6.4.4.4-4.2.3.0 or a later version.

Enabling Presence Analytics Service

Presence Analytics is available only if the Presence Analytics service is enabled on an Instant AP. To start using the Presence Analytics service, contact the Aruba Central Sales team and obtain a subscription.

If you have a valid subscription, enable the **Presence Analytics** service on your APs using the following steps:

1. In the **Account Home** page, under **Global Settings**, select **Subscription Assignment**.
2. Select the device from the devices table.
3. From the list of subscriptions, select the devices that requires the Presence Analytics service subscription.
4. Drag and drop the device to the Presence Analytics service in the subscriptions table.
5. Click **Yes** to confirm the subscription assignment.



If the Presence Analytics service subscription is enabled on one Instant AP in the cluster, the other Instant APs in the cluster inherit the Presence Analytics configuration settings, and send the RSSI feeds to Aruba Central. However, the Presence and Loyalty statistics are displayed only for the Instant APs on which the Presence Analytics feature is enabled.

Using Presence Analytics

In the **Network Operations** app, filter a group. Navigate to **Manage > Guests > Presence Analytics**.

Presence Analytics displays data either for all sites or per site. A site in Aruba Central represents a physical location such as a venue or store. If your account does not have any sites configured, ensure that you create a site. For more information on creating sites and adding devices, see [Managing Sites on page 84](#).

The Presence Analytics page is available The **Presence Analytics** page displays the following menu options:

- **Activity**—A dashboard that shows the client presence details, loyalty metrics, and connected client metrics.
- **Configuration**—The configuration page in which the RSSI threshold and dwell time for the clients can be set

Activity Dashboard

The Activity dashboard displays the following details:

- Presence metrics for passerby clients and visitors
- Loyalty metrics for visitors

- Connected-client device metrics on Guest and Employee networks

Presence Details

Based on the proximity of the client device to a specific site, the Wi-Fi signal strength, and the time spent at the sites, the clients are classified as follows:

- **Passersby**—An associated or unassociated client who is in the vicinity of a specific site and has an RSSI value greater than -90 dBm. You can customize the RSSI value for Passerby on the **Presence Analytics > Configuration** page.
- **Visitors**—The passerby clients who spend more than 5 minutes at the site and have an RSSI value greater than -65 dBm. You can customize dwell time and RSSI values on the **Presence Analytics > Configuration** page.



If a client is idle for more than 30 minutes, Aruba Central removes the presence instance for that client. When the client reappears, Aruba Central creates a new instance for that client and applies the same presence classification criteria.

The **Presence** graphs on the dashboard provide statistical analysis of the aggregate count of passerby clients, the dwell time of these clients at the sites, the rate at which the passerby clients converted to visitors, and the aggregate count of visitors over a specific duration.

Loyalty Metrics

Based on the engagement pattern and the time spent by the clients at the site, Aruba Central classifies clients as visitors. It also maintains a record of the number of repeat visits made by these clients over a specific duration. Based on these records, it plots the frequency at which the visitors return to the sites, and classifies these repeat visitors as loyal visitors.

The **Loyalty** graphs on the dashboard provide a statistical analysis of the clients classified as unique, new, and loyal visitors for a given time range.

Wi-Fi Connected Devices

The dashboard includes the Wi-Fi Connected Clients as listed below:

- **Connected Devices**—A Wi-Fi client associated to a Guest or Employee network on the device.
- **Guest Devices**—A Wi-Fi client associated to the Guest networks on the device.
- **Employee Devices**—A Wi-Fi client associated to the Employee or Voice network on the device.

The Wi-Fi Connected Clients graphs on the dashboard provide statistical analysis of the aggregate count of associated clients over a specific duration.

Viewing Dashboard Contents

By default, the **Activity** page displays data for all sites for a time range of 3 hours.

See [Table 166](#) for general guidelines on filtering content and analyzing data:

Table 166: *Presence Analytics Data Metrics and Filters*

| Dashboard View | Description |
|---|---|
| Time range filter | <p>You can view the clients' presence data for the following time ranges:</p> <ul style="list-style-type: none">■ 3 Hours— Data for the last 3 hours, with the current time taken as the basis for calculation.■ 1 Day—Data for the last 24 hours, with the current time taken as the basis for calculation.■ 1 Week— Data for the last 1 week, with 00:00 hour of the current week taken as the basis for calculation.■ 1 Month— Data for the last one month, with 00:00 hour of the current month taken as basis for calculation. <p>The granularity of data points for activity trends is as follows:</p> <ul style="list-style-type: none">■ 5 minutes for a time range of 3 hours■ 1 hour for a time range of 1 day■ 1 day for a time range of 1 week and 1 month |
| Baseline and Change Metrics | <p>The Baseline and Change metrics are shown for most of the graphs displayed on the Activity page.</p> <p>The baseline metric for presence data is calculated for each time range in the following way:</p> <ul style="list-style-type: none">■ 3 Hours—The baseline metric is not applicable.■ 1 Day—The baseline value is derived from the average of the presence data collected in the last 30 days.■ 1 Week and 1 Month—The baseline value is derived from the presence data collected in the last 6 months. |
| Baseline Versus Aggregate trends | <p>Displays the aggregate or average values across the selected time range in comparison to the baseline value.</p> |

The **Activity** page allows you to set your dashboard view so as to show a quick summary or detailed information. To view more details about presence, Wi-Fi-connected clients, or loyalty metrics, enable the **Advanced** mode. See [Table 167](#) for information on default and advanced views of the **Activity** dashboard.

Table 167: Activity Dashboard

| Dashboard Content | Description | Default View | Advanced View |
|---|--|--------------|---------------|
| Presence | | | |
| Presence | <p>The Presence graphs display presence metrics for passerby clients and visitors. The following graphs with presence metrics are displayed for all sites or a specific site.</p> <ul style="list-style-type: none"> ■ Passersby—Shows the aggregate count of passerby clients for the selected time range. The graph also shows the following details: <ul style="list-style-type: none"> ● Baseline value for the passerby clients based on the selected time range ● Percentage of change in the count of passerby clients in comparison to the baseline value ■ Visitors—Shows the aggregate count of visitors. The graph also shows the following data: <ul style="list-style-type: none"> ● Baseline value for the visitors trend based on the selected time range ● Percentage of change in the count of visitors in comparison to the baseline value ■ Draw Rate—Refers to the percentage of passerby clients that is converted to visitors for a specific time duration. The Draw Rate graph shows average draw rate. It also shows the following data: <ul style="list-style-type: none"> ● Baseline value for the draw rate metric based on the time range selection ● Percentage of change in draw rate compared to the baseline value ■ Dwell Time—Refers to the average time spent by visitors at a site at a given point in time. This graph shows the average dwell time of the visitors for all sites or a specific site. It also shows the following data: <ul style="list-style-type: none"> ● Baseline value for the dwell time metric based on the time range selection ● Percentage of change in the dwell time compared to the baseline value <p>To view detailed presence information along with baseline change percentage graph, switch to the Advanced mode.</p> | Yes | Yes |
| Passersby & Draw Rate Graphs | <ul style="list-style-type: none"> ■ The Passersby chart plots the passerby clients' trend for the selected time range. For example, if the time range is set to 3 hours, it shows the passerby clients' count for every 5 minutes for the last 3 hours. Similarly, when the time range is set to 1 day, the count is displayed for every one hour. ■ The Draw Rate shows the rate of conversion of passerby clients to visitors for the selected time range. For example, if the time range is set to 3 hours, it shows the conversion count for every 5 minutes for the last 3 hours. Similarly, when the time range is set to 1 day, the count is displayed for every one hour. <ul style="list-style-type: none"> ● 5th Percentile—The 5th percentile is the value of draw rate below which 5% of the sites could be found. The graph plots the draw rate trend at 5th percentile. ● 95th Percentile—The 95th percentile is the value of draw rate below which 95% of the sites may be found. The graph plots draw rate trend at the 95th percentile. | No | Yes |
| Top & Bottom 5 | <p>Displays the top 5 and bottom 5 sites and plots trends for these sites for categories such as the following categories:</p> <ul style="list-style-type: none"> ■ Passersby ■ Visitors ■ Draw Rate | No | Yes |

Table 167: Activity Dashboard

| Dashboard Content | Description | Default View | Advanced View |
|---|---|--------------|---------------|
| | <ul style="list-style-type: none"> ■ Dwell Time <p>The graph also shows the median that is derived based on the values. This information is gathered based on the trends observed for a selected metric across all sites for the selected time period.</p> <p>NOTE: If the number of sites is less than 10, the graph does not show the bottom 5 trends.</p> | | |
| View Presence Data | <p>Displays the presence data for all sites. The All Sites table shows the passerby clients' count, visitors' count, draw rate, and dwell time metrics.</p> <p>Click the Download All Sites Data icon to download the presence data for all sites for a given time range.</p> | Yes | Yes |
| Loyalty | | | |
| Loyalty | <p>The Loyalty area displays the following graphs with loyalty metrics for visitors:</p> <ul style="list-style-type: none"> ■ Unique Visitors—Shows the unique visitors' count, which is the sum of new and loyal visitors for the selected time range. Rephrase this sentence to make this as list items-- The graph also shows the following data: <ul style="list-style-type: none"> ● Baseline metric calculated for a given time range ● Percentage of change in the unique visitors' count in relation to the baseline metric. ■ New Visitors—Shows the aggregate count of the new visitors. Visitors who have visited only once in the last 1 month are referred to as the new visitors. The graph also shows the following data: <ul style="list-style-type: none"> ● Baseline metric calculated for a given time range ● Percentage of change in the new visitors' count in relation to the baseline metric ■ Loyal Visitors—Shows the aggregate count of the visitors categorized as loyal. Visitors who have visited a site more than once in the last 1 month are referred to as loyal visitors. The graph also shows the following information: <ul style="list-style-type: none"> ● Baseline metric calculated for a given time range ● Percentage of change in the loyal visitors' count in relation to the baseline metric <p>To view the detailed loyalty information along with the baseline change percentage graph, switch to the Advanced mode.</p> | Yes | Yes |
| Visitor Loyalty Composition | Shows the number of visitors categorized as new and loyal visitors for a specific time range. | No | Yes |
| Loyal Visitors - Visits in the last 3 months | Shows the number of visits the loyal visitors made to a site in the last three months. | No | Yes |
| Top & Bottom 5 | <p>Shows the top 5 sites and bottom 5 sites for:</p> <ul style="list-style-type: none"> ■ New visitors ■ Unique visitors ■ Loyal visitors <p>The graph also shows the following:</p> <ul style="list-style-type: none"> ■ Trends for the top and bottom sites for the selected category. | No | Yes |

Table 167: Activity Dashboard


| Dashboard Content | Description | Default View | Advanced View |
|---|--|--------------|---------------|
| | <ul style="list-style-type: none"> Median derived based on the values gathered from the trends observed for a selected metric across all sites for the selected time period. <p>NOTE: If the number of sites is less than 10, the graph does not show the bottom 5 trends.</p> | | |
| View Loyalty Data | Displays the loyalty metrics for all sites. The All Sites table shows unique visitors, new visitors, and loyal visitors. Click the Download All Sites Data icon to download the loyalty metrics for all sites for a given time range. | Yes | Yes |
| Wi-Fi Connected Devices | | | |
| Wi-Fi Connected Devices | <p>Displays the following graphs for Wi-Fi connected devices:</p> <ul style="list-style-type: none"> Connected Devices—Displays the aggregate count of associated clients for the selected time range. The graph also shows the baseline value for the associated clients based on the selected time range, and the percentage of change in the count of the associated clients in comparison to the baseline value. Guest Devices—Displays the aggregate count of associated clients on Guest Networks for the selected time range. The graph also shows the baseline value for the associated clients on Guest Networks based on the selected time range, and the percentage of change in the count of the associated clients on Guest Networks in comparison to the baseline value. Employee Devices—Displays the average count of associated clients on Employee Networks for the selected time range. The graph also shows the baseline value for the associated clients on Employee Networks based on the selected time range, and the percentage of change in the count of the associated clients on Employee Networks in comparison to the baseline value. <p>To view detailed Wi-Fi connected device information along with baseline change percentage graph, switch to the Advanced mode.</p> | Yes | Yes |
| Connected Devices Vs Visitors | Displays the total count of client devices categorized as Employee, Guest and Visitor devices. This includes both associated and unassociated client devices. | No | Yes |
| Top and Bottom 5 Connected Devices | <p>Displays the top 5 and bottom 5 sites and plots trends for these sites for the following categories:</p> <ul style="list-style-type: none"> Connected Devices Guest Devices Employee Devices <p>The graph also shows the following:</p> <ul style="list-style-type: none"> Trends for the top and bottom sites for the selected category. Median derived based on the values gathered from the trends observed for a selected metric across all sites for the selected time period. <p>NOTE: If number of sites is 10 or lower than 10, the graph does not show the bottom 5 trends.</p> | No | Yes |
| View Wi-Fi Connected Devices Data | Displays Wi-Fi connected devices data for all sites. The All Sites table shows the metrics for Connected devices, Guest devices, and Employee devices for all the sites. Click the Download All Sites Data icon to download the connected clients data for all sites for a given time range. | Yes | Yes |

Setting RSSI Threshold and Dwell Time

The RSSI and dwell time configuration allows the administrators to perform the following actions:

- Classify the type of client.
- Analyze presence patterns.
- Determine if the usage has increased over a period of time.

To modify the default RSSI and dwell time configuration parameters, complete the following steps:

1. In the **Network Operations** app, filter a group or a device.
2. Under **Manage**, click **Guests > Presence Analytics**.
3. Click the  configuration icon.
4. Under **Passersby**, specify the value for **RSSI threshold**. By default, the RSSI threshold value is set to -65 dBm. You can specify a value within the range of -100 to 0.
5. Under **Passersby to Visitor**, specify the values for **RSSI threshold** and **Dwell Time** parameters. By default, the RSSI threshold is set to -60 dBm and the dwell time is set to 5 minutes.
6. Click **Save Settings**.

The growing use of Wi-Fi and the proliferation of mobile tablet and smartphone clients cause control and visibility challenges for communication and collaboration applications. To overcome these challenges, Aruba offers the Unified Communications application to manage your enterprise communication ecosystem.

The Unified Communications application on Aruba devices provides a seamless user experience for voice calls, video calls, and application sharing when using communication and collaboration tools. The Unified Communications application actively monitors voice, video, and application sharing sessions, provides traffic visibility, and allows you to prioritize the required sessions. The Unified Communications application also leverages the functions of the service engine on the cloud platform and provides rich visual metrics for analytical purposes.

The Unified Communications application supports the following functions based on the type of device used in the solution:

- **Session visibility**—The unified communications application provides call session visibility correlated across the network to simplify operations for the network administrator. The administrators can monitor wireless and wired network connectivity health on a per-session basis and analyze the quality of experience.
- **Session prioritization**—Based on the type of device provisioned in your network, the Aruba Central server receives call control information from devices like Instant AP, controllers, and switches. The Unified Communications application uses this data to detect and classify the traffic type and dynamically prioritize the voice and video traffic over data traffic. The heuristics method is used for session prioritization. A built-in heuristics engine detects the unified communications traffic and prioritizes the require traffic. The heuristics data detection and classification method is used to identify clients in the call, classify, and prioritize media packets. Switches do not support heuristics-based prioritization.

Heuristics Classification

In the heuristics method, Aruba devices like Instant AP perform deep packet inspection on the traffic to determine voice and video traffic. For the heuristics classification method, no changes or additional components are required on the unified communications servers.

The heuristics classification method includes the following steps:

- When the voice or video call is established, classify-media in the ACL is triggered and clients are marked as media-capable clients.
- Any subsequent UDP data flow with source/destination port numbers above 1023 from or to media-capable users go through the DPI engine.
- If an RTP session is based on DPI, the payload type in the RTP header is used to determine if it is a voice or video session.

Enabling Unified Communications

To access the Unified Communications application, obtain a valid subscription. To obtain a subscription for the **Unified Communications** application, contact the Aruba Central Sales team.


If you have a valid subscription, follows these steps to enable the **Unified Communications** service on your devices:

1. In the **Accounts Home** page, click **Global Settings > Subscription Assignment**.

2. From the list of subscriptions, select **UCC**.
3. Select the device from the **Devices** table.
4. Drag and drop the device from the **Devices** table to the **Subscriptions** table.
5. Click **Yes** to confirm the subscription assignment.

Enabling Call Prioritization

To enable call prioritization:

1. In the **Network Operations** app, use the filter to select a group or device.
2. Under **Manage**, click **Applications > UCC**.
3. Click the  icon.
4. Move the **Enable Call Prioritization** slider to the right.

Editing Protocol

To edit a protocol:



1. In the **Network Operations** app, use the filter to select a group or device.
2. Under **Manage**, click **Applications > UCC**.
3. Click the  icon.
4. Hover over the required protocol and click the  icon under **Action**. Unified Communications supports Facetime, Skype for Business, and Wi-Fi Calling protocols.
5. Edit the parameters listed in [Protocol Parameters](#).

Table 168: *Protocol Parameters*

| Parameter | Description |
|-----------------|---|
| Voice | Configure voice priority tag. |
| Video | Configure video priority tag. |
| Desktop Sharing | Configure desktop sharing priority tag. |
| DNS Server | Configure DNS server priority tag. |

6. Click **Save**.

Unified Communications Dashboard

The **Application > UCC** page provides a variety of charts and lists that allow you to assess the quality of calls in the network. The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.
- **Fair**—Displays the total number of fair calls. that have ended.
- **Poor**—Displays the total number of poor calls that have ended.
- **Unknown**—Displays the total number of calls whose status is unknown.

The **Summary** view in the **Applications > UCC** page provides the following charts:

- **Calls**—Displays the chart of all, good, fair, poor, or unknown calls. Chart can be viewed by Health, SSID, Protocol, Operating System, Session Type, or Quality. In any chart, hover your mouse over any segment of the chart to view additional information.
- **Access Points**—Displays the chart of access points. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.
- **Clients**—Displays the chart of clients. Chart can be viewed by Poor Quality % or Most Calls. Use **Show More** to view more details of the calls.

The **Show More** option in the **Access Points** chart displays the following details of the calls:

Table 169: *Access Points with Calls*

| Parameter | Description |
|-----------------------|---|
| Access Point Name | Displays the name of the AP. |
| Calls Total | Displays the total number of calls. |
| Calls Good | Displays the total number of good calls. |
| Calls Fair | Displays the total number of fair calls. |
| Calls Poor | Displays the total number of poor calls. |
| Calls Poor Percentage | Displays the percentage of poor calls. |
| Calls Unknown | Displays the total number of unknown calls. |

Hover over any row in the list to view additional information.

The **Show More** option in the **Clients** chart displays the following details of the calls:

Table 170: *Clients with Calls*

| Parameter | Description |
|-----------------------|---|
| Client Name | Displays the name of the client. |
| Calls Total | Displays the total number of calls from the client. |
| Calls Good | Displays the total number of good calls from the client. |
| Calls Fair | Displays the total number of fair calls from the client. |
| Calls Poor | Displays the total number of poor calls from the client. |
| Calls Poor Percentage | Displays the percentage of poor calls from the client. |
| Calls Unknown | Displays the total number of unknown calls from the client. |

Hover over any row in the list to view additional information.

The **List** view in the **Applications > UCC** page provides a variety of lists that allow you to assess the quality of calls in the network. The banner in the header pane shows the following details:

- **Calls**—Displays the total number of calls that have ended.
- **Good**—Displays the total number of good calls that have ended.

- Fair—Displays the total number of fair calls that have ended.
- Poor—Displays the total number of poor calls that have ended.
- Unknown—Displays the total number of calls whose status is unknown in the last 5 minutes.

The **Calls** list displays the following details of the calls:

Table 171: *Call Details*

| Parameter | Description |
|------------|--|
| From | Displays the device originating the call. |
| To | Displays the device receiving the call. |
| Start Time | Displays the date and time when the call originated. |
| Duration | Displays the duration of the call. |
| State | Displays the state of the call. Possible values are: <ul style="list-style-type: none"> ■ Active ■ Success ■ Terminated |
| Quality | Displays the quality of the call. Possible values are: <ul style="list-style-type: none"> ■ Good ■ Fair ■ Poor ■ Unknown |
| AP Name | Displays the name of the AP. |
| Client | Displays the name of the client. |



The Call Detail Record (CDR) for FaceTime and Skype for Business calls may be incorrect. The CDR for a Facetime call may be empty or it may display the quality of the call as **unknown**. Duplicate CDRs may be created for a Skype for Business call.

Site installations and device deployments at customer premises require extensive coordination between the IT administrators and installation personnel. If there are multiple sites to deploy, businesses may require more time and manual effort to coordinate and manage site installations. The Aruba Installation Management service simplifies and automates site deployments, and helps IT administrators manage site installations with ease.

The Installation Management service includes the following components:

- **Install Manager on Aruba Central portal**—Intended for IT administrators who oversee the installation management activities in an organization. Using Install Manager, network administrators can create installer profiles, assign site deployments to installers, and monitor deployment status for each site from a remote location. Aruba Central users can access the Install Manager application from the app selection pane in the UI.
- **Aruba Installer mobile app**—Intended for the installation personnel who deploy devices on a site. The Aruba Installer mobile app allows the installers to scan devices and add them to the provisioning network. The Aruba Installer mobile app is available for downloads on Apple® App Store and Google Play Store.

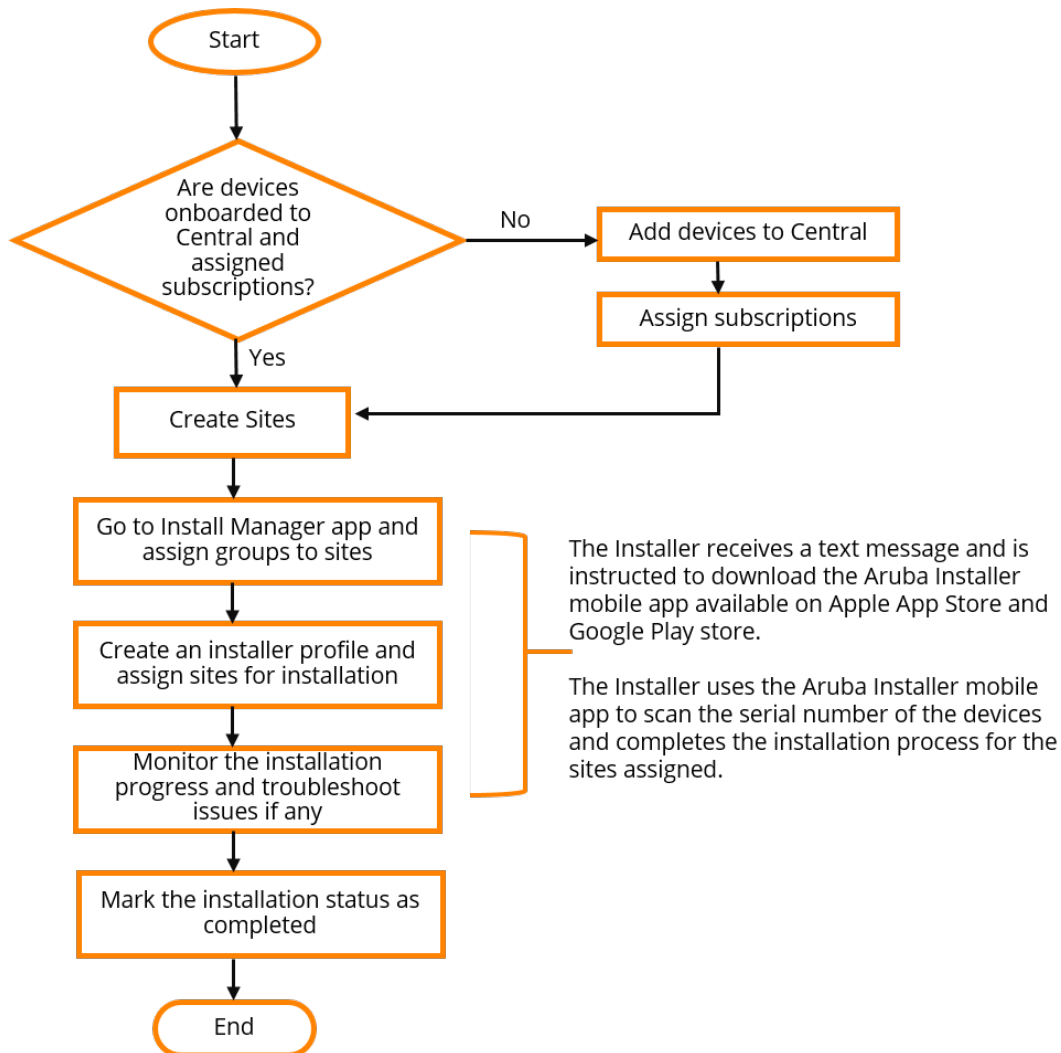
Installation Management and Monitoring

The Install Manager feature in Aruba Central includes the following menu options:

- **Site Installations** —Displays a list of sites associated with an Aruba Central account.
- **Installers**—Displays a list of installers added using the Install Manager application.
- **Audit Trail**—Displays the audit log for the devices deployed at a site.

Installation Management Workflow

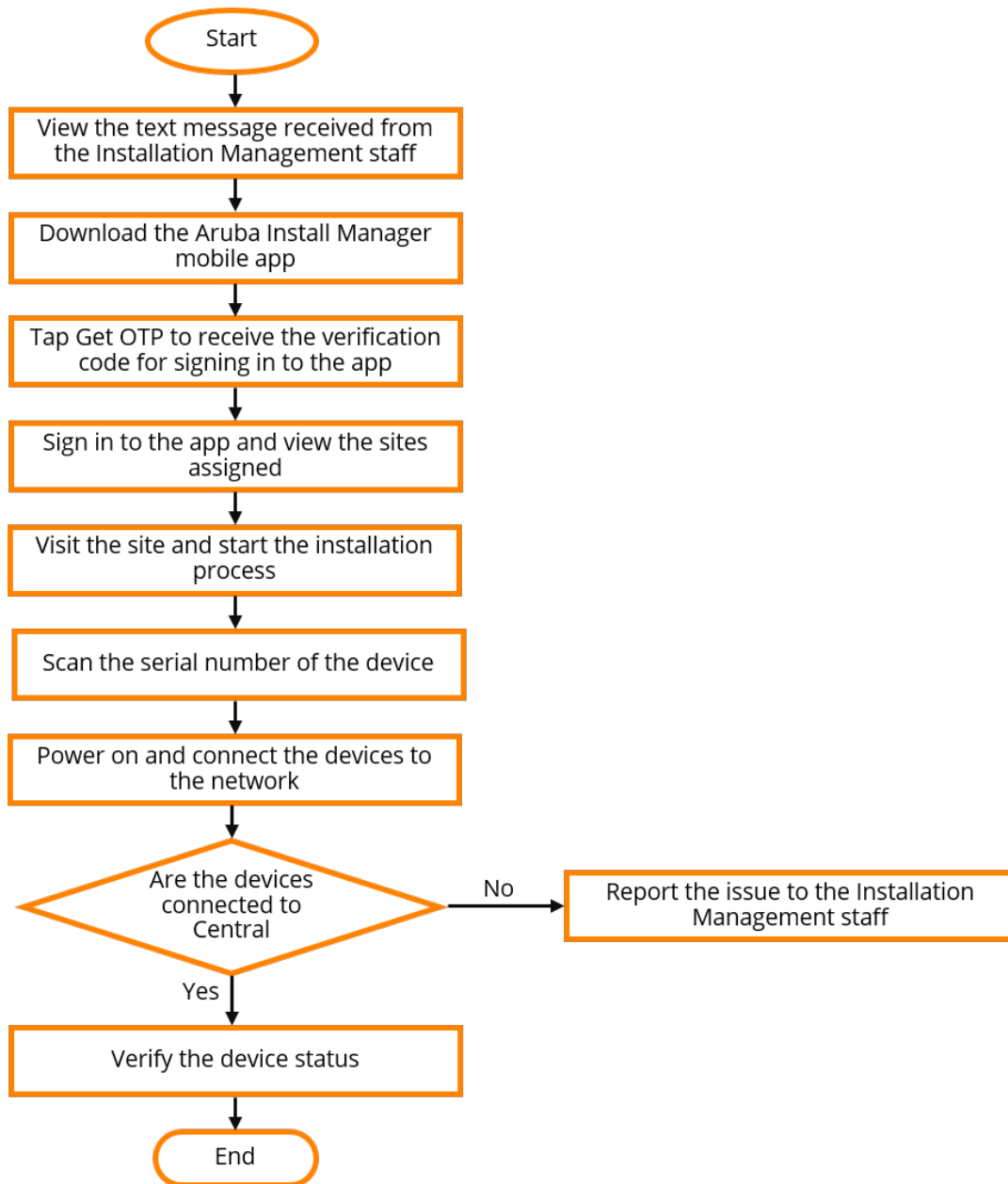
The following figure illustrates the installation management workflow for the Install Manager users:



Installer Workflow

Installers are technicians who are assigned the task of visiting a physical site or location, and install devices. The Aruba Installer mobile app enables installers to scan devices and report the task status to IT administrators.

The following figure illustrates the installation workflow for the Aruba Installer mobile app users:



Managing Site Deployments

Before you begin, ensure that the following tasks are completed:

- [Onboarding Devices on page 72](#)
- [Managing Subscriptions on page 78](#)

The steps required for completing a site installation procedure are listed in the following table:

Table 172: *Installation Management*

| Administrator Workflow | Installer Workflow |
|--|---|
| <ul style="list-style-type: none">■ Creating a Site■ Assigning Groups to a Site■ Adding an Installer and Assigning Sites for Installation■ Monitoring and Troubleshooting Installation Issues | <ul style="list-style-type: none">■ Downloading the Installer Mobile App■ Registering as an Aruba Installer■ Installing Devices on a Site |

Creating a Site

To create a site in Aruba Central, complete the steps described in [Creating a Site on page 84](#).

Assigning Groups to a Site

To assign groups to a site:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Select the **Install Manager** tab.
4. On the **Site Installations** page, click on the site you want to edit.
5. Select the group for each device category.
6. Click **Save**.

To assign groups to multiple sites:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Select the **Install Manager** tab.
4. On the **Site Installations** page, select the sites. The **Assign Groups** button is displayed.
5. Click **Assign Groups**.
6. In the **Assign Groups to Sites** pop-up window, select a group for each device category.
7. Click **Save**.



You can also add installation notes for sites. The installers can view the notes by clicking the info icon in the Installer mobile app.

Adding an Installer and Assigning Sites for Installation

Administrators can add installers and assign installation tasks to these installers through the Aruba Installer mobile app.

To add an installer profile in Aruba Central, complete the following steps:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Select the **Install Manager** tab.
4. In the **Install Manager** tab, click **Installers**. The **Installers** page opens.
5. Click **+ Add Installer**. The **Add Installer** pop-up window opens.

6. Enter the name and phone number of the technician to whom you want to assign a site for installing the devices.
7. Specify the time until which the installer's profile is valid. The technicians will be automatically logged out of the Aruba Installer app on the specified date.
8. From the **Sites to Manage** drop-down, select the sites that you want to assign to the installer.
9. Click **Save**. An SMS notification is sent to the installer's mobile device.

To start the installation, the installer must download the Aruba Installer mobile app and sign up as an installer. The administrators can verify the installer registration status on the **Installers** dashboard in the Install Manager application in Aruba Central. The **Installers** dashboard displays the following status indicators for installers.

- **Invited**—The installer is added and an SMS notification is sent to the installer.
- **Registered**—The installer has registered using the Aruba Installer mobile app.
- **Verified**—The installer has accepted the installation invite and successfully completed the registration with the Aruba Installer app.

Downloading the Installer Mobile App

When an installer is added in the Install Manager application in Aruba Central, an SMS notification is sent to the installer's mobile device. The SMS notification includes the links for downloading the Aruba Installer mobile app.

If you are an installer and have received the SMS notification with the Aruba Installer mobile app details, download the Aruba Installer mobile app. The Aruba Installer mobile app is available in [App Store for iOS devices](#) and [Google Play Store for Android devices](#).

Registering as an Aruba Installer

To register as an installer:

1. Open the Aruba Installer app.
2. In the **Sign Up** tab, enter your first name, last name, country code and mobile number.
3. Click **Register**. A verification code is sent to your mobile device.
4. Enter the verification code received through the text message in the **Code** field.
5. Click **Validate Code**. If the code is valid, the installer is registered.

Installing Devices on a Site

To install a device on a site:

1. Sign in to Aruba Installer mobile app.
2. View the sites assigned for deployment.
3. Select the site that you want to deploy.
4. Note the devices assigned for the site and installation notes if any.
5. Click **Scan Device**. Scan the serial number of the device. The Aruba Installer app verifies if the device is onboarded to Aruba Central device inventory and is assigned a valid subscription.
6. Power on the device and connect it to the Internet. The device automatically connects to Aruba Central and is provisioned in the group to which it is already assigned.
7. Verify the installation status and report errors if any.



Before scanning a device, ensure that the device is not connected to Aruba Central. If the device is already connected to Aruba Central, Install Manager will not assign it to a group.

Monitoring and Troubleshooting Installation Issues

To monitor the installation progress:

1. In the **Network Operations** app, filter **All Devices**.
2. Under **Maintain**, click **Organization**.
3. Select the **Install Manager** tab. The **Site Installations** table is displayed.
4. To view the status of a site installation, check the **Status** column. The **Status** column uses the following indicators for displaying the installation status:
 - Red bullet icon (ERROR)—Indicates an error in device installation on the site; for example, when an unlicensed device is added on the site, device cannot connect to Aruba Central.
 - Orange bullet icon (PENDING)—Indicates a pending state. By default, all sites are displayed in pending state even if the sites are not assigned to any installer.
 - Green bullet icon (IN PROGRESS)—Indicates that the device installation is in progress; for example, the site status moves from pending to in progress when device are added to the site.
 - White disk icon (COMPLETED) —Indicates that the device installation is completed.

If the installation status displays an error:

- Check if the devices are onboarded to Aruba Central.
 - Verify if the devices are assigned a valid subscription.
 - Check if the sites are assigned to a group.
 - View the audit trails.
5. If the installation is completed, click the site and then click **Mark as Completed**.

The following table provides a brief description of the terminology used in this guide.

3DES

Triple Data Encryption Standard. 3DES is a symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

3G

Third Generation of Wireless Mobile Telecommunications Technology. See W-CDMA.

3GPP

Third Generation Partnership Project. 3GPP is a collaborative project aimed at developing globally acceptable specifications for third generation mobile systems.

4G

Fourth Generation of Wireless Mobile Telecommunications Technology. See LTE.

802.11

802.11 is an evolving family of specifications for wireless LANs developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and Carrier Sense Multiple Access with collision avoidance (CSMA/CA) for path sharing.

802.11 bSec

802.11 bSec is an alternative to 802.11 i. The difference between bSec and standard 802.11 i is that bSec implements Suite B algorithms wherever possible. Notably, Advanced Encryption Standard-Counter with CBC-MAC is replaced by Advanced Encryption Standard - Galois/Counter Mode, and the Key Derivation Function (KDF) of 802.11 i is upgraded to support SHA-256 and SHA-384.

802.11a

802.11 a provides specifications for wireless systems. Networks using 802.11 a operate at radio frequencies in the 5 GHz band. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. The maximum data transfer rate is 54 Mbps.

802.11ac

802.11 ac is a wireless networking standard in the 802.11 family that provides high-throughput WLANs on the 5 GHz band.

802.11b

802.11 b is a WLAN standard often called Wi-Fi and is backward compatible with 802.11. Instead of the Phase-Shift Keying (PSK) modulation method used in 802.11 standards, 802.11 b uses Complementary Code Keying (CCK) that allows higher data speeds and makes it less susceptible to multipath-propagation interference. 802.11 b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.

802.11d

802.11d is a wireless network communications specification for use in countries where systems using other standards in the 802.11 family are not allowed to operate. Configuration can be fine-tuned at the Media Access Control (MAC) layer level to comply with the rules of the country or district in which the network is to be used. Rules are subject to variation and include allowed frequencies, allowed power levels, and allowed signal bandwidth. 802.11d facilitates global roaming.

802.11e

802.11e is an enhancement to the 802.11a and 802.11b specifications that enhances the 802.11 Media Access Control layer with a coordinated Time Division Multiple Access (TDMA) construct. It adds error-correcting mechanisms for delay-sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability between business, home, and public environments such as airports and hotels, and offers all subscribers high-speed Internet access with full-motion video, high-fidelity audio, and VoIP.

802.11g

802.11g offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b standard. 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speed of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.

802.11h

802.11h is intended to resolve interference issues introduced by the use of 802.11a in some locations, particularly with military Radar systems and medical devices. Dynamic Frequency Selection (DFS) detects the presence of other devices on a channel and automatically switches the network to another channel if and when such signals are detected. Transmit Power Control (TPC) reduces the radio frequency (RF) output power of each network transmitter to a level that minimizes the risk of interference.

802.11i

802.11i provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards. It requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).

802.11j

802.11j is a proposed addition to the 802.11 family of standards that incorporates Japanese regulatory extensions to 802.11a; the main intent is to add channels in the radio frequency (RF) band of 4.9 GHz to 5.0 GHz.

802.11k

802.11k is an IEEE standard that enables APs and client devices to discover the best available radio resources for seamless BSS transition in a WLAN.

802.11m

802.11m is an Initiative to perform editorial maintenance, corrections, improvements, clarifications, and interpretations relevant to documentation for 802.11 family specifications.

802.11n

802.11n is a wireless networking standard to improve network throughput over the two previous standards, 802.11a and 802.11g. With 802.11n, there will be a significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps with the use of four spatial streams at a channel width of 40 MHz.

802.11r

802.11r is an IEEE standard for enabling seamless BSS transitions in a WLAN. 802.11r standard is also referred to as Fast BSS transition.

802.11u

802.11u is an amendment to the IEEE 802.11 WLAN standards for connection to external networks using common wireless devices such as smartphones and tablet PCs. The 802.11u protocol provides wireless clients with a streamlined mechanism to discover and authenticate to suitable networks, and allows mobile users to roam between partner networks without additional authentication. An 802.11u-capable device supports the Passpoint technology from the Wi-Fi Alliance Hotspot 2.0 R2 Specification that simplifies and automates access to public Wi-Fi.

802.11v

802.11v is an IEEE standard that allows client devices to exchange information about the network topology and RF environment. This information is used for assigning best available radio resources for the client devices to provide seamless connectivity.

802.1Q

802.1Q is an IEEE standard that enables the use of VLANs on an Ethernet network. 802.1Q supports VLAN tagging.

802.1X

802.1X is an IEEE standard for port-based network access control designed to enhance 802.11 WLAN security. 802.1X provides an authentication framework that allows a user to be authenticated by a central authority.

802.3af

802.3af is an IEEE standard for Power over Ethernet (PoE) version that supplies up to 15.4W of DC power. See PoE.

802.3at

802.3at is an IEEE standard for PoE version that supplies up to 25.5W of DC power. See PoE+.

A-MPDU

Aggregate MAC Protocol Data Unit. A-MPDU is a method of frame aggregation, where several MPDUs are combined into a single frame for transmission.

A-MSDU

Aggregate MAC Service Data Unit. A-MSDU is a structure containing multiple MSDUs, transported within a single (unfragmented) data MAC MPDU.

AAA

Authentication, Authorization, and Accounting. AAA is a security framework to authenticate users, authorize the type of access based on user credentials, and record authentication events and information about the network access and network resource consumption.

ABR

Area Border Router. ABR is used for establishing connection between the backbone networks and the Open Shortest Path First (OSPF) areas. ABR is located near the border of one or more OSPF areas.

AC

Access Category. As per the IEEE 802.11e standards, AC refers to various levels of traffic prioritization in Enhanced Distributed Channel Access (EDCA) operation mode. The WLAN applications prioritize traffic based on the Background, Best Effort, Video, and Voice access categories. AC can also refer to Alternating Current, a form of electric energy that flows when the appliances are plugged to a wall socket.

ACC

Advanced Cellular Coexistence. The ACC feature in APs enable WLANs to perform at peak efficiency by minimizing interference from 3G/4G/LTE networks, distributed antenna systems, and commercial small cell/femtocell equipment.

Access-Accept

Response from the RADIUS server indicating successful authentication and containing authorization information.

Access-Reject

Response from RADIUS server indicating that a user is not authorized.

Access-Request

RADIUS packet sent to a RADIUS server requesting authorization.

Accounting-Request

RADIUS packet type sent to a RADIUS server containing accounting summary information.

Accounting-Response

RADIUS packet sent by the RADIUS server to acknowledge receipt of an Accounting-Request.

ACE

Access Control Entry. ACE is an element in an ACL that includes access control information.

ACI

Adjacent Channel Interference. ACI refers to interference or interruptions detected on a broadcasting channel, caused by too much power on an adjacent channel in the spectrum.

ACL

Access Control List. ACL is a common way of restricting certain types of traffic on a physical port.

Active Directory

Microsoft Active Directory. The directory server that stores information about a variety of things, such as organizations, sites, systems, users, shares, and other network objects or components. It also provides authentication and authorization mechanisms, and a framework within which related services can be deployed.

ActiveSync

Mobile data synchronization app developed by Microsoft that allows a mobile device to be synchronized with either a desktop or a server running compatible software products.

ad hoc network

An ad hoc network is a network composed of individual devices communicating with each other directly. Many ad hoc networks are Local Area Networks (LANs) where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

ADO

Active X Data Objects is a part of Microsoft Data Access Components (MDACs) that enables client applications to access data sources through an (Object Linking and Embedding Database) OLE DB provider. ADO supports key features for building client-server and Web-based applications.

ADP

Aruba Discovery Protocol. ADP is an Aruba proprietary Layer 2 protocol. It is used by the APs to obtain the IP address of the TFTP server from which it downloads the AP boot image.

AES

Advanced Encryption Standard. AES is an encryption standard used for encrypting and protecting electronic data. The AES encrypts and decrypts data in blocks of 128 bits (16 bytes), and can use keys of 128 bits, 192 bits, and 256 bits.

AIFSN

Arbitrary Inter-frame Space Number. AIFSN is set by the AP in beacon frames and probe responses. AIFS is a method of prioritizing a particular category of traffic over the other, for example prioritizing voice or video messages over email.

AirGroup

The application that allows the end users to register their personal mobile devices on a local network and define a group of friends or associates who are allowed to share them. AirGroup is primarily designed for colleges and other institutions. AirGroup uses zero configuration networking to allow Apple mobile devices, such as the AirPrint wireless printer service and the AirPlay mirroring service, to communicate over a complex access network topology.

AirWave Management Client

AirWave Management Client is a Windows software utility that enables client devices (such as a laptop) to act as passive RF sensors and augments the AirWave RAPIDS module.

ALE

Analytics and Location Engine. ALE gives visibility into everything the wireless network knows. This enables customers and partners to gain a wealth of information about the people on their premises. This can be very important for many different verticals and use cases. ALE includes a location engine that calculates associated and unassociated device location periodically using context streams, including RSSI readings, from WLAN controllers or Instant clusters.

ALG

Application Layer Gateway. ALG is a security component that manages application layer protocols such as SIP, FTP and so on.

AM

Air Monitor. AM is a mode of operation supported on wireless APs. When an AP operates in the Air Monitor mode, it enhances the wireless networks by collecting statistics, monitoring traffic, detecting intrusions, enforcing security policies, balancing wireless traffic load, self-healing coverage gaps, and more. However, clients cannot connect to APs operating in the AM mode.

AMON

Advanced Monitoring. AMON is used in Aruba WLAN deployments for improved network management, monitoring and diagnostic capabilities.

AMP

AirWave Management Platform. AMP is a network management system for configuring, monitoring, and upgrading wired and wireless devices on your network.

ANQP

Access Network Query Protocol. ANQP is a query and a response protocol for Wi-Fi hotspot services. ANQP includes information Elements (IEs) that can be sent from the AP to the client to identify the AP network and service provider. The IEs typically include information about the domain name of the AP operator, the IP addresses available at the AP, and information about potential roaming partners accessible through the AP. If the client responds with a request for a specific IE, the AP will send a Generic Advertisement Service (GAS) response frame with the configured ANQP IE information.

ANSI

American National Standards Institute. It refers to the ANSI compliance standards for products, systems, services, and processes.

API

Application Programming Interface. Refers to a set of functions, procedures, protocols, and tools that enable users to build application software.

ARM

Adaptive Radio Management. ARM dynamically monitors and adjusts the network to ensure that all users are allowed ready access. It enables full utilization of the available spectrum to support maximum number of users by intelligently choosing the best RF channel and transmit power for APs in their current RF environment.

ARP

Address Resolution Protocol. ARP is used for mapping IP network address to the hardware MAC address of a device.

Aruba Activate

Aruba Activate is a cloud-based service that helps provision your Aruba devices and maintain your inventory. Activate automates the provisioning process, allowing a single IT technician to easily and rapidly deploy devices throughout a distributed enterprise network.

AS

Autonomous System An autonomous system is a single network or a collection of networks that is under a single administrative control. The routing devices in an Autonomous System generally use a single interior gateway protocol (IGP) for routing information. Routing between two Autonomous Systems is handled by the Exterior Gateway Protocols like BGP.

ASCII

American Standard Code for Information Interchange. An ASCII code is a numerical representation of a character or an action.

ASN

Autonomous System Number ASN is a unique number assigned to an autonomous system. ASN is used for identifying an autonomous system when exchanging exterior routing information with other neighboring autonomous systems.

Autonomous System

Also referred to as AS. An autonomous system is a single network or a collection of networks that is under a single administrative control. The routing devices in an Autonomous System generally use a single interior gateway protocol (IGP) for routing information. Routing between two Autonomous Systems is handled by the Exterior Gateway Protocols like BGP.

B-RAS

Broadband Remote Access Server. A B-RAS is a server that facilitates and converges traffic from multiple Internet traffic resources such as cable, DSL, Ethernet, or Broadband wireless.

band

Band refers to a specified range of frequencies of electromagnetic radiation.

BGP

Border Gateway Protocol. BGP is a routing protocol for exchanging data and information between different host gateways or autonomous systems on the Internet.

BLE

Bluetooth Low Energy. The BLE functionality is offered by Bluetooth® to enable devices to run for long durations with low power consumption.

BMC

Beacon Management Console. BMC manages and monitors beacons from the BLE devices. The BLE devices are used for location tracking and proximity detection.

BPDU

Bridge Protocol Data Unit. A BPDU is a data message transmitted across a local area network to detect loops in network topologies.

BRE

Basic Regular Expression. The BRE syntax standards designed by the IEEE provides extension to the traditional Simple Regular Expressions syntax and allows consistency between utility programs such as grep, sed, and awk.

BSS

Basic Service Set. A BSS is a set of interconnected stations that can communicate with each other. BSS can be an independent BSS or infrastructure BSS. An independent BSS is an ad hoc network that does not include APs, whereas the infrastructure BSS consists of an AP and all its associated clients.

BSSID

Basic Service Set Identifier. The BSSID identifies a particular BSS within an area. In infrastructure BSS networks, the BSSID is the MAC address of the AP. In independent BSS or ad hoc networks, the BSSID is generated randomly.

BYOD

Bring Your Own Device. BYOD refers to the use of personal mobile devices within an enterprise network infrastructure.

CA

Certificate Authority or Certification Authority. Entity in a public key infrastructure system that issues certificates to clients. A certificate signing request received by the CA is converted into a certificate when the CA adds a signature generated with a private key. See digital certificate.

CAC

Call Admission Control. CAC regulates traffic volume in voice communications. CAC can also be used to ensure or maintain a certain level of audio quality in voice communications networks.

CALEA

Communications Assistance for Law Enforcement Act. To comply with the CALEA specifications and to allow lawful interception of Internet traffic by the law enforcement and intelligence agencies, the telecommunications carriers and manufacturers of telecommunications equipment are required to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

Campus AP

Campus APs are used in private networks where APs connect over private links (LAN, WLAN, WAN or MPLS) and terminate directly on controllers. Campus APs are deployed as part of the indoor campus solution in enterprise office buildings, warehouses, hospitals, universities, and so on.

captive portal

A captive portal is a web page that allows the users to authenticate and sign in before connecting to a public-access network. Captive portals are typically used by business centers, airports, hotel lobbies, coffee shops, and other venues that offer free Wi-Fi hotspots for the guest users.

CCA

Clear Channel Assessment. In wireless networks, the CCA method detects if a channel is occupied or clear, and determines if the channel is available for data transmission.

CDP

Cisco Discovery Protocol. CDP is a proprietary Data Link Layer protocol developed by Cisco Systems. CDP runs on Cisco devices and enables networking applications to learn about the neighboring devices directly connected to the network.

CDR

Call Detail Record. A CDR contains the details of a telephone or VoIP call, such as the origin and destination addresses of the call, the start time and end time of the call, any toll charges that were added through the network or charges for operator services, and so on.

CEF

Common Event Format. The CEF is a standard for the interoperability of event or log-generating devices and applications. The standard syntax for CEF includes a prefix and a variable extension formatted as key-value pairs.

CGI

Common Gateway Interface. CGI is a standard protocol for exchanging data between the web servers and executable programs running on a server to dynamically process web pages.

CHAP

Challenge Handshake Authentication Protocol. CHAP is an authentication scheme used by PPP servers to validate the identity of remote clients.

CIDR

Classless Inter-Domain Routing. CIDR is an IP standard for creating and allocating unique identifiers for networks and devices. The CIDR IP addressing scheme is used as a replacement for the older IP addressing scheme based on classes A, B, and C. With CIDR, a single IP address can be used to designate many unique IP addresses. A CIDR IP address ends with a slash followed by the IP network prefix, for example, 192.0.2.0/24.

ClearPass

ClearPass is an access management system for creating and enforcing policies across a network to all devices and applications. The ClearPass integrated platform includes applications such as Policy Manager, Guest, Onboard, OnGuard, Insight, Profile, QuickConnect, and so on.

ClearPass Guest

ClearPass Guest is a configurable ClearPass application for secure visitor network access management.

ClearPass Policy Manager

ClearPass Policy Manager is a baseline platform for policy management, AAA, profiling, network access control, and reporting. With ClearPass Policy Manager, the network administrators can configure and manage secure network access that accommodates requirements across multiple locations and multivendor networks, regardless of device ownership and connection method.

CN

Common Name. CN is the primary name used to identify a certificate.

CNA

Captive Network Assistant. CNA is a popup page shown when joining a network that has a captive portal.

CoA

Change of Authorization. The RADIUS CoA is used in the AAA service framework to allow dynamic modification of the authenticated, authorized, and active subscriber sessions.

CoS

Class of Service. CoS is used in data and voice protocols for classifying packets into different types of traffic (voice, video, or data) and setting a service priority. For example, voice traffic can be assigned a higher priority over email or HTTP traffic.

CPE

Customer Premises Equipment. It refers to any terminal or equipment located at the customer premises.

CPsec

Control Plane Security. CPsec is a secure form of communication between a controller and APs to protect the control plane communications. This is performed by means of using public-key self-signed certificates created by each master controller.

CPU

Central Processing Unit. A CPU is an electronic circuitry in a computer for processing instructions.

CRC

Cyclic Redundancy Check. CRC is a data verification method for detecting errors in digital data during transmission, storage, or retrieval.

CRL

Certificate Revocation List. CRL is a list of revoked certificates maintained by a certification authority.

cryptobinding

Short for cryptographic binding. A procedure in a tunneled EAP method that binds together the tunnel protocol and the tunneled authentication methods, ensuring the relationship between a collection of data assets. Cryptographic binding focuses on protecting the server; mutual cryptographic binding protects both peer and server.

CSA

Channel Switch Announcement. The CSA element enables an AP to advertise that it is switching to a new channel before it begins transmitting on that channel. This allows the clients, which support CSA, to transition to the new channel with minimal downtime.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance. CSMA/CA is a protocol for carrier transmission in networks using the 802.11 standard. CSMA/CA aims to prevent collisions by listening to the broadcasting nodes, and informing devices not to transmit any data until the broadcasting channel is free.

CSR

Certificate Signing Request. In PKI systems, a CSR is a message sent from an applicant to a CA to apply for a digital identity certificate.

CSV

Comma-Separated Values. A file format that stores tabular data in the plain text format separated by commas.

CTS

Clear to Send. The CTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See RTS.

CW

Contention Window. In QoS, CW refers to a window set for access categories based on the type of traffic. Based on the type and volume of the traffic, the minimum and maximum values can be calculated to provide a wider window when necessary.

DAI

Dynamic ARP inspection. A security feature that validates ARP packets in a network.

DAS

Distributed Antenna System. DAS is a network of antenna nodes strategically placed around a geographical area or structure for additional cellular coverage.

dB

Decibel. Unit of measure for sound or noise and is the difference or ratio between two signal levels.

dBm

Decibel-Milliwatts. dBm is a logarithmic measurement (integer) that is typically used in place of mW to represent receive-power level. AMP normalizes all signals to dBm, so that it is easy to evaluate performance between various vendors.

DCB

Data Center Bridging. DCB is a collection of standards developed by IEEE for creating a converged data center network using Ethernet.

DCE

Data Communication Equipment. DCE refers to the devices that establish, maintain, and terminate communication network sessions between a data source and its destination.

DCF

Distributed Coordination Function. DCF is a protocol that uses carrier sensing along with a four-way handshake to maximize the throughput while preventing packet collisions.

DDMO

Distributed Dynamic Multicast Optimization. DDMO is similar to Dynamic Multicast Optimization (DMO) where the multicast streams are converted into unicast streams on the AP instead of the controller, to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DES

Data Encryption Standard. DES is a common standard for data encryption and a form of secret key cryptography, which uses only one key for encryption and decryption.

designated router

Designated router refers to a router interface that is elected to originate network link advertisements for networks using the OSPF protocol.

destination NAT

Destination Network Address Translation. Destination NAT is a process of translating the destination IP address of an end route packet in a network. Destination NAT is used for redirecting the traffic destined to a virtual host to the real host, where the virtual host is identified by the destination IP address and the real host is identified by the translated IP address.

DFS

Dynamic Frequency Selection. DFS is a mandate for radio systems operating in the 5 GHz band to be equipped with means to identify and avoid interference with Radar systems.

DFT

Discrete Fourier Transform. DFT converts discrete-time data sets into a discrete-frequency representation. See FFT.

DHCP

Dynamic Host Configuration Protocol. A network protocol that enables a server to automatically assign an IP address to an IP-enabled device from a defined range of numbers configured for a given network.

DHCP snooping

DHCP snooping enables the switch to monitor and control DHCP messages received from untrusted devices that are connected to the switch.

digital certificate

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity—information such as the name of a person or an organization, address, and so forth.

Digital wireless pulse

A wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance. Ultra Wideband radio can carry a huge amount of data over a distance up to 230 ft at very low power (less than 0.5 mW), and has the ability to carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power.

Disconnect-Ack

Disconnect-Ack is a NAS response packet to a Disconnect-Request, which indicates that the session was disconnected.

Disconnect-Nak

Disconnect-Nak is NAS response packet to a Disconnect-Request, which indicates that the session was not disconnected.

Disconnect-Request

Disconnect-Request is a RADIUS packet type sent to a NAS requesting that a user or session be disconnected.

distribution certificate

Distribution certificate is used for digitally signing iOS mobile apps to enable enterprise app distribution. It verifies the identity of the app publisher.

DLNA

Digital Living Network Alliance. DLNA is a set of interoperability guidelines for sharing digital media among multimedia devices.

DMO

Dynamic Multicast Optimization. DMO is a process of converting multicast streams into unicast streams over a wireless link to enhance the quality and reliability of streaming videos, while preserving the bandwidth available to non-video clients.

DN

Distinguished Name. A series of fields in a digital certificate that, taken together, constitute the unique identity of the person or device that owns the digital certificate. Common fields in a DN include country, state, locality, organization, organizational unit, and the "common name", which is the primary name used to identify the certificate.

DNS

Domain Name System. A DNS server functions as a phone book for the intranet and Internet users. It converts human-readable computer host names into IP addresses and IP addresses into host names. It stores several records for a domain name such as an address 'A' record, name server (NS), and mail exchanger (MX) records. The Address 'A' record is the most important record that is stored in a DNS server, because it provides the required IP address for a network peripheral or element.

DOCSIS

Data over Cable Service Interface Specification. A telecommunication standard for Internet access through cable modem.

DoS

Denial of Service. DoS is any type of attack where the attackers send excessive messages to flood traffic and thereby preventing the legitimate users from accessing the service.

DPD

Dead Peer Detection. A method used by the network devices to detect the availability of the peer devices.

DPI

Deep Packet Inspection. DPI is an advanced method of network packet filtering that is used for inspecting data packets exchanged between the devices and systems over a network. DPI functions at the Application layer of the Open Systems Interconnection (OSI) reference model and enables users to identify, categorize, track, reroute, or stop packets passing through a network.

DRT

Downloadable Regulatory Table. The DRT feature allows new regulatory approvals to be distributed for APs without a software upgrade or patch.

DS

Differentiated Services. The DS specification aims to provide uninterrupted quality of service by managing and controlling the network traffic, so that certain types of traffic get precedence.

DSCP

Differentiated Services Code Point. DSCP is a 6-bit packet header value used for traffic classification and priority assignment.

DSL

Digital Subscriber Line. The DSL technology allows the transmission of digital data over telephone lines. A DSL modem is a device used for connecting a computer or router to a telephone line that offers connectivity to the Internet.

DSSS

Direct-Sequence Spread Spectrum. DSSS is a modulation technique used for reducing overall signal interference. This technique multiplies the original data signal with a pseudo random noise spreading code. Spreading of this signal makes the resulting wideband channel more noisy, thereby increasing the resistance to interference. See FHSS.

DST

Daylight Saving Time. DST is also known as summer time that refers to the practice of advancing clocks, so that evenings have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

DTE

Data Terminal Equipment. DTE refers to a device that converts user information into signals or re-converts the received signals.

DTIM

Delivery Traffic Indication Message. DTIM is a kind of traffic indication map. A DTIM interval determines when the APs must deliver broadcast and multicast frames to their associated clients in power save mode.

DTLS

Datagram Transport Layer Security. DTLS communications protocol provides communications security for datagram protocols.

dynamic authorization

Dynamic authorization refers to the ability to make changes to a visitor account's session while it is in progress. This might include disconnecting a session or updating some aspect of the authorization for the session.

dynamic NAT

Dynamic Network Address Translation. Dynamic NAT maps multiple public IP addresses and uses these addresses with an internal or private IP address. Dynamic NAT helps to secure a network by masking the internal configuration of a private network.

EAP

Extensible Authentication Protocol. An authentication protocol for wireless networks that extends the methods used by the PPP, a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication.

EAP-FAST

EAP – Flexible Authentication Secure Tunnel (tunneled).

EAP-GTC

EAP – Generic Token Card. (non-tunneled).

EAP-MD5

EAP – Method Digest 5. (non-tunneled).

EAP-MSCHAP

EAP Microsoft Challenge Handshake Authentication Protocol.

EAP-MSCHAPv2

EAP Microsoft Challenge Handshake Authentication Protocol Version 2.

EAP-PEAP

EAP-Protected EAP. A widely used protocol for securely transporting authentication data across a network (tunneled).

EAP-PWD

EAP-Password. EAP-PWD is an EAP method that uses a shared password for authentication.

EAP-TLS

EAP-Transport Layer Security. EAP-TLS is a certificate-based authentication method supporting mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints. See RFC 5216.

EAP-TTLS

EAP-Tunneled Transport Layer Security. EAP-TTLS is an EAP method that encapsulates a TLS session, consisting of a handshake phase and a data phase. See RFC 5281.

EAPoL

Extensible Authentication Protocol over LAN. A network port authentication protocol used in IEEE 802.1X standards to provide a generic network sign-on to access network resources.

ECC

Elliptical Curve Cryptography or Error correcting Code memory. Elliptical Curve Cryptography is a public-key encryption technique that is based on elliptic curve theory used for creating faster, smaller, and more efficient cryptographic keys. Error Correcting Code memory is a type of computer data storage that can detect and correct the most common kinds of internal data corruption. ECC memory is used in most computers where data corruption cannot be tolerated under any circumstances, such as for scientific or financial computing.

ECDSA

Elliptic Curve Digital Signature Algorithm. ECDSA is a cryptographic algorithm that supports the use of public or private key pairs for encrypting and decrypting information.

EDCA

Enhanced Distributed Channel Access. The EDCA function in the IEEE 802.11e Quality of Service standard supports differentiated and distributed access to wireless medium based on traffic priority and Access Category types. See WMM and WME.

EIGRP

Enhanced Interior Gateway Routing Protocol. EIGRP is a routing protocol used for automating routing decisions and configuration in a network.

EIRP

Effective Isotropic Radiated Power or Equivalent Isotropic Radiated Power. EIRP refers to the output power generated when a signal is concentrated into a smaller area by the Antenna.

ESI

External Services Interface. ESI provides an open interface for integrating security solutions that solve interior network problems such as viruses, worms, spyware, and corporate compliance.

ESS

Extended Service Set. An ESS is a set of one or more interconnected BSSs that form a single sub network.

ESSID

Extended Service Set Identifier. ESSID refers to the ID used for identifying an extended service set.

Ethernet

Ethernet is a network protocol for data transmission over LAN.

EULA

End User License Agreement. EULA is a legal contract between a software application publisher or author and the users of the application.

FCC

Federal Communications Commission. FCC is a regulatory body that defines standards for the interstate and international communications by radio, television, wire, satellite, and cable.

FFT

Fast Fourier Transform. FFT is a frequency analysis mechanism that aims at faster conversion of a discrete signal in time domain into a discrete frequency domain representation. See also DFT.

FHSS

Frequency Hopping Spread Spectrum. FHSS is transmission technique that allows modulation and transmission of a data signal by rapidly switching a carrier among many frequency channels in a random but predictable sequence. See also DSSS.

FIB

Forwarding Information Base. FIB is a forwarding table that maps MAC addresses to ports. FIB is used in network bridging, routing, and similar functions to identify the appropriate interface for forwarding packets.

FIPS

Federal Information Processing Standards. FIPS refers to a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies, and by government contractors and vendors who work with these agencies.

firewall

Firewall is a network security system used for preventing unauthorized access to or from a private network.

FQDN

Fully Qualified Domain Name. FQDN is a complete domain name that identifies a computer or host on the Internet.

FQLN

Fully Qualified Location Name. FQLN is a device location identifier in the format:
APname.Floor.Building.Campus.

frequency allocation

Use of radio frequency spectrum as regulated by governments.

FSPL

Free Space Path Loss. FSPL refers to the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space (usually air), with no obstacles nearby to cause reflection or

diffraction.

FTP

File Transfer Protocol. A standard network protocol used for transferring files between a client and server on a computer network.

GARP

Generic Attribute Registration Protocol. GVRP is a LAN protocol that allows the network nodes to register and de-register attributes, such as network addresses, with each other.

GAS

Generic Advertisement Service. GAS is a request-response protocol, which provides Layer 2 transport mechanism between a wireless client and a server in the network prior to authentication. It helps in determining a wireless network infrastructure before associating clients, and allows clients to send queries to multiple 802.11 networks in parallel.

Gbps

Gigabits per second.

GBps

Gigabytes per second.

GET

GET refers HTTP request method or an SNMP operation method. The GET HTTP request method submits data to be processed to a specified resource. The GET SNMP operation method obtains information from the Management Information Base (MIB).

GHz

Gigahertz.

GMT

Greenwich Mean Time. GMT refers to the mean solar time at the Royal Observatory in Greenwich, London. GMT is the same as Coordinated Universal Time (UTC) standard, written as an offset of UTC +/- 00:00.

goodput

Goodput is the application level throughput that refers to the ratio of the total bytes transmitted or received in the network to the total air time required for transmitting or receiving the bytes.

GPS

Global Positioning System. A satellite-based global navigation system.

GRE

Generic Routing Encapsulation. GRE is an IP encapsulation protocol that is used to transport packets over a network.

GTC

Generic Token Card. GTC is a protocol that can be used as an alternative to MSCHAPv2 protocol. GTC allows authentication to various authentication databases even in cases where MSCHAPv2 is not supported by the database.

GVRP

GARP VLAN Registration Protocol or Generic VLAN Registration Protocol. GARP is an IEEE 802.1Q-compliant protocol that facilitates VLAN registration and controls VLANs within a larger network.

H2QP

Hotspot 2.0 Query Protocol.

hot zone

Wireless access area created by multiple hotspots that are located in close proximity to one another. Hot zones usually combine public safety APs with public hotspots.

hotspot

Hotspot refers to a WLAN node that provides Internet connection and virtual private network (VPN) access from a given location. A business traveler, for example, with a laptop equipped for Wi-Fi can look up a local hotspot, contact it, and get connected through its network to reach the Internet.

HSPA

High-Speed Packet Access.

HT

High Throughput. IEEE 802.11n is an HT WLAN standard that aims to achieve physical data rates of close to 600 Mbps on the 2.4 GHz and 5 GHz bands.

HTTP

Hypertext Transfer Protocol. The HTTP is an application protocol to transfer data over the web. The HTTP protocol defines how messages are formatted and transmitted, and the actions that the web servers and browsers should take in response to various commands.

HTTPS

Hypertext Transfer Protocol Secure. HTTPS is a variant of the HTTP that adds a layer of security on the data in transit through a secure socket layer or transport layer security protocol connection.

IAS

Internet Authentication Service. IAS is a component of Windows Server operating systems that provides centralized user authentication, authorization, and accounting.

ICMP

Internet Control Message Protocol. ICMP is an error reporting protocol. It is used by network devices such as routers, to send error messages and operational information to the source IP address when network problems prevent delivery of IP packets.

IDS

Intrusion Detection System. IDS monitors a network or systems for malicious activity or policy violations and reports its findings to the management system deployed in the network.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol. Communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships.

IGMP snooping

IGMP snooping prevents multicast flooding on Layer 2 network by treating multicast traffic as broadcast traffic. Without IGMP snooping, all streams could be flooded to all ports on that VLAN. When multicast flooding occurs, end-hosts that happen to be in the same VLAN would receive all the streams only to be discarded without snooping.

IGP

Interior Gateway Protocol. IGP is used for exchanging routing information between gateways within an autonomous system (for example, a system of corporate local area networks).

IGRP

Interior Gateway Routing Protocol. IGRP is a distance vector interior routing protocol used by routers to exchange routing data within an autonomous system.

IKE

Internet Key Exchange. IKE is a key management protocol used with IPsec protocol to establish a secure communication channel. IKE provides additional feature, flexibility, and ease of configuration for IPsec standard.

IKEv1

Internet Key Exchange version 1. IKEv1 establishes a secure authenticated communication channel by using either the pre-shared key (shared secret), digital signatures, or public key encryption. IKEv1 operates in Main and Aggressive modes. See RFC 2409.

IKEv2

Internet Key Exchange version 2. IKEv2 uses the secure channel established in Phase 1 to negotiate Security Associations on behalf of services such as IPsec. IKEv2 uses pre-shared key and Digital Signature for authentication. See RFC 4306.

IoT

Internet of Things. IoT refers to the internetworking of devices that are embedded with electronics, software, sensors, and network connectivity features allowing data exchange over the Internet.

IPM

Intelligent Power Monitoring. IPM is a feature supported on certain APs that actively measures the power utilization of an AP and dynamically adapts to the power resources.

IPS

Intrusion Prevention System. The IPS monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, log the information, attempt to block the activity, and report it.

IPsec

Internet Protocol security. IPsec is a protocol suite for secure IP communications that authenticates and encrypts each IP packet in a communication session.

IPSG

Internet Protocol Source Guard. IPSG restricts IP address from untrusted interface by filtering traffic based on list of addresses in the DHCP binding database or manually configured IP source bindings. It prevents IP spoofing attacks.

IrDA

An industry-sponsored organization set up in 1993 to create international standards for the hardware and software used in infrared communication links. In this special form of radio transmission, a focused ray of light in the infrared frequency spectrum, measured in terahertz (THz), or trillions of hertz (cycles per second), is modulated with information and sent from a transmitter to a receiver over a relatively short distance.

ISAKMP

Internet Security Association and Key Management Protocol. ISAKMP is used for establishing Security Associations and cryptographic keys in an Internet environment.

ISP

Internet Service Provider. An ISP is an organization that provides services for accessing and using the Internet.

JSON

JavaScript Object Notation. JSON is an open-standard, language-independent, lightweight data-interchange format used to transmit data objects consisting of attribute–value pairs. JSON uses a "self-describing" text format that is easy for humans to read and write, and that can be used as a data format by any programming language.

Kbps

Kilobits per second.

KBps

Kilobytes per second.

keepalive

Signal sent at periodic intervals from one device to another to verify that the link between the two devices is working. If no reply is received, data will be sent by a different path until the link is restored. A keepalive can also be used to indicate that the connection should be preserved so that the receiving device does not consider it timed out and drop it.

L2TP

Layer-2 Tunneling Protocol. L2TP is a networking protocol used by the ISPs to enable VPN operations.

LACP

Link Aggregation Control Protocol. LACP is used for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LAG

Link Aggregation Group . A LAG combines a number of physical ports together to make a single high-bandwidth data path. LAGs can connect two switches to provide a higher-bandwidth connection to a public network.

LAN

Local Area Network. A LAN is a network of connected devices within a distinct geographic area such as an office or a commercial establishment and share a common communications line or wireless link to a server.

LCD

Liquid Crystal Display. LCD is the technology used for displays in notebook and other smaller computers. Like LED and gas-plasma technologies, LCDs allow displays to be much thinner than the cathode ray tube technology.

LDAP

Lightweight Directory Access Protocol. LDAP is a communication protocol that provides the ability to access and maintain distributed directory information services over a network.

LDPC

Low-Density Parity-Check. LDPC is a method of transmitting a message over a noisy transmission channel using a linear error correcting code. An LDPC is constructed using a sparse bipartite graph.

LEAP

Lightweight Extensible Authentication Protocol. LEAP is a Cisco proprietary version of EAP used in wireless networks and Point-to-Point connections.

LED

Light Emitting Diode. LED is a semiconductor light source that emits light when an electric current passes through it.

LEEF

Log Event Extended Format. LEEF is a type of customizable syslog event format. An extended log file contains a sequence of lines containing ASCII characters terminated by either the sequence LF or CRLF.

LI

Lawful Interception. LI refers to the procedure of obtaining communications network data by the Law Enforcement Agencies for the purpose of analysis or evidence.

LLDP

Link Layer Discovery Protocol. LLDP is a vendor-neutral link layer protocol in the Internet Protocol suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, which is principally a wired Ethernet.

LLDP-MED

LLDP–Media Endpoint Discovery. LLDP-MED facilitates information sharing between endpoints and network infrastructure devices.

LMS

Local Management Switch. In multi-controller networks, each controller acts as an LMS and terminates user traffic from the APs, processes, and forwards the traffic to the wired network.

LNS

L2TP Network Server. LNS is an equipment that connects to a carrier and handles the sessions from broadband lines. It is also used for dial-up and mobile links. LNS handles authentication and routing of the IP addresses. It also handles the negotiation of the link with the equipment and establishes a session.

LTE

Long Term Evolution. LTE is a 4G wireless communication standard that provides high-speed wireless communication for mobile phones and data terminals. See 4G.

MAB

MAC Authentication Bypass. Endpoints such as network printers, Ethernet-based sensors, cameras, and wireless phones do not support 802.1X authentication. For such endpoints, MAC Authentication Bypass mechanism is used. In this method, the MAC address of the endpoint is used to authenticate the endpoint.

MAC

Media Access Control. A MAC address is a unique identifier assigned to network interfaces for communications on a network.

MAM

Mobile Application Management. MAM refers to software and services used to secure, manage, and distribute mobile applications used in enterprise settings on mobile devices like smartphones and tablet computers. Mobile Application Management can apply to company-owned mobile devices as well as BYOD.

Mbps

Megabits per second

MBps

Megabytes per second

MCS

Modulation and Coding Scheme. MCS is used as a parameter to determine the data rate of a wireless connection for high throughput.

MD4

Message Digest 4. MD4 is an earlier version of MD5 and is an algorithm used to verify data integrity through the creation of a 128-bit message digest from data input.

MD5

Message Digest 5. The MD5 algorithm is a widely used hash function producing a 128-bit hash value from the data input.

MDAC

Microsoft Data Access Components. MDAC is a framework of interrelated Microsoft technologies that provides a standard database for Windows OS.

MDM

Mobile Device Management. MDM is an administrative software to manage, monitor, and secure mobile devices of the employees in a network.

mDNS

Multicast Domain Name System. mDNS provides the ability to perform DNS-like operations on the local link in the absence of any conventional unicast DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets, and is implemented by the Apple Bonjour and Linux NSS-mDNS services. mDNS works in conjunction with DNS Service Discovery (DNS-SD), a companion zero-configuration technique specified. See RFC 6763.

MFA

Multi-factor Authentication. MFA lets you require multiple factors, or proofs of identity, when authenticating a user. Policy configurations define how often multi-factor authentication will be required, or conditions that will trigger it.

MHz

Megahertz

MIB

Management Information Base. A hierarchical database used by SNMP to manage the devices being monitored.

microwave

Electromagnetic energy with a frequency higher than 1 GHz, corresponding to wavelength shorter than 30 centimeters.

MIMO

Multiple Input Multiple Output. An antenna technology for wireless communications in which multiple antennas are used at both source (transmitter) and destination (receiver). The antennas at each end of the communications circuit are combined to minimize errors and optimize data speed.

MISO

Multiple Input Single Output. An antenna technology for wireless communications in which multiple antennas are used at the source (transmitter). The antennas are combined to minimize errors and optimize

data speed. The destination (receiver) has only one antenna.

MLD

Multicast Listener Discovery. A component of the IPv6 suite. It is used by IPv6 routers for discovering multicast listeners on a directly attached link.

MPDU

MAC Protocol Data Unit. MPDU is a message exchanged between MAC entities in a communication system based on the layered OSI model.

MPLS

Multiprotocol Label Switching. The MPLS protocol speeds up and shapes network traffic flows.

MPPE

Microsoft Point-to-Point Encryption. A method of encrypting data transferred across PPP-based dial-up connections or PPTP-based VPN connections.

MS-CHAP

Microsoft Challenge Handshake Authentication Protocol. MS-CHAP is Password-based, challenge-response, mutual authentication protocol that uses MD4 and DES encryption.

MS-CHAPv1

Microsoft Challenge Handshake Authentication Protocol version 1. MS-CHAPv1 extends the user authentication functionality provided on Windows networks to remote workstations. MS-CHAPv1 supports only one-way authentication.

MS-CHAPv2

Microsoft Challenge Handshake Authentication Protocol version 2. MS-CHAPv2 is an enhanced version of the MS-CHAP protocol that supports mutual authentication.

MSS

Maximum Segment Size. MSS is a parameter of the options field in the TCP header that specifies the largest amount of data, specified in bytes, that a computer or communications device can receive in a single TCP segment.

MSSID

Mesh Service Set Identifier. MSSID is the SSID used by the client to access a wireless mesh network.

MSTP

Multiple Spanning Tree Protocol. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

MTU

Maximum Transmission Unit. MTU is the largest size packet or frame specified in octets (eight-bit bytes) that can be sent in networks such as the Internet.

MU-MIMO

Multi-User Multiple-Input Multiple-Output. MU-MIMO is a set of multiple-input and multiple-output technologies for wireless communication, in which users or wireless terminals with one or more antennas communicate with each other.

MVRP

Multiple VLAN Registration Protocol. MVRP is a Layer 2 network protocol used for automatic configuration of VLAN information on switches.

mW

milliWatts. mW is 1/1000 of a Watt. It is a linear measurement (always positive) that is generally used to represent transmission.

NAC

Network Access Control. NAC is a computer networking solution that uses a set of protocols to define and implement a policy that describes how devices can secure access to network nodes when they initially attempt to connect to a network.

NAD

Network Access Device. NAD is a device that automatically connects the user to the preferred network, for example, an AP or an Ethernet switch.

NAK

Negative Acknowledgement. NAK is a response indicating that a transmitted message was received with errors or it was corrupted, or that the receiving end is not ready to accept transmissions.

NAP

Network Access Protection. The NAP feature in the Windows Server allows network administrators to define specific levels of network access based on identity, groups, and policy compliance. The NAP Agent is a service that collects and manages health information for NAP client computers. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAS

Network Access Server. NAS provides network access to users, such as a wireless AP, network switch, or dial-in terminal server.

NAT

Network Address Translation. NAT is a method of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device.

NetBIOS

Network Basic Input/Output System. A program that lets applications on different computers communicate within a LAN.

NFC

Near-Field Communication. NFC is a short-range wireless connectivity standard (ECMA-340, ISO/IEC 18092) that uses magnetic field induction to enable communication between devices when they touch or are brought closer (within a few centimeters of distance). The standard specifies a way for the devices to establish a peer-to-peer (P2P) network to exchange data.

NIC

Network Interface Card. NIC is a hardware component that allows a device to connect to the network.

Nmap

Network Mapper. Nmap is an open-source utility for network discovery and security auditing. Nmap uses IP packets to determine such things as the hosts available on a network and their services, operating systems and versions, types of packet filters/firewalls, and so on.

NMI

Non-Maskable Interrupt. NMI is a hardware interrupt that standard interrupt-masking techniques in the system cannot ignore. It typically occurs to signal attention for non-recoverable hardware errors.

NMS

Network Management System. NMS is a set of hardware and/or software tools that allow an IT professional to supervise the individual components of a network within a larger network management framework.

NOE

New Office Environment. NOE is a proprietary VoIP protocol designed by Alcatel-Lucent Enterprise.

NTP

Network Time Protocol. NTP is a protocol for synchronizing the clocks of computers over a network.

OAuth

Open Standard for Authorization. OAuth is a token-based authorization standard that allows websites or third-party applications to access user information, without exposing the user credentials.

OCSP

Online Certificate Status Protocol. OCSP is used for determining the current status of a digital certificate without requiring a CRL.

OFDM

Orthogonal Frequency Division Multiplexing. OFDM is a scheme for encoding digital data on multiple carrier frequencies.

OID

Object Identifier. An OID is an identifier used to name an object. The OIDs represent nodes or managed objects in a MIB hierarchy. The OIDs are designated by text strings and integer sequences and are formally defined as per the ASN.1 standard.

OKC

Opportunistic Key Caching. OKC is a technique available for authentication between multiple APs in a network where those APs are under common administrative control. Using OKC, a station roaming to any AP in the network will not have to complete a full authentication exchange, but will instead just perform the 4-way handshake to establish transient encryption keys.

OpenFlow

OpenFlow is an open communications interface between control plane and the forwarding layers of a network.

OpenFlow agent

OpenFlow agent. OpenFlow is a software module in Software-Defined Networking (SDN) that allows the abstraction of any legacy network element, so that it can be integrated and managed by the SDN controller. OpenFlow runs on network devices such as switches, routers, wireless controllers, and APs.

Optical wireless

Optical wireless is combined use of conventional radio frequency wireless and optical fiber for telecommunication. Long-range links are provided by using optical fibers; the links from the long-range endpoints to end users are accomplished by RF wireless or laser systems. RF wireless at Ultra High Frequencies and microwave frequencies can carry broadband signals to individual computers at substantial data speeds.

OSI

Open Systems Interconnection. OSI is a reference model that defines a framework for communication between the applications in a network.

OSPF

Open Shortest Path First. OSPF is a link-state routing protocol for IP networks. It uses a link-state routing algorithm and falls into the group of interior routing protocols that operates within a single Autonomous System (AS).

OSPFv2

Open Shortest Path First version 2. OSPFv2 is the version 2 of the link-state routing protocol, OSPF. See RFC 2328.

OUI

Organizationally Unique Identifier. Synonymous with company ID or vendor ID, an OUI is a 24-bit, globally unique assigned number, referenced by various standards. The first half of a MAC address is OUI.

OVA

Open Virtualization Archive. OVA contains a compressed installable version of a virtual machine.

OVF

Open Virtualization Format. OVF is a specification that describes an open-standard, secure, efficient, portable and extensible format for packaging and distributing software for virtual machines.

PAC

Protected Access Credential. PAC is distributed to clients for optimized network authentication. These credentials are used for establishing an authentication tunnel between the client and the authentication server.

PAP

Password Authentication Protocol. PAP validates users by password. PAP does not encrypt passwords for transmission and is thus considered insecure.

PAPI

Process Application Programming Interface. PAPI controls channels for ARM and Wireless Intrusion Detection System (WIDS) communication to the master controller. A separate PAPI control channel connects to the local controller where the SSID tunnels terminate.

PBR

Policy-based Routing. PBR provides a flexible mechanism for forwarding data packets based on policies configured by a network administrator.

PDU

Power Distribution Unit or Protocol Data Unit. Power Distribution Unit is a device that distributes electric power to the networking equipment located within a data center. Protocol Data Unit contains protocol control information that is delivered as a unit among peer entities of a network.

PEAP

Protected Extensible Authentication Protocol. PEAP is a type of EAP communication that addresses security issues associated with clear text EAP transmissions by creating a secure channel encrypted and protected by TLS.

PEF

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFNG

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PEFV

Policy Enforcement Firewall. PEF also known as PEFNG provides context-based controls to enforce application-layer security and prioritization. The customers using Aruba mobility controllers can avail PEF features and services by obtaining a PEF license. PEF for VPN users—Customers with PEF for VPN license can apply firewall policies to the user traffic routed to a controller through a VPN tunnel.

PFS

Perfect Forward Secrecy. PFS refers to the condition in which a current session key or long-term private key does not compromise the past or subsequent keys.

PHB

Per-hop behavior. PHB is a term used in DS or MPLS. It defines the policy and priority applied to a packet when traversing a hop (such as a router) in a DiffServ network.

PIM

Protocol-Independent Multicast. PIM refers to a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet.

PIN

Personal Identification Number. PIN is a numeric password used to authenticate a user to a system.

PKCS#n

Public-key cryptography standard n. PKCS#n refers to a numbered standard related to topics in cryptography, including private keys (PKCS#1), digital certificates (PKCS#7), certificate signing requests (PKCS#10), and secure storage of keys and certificates (PKCS#12).

PKI

Public Key Infrastructure. PKI is a security technology based on digital certificates and the assurances provided by strong cryptography. See also certificate authority, digital certificate, public key, private key.

PLMN

Public Land Mobile Network. PLMS is a network established and operated by an administration or by a Recognized Operating Agency for the specific purpose of providing land mobile telecommunications services to the public.

PMK

Pairwise Master Key. PMK is a shared secret key that is generated after PSK or 802.1X authentication.

PoE

Power over Ethernet. PoE is a technology for wired Ethernet LANs to carry electric power required for the device in the data cables. The IEEE 802.3af PoE standard provides up to 15.4 W of power on each port.

PoE+

Power over Ethernet+. PoE+ is an IEEE 802.3at standard that provides 25.5W power on each port.

POST

The HTTP POST method is used for transferring data from a client (browser) to a server using the HTTP protocol. The POST method is considered a secure way of transferring data from a client as it carries the request parameter in the message body and does not append it in the URL string.

PPP

Point-to-Point Protocol. PPP is a data link (layer 2) protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption, and compression.

PPPoE

Point-to-Point Protocol over Ethernet. PPPoE is a method of connecting to the Internet, typically used with DSL services, where the client connects to the DSL modem.

PPTP

Point-to-Point Tunneling Protocol. PPTP is a method for implementing virtual private networks. It uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets.

private key

The part of a public-private key pair that is always kept private. The private key encrypts the signature of a message to authenticate the sender. The private key also decrypts a message that was encrypted with the public key of the sender.

PRNG

Pseudo-Random Number Generator. PRNG is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers.

PSK

Pre-shared key. A unique shared secret that was previously shared between two parties by using a secure channel. This is used with WPA security, which requires the owner of a network to provide a passphrase to users for network access.

PSU

Power Supply Unit. PSU is a unit that supplies power to an equipment by converting mains AC to low-voltage regulated DC power.

public key

The part of a public-private key pair that is made public. The public key encrypts a message and the message is decrypted with the private key of the recipient.

PVST

Per-VLAN Spanning Tree. PVST provides load balancing of VLANs across multiple ports resulting in optimal usage of network resources.

PVST+

Per-VLAN Spanning Tree+. PVST+ is an extension of the PVST standard that uses the 802.1Q trunking technology.

QoS

Quality of Service. It refers to the capability of a network to provide better service and performance to a specific network traffic over various technologies.

RA

Router Advertisement. The RA messages are sent by the routers in the network when the hosts send multicast router solicitation to the multicast address of all routers.

Radar

Radio Detection and Ranging. Radar is an object-detection system that uses radio waves to determine the range, angle, or velocity of objects.

RADIUS

Remote Authentication Dial-In User Service. An Industry-standard network access protocol for remote authentication. It allows authentication, authorization, and accounting of remote users who want to access network resources.

RAM

Random Access Memory.

RAPIDS

Rogue Access Point identification and Detection System. An AMP module that is designed to identify and locate wireless threats by making use of all of the information available from your existing infrastructure.

RARP

Reverse Address Resolution Protocol. RARP is a protocol used by a physical machine in a local area network for determining the IP address from the ARP table or cache of the gateway server.

Regex

Regular Expression. Regex refers to a sequence of symbols and characters defining a search pattern.

Registration Authority

Type of Certificate Authority that processes certificate requests. The Registration Authority verifies that requests are valid and comply with certificate policy, and authenticates the user's identity. The Registration Authority then forwards the request to the Certificate Authority to sign and issue the certificate.

Remote AP

Remote APs extend corporate network to the users working from home or at temporary work sites. Remote APs are deployed at branch office sites and are connected to the central network on a WAN link.

REST

Representational State Transfer. REST is a simple and stateless architecture that the web services use for providing interoperability between computer systems on the Internet. In a RESTful web service, requests made to the URI of a resource will elicit a response that may be in XML, HTML, JSON or some other defined format.

RF

Radio Frequency. RF refers to the electromagnetic wave frequencies within a range of 3 kHz to 300 GHz, including the frequencies used for communications or Radar signals.

RFC

Request For Comments. RFC is a commonly used format for the Internet standards documents.

RFID

Radio Frequency Identification. RFID uses radio waves to automatically identify and track the information stored on a tag attached to an object.

RIP

Routing Information Protocol. RIP prevents the routing loops by limiting the number of hops allowed in a path from source to destination.

RJ45

Registered Jack 45. RJ45 is a physical connector for network cables.

RMA

Return Merchandise Authorization. RMA is a part of the product returning process that authorizes users to return a product to the manufacturer or distributor for a refund, replacement, or repair. The customers who want to return a product within its Warranty period contact the manufacturer to initiate the product returning process. The manufacturer or the seller generates an authorization number for the RMA, which is used by the customers, when returning a product to the warehouse.

RMON

Remote Monitoring. RMON provides standard information that a network administrator can use to monitor, analyze, and troubleshoot a group of distributed LANs.

RoW

Rest of World. RoW or RW is an operating country code of a device.

RSA

Rivest, Shamir, Adleman. RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSSI

Received Signal Strength Indicator. RSSI is a mechanism by which RF energy is measured by the circuitry on a wireless NIC (0-255). The RSSI is not standard across vendors. Each vendor determines its own RSSI scale/values.

RSTP

Rapid Spanning Tree Protocol. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this.

RTCP

RTP Control Protocol. RTCP provides out-of-band statistics and control information for an Real-Time Transport Protocol session.

RTLS

Real-Time Location Systems. RTLS automatically identifies and tracks the location of objects or people in real time, usually within a building or other contained area.

RTP

Real-Time Transport Protocol. RTP is a network protocol used for delivering audio and video over IP networks.

RTS

Request to Send. RTS refers to the data transmission and protection mechanism used by the 802.11 wireless networking protocol to prevent frame collision occurrences. See CTS.

RTSP

Real Time Streaming Protocol. RTSP is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.

RVI

Routed VLAN Interface. RVI is a switch interface that forwards packets between VLANs.

RW

Rest of World. RoW or RW is an operating country code of a device.

SA

Security Association. SA is the establishment of shared security attributes between two network entities to support secure communication.

SAML

Security Assertion Markup Language. SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. SAML enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication.

SCEP

Simple Certificate Enrollment Protocol. SCEP is a protocol for requesting and managing digital certificates.

SCP

Secure Copy Protocol. SCP is a network protocol that supports file transfers between hosts on a network.

SCSI

Small Computer System Interface. SCSI refers to a set of interface standards for physical connection and data transfer between a computer and the peripheral devices such as printers, disk drives, CD-ROM, and so on.

SD-WAN

Software-Defined Wide Area Network. SD-WAN is an application for applying SDN technology to WAN connections that connect enterprise networks across disparate geographical locations.

SDN

Software-Defined Networking. SDN is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible as the virtualized server and storage infrastructure of the modern data center.

SDR

Server Derivation Rule. An SDR refers to a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on the rules defined under a server group. The SDRs override the default authentication roles and VLANs defined in the AAA and Virtual AP profiles.

SDU

Service Data Unit. SDU is a unit of data that has been passed down from an OSI layer to a lower layer and that has not yet been encapsulated into a PDU by the lower layer.

SFP

The Small Form-factor Pluggable. SFP is a compact, hot-pluggable transceiver that is used for both telecommunication and data communications applications.

SFP+

Small Form-factor Pluggable+. SFP+ supports up to data rates up to 16 Gbps.

SFTP

Secure File Transfer Protocol. SFTP is a network protocol that allows file access, file transfer, and file management functions over a secure connection.

SHA

Secure Hash Algorithm. SHA is a family of cryptographic hash functions. The SHA algorithm includes the SHA, SHA-1, SHA-2 and SHA-3 variants.

SIM

Subscriber Identity Module. SIM is an integrated circuit that is intended to securely store the International Mobile Subscriber Identity (IMSI) number and its related key, which are used for identifying and authenticating subscribers on mobile telephony devices.

SIP

Session Initiation Protocol. SIP is used for signaling and controlling multimedia communication session such as voice and video calls.

SIRT

Security Incident Response Team. SIRT is responsible for reviewing as well as responding to computer security incident reports and activity.

SKU

Stock Keeping Unit. SKU refers to the product and service identification code for the products in the inventory.

SLAAC

Stateless Address Autoconfiguration. SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router through router advertisements.

SMB

Server Message Block or Small and Medium Business. Server Message Block operates as an application-layer network protocol mainly used for providing shared access to files, printers, serial ports, and for miscellaneous communications between the nodes on a network.

SMS

Short Message Service. SMS refers to short text messages (up to 140 characters) sent and received through mobile phones.

SMTP

Simple Mail Transfer Protocol. SMTP is an Internet standard protocol for electronic mail transmission.

SNIR

Signal-to-Noise-Plus-Interference Ratio. SNIR refers to the power of a central signal of interest divided by the sum of the interference power and the power of the background noise. SINR is defined as the power of a certain signal of interest divided by the sum of the interference power (from all the other interfering signals) and the power of some background noise.

SNMP

Simple Network Management Protocol. SNMP is a TCP/IP standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMPv1

Simple Network Management Protocol version 1. SNMPv1 is a widely used network management protocol.

SNMPv2

Simple Network Management Protocol version 2. SNMPv2 is an enhanced version of SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications.

SNMPv2c

Community-Based Simple Network Management Protocol version 2. SNMPv2C uses the community-based security scheme of SNMPv1 and does not include the SNMPv2 security model.

SNMPv3

Simple Network Management Protocol version 3. SNMPv3 is an enhanced version of SNMP that includes security and remote configuration features.

SNR

Signal-to-Noise Ratio. SNR is used for comparing the level of a desired signal with the level of background noise.

SNTP

Simple Network Time Protocol. SNTP is a less complex implementation of NTP. It uses the same , but does not require the storage of state over extended periods of time.

SOAP

Simple Object Access Protocol. SOAP enables communication between the applications running on different operating systems, with different technologies and programming languages. SOAP is an XML-based messaging protocol for exchanging structured information between the systems that support web services.

SoC

System on a Chip. SoC is an Integrated Circuit that integrates all components of a computer or other electronic system into a single chip.

source NAT

Source NAT changes the source address of the packets passing through the router. Source NAT is typically used when an internal (private) host initiates a session to an external (public) host.

SSH

Secure Shell. SSH is a network protocol that provides secure access to a remote device.

SSID

Service Set Identifier. SSID is a name given to a WLAN and is used by the client to access a WLAN network.

SSL

Secure Sockets Layer. SSL is a computer networking protocol for securing connections between network application clients and servers over the Internet.

SSO

Single Sign-On. SSO is an access-control property that allows the users to log in once to access multiple related, but independent applications or systems to which they have privileges. The process authenticates the user across all allowed resources during their session, eliminating additional login prompts.

STBC

Space-Time Block Coding. STBC is a technique used in wireless communications to transmit multiple copies of a data stream across a number of antennas and to exploit the various received versions of the data to improve the reliability of data transfer.

STM

Station Management. STM is a process that handles AP management and user association.

STP

Spanning Tree Protocol. STP is a network protocol that builds a logical loop-free topology for Ethernet networks.

SU-MIMO

Single-User Multiple-Input Multiple-Output. SU-MIMO allocates the full bandwidth of the AP to a single high-speed device during the allotted time slice.

subnet

Subnet is the logical division of an IP network.

SVP

SpectraLink Voice Priority. SVP is an open, straightforward QoS approach that has been adopted by most leading vendors of WLAN APs. SVP favors isochronous voice packets over asynchronous data packets when contending for the wireless medium and when transmitting packets onto the wired LAN.

SWAN

Structured Wireless-Aware Network. A technology that incorporates a Wireless Local Area Network (WLAN) into a wired Wide Area Network (WAN). SWAN technology can enable an existing wired network to serve hundreds of users, organizations, corporations, or agencies over a large geographic area. SWAN is said to be scalable, secure, and reliable.

TAC

Technical Assistance Center.

TACACS

Terminal Access Controller Access Control System. TACACS is a family of protocols that handles remote authentication and related services for network access control through a centralized server.

TACACS+

Terminal Access Controller Access Control System+. TACACS+ provides separate authentication, authorization, and accounting services. It is derived from, but not backward compatible with, TACACS.

TCP

Transmission Control Protocol. TCP is a communication protocol that defines the standards for establishing and maintaining network connection for applications to exchange data.

TCP/IP

Transmission Control Protocol/ Internet Protocol. TCP/IP is the basic communication language or protocol of the Internet.

TFTP

Trivial File Transfer Protocol. The TFTP is a software utility for transferring files from or to a remote host.

TIM

Traffic Indication Map. TIM is an information element that advertises if any associated stations have buffered unicast frames. APs periodically send the TIM within a beacon to identify the stations that are using power saving mode and the stations that have undelivered data buffered on the AP.

TKIP

Temporal Key Integrity Protocol. A part of the WPA encryption standard for wireless networks. TKIP is the next-generation Wired Equivalent Privacy (WEP) that provides per-packet key mixing to address the flaws encountered in the WEP standard.

TLS

Transport Layer Security. TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections above the Transport Layer by using

asymmetric cryptography for key exchange, symmetric encryption for privacy, and message authentication codes for message integrity.

TLV

Type-length-value or Tag-Length-Value. TLV is an encoding format. It refers to the type of data being processed, the length of the value, and the value for the type of data being processed.

ToS

Type of Service. The ToS field is part of the IPv4 header, which specifies datagrams priority and requests a route for low-delay, high-throughput, or a highly reliable service.

TPC

Transmit Power Control. TPC is a part of the 802.11h amendment. It is used to regulate the power levels used by 802.11a radio cards.

TPM

Trusted Platform Module. TPM is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices.

TSF

Timing Synchronization Function. TSF is a WLAN function that is used for synchronizing the timers for all the stations in a BSS.

TSPEC

Traffic Specification. TSPEC allows an 802.11e client or a QoS-capable wireless client to signal its traffic requirements to the AP.

TSV

Tab-Separated Values. TSV is a file format that allows the exchange of tabular data between applications that use different internal data formats.

TTL

Time to Live. TTL or hop limit is a mechanism that sets limits for data expiry in a computer or network.

TTY

TeleTypeWriter. TTY-enabled devices allow telephones to transmit text communications for people who are deaf or hard of hearing as well as transmit voice communication.

TXOP

Transmission Opportunity. TXOP is used in wireless networks supporting the IEEE 802.11e Quality of Service (QoS) standard. Used in both EDCA and HCF Controlled Channel Access modes of operation, TXOP is a bounded time interval in which stations supporting QoS are permitted to transfer a series of frames. TXOP is defined by a start time and a maximum duration.

U-APSD

Unscheduled Automatic Power Save Delivery. U-APSD is a part of 802.11e and helps considerably in increasing the battery life of VoWLAN terminals.

UAM

Universal Access Method. UAM allows subscribers to access a wireless network after they successfully log in from a web browser.

UCC

Unified Communications and Collaboration. UCC is a term used to describe the integration of various communications methods with collaboration tools such as virtual whiteboards, real-time audio and video conferencing, and enhanced call control capabilities.

UDID

Unique Device Identifier. UDID is used to identify an iOS device.

UDP

User Datagram Protocol. UDP is a part of the TCP/IP family of protocols used for data transfer. UDP is typically used for streaming media. UDP is a stateless protocol, which means it does not acknowledge that the packets being sent have been received.

UDR

User Derivation Rule. UDR is a role assignment model used by the controllers running ArubaOS to assign roles and VLANs to the WLAN users based on MAC address, BSSID, DHCP-Option, encryption type, SSID, and the location of a user. For example, for an SSID with captive portal in the initial role, a UDR can be configured for scanners to provide a role based on their MAC OUI.

UHF

Ultra high frequency. UHF refers to radio frequencies between the range of 300 MHz and 3 GHz. UHF is also known as the decimeter band as the wavelengths range from one meter to one decimeter.

UMTS

Universal Mobile Telecommunication System. UMTS is a third generation mobile cellular system for networks. See 3G.

UPnP

Universal Plug and Play. UPnP is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi APs, and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

URI

Uniform Resource Identifier. URI identifies the name and the location of a resource in a uniform format.

URL

Uniform Resource Locator. URL is a global address used for locating web resources on the Internet.

USB

Universal Serial Bus. USB is a connection standard that offers a common interface for communication between the external devices and a computer. USB is the most common port used in the client devices.

UTC

Coordinated Universal Time. UTC is the primary time standard by which the world regulates clocks and time.

UWB

Ultra-Wideband. UWB is a wireless technology for transmitting large amounts of digital data over a wide spectrum of frequency bands with very low power for a short distance.

VA

Virtual Appliance. VA is a pre-configured virtual machine image, ready to run on a hypervisor.

VBR

Virtual Beacon Report. VBR displays a report with the MAC address details and RSSI information of an AP.

VHT

Very High Throughput. IEEE 802.11ac is an emerging VHT WLAN standard that could achieve physical data rates of close to 7 Gbps for the 5 GHz band.

VIA

Virtual Intranet Access. VIA provides secure remote network connectivity for Android, Apple iOS, Mac OS X, and Windows mobile devices and laptops. It automatically scans and selects the best secure connection to the corporate network.

VLAN

Virtual Local Area Network. In computer networking, a single Layer 2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them through one or more routers; such a domain is referred to as a Virtual Local Area Network, Virtual LAN, or VLAN.

VM

Virtual Machine. A VM is an emulation of a computer system. VMs are based on computer architectures and provide functionality of a physical computer.

VoIP

Voice over IP. VoIP allows transmission of voice and multimedia content over an IP network.

VoWLAN

Voice over WLAN. VoWLAN is a method of routing telephone calls for mobile users over the Internet using the technology specified in IEEE 802.11b. Routing mobile calls over the Internet makes them free, or at least much less expensive than they would be otherwise.

VPN

Virtual Private Network. VPN enables secure access to a corporate network when located remotely. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

VRD

Validated Reference Design. VRDs are guides that capture the best practices for a particular technology in field.

VRF

VisualRF. VRF is an AirWave Management Platform (AMP) module that provides a real-time, network-wide views of your entire Radio Frequency environment along with floor plan editing capabilities. VRF also includes overlays on client health to help diagnose issues related to clients, floor plan, or a specific location.

VRF Plan

VisualRF Plan. A stand-alone Windows client used for basic planning procedures such as adding a floor plan, provisioning APs, and generating a Bill of Materials report.

VRRP

Virtual Router Redundancy Protocol. VRRP is an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN.

VSA

Vendor-Specific Attribute. VSA is a method for communicating vendor-specific information between NASs and RADIUS servers.

VTP

VLAN Trunking Protocol. VTP is a Cisco proprietary protocol for propagating VLANs on a LAN.

W-CDMA

Wideband Code-Division Multiple Access. W-CDMA is a third-generation (3G) mobile wireless technology that promises much higher data speeds to mobile and portable wireless devices.

walled garden

Walled garden is a feature that allows blocking of unauthorized users from accessing network resources.

WAN

Wide Area Network. WAN is a telecommunications network or computer network that extends over a large geographical distance.

WASP

Wireless Application Service Provider. WASP provides a web-based access to applications and services that would otherwise have to be stored locally and makes it possible for customers to access the service from a variety of wireless devices, such as a smartphone or Personal Digital Assistant (PDA).

WAX

Wireless abstract XML. WAX is an abstract markup language and a set of tools that is designed to help wireless application development as well as portability. Its tags perform at a higher level of abstraction than that of other wireless markup languages such as HTML, HDML, WML, XSL, and more.

web service

Web services allow businesses to share and process data programmatically. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

WEP

Wired Equivalent Privacy. WEP is a security protocol that is specified in 802.11b and is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN.

WFA

Wi-Fi Alliance. WFA is a non-profit organization that promotes Wi-Fi technology and certifies Wi-Fi products if they conform to certain standards of interoperability.

Wi-Fi

Wi-Fi is a technology that allows electronic devices to connect to a WLAN network, mainly using the 2.4 GHz and 5 GHz radio bands. Wi-Fi can apply to products that use any 802.11 standard.

WIDS

Wireless Intrusion Detection System. WIDS is an application that detects the attacks on a wireless network or wireless system.

WiMAX

Worldwide Interoperability for Microwave Access. WiMAX refers to the implementation of IEEE 802.16 family of wireless networks standards set by the WiMAX forum.

WIP

Wireless Intrusion Protection. The WIP module provides wired and wireless AP detection, classification, and containment. It detects Denial of Service (DoS) and impersonation attacks, and prevents client and network intrusions.

WIPS

Wireless Intrusion Prevention System. WIPS is a dedicated security device or integrated software application that monitors the radio spectrum of WLAN network for rogue APs and other wireless threats.

WISP

Wireless Internet Service Provider. WISP allows subscribers to connect to a server at designated hotspots using a wireless connection such as Wi-Fi. This type of ISP offers broadband service and allows subscriber computers called stations, to access the Internet and the web from anywhere within the zone of coverage provided by the server antenna, usually a region with a radius of several kilometers.

WISPr

Wireless Internet Service Provider Roaming. The WISPr framework enables the client devices to roam between the wireless hotspots using different ISPs.

WLAN

Wireless Local Area Network. WLAN is a 802.11 standards-based LAN that the users access through a wireless connection.

WME

Wireless Multimedia Extension. WME is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE) and background (AC_BK). See WMM.

WMI

Windows Management Instrumentation. WMI consists of a set of extensions to the Windows Driver Model that provides an operating system interface through which instrumented components provide information and notification.

WMM

Wi-Fi Multimedia. WMM is also known as WME. It refers to a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic QoS features to IEEE 802.11 networks. WMM prioritizes traffic according to four ACs: voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

WPA

Wi-Fi Protected Access. WPA is an interoperable wireless security specification subset of the IEEE 802.11 standard. This standard provides authentication capabilities and uses TKIP for data encryption.

WPA2

Wi-Fi Protected Access 2. WPA2 is a certification program maintained by IEEE that oversees standards for security over wireless networks. WPA2 supports IEEE 802.1X/EAP authentication or PSK technology, but includes advanced encryption mechanism using CCMP that is referred to as AES.

WSDL

Web Service Description Language. WSDL is an XML-based interface definition language used to describe the functionality provided by a web service.

WSP

Wireless Service Provider. The service provider company that offers transmission services to users of wireless devices through Radio Frequency (RF) signals rather than through end-to-end wire communication.

WWW

World Wide Web.

X.509

X.509 is a standard for a public key infrastructure for managing digital certificates and public-key encryption. It is an essential part of the Transport Layer Security protocol used to secure web and email communication.

XAuth

Extended Authentication. XAuth provides a mechanism for requesting individual authentication information from the user, and a local user database or an external authentication server. It provides a method for storing the authentication information centrally in the local network.

XML

Extensible Markup Language. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

XML-RPC

XML Remote Procedure Call. XML-RPC is a protocol that uses XML to encode its calls and HTTP as a transport mechanism. Developers who want to provide integrated applications can use the API to programmatically perform actions that would otherwise require manual operation of the user interface.

ZTP

Zero Touch Provisioning. ZTP is a device provisioning mechanism that allows automatic and quick provisioning of devices with a minimal or at times no manual intervention.