Aruba Central

a Hewlett Packard
Enterprise company

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 Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company

Attn: General Counsel

3000 Hanover Street

Palo Alto, CA 94304

USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at dl-gplquery@arubanetworks.com.

This document describes how to sign up for Aruba Central subscription, manage your subscriptions and licenses, and provision devices such as Aruba Access Points and Switches.

Intended Audience

This guide is intended for customers who use Aruba Central to manage and configure devices.

Related Documents

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

- *Aruba Central User Guide*
- *Aruba Central Online Help*
- *Aruba Central Release Notes*

Conventions

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

Table 1: *Typographical Conventions*

Type Style	Description
Italics	This style is used to emphasize important terms and to mark the titles of books.
`System items`	This fixed-width font depicts the following: • 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 Aruba Networks

Table 2: *Contact Information*

Main Site	http://www.arubanetworks.com/
Support Site	https://support.arubanetworks.com/
Airheads Social Forums and Knowledge Base	http://community.arubanetworks.com/
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	http://www.arubanetworks.com/support-services/contact-support/
Software Licensing Site	https://licensing.arubanetworks.com/
End-of-life Information	http://www.arubanetworks.com/support-services/end-of-life/
Security Incident Response Team (SIRT)	http://www.arubanetworks.com/support-services/security-bulletins/
Support Email Addresses	
Americas, EMEA, and APAC	support@arubanetworks.com
Security Incident Response Team (SIRT)	sirt@arubanetworks.com

Aruba Central is a cloud-based platform that enables you to manage your Aruba wireless network. Designed as a software-as-a-service (SAAS) subscription, Central provides a standard web-based interface that allows you to configure and monitor multiple Aruba Wi-Fi networks from anywhere, provided you have an Internet connection.

Central offers the following key features:

- Streamlined management of devices
- Dashboard view of network and client health
- Easy grouping of devices
- Centralized configuration and firmware updates
- Guest Wi-Fi access configuration
- Reporting
- Remote troubleshooting and client information
- API gateway to manage APIs

Supported Devices

Central supports the following Access Points (APs) and Switch platforms.

Supported IAPs

The current release of Central supports the following IAP platforms:

- IAP-324/325
- IAP-277
- IAP-228
- IAP-205H
- IAP-103 Series
- IAP-114/115
- IAP-204/205
- IAP-214/215
- IAP-274/275
- IAP-224/225
- RAP-3WN/3WNP
- RAP-108/109
- RAP-155/155P
- IAP-175P/175AC
- IAP-134/135
- IAP-104/105
- IAP-92/93

Supported IAP Versions

The current release of Central supports only the following IAP firmware versions:

- 6.4.2.0-4.1.1.9 or later
- 6.4.2.3-4.1.2.3
- 6.4.3.1-4.2.0.3
- 6.4.3.4-4.2.1.0
- 6.4.4.3-4.2.2.0
- 6.4.4.4-4.2.3.0
- 6.4.4.4-4.2.3.1
- 6.4.4.4-4.2.3.2
- 6.4.4.6-4.2.4.0

Supported Switches

The following sections list the Switch models supported in Central.

New Switch Platforms

- Aruba 2920 Switch Series
- Aruba 2930F Switch Series

Supported Firmware Versions

Central supports the following firmware versions on Aruba switches:

- Aruba 2920 Switch Series—WB.16.02.0010 or later
- Aruba 2930F Switch Series—WC.16.02.0010 or later

Legacy Aruba Switch Platforms

Central also supports the following legacy Switch models:

- S1500-12P
- S1200-24P
- S2500-24P
- S3500-24T

Supported Firmware Versions

The following ArubaOS software versions are supported on the legacy Switch platforms:

- 7.3.2.6
- 7.4.0.3
- 7.4.1.4

Central offers a 90-day evaluation license for customers who want to try the Aruba cloud solution for managing their Wi-Fi networks. When you create an account with Central, an evaluation license is automatically assigned, unless you have a paid subscription. To obtain license keys, contact the Aruba IT team.

Signing up for Aruba Central

To sign up as a customer for Central:

1. Go to http://www.arubanetworks.com/products/sme/eval/.
2. Enter your email address and click **Continue**.

- If you are signing up for Central for the first time, the registration page is displayed. Complete the registration process (see step 3 through step 8).
- If you are an existing customer and your email address is already in the Central database, and you have verified your email address, the Central login page is displayed.
- If your email address already exists in the Central database and you have not verified your email address, click **Resend Verification Email** and verify your email address by clicking the **Activate Your Account** link.
- If you are an existing Aruba customer with SSO login credentials and you are signing up for Central for the first time:
  - Validate your account by providing your SSO password. On successful authentication, the registration page is displayed. Complete the registration process to gain access to Central (see step 3 through step 8).
  - If you have forgotten your SSO password, click **Forgot Password** and complete the steps to retrieve your password.
  - To sign up again, click **Try Signing up again** and complete the steps to sign up for an Central account.

3. On the Registration page, enter first name, last name, and address details. If you are a new user, enter the password. For registered users and those with SSO login credentials, the **Password** field is disabled.
4. If you have Aruba Activate user credentials, select **I have an Aruba Activate account** check box and enter your user name and password for the Activate account.

You can use your Aruba Activate account to manually import devices into Central. However, Central allows each user account to import devices using Aruba Activate account only once.

5. Select the **I agree to the Terms and Conditions** check box.
6. Click **Sign Up**. On successfully completing the registration, a verification email is sent to your email address.
7. Access your email account and click the **Activate Your Account** link. If the email verification is successful, the **Log in to Aruba Central** button is displayed.
8. Click **Log in to Aruba Central** and provide your registered user name and password. If an account has multiple customers configured , the accounts selection page is displayed.
9. Select an account to access the Central dashboard.

When you sign up for Aruba Central, a user account on Aruba Centraland Aruba Activate is created.

Binding Devices to Your License

After you successfully log in to Central, a welcome message is displayed in the Central UI. To bind devices to your license, click **Manage Your License**. The **Device Management** pane is displayed. To view the subscription key details before binding devices, click **Subscription Keys**.

Central supports zero touch provisioning of the devices. It automatically retrieves the devices associated with your license and Central subscription. However, if the retrieval of devices is not complete or successful due to process errors, you can manually add the devices.

Central allows you to import devices using your Aruba Activate user credentials, the MAC address and cloud activation key of a device, or the MAC address and Serial Number of a device. You can specify the method for importing devices when adding a device.

For users with the evaluation subscription, the devices are not automatically synchronized. Therefore, the users must manually add the devices.

The evaluation subscription key allows you to add only five IAP devices and two Aruba Switches.

For IAPs that dynamically form a cluster, the users must add the master IAP from the **Device Management** page every time a slave IAP joins the cluster, so that the slave IAP details are synchronized.

To manually add a device:

1. In the **Device Management** page, click **Add Devices**. The **Manually Add Devices** window opens. Select one of the following device addition options:

Table 3: *Adding Devices*

Device Addition Option	Description
Aruba Activate Credentials	To retrieve all devices associated to an Activate user account: 1. Select **Aruba Activate Credentials** from the **Add devices using** drop-down list. 2. Enter the username and password of the Activate user account. 3. Click **Next**. The Activate account details and the total number of devices associated with this account are displayed. 4. To add all devices, click **Add <Number> Devices** button. The devices associated with the Activate account are retrieved and added to the list of devices displayed on the **Device Management** page. **NOTE:** You can use this option only once. After the devices are added, Central does not allow you to modify or re-import the devices using your Aruba Activate credentials.
Bulk addition of devices based on cloud activation key	To retrieve multiple devices from a single purchase order by providing the cloud activation key: 1. Note the Cloud Activation Key and MAC address of the device. To obtain these details: ● For IAPs, execute the **show about** command at the IAP CLI or click **Maintenance >About** in the IAP UI. ● For legacy Switches, execute the **show inventory | include HW** and **show version** commands on the Switch CLI. ● For the other ArubaSwitches, to view the MAC address and the serial number, run the **sh system | in Base** and **sh system | in Serial** commands at the CLI. You can also view the cloud activation key in the **Maintenance** > **About** tab of the switch UI. The activation key is enabled only if the Switch has access to the Internet. 2. Select **Cloud Activation Key** from the **Add devices using** drop-down list. 3. Enter the **MAC address** and **Cloud Activation Key** of the device. 4. Click **Next**. Central retrieves all devices that belong to the same purchase order and displays the list. A list of blocked devices is displayed if any of the device belongs to another customer account or is used by other services. As Central does not allow you to add blocked devices, you may have to release the blocked devices from another customer account. 5. To continue adding devices, click **Add <x> Devices**. 6. To restart the device addition procedure, click **Start Again**.
Adding up to 32 devices	To manually add devices by using the serial number and MAC address of the device: 1. Select **Device List (Up to 32 Devices)** from the **Add device using** drop-down list. 2. Enter the MAC address and serial number of the device. 3. Click **Next**. The list of available devices is displayed. 4. Click **Add <x> Devices**. **NOTE:** Central allows you to add up to 32 devices.

5. To assign a license to the device, select the device and click **Assign License(s)**.

The provisioning of the legacy Aruba 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.

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

Adding User Accounts

To add user accounts to your license, complete the following steps:

1. Click **Maintenance > User Management**.
2. On the **User Management** pane, click **Add User**. The **Create User** window is displayed.

3. Enter the email address of the user in the **Username** text box.
4. From the **User Scope** drop-down list, select the group to which you want to assign the user.
5. Select the user access level that you want to assign to the user from the **Access Level** drop-down list.

Central supports following types of users:

- **Admin**—The Admin users have full access to all the groups and have special rights to create or update user details, groups, and to provision devices.
- **Read/Write**—The users with read/write privileges can access the groups or devices assigned by the Admin user. The users with Read/Write privileges can perform operations that can change the behavior of devices or groups such as modifying the configuration of a device, deleting a device and so on.
- **Read only**—The users with read-only privileges can access the groups or devices assigned by the Admin user and view details of the groups and devices.
- **Guest operator**—The guest operators have access to guest management operations only. These users can add guest users and configure splash page profiles.

A user cannot have different access rights for different groups.

6. Click **Save**. When the user account is successfully created:

- New users will receive a welcome email with the registration link. Complete the registration steps described in step 7 through step 11.
- Users with an existing Central account will receive an email invite with a link to the Central portal. Click the link to access the Central UI.

If the user has not received the registration email, click **Resend Invite Email** in the **User Management** pane to resend the invite.

7. To register, click **Register Your Account** link. The **Sign up with Aruba Central** page is displayed.
8. Enter the password, , first name, last name, and address details.
9. Select a country and state.
10. Select the **I agree to the Terms and Conditions** check box.
11. Click **Sign Up**. On successful completion of registration, the user account is created.
12. Log in to Central with the registered credentials.

Creating Additional Customer Accounts

If you want to manage Wi-Fi networks in multiple regions, you can create additional customer accounts. Central allows you to create up to five customer accounts.

To create an additional customer account:

1. Click the **Settings** icon next to your user name on the main pane. Click **Switch Customer**. The customer account selection page is displayed.
2. Click the + icon to add a new account. The **Sign up with Aruba Central** page is displayed.
3. Enter your address, and select the country and state.
4. Enter the city and ZIP code details.
5. Select the **I agree to the Terms and Conditions** check box.
6. Click **Sign Up**. The customer account is added.
7. Repeat the procedure to add another customer account.

To log in with a different customer account, click **Switch Customer** and click the account that you want to access.

You can provision devices automatically or manually connect the devices to an existing provisioning network. When you manually connect an IAP to an existing network on the same VLAN or subnet, the new IAP joins the existing operational cluster.

The IAPs boot with factory default configuration and will try to provision automatically. If the automatic provisioning is successful, the default SSID (instant) will not be available. This SSID needs to be configured through Central. If Central is not reachable and the automatic provisioning fails, the instant SSID becomes available and the users can connect to a provisioning network by using the instant SSID.

Creating a WLAN SSID

To create a wireless network in the Central UI:

1. From the Central UI main window, navigate to **Configuration > Networks**.
2. Select a group to which you want apply the new SSID configuration.
3. Click the + icon. The **Create A New Network** page is displayed.
4. Under **General** > **Basic Settings**, enter a name (SSID) for the network. This name is used for identifying the network.
5. Select the type of network as **Wireless**.
6. For **Primary Usage**, select any of the following options:
   - Employee
   - Guest
7. Click **Next**. The **VLANs** tab is displayed.
8. Configure the IP assignment and VLAN assignment methods for the IAP clients.
9. Click **Next**. The **Security** tab is displayed.
10. On the **Security** tab, enter a unique passphrase and retype it to confirm. You can use the default values or customize security settings as per your requirement.
11. Click **Next**. The **Access** tab is displayed.
12. On the **Access** tab, select **Unrestricted** to configure unrestricted access control.
13. Click **Finish**. The new network is added and displayed in the Networks page.

For more information on configuring APs, see the *Aruba Central User Guide*.

Verifying the Operational State of IAPs

After setting up an IAP and creating a wireless networks, use the LEDs to verify if the IAPs are operational.

Verifying AP Status Using LEDs

You can use the LEDs to verify that both radios are active after the IAP initialization and configuration. For information on the IAP LED status indicators, see the IAP Installation Guide available with the IAP package.

On extending or renewing the subscription, a new subscription key is assigned and is sent to the user. To activate the subscription key:

1. Click **Maintenance** > **Subscription**. The **Subscription Keys** pane is displayed.
2. Click **Add Another Subscription Key** and enter the subscription ID.
3. Click **Activate**. The subscription key is added to the list.

Acronyms and Abbreviations

The following table lists the acronyms and abbreviations used in this guide.

Table 4: *Acronyms And Abbreviations*

Abbreviation	Expansion
AP	Access Point
ARM	Adaptive Radio Management
ARP	Address Resolution Protocol
BSS	Basic Server Set
BSSID	Basic Server Set Identifier
CA	Certification Authority
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
EAP-TLS	Extensible Authentication Protocol- Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol-Tunneled Transport Layer Security
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
LEAP	Lightweight Extensible Authentication Protocol
MX	Mail Exchanger

Table 4: *Acronyms And Abbreviations*

Abbreviation	Expansion
MAC	Media Access Control
NAS	Network Access Server
NAT	Network Address Translation
NS	Name Server
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PoE	Power over Ethernet
RADIUS	Remote Authentication Dial In User Service
VC	Virtual Controller
VSA	Vendor-Specific Attributes
WLAN	Wireless Local Area Network

Glossary

The following table lists the terms and their definitions in this guide.

Table 5: *Terms And Definitions*

Term	Definition
802.11	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 CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing.
802.11a	Provides specifications for wireless systems. Networks using 802.11a operate at radio frequencies in the 5GHz 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.
802.11b	WLAN standard often called Wi-Fi; backward compatible with 802.11. Instead of the phase-shift keying (PSK) modulation method historically used in 802.11 standards, 802.11b uses complementary code keying (CCK), which allows higher data speeds and is less susceptible to multipath-propagation interference. 802.11b operates in the 2.4 GHz band and the maximum data transfer rate is 11 Mbps.
802.11g	Offers transmission over relatively short distances at up to 54 Mbps, compared with the 11 Mbps theoretical maximum of 802.11b. 802.11g operates in the 2.4 GHz band and 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 speeds of 11 Mbps, so that 802.11b and 802.11g devices can be compatible within a single network.
802.11n	Wireless networking standard to improve network throughput over the two previous standards 802.11a and 802.11g with 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. 802.11n operates in the 2.4 and 5.0 bands.
AP	An access point (AP) connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.
access point mapping	The act of locating and possibly exploiting connections to WLANs while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. Because a WLAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.

Table 5: *Terms And Definitions*

Term	Definition
ad-hoc network	A LAN or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network.
band	A specified range of frequencies of electromagnetic radiation.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is an auto-configuration protocol used on IP networks. Computers or any network peripherals that are connected to IP networks must be configured, before they can communicate with other computers on the network. DHCP allows a computer to be configured automatically, eliminating the need for a network administrator. DHCP also provides a central database to keep track of computers connected to the network. This database helps in preventing any two computers from being configured with the same IP address.
DNS Server	A Domain Name System (DNS) server functions as a phonebook for the Internet and Internet users. It converts human readable computer hostnames into IP addresses and vice-versa. A DNS server 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.
DST	Daylight saving time (DST), also known as summer time, is 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.
EAP	Extensible authentication protocol (EAP) refers to the authentication protocol in wireless networks that expands on methods used by the point-to-point protocol (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.
fixed wireless	Wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are compromised compared with fixed systems.
frequency allocation	Use of radio frequency spectrum regulated by governments.
frequency spectrum	Part of the electromagnetic spectrum.

Table 5: *Terms And Definitions*

Term	Definition
hotspot	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 hot spot, contact it, and get connected through its network to reach the Internet and their own company remotely with a secure connection. Increasingly, public places, such as airports, hotels, and coffee shops are providing free wireless access for customers.
IEEE 802.11 standards	The IEEE 802.11 is a set of standards that are categorized based on the radio wave frequency and the data transfer rate.
POE	Power over Ethernet (PoE) is a method of delivering power on the same physical Ethernet wire used for data communication. Power for devices is provided in one of the following two ways: • Endspan— The switch that an AP is connected for power supply. • Midspan— A device can sit between the switch and APs The choice of endspan or midspan depends on the capabilities of the switch to which the IAP is connected. Typically if a switch is in place and does not support PoE, midspan power injectors are used.
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.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to a specific network traffic over various technologies.
RF	Radio Frequency (RF) refers to the portion of electromagnetic spectrum in which electromagnetic waves are generated by feeding alternating current to an antenna.
VPN	A Virtual Private Network (VPN) network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). Data is encrypted at the sending end and decrypted at the receiving end.
W-CDMA	Officially known as IMT-2000 direct spread; ITU standard derived from Code-Division Multiple Access (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 than commonly offered in today's market.
Wi-Fi	A term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.

Table 5: *Terms And Definitions*

Term	Definition
WEP	Wired equivalent privacy (WEP) is a security protocol specified in 802.11b, designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.
wireless	Describes telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
wireless network	In a Wireless LAN (WLAN), laptops, desktops, PDAs, and other computer peripherals are connected to each other without any network cables. These network elements or clients use radio signals to communicate with each other. Wireless networks are set up based on the IEEE 802.11 standards.
WISP	Wireless ISP (WISP) refers to an Internet service provider (ISP) that allows subscribers to connect to a server at designated hot spots (access points) 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.
wireless service provider	A company that offers transmission services to users of wireless devices through radio frequency (RF) signals rather than through end-to-end wire communication.
WLAN	Wireless local area network (WLAN) is a Local Area Network (LAN) that the users access through a wireless connection.