ArubaOS 8.10.0.0 Getting Started Guide

a Hewlett Packard
Enterprise company

Copyright Information

Open Source Code

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

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
About This Guide

This document describes the initial setup of an Aruba user-centric network that consists of an Aruba managed device and Aruba Access Points (APs).

Following are the topics covered in this guide:

- Installing Mobility Conductor and Managed Devices
- Initial Setup
- Manual Setup
- Automatic Setup
- Configuring the Managed Devices and APs

Related Documents

The following guides are part of the complete documentation for the Aruba user-centric network:

- *ArubaOS 8.10.0.0 Getting Started Guide Release Notes*
- *ArubaOS User Guide*
- *ArubaOS CLI Reference Guide*
- *ArubaOS API Guide*
- *Aruba Mobility Conductor Licensing Guide*
- *Aruba Virtual Appliance Installation Guide*
- *Aruba Mobility Conductor Hardware Appliance Installation Guide*
- *Aruba Wireless Access Point Installation Guide*

Supported Browsers

The following browsers are officially supported for use with the ArubaOS WebUI:

- Microsoft Internet Explorer 11 on Windows 7 and Windows 8
- Microsoft Edge (Microsoft Edge 92.0.902.62 and Microsoft EdgeHTML 18.19041) on Windows 10
- Firefox (91.0) on Windows 7, Windows 8, Windows 10, and macOS
- Apple Safari 8.0 or later on macOS
- Google Chrome (92.0.4515.131) on Windows 7, Windows 8, Windows 10, and macOS

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	https://asp.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

Overview

This section provides an overview on how to install the Mobility Conductor and managed devices.

Perform the following steps to install the Mobility Conductor and managed devices:

1. Launch the WebUI or Console Setup Wizard to configure the managed device.
2. Connect the managed device to the wired network.
3. Configure the managed device to the Mobility Conductor. The Mobility Conductor - Managed Device topology or stand-alone controller topology is supported.
4. If it is a stand-alone controller deployment, installing the Mobility Conductor is not required.
5. Install and connect your APs to the network.

Installing Mobility Conductor and Managed Devices

The Aruba Mobility Conductor provides a 64-bit virtualized software-based managed platform on VM architecture.

The Mobility Conductor is the centralized management platform for the deployment in the virtualized network infrastructure. The Mobility Conductor operates on the VM platforms in the VMware environment and can reside with other virtualized appliances.

Installing the Managed Devices

The WebUI Startup Wizard allows you to configure access to the managed device. The Startup Wizard is available the first time you connect to and log into the managed device or whenever the managed device is reset to its factory default configuration. The serial console setup dialog allows you to configure basic managed device settings through a serial port connection to the managed device.

NOTE

The Startup Wizard works only on 0/0/1 port on all controllers,

After you complete the Startup Wizard or serial console setup procedure, the managed device reboots using the new configuration information you entered.

Do not connect the managed device to your network when running the Setup Wizard or serial console setup dialog. The factory-default managed device boots up with a default IP address and both DHCP server and spanning tree functions enabled. Once you have completed setup and rebooted the managed device, the managed device should appear on the Mobility Conductor for the management of managed device from the Mobility Conductor.

In addition to the traditional method mentioned above, the 7000 Series controllers running ArubaOS 8.9.0.0 can be configured without user intervention with zero touch provisioning (ZTP). This option automatically configures the managed device using Activate. For more details, see Automatic Setup.

Chapter 2
Initial Setup

You can launch the setup wizard using any PC or workstation that can run a supported Web browser.

The PC or workstation must either be configured to obtain its IP address using DHCP, or configured to have a static IP address on the 172.16.0.254/24 sub-network. The default IP address of the managed device is 172.16.0.254/24. Connect a PC or workstation to 0/0/1 port on the managed device, then enter this IP address into a supported Web browser to launch the Setup Wizard.

To run the Setup Wizard:

1. Connect your PC or workstation to 0/0/1 port on the managed device.
2. Make sure that the managed device is not connected to any device on your network.
3. Boot up the managed device.
4. On your PC or workstation, open a Web browser and connect to https://172.16.0.254/24.
5. The initial window of the **Mobility Controller Setup** Wizard asks you to select one of the following deployment modes. Select **Standalone** or **Managed** then click **Continue**.
   - **Standalone Controller**: This is the only controller on the network.
   - **Managed Controller**: This managed device will be managed by a Mobility Conductor.

Initial Setup on a Serial Port Connection

The serial port is located on the front panel (back panel in case of 7024 and 7008 controllers) of the managed device. You can start the Initial Setup dialog when you connect a terminal, PC or workstation running a terminal emulation program to the serial port on the managed device.

The serial port connection only allows you to configure the basic configuration required to connect the managed device to the network. The recommended browser-based configuration Wizard allows you to also install software licenses and configure internal and guest WLANs. If you use the Initial Setup dialog to configure the managed device, the browser-based Setup Wizard will not be available unless you reset the managed device to its factory default configuration.

To run the Initial full setup dialog from a serial connection:

1. Configure your terminal or terminal emulation program to use the following communication settings:

Table 3: *Terminal Communication Settings*

Baud Rate	Data Bits	Parity	Stop Bits	Flow Control
9600	8	None	1	None

2. Connect your terminal or PC/workstation to the serial port on the managed devices using an RS-232 serial cable. RJ-45 cable and DB-9 to RJ-45 adapter is required. You may need a USB adapter to connect the serial cable to your PC.
3. Boot up the managed device. After the managed device has booted up, you should see a screen similar to the following setup dialog for managed devices:

```
Auto-provisioning is in progress. Choose one of the following options to override or
debug...
```

```
'enable-debug' : Enable auto-provisioning debug logs
'disable-debug': Disable auto-provisioning debug logs
'mini-setup'   : Stop auto-provisioning and start mini setup dialog for smart-branch role
'full-setup'   : Stop auto-provisioning and start full setup dialog for any role

Enter Option (partial string is acceptable):f
Are you sure that you want to stop auto-provisioning and start full setup dialog?
(yes/no): y
Reading configuration from factory-default.cfg
```

4. (Applicable to managed devices using ZTP) enter **f** to invoke full-setup.

5. The Serial Port Configuration Dialog displays the configuration prompts. The prompts may vary, depending upon the switch role you choose. Enter the required information at each prompt, then press **Enter** to continue to the next question.

Table 4: *Serial Console Configuration Dialog*

Console Prompt	Description
Enter System Name	Enter a name for the managed device, or press **Enter** to use the default system name. You can specify a name of up to 63 characters.
Enter Switch Role, (stand-alone|md)	Specify one of the following roles: **Stand-alone:** This is the only self-managed controller on your network. **md:** This device will be managed by a Mobility Conductor. You are prompted to specify the type of authentication to be used by the managed device. If you are configuring a managed device to use pre-shared key authentication to communicate with the Mobility Conductor, enter the IP address of the Mobility Conductor and the pre-shared key. If you are configuring a managed device to use certificate authentication, specify the MAC addresses of the Mobility Conductor.
IP type to terminate IPSec tunnel	Specify if the IP type to which the IPsec tunnels use to terminate. The IP types are IPv4 and IPv6.
Conductor switch IP address or FQDN	Specify the IP or fully qualified name of the Mobility Conductor.
Is this a VPN concentrator for managed device to reach Conductor switch	Enter **No**. Most of the installations would not have a VPN concentrator installed. **NOTE:** Enter **Yes** only if a VPN concentrator is installed in the network.
Conductor switch Authentication method	Provide a choice of PSKwithIP or PSKwithMAC. If you choose PSKwithMAC, then the peer MAC address value to be configured on a device for tunnel establishment is based on the platform type of the peer device. For more information on the type of MAC address to be configured as peer MAC address, see *Peer MAC Address Configuration for PSK with MAC*.
IPsec Pre-shared Key	Security key for the IPsec tunnel between the managed device and the Mobility Conductor, 6 to 64 characters.
Uplink Vlan ID	Specify the VLAN ID which is an integer. Value range- 1 to 4094

Console Prompt	Description
Uplink port	The value is not 1 or 0, value should be 1/0 or 0/0/0 or any port based on the managed device platforms.
Uplink port mode	Specify the port mode as either Access or Trunk. In trunk mode, a port can carry traffic for multiple VLANs. In access mode, the port forwards untagged packets received to the managed device and they appear on the configured access mode VLAN.
Enter Native VLAN ID [1]	Specify a particular vlan to be configured as a native vlan.
Uplink Vlan IP assignment method	Assign manually the IP addressing of the uplink or via DHCP.
Uplink Vlan Static IP address	The managed device takes its IP address from VLAN 1 and uses this IP address to communicate with other managed devices and with APs. Enter an IPv4 VLAN 1 interface IP address, or press **Enter** without specifying an IP address to use the default address 172.16.0.254/24.
Uplink Vlan Static IP netmask	Enter an IPv4 VLAN 1 interface IP subnet mask, or press Enter without specifying an IP address to use the default address 255.255.255.0.
IP default gateway	This is usually the IP address of the interface on the upstream switch or router to which you will connect the managed devices. The default gateway and the VLAN 1 IP address need to be in the same network. Enter an IPv4 gateway IP address, or press Enter to continue without specifying an IP gateway.
DNS IP address	IP address of the DNS server.
IPV6 address on vlan	IPv6 address of the managed device.
Do you want to configure port-channel (yes|no) [no]	Specify if you want to configure the port-channel. LACP will be configured on port members with port-channel ID as LACP group ID.
Enter Port-channel ID [0]	Specify the port-channel ID.
Uplink Vlan Static IPv6 address	The managed device takes its IP address from VLAN 1 and uses this IP address to communicate with other managed devices and with APs. Supported subnets are: Global Unicast: 2000::/3, Unique local unicast: fc00::/7 Enter an IPv6 VLAN 1 interface IP address, or press **Enter** without specifying an IP address to use the default address 2000::1.
Uplink Vlan interface IPV6 prefix length	Enter a value from 0 to 128 to define an IPv6 VLAN 1 interface IP prefix length, or press **Enter** without specifying a prefix length to use the default value of 64.
IPv6 default gateway	This optional value is usually the IP address of the interface on the upstream switch or router to which you will connect the managed device. The default gateway and the VLAN 1 IP address need to be in the same network. Enter an IPv6 gateway IP address to configure this setting, or press **Enter** to continue without specifying an IP gateway.

Console Prompt	Description
Country code	If your managed device has a country code that restricts its usage, enter **yes** to confirm this code.
Time Zone	Enter the time zone for the managed device, or press **Enter** to select the default time zone.
Time in UTC	Enter the current time in UTC format, or press **Enter** to select the default time.
Date	Enter the current date, or press **Enter** to select the default date.
Password for admin login	Enter a password to allow the admin user to login to the WebUI, CLI and console interfaces. This password can be up to 32 alphanumeric characters long.
Re-type password for admin login	Confirmation for the admin login password

6. At the end of the Initial Setup, you are asked to review and confirm your configuration changes. Enter **y** to accept the changes. The managed device reboots.

NOTE

If you want to complete optional configuration options (e.g. disabling spanning tree or installing software licenses) before connecting the managed device to the network, refer to the *ArubaOS 8.9.0.0 User Guide* for additional information on configuration.

Chapter 3
Manual Setup

Following lists the high-level configurations to be performed to setup either a managed device or a stand-alone controller manually:

1. Add the system information
2. Add the Mobility Conductor information
3. Add the Uplink information
4. Add the AirWave information

If you select **Stand-alone Controller** or **Managed Controller** in the initial window of the **Mobility Controller Setup** Wizard, you will be prompted to enter the information described in the following sections.

Add System Information

You can add the system information like Host name, country code, password, clock information.

Table 5: *Controller Information*

Requirement	Description
System Information	
Host Name	A user-defined name by which the managed device will be referenced. You can specify a name of up to 63 characters.
Country Code	The country in which the managed device will operate. The country code determines the 802.11 wireless transmission spectrum. You cannot change the country code for managed devices designated for certain countries, such as the U.S. or Israel. Improper country code assignment can disrupt wireless transmissions. Most countries impose penalties and sanctions for operators of wireless networks with devices set to improper country codes.
Admin Password	Password of up to 32 characters for the admin user to log in to the managed device.
Clock	
Time	You can either manually set the date, time, and GMT time zone.
NTP server IP address	Enter the IP address of an NTP server from which the managed device will obtain its date and time settings.
Timezone	Enter the GMT time zone.

NOTE

The default certificate installed in the managed device does not guarantee security in production networks. Aruba strongly recommends that you replace the default certificate with a custom certificate issued for your site or domain by a trusted Certificate Authority. See the *ArubaOS 8.9.0.0 User Guide* for more information about certificates.

Add Mobility Conductor Information

After entering the system information, you will be prompted to add the details of the Mobility Conductor so that the managed device can connect with the Mobility Conductor.

Table 6: *Mobility Conductor Information*

Requirement	Description
Connection to Mobility Conductor	Determine if the connectivity to the Mobility Conductor is direct or via a VPN concentrator.
Connection to Mobility Conductor is Direct	
Conductor IPv4 address	Specify the IPv4 address or fully qualified domain name of the Mobility Conductor.
Conductor IPv6 address	Optionally, specify the IPv6 address or fully qualified domain name of the Mobility Conductor on IPv6 networks.
Conductor is a virtual machine	Select **Yes** or **No** to specify whether the Mobility Conductor is a virtual machine or not.
IPSec key	Security key for the IPsec tunnel between the managed device and the Mobility Conductor. This field supports 6 to 64 characters.
Retype IPSec key	Confirmation of the security key.
Authentication	Provide a choice of **Factory certificate** or **Pre-Shared Key**. **NOTE:** This option is displayed when **Conductor is a virtual machine** is set to **No**.
Conductor MAC address	Specify the MAC of the Mobility Conductor.
Redundant conductor MAC address	Optionally, specify the MAC of the redundant Mobility Conductor.
Connection to Mobility Conductor is Via VPN Concentrator	
Conductor IPv4 address	Specify the IPv4 address or fully qualified domain name of the Mobility Conductor.
Conductor IPv6 address	Optionally, specify the IPv6 address or fully qualified domain name of the Mobility Conductor on IPv6 networks.
Concentrator IPv4 address	Specify the IPv4 address of the VPN concentrator to connect to, in order to reach the Mobility Conductor.
Concentrator IPv6 address	Specify the IPv6 address of the VPN concentrator to connect to, in order to reach the Mobility Conductor on IPv6 networks.
Concentrator MAC address	Specify the IP address of the VPN concentrator to connect to in order to reach the Mobility Conductor.
Redundant concentrator MAC address	Optionally, specify the MAC address of the eventual redundant VPN concentrator.
Authentication	Provide a choice of **Factory certificate** or **Pre-Shared Key**.

Requirement	Description
IPSec key	Security key for the IPsec tunnel between the managed device and the VPN concentrator, 6 to 64 characters.
Retype IPSec key	Confirmation of the security key.

Add Uplink Information

After adding the Mobility Conductor information, click **Next** and specify the uplink setting for the managed device to reach the Mobility Conductor.

Table 7: *Uplink Settings Information*

Requirement	Description
Uplink VLAN ID	Specify the VLAN ID which is an integer. Value range- 1 to 4094.
Port	Specify the default communication interface.
Port mode	Specify the port mode as either **Access** or **Trunk**.
IP address assignment	Select Static IP addressing or via DHCP.
VLAN IPv4 address	Specify the managed device’s IPv4 address.
Netmask	Specify the Netmask used to calculate the IP subnet.
IPv4 default gateway	Specify the default IPv4 gateway used to setup default routes.
DNS IPv4 address	Specify the IPv4 address of the DNS server.
VLAN IPv6 address	Specify the managed device’s IP address on IPv6 networks.
IPv6 prefix	Specify IPv6 VLAN 1 interface IP prefix length.
IPv6 default gateway	Specify the default gateway on IPv6 networks.
DNS IPv6 address	Specify the IPv6 address of the DNS server.

NOTE

A summary of the setup is displayed after you add the Uplink information.

Add AirWave Information

The following step applies only to stand-alone controllers. After you have completed the basic configuration, you will be prompted to add the AirWave information as described in the below table:

Table 8: *AirWave Stand-alone Controller Information*

Requirement	Description
Connect to AirWave	Specify if this controller is managed via an AirWave platform or not.

Requirement	Description
AirWave IP address	Specify the IPv4 or IPv6 address of the AirWave platform.
SNMP version	Specify which SNMP protocol version is used (v2 or v3).
SNMP version v2	
Community string	Enter a string with 4 to 31 characters.
SNMP version v3	
Username	Enter the username with 1 to 31 characters.
Authentication password	Enter the password with 4 to 128 characters.
Retype password	Confirmation of the Authentication password.
Privacy password	Enter a privacy password with 4 to 128 characters.
Retype password	Confirmation of the Privacy password.
NTP server IP address	Specify the network time server to use. This option is available only if time is set to **Set time from this machine** in the controller information provided in Table 2.
Traps	Generate all traps or just the ones for AirWave.
Send system logs to AirWave	Send additional logs to AirWave for further analysis.

NOTE

After entering the AirWave information, you will be prompted to add connectivity and licensing information.

Chapter 4
Automatic Setup

ZTP makes the deployment of managed device plug-n-play. The managed device now learns all the required information from the network and provisions itself automatically.

With ZTP, a managed device automatically gets its local and global configuration and license limits from a central managed device. A manage device with factory default settings gather the required information from the network and then provision itself automatically.

Zero Touch Provisioning

The main elements for ZTP are:

- Auto discovery of Mobility Conductor.
- Configuration download from the Mobility Conductor.

Provisioning Modes

The following modes are supported:

- **auto:** In this mode, managed device provisions completely automatically. The managed device gets the local IP address and routing information from DHCP and gets the Mobility Conductor information and regulatory domain from one of the supported servers. Then, it downloads the entire configuration from the Mobility Conductor.
- **mini-setup:** In this mode, managed device gets its local IP address and routing information from DHCP server. However, user is required to provide Mobility Conductor information and regulatory domain. Then, it downloads the entire configuration from the Mobility Conductor.
- **full-setup:** In this mode, managed device gets all the basic provisioning information from user inputs. However, even in this mode, controller can download configuration from the Mobility Conductor if the managed device role is specified as a managed device.

NOTE

In the default state, controller starts in complete auto mode. While the controller is trying to provision automatically, user are also provided an option to override the auto-mode at any time and select the desired mode. If there is "NO" ZTP provisioning in activate, then quick setup will wait for the user to provide inputs.

For auto provisioning, last physical interface port of a 7000 Series controller should be connected as uplink which will be in VLAN 4094 and act as a DHCP client.

Automatically Provisioning a Managed Device

An auto provisioning managed device acts as a DHCP client to get its local IP address, routing information, and Mobility Conductor information and regulatory domain from a DHCP server or Activate server. A factory-default managed device boots in auto provisioning mode. To interrupt the auto provisioning process, enter the string mini-setup or full-setup at the initial setup dialog prompt shown below:

```
Auto-provisioning is in progress. Choose one of the following options to override or
debug...
'enable-debug' : Enable auto-provisioning debug logs
'disable-debug': Disable auto-provisioning debug logs
```

```
'mini-setup' : Stop auto-provisioning and start mini setup dialog for smart-branch role
'full-setup' : Stop auto-provisioning and start full setup dialog for any role
Enter Option (partial string is acceptable):_
```

If the managed device can not complete ZTP provisioning through Activate, then the initial setup process waits for the user to provide input

Activate

The managed device interacts with the activate server to get Mobility Conductor information. The managed device establishes HTTPS connection with the activate server and posts provision requests to it. The activate server authenticates the managed device and provides the Mobility Conductor information and country code to the managed device.

Activate Interface– The managed device and the Mobility Conductor interact with the activate server to receive information about each other. Once all the information is available in the activate server, the relationship between a Mobility Conductor and all the managed device managed by it is provisioned automatically.

The managed device interacts with the activate server to learn about their role, Mobility Conductor information, and their regulatory domain. The Mobility Conductor sends its own information and not managed device information. Activate reuses existing AP-information field for managed device interactions. To achieve this, the following two steps are performed:

1. Mobility Conductor retrieving allowlist db from activate server. The following steps are involved to get the allowlist db:

   a. Mobility Conductor sends initial post with 'keep-alive' connection type with the following information:

   - Type as provision update, mode as managed device, session id, Ap-information that includes <serial number>, <mac>, <model>.

   b. Activate responds with the following information:

   - Type as provision update, activate assigned session id, status, and connection as keep alive.

   c. Mobility Conductor then sends a second POST with 'close' connection type with the following information:

   - Type as provision update, session id received from activate, Ap-information that includes <serial number>, <mac>, <model>, length of certificate, signed certificate, and device certificate.

   d. Activate then responds with the following information:

   - Type as provision update, the same session id that activate assigned in the first response, status as success or failure, mode as conductor, and the list of managed devices with the allowlist db that contains <MAC address>,<Serial number>,<Model>,<Mode>,<Hostname>, and <Config group>.

2. Managed device contacting activate and retrieving the provisioning rule

   The following steps are involved to retrieve the provision rule:

   a. Navigate to the device list and select a device that you want to designate as Mobility Conductor.

   b. Edit the selected device and set its mode to Conductor.

   c. Go to setup and create a folder with the managed device_to_Conductor rule.

   d. Populate the rule with the following information:

   - Select conductor device.
   - Specify IP address of the conductor.
   - Specify country code for managed device that will be in this folder.
   - Specify configuration group for managed device that will be in this folder.

NOTE

A folder can contain only one type of managed device that have the same country code and map to the same configuration group. Different folders need to be created for each such group, if the country code or mapping to the configuration changes.

e. Again, navigate to the device list and select a device that you intend to designate as managed device.

f. Edit the selected device and set its name to the desired hostname. If the name is not set, it will be autogenerated.

g. Move the selected managed device to the folder created in step c.

Using ZTP with DHCP to Provision a Managed Device

When a factory-default controller boots, it starts the auto-provisioning process. The following sections describe the provisioning workflow, and the process to prepare your network for ZTP using DHCP for a managed device.

The managed device can get the information required for provisioning from a DHCP server instead of Activate. Using DHCP helps the ZTP controllers get conductorinformation when the users are unable to use Activate. Option 43 of DHCP can be used for broadcasting the conductor information to the managed devices.

This feature supports the following topologies:

- VMM with VPNC
- HMM with VPNC
- HMM without VPNC

NOTE

VPNC must be a hardware controller and not a virtual machine.

This feature also supports L2 and L3 Mobility Conductor redundancy scenarios, where the managed device can get primary Mobility Conductor and standby Mobility Conductor (L2 or L3 standby conductor) information.

In VPNC scenarios, the managed devices can get primary Mobility Conductor information, standby Mobility Conductor, Primary VPNC and standby VPNC information.

Option 43 contains the following information to help provision a managed device:

- Conductor IP
- VPNC IP
- Primary Conductor MAC
- Redundant Conductor MAC
- Primary VPNC MAC
- Redundant VPNC MAC
- Country Code

Option 43 contains the following information:

- conductorip, country-code, conductor-mac1 (No L2 redundant Conductor)
- conductorip, country-code, conductor-mac1, conductor-mac2 (L2 Redundant Conductor)
- conductorip, country-code, vpnc ip, vpnc-mac1 (No L2 Redundant VPNC)
- conductorip, country-code, vpnc ip, vpnc-mac1, vpnc-mac2 (L2 Redundant VPNC)

Chapter 5
Configuring the Managed Devices and APs

The following section describes how to configure a Peer MAC address, connect the managed devices, and install the APs.

Peer MAC Address Configuration for PSK with MAC

The Peer MAC address configuration on a device for PSK with MAC authentication is based on the platform type of the peer device.

The following table lists the type of MAC address to be configured as the peer MAC address for different platform combinations of a Mobility Conductor-Managed Device pair:

Table 9: *Peer MAC Address Configuration*

Mobility Conductor Platform	Managed Device Platform	Peer MAC on the Mobility Conductor	Peer MAC on the Managed Device
Mobility Conductor Virtual Appliance	7000 Series controllers	MAC address of the VLAN 1 interface of the managed device	Management MAC address of the Conductor.
Mobility Conductor Virtual Appliance	Mobility Controller Virtual Appliance	Management MAC address of the managed device	Management MAC address of the Conductor.
Mobility Conductor Hardware Appliance	7000 Series controllers	MAC address of the VLAN interface	Management MAC address of the Conductor.
Mobility Conductor Hardware Appliance	Mobility Controller Virtual Appliance	Management MAC address of the managed device	Management MAC address of the Conductor.

Identify the MAC Address on a Device

Execute the following command to view the Management MAC address (Applicable only for Mobility Conductor Virtual Appliance or Mobility Conductor Hardware Appliance) or the MAC address of the VLAN1 interface for any device:

```
(host) [mynode] (config) #show switchinfo
…
…
Boot Partition: PARTITION 0
mgmt is administratively down line protocol is down
Hardware is Ethernet, address is 00:0C:29:56:33:FE
VLAN1 is up line protocol is down
Hardware is CPU Interface, Interface address is 00:0C:29:56:33:08 (bia 00:0C:29: 56:33:08)
Description: 802.1Q VLAN
…
…
```

Connect the Managed Device to the Wired Network

Once managed device setup is complete, connect a port on the managed device to the appropriately configured port on a Layer-2 switch or router. Make sure that you have the correct cables and that the port LEDs indicate proper connections and cable descriptions.

Configure the Managed Device to Support APs

Before you install APs in a network environment, you must ensure that the APs will be able to locate and connect to the managed device when powered on. Specifically, you need to ensure the following:

- When connected to the network, each AP is assigned a valid IP address
- APs are able to locate the managed devices

Each Aruba AP requires a unique IP address on a subnetwork that has connectivity to a managed device. Aruba recommends using the DHCP to provide IP addresses for APs; the DHCP server can be an existing network server or an Aruba managed device configured as a DHCP server.

If an AP is on the same subnetwork as the Mobility Conductor, you can configure the managed device as a DHCP server to assign an IP address to the AP. The managed device must be the only DHCP server for this subnetwork.

Enable DHCP Server Capability

Use the following procedure to use the WebUI to enable DHCP server capability:

1. Enter the IP address of the managed device in the URL of a browser window to access the WebUI.
2. At the WebUI login page, enter the **admin** user name and the password you entered during the Initial Setup.
3. Navigate to the **Configuration > Services** window.
4. Open the **DHCP Server** tab.
5. Select **Enable** from either **IPv4** or **IPv6 DHCP server** drop-down list.
6. In the **Pool Configuration** table, click +.
7. Enter information about the subnetwork for which IP addresses are to be assigned.
8. Click **Submit**.
9. If there are addresses that should not be assigned in the subnetwork:
   a. Click + in the **Excluded Address Range** section.
   b. Enter the address range in the **Add Excluded Address** section.
   c. Click **Submit**.

10. Click **Pending Changes**.
11. In the **Pending Changes** window, select the check box and click **Deploy changes**.

Managed Device Discovery

An Aruba AP can discover the IP address of the manage device in one of several ways. The ADP is enabled by default on all Aruba APs and managed devices. If all APs and managed devices are connected to the same Layer-2 network, APs will use ADP to discover their managed devices. If the devices are on different networks, you must configure the AP to use a Layer-3 compatible discovery mechanism such as DNS, DHCP, or IGMP forwarding after installing the AP on the network. For details, refer to the *ArubaOS 8.9.0.0 User Guide.*

With ADP, APs send out periodic multicast and broadcast queries to locate the . If the APs are in the same broadcast domain as the managed device, the managed device automatically responds to the APs' queries with its IP address. If the APs are not in the same broadcast domain as the managed device, you need to enable multicast on the network. If multicast is not an option, then the APs can be configured to use DNS or DHCP based provisioning to contact the managed device.

As APs do not terminate on the Mobility Conductor in ArubaOS 8.9.0.0, they are pointed to a managed device that has the configuration for the AP's **AP-group**.

Install the Access Points

Refer to the AP placement map generated by RF Plan to identify the locations in which to physically install your APs. You can either connect the AP directly to a port on the managed device, or connect the AP to another switch or router that has Layer-2 or Layer-3 connectivity to the managed device. If the Ethernet port on the managed device is an 802.3af PoE port, the AP automatically uses it to power up. If a PoE port is not available, contact your Aruba vendor to obtain an AC adapter for the AP.

Once an AP is connected to the network and powered up, it will automatically attempt to locate the managed device. You can view a list of all APs connected to the managed device by accessing the **Configuration > Access Points** page in the WebUI of the Mobility Conductor. An AP installed on the network advertises its default SSID. Wireless users can connect to this SSID, but will not have access to the network until you configure authentication policies and user roles for your wireless users. For complete details on authentication policies and user roles, refer to the *ArubaOS 8.9.0.0 User Guide.*