Configuring an AP using the Provisioning Wizard

The easiest way to provision any AP is to use the AP Wizard in the controller WebUI. This wizard will walk you through the specific steps required to provision a campus, remote or Mesh AP. The Wizard includes a help tab that further describes each of the configuration tasks for that deployment type.

To access the AP wizard to provision a AP:

1. Select Configuration>Wizards>AP Wizard. The **Specify Deployment Scenario** window appears.
2. Select the deployment for the new AP, then click **Next** to continue to the next window in the Wizard.
3. Continue working your way through the Wizard to complete the provisioning process.

Configuring a AP using the WebUI

The following basic steps configure a campus AP on a LAN.

Remote APs and mesh APs require additional configuration steps not required for campus APs. For more information, see Configuring a Remote AP and

1. Navigate to the **Configuration > Wireless > AP Installation > Provisioning** window.
2. Click the checkbox by the AP you want to provision, then click **Provision**. The Provisioning window opens.
3. In the **AP Parameters** section, click the **AP Group** drop-down list and select the AP group to which this AP should be assigned. The AP group must have at least one virtual AP.
4. (Optional) Some AP models support an external antenna in addition to their internal antenna. If the AP you are provisioning supports an external antenna, the Provisioning window displays an additional **Antenna Parameters** section. If you want to use an External antenna for the remote AP you are provisioning, select **External Antenna** and define settings for that antenna. Otherwise, the remote AP will use its internal antenna by default.
5. If your AP will use Point-to-Point Protocol over Ethernet (PPPoE) to authenticate itself to a service provider, select the **PPPoE Parameters** checkbox and enter the following PPPoE values:
   - PPPoE User Name: Set the PPPoE User Name for this remote AP.
   - PPPoE Password: Enter and then confirm the PPPoE password for this remote AP.
   - PPPoE Service Name: Either an ISP name or a class of service configured on the PPPoE server.
6. (Optional) To allow the remote AP to use PEAP to authenticate to 802.1X networks, enter a user name and password in the 802.1X Parameter using PEAP section.
7. In the **Master Discovery** section, define how the AP should identify its WLAN controller. For more information on the different controller discovery methods, see Enable Controller Discovery.
8. (Optional) Define the uplink VLAN. If you configure an uplink VLAN on an AP connected to a port in trunk mode, the AP sends and receives frames tagged with this VLAN on its Ethernet uplink. To define the uplink VLAN, entering a VLAN ID from 1-4095 (inclusive) in the **IP Settings** section of the **Provisioning** window,
9. Define how the AP should obtain its IP address. If you have configured an DHCP server to allow APs to get addresses using DHCP, select **Obtain IP address using DHCP**. For more information on configuring a DHCP server, see Enable DHCP to Provide APs with IP Addresses. Otherwise, select **Use the Following IP address** and enter the appropriate values in the following fields:
   - **IP address**: IP address for the AP, in dotted-decimal format
   - **Subnet mask**: Subnet mask for the IP, in dotted-decimal format.
   - **Gateway IP address**: The IP address the AP uses to reach other networks.

- **DNS IP address**: The IP address of the Domain Name Server.
- **Domain name**: (optional) The default domain name.

10. (Optional) Access points can be configured in single-chain mode, allowing the radios of those APs to transmit and receive data using only legacy rates and single-stream HT and VHT rates on a single radio chain and single antenna or antenna interface. On APs with external antennas, this feature uses the external antenna interface labeled **A0** or **ANT0** (radio chain 0); the other (one or two) antenna interfaces are left unused. If you are provisioning an 802.11n-capable AP, select the **Enable for Radio-0** or **Enable for Radio-1** checkboxes in the **Single-Chain Mode** section to enable single-chain mode for the selected radio. AP radios in single-chain mode will transmit and receive data using only legacy rates and single-stream HT rates up to MCS 7. This feature is disabled by default.
11. (Optional) Define the AP name or SNMP location. The **AP list** section displays current information for an AP, and allows you to define additional parameters for your AP, such as AP Name, SNMP System Location.
12. Click **Apply and Reboot**. (Reprovisioning the AP causes it to automatically reboot).

Configuring a Remote AP

A remote AP (RAP) is recommended when the network between the AP and controller is an un-trusted/non-routable network, such as the Internet. Furthermore, a RAP supports an internal DHCP server, while a campus AP does not.

Remote Authentication

The two most common ways to provision an AP for remote authentication are certificate-based AP provisioning and provisioning using a pre-shared key. Although both options allow for a simple secure setup of your remote network, you should make sure that the procedure you select is supported by your controller, the AP model type and the end user's client software. If you must provision your APs using a pre-shared key, you need to know which controller models you have that do not support certificate-based provisioning.

- **Certificate based authentication** allows a controller to authenticate a AP using its certificates instead of a PSK. You can manually provision an individual AP with a full set of provisioning parameters, or simultaneously provision an entire group of APs by defining a provisioning profile which contains a smaller set of provisioning parameters that can be applied the entire AP group. When you manually provision an individual AP to use certificated-based authentication, you must connect that AP to the controller before you can define its provisioning settings.
- Use **Pre-Shared Key (PSK) authentication** to provision an individual remote AP or a group of remote APs using an Internet Key Exchange Pre-Shared Key (IKE PSK).

RAP Configuration

The steps to configure a remote AP using the WebUI are similar to the steps described in Configuring a AP using the WebUI , although some additional steps are required.

1. In the **Configuration > Wireless > AP Installation > Provisioning** window, select **Yes** for the **Remote AP** option.
2. In the **Remote IP Authentication Method** section, select either **Pre-shared key** or **certificate** authentication type. The Pre-shared key option requires you to perform the following additional steps:
   a. Enter and confirm the pre-shared key (IKE PSK).
   b. In the User credential assignment section, specify if you want to use a **Global User Name/password** or a **Per AP User Name/Password**.
      - If you use the Per AP User Names/Passwords option, each RAP is given its own user name and password.
      - If you use the Global User Name/Password option, all selected RAPs are given the same (shared) user name and password.

c. Enter the user name, and enter and confirm the password. If you want the controller to automatically generate a user name and password, select **Use Automatic Generation**, then click **Generate** by the **User Name** and **Password** fields.

3. If you are provisioning remote AP models that support USB modems, you must complete the fields in the **USB settings** section. USB settings will not appear in the Provisioning window unless you are provisioning an AP that supports these features.

Configuring a Mesh AP

The steps to configure a remote AP using the WebUI are similar to the steps described in Configuring a AP using the WebUI , although some additional steps are required.

1. Define and configure the mesh cluster profile.
2. Define and configure the mesh radio profile
3. In the **AP list** section of the **Configuration > Wireless > AP Installation > Provisioning** window, select one of the following mesh for on the AP:
   - Mesh portal–The gateway between the wireless mesh network and the enterprise wired LAN.
   - Mesh point–APs that can provide traditional Aruba WLAN services (such as client connectivity, intrusion detection system (IDS) capabilities, user roles association, LAN-to-LAN bridging, and Quality of Service (QoS) for LAN-to-mesh communication) to clients on one radio and perform mesh backhaul/network connectivity on the other radio. Mesh points can also provide LAN-to-LAN bridging through their Ethernet interfaces and provide WLAN services on the backhaul radio
   - Remote Mesh Portal: The Remote Mesh Portal feature allows you to configure a remote AP at a branch office to operate as a mesh portal for a mesh cluster.

For detailed provisioning guidelines, caveats, and instructions, see Secure Enterprise Mesh on page 515.