



## Configuring AP Authentication

Access point authentication ensures only authorized access points can connect to the controller.

If you want to control which access points can connect to the corporate Wireless LAN Controller, follow this process.

If you want to allow any access point to connect to the Wireless LAN Controller, skip to the next process.

- [Configuring AP Authentication in WLC, page 1](#)

## Configuring AP Authentication in WLC

To configure the AP authentication in WLC, perform the following steps:

### Procedure

**Step 1** Navigate to **Security > AAA > AP Policies**.

**Step 2** Under **Policy Configuration**, select **Authorize MIC APs against auth-list or AAA**, and then click **Apply**.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The 'SECURITY' tab is selected. On the left, the 'Security' menu is expanded to 'AAA', and 'AP Policies' is selected. The main content area shows the 'AP Policies' configuration page with the following options:

Policy Configuration	Checkbox
Accept Self Signed Certificate (SSC)	<input type="checkbox"/>
Accept Manufactured Installed Certificate (MIC)	<input checked="" type="checkbox"/>
Accept Local Significant Certificate (LSC)	<input type="checkbox"/>
Authorize MIC APs against auth-list or AAA	<input checked="" type="checkbox"/>
Authorize LSC APs against auth-list	<input type="checkbox"/>

Below the policy configuration, there is an 'AP Authorization List' section with 'Entries 1 - 1 of 1'. It includes a search bar and a table with the following data:

MAC Address	Certificate Type	SHA1 Key Hash
00:50:56:a2:5d:96	SSC	b62741ab695f6ef95e5a3fc7b84496ee8972cd8f

