

```
ssid-profile WLAN-01

ap-group first-floor
  virtual-ap WLAN-01_first-floor
ap-group second-floor
  virtual-ap WLAN-01_second-floor
```

Mixed Authentication Modes

Use `l2-auth-fail-through` command to perform mixed authentication which includes both MAC and 802.1x authentication. When MAC authentication fails, enable the `l2-auth-fail-through` command to perform 802.1x authentication.



By default the `l2-auth-fail-through` command is disabled.

Table 58 describes the different authentication possibilities

Table 58 *Mixed Authentication Modes*

Authentication	1	2	3	4	5	6
MAC authentication	Success	Success	Success	Fail	Fail	Fail
802.1x authentication	Success	Fail	—	Success	Fail	—
Association	dynamic-wep	No Association	static-wep	dynamic-wep	No Association	static-wep
Role Assignment	802.1x	—	MAC	802.1x	—	logon

Using the CLI

```
aaa profile test
  l2-auth-fail-through
```

Advanced Configuration Options for 802.1x

This section describes advanced configuration options for 802.1x authentication.

Configuring reauthentication with Unicast Key Rotation

When enabled, unicast and multicast keys are updated after each reauthorization. It is a best practice to configure the time intervals for reauthentication, multicast key rotation, and unicast key rotation to be at least 15 minutes. Make sure these intervals are mutually prime, and the factor of the unicast key rotation interval and the multicast key rotation interval is less than the reauthentication interval.



Unicast key rotation depends upon both the AP/controller and wireless client behavior. It is known that some wireless NICs have issues with unicast key rotation.

The following is an example of the parameters you can configure for reauthentication with unicast and multicast key rotation: