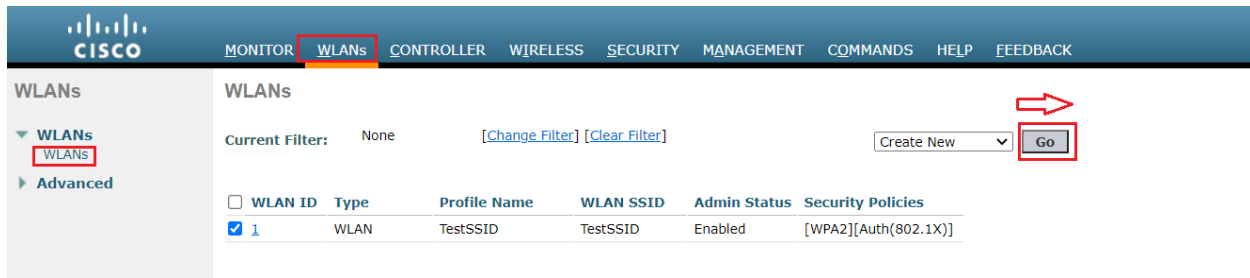
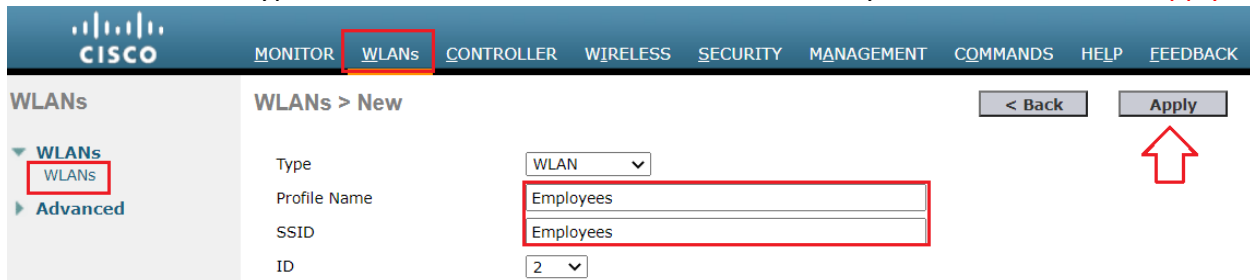


WLC WLAN Setup:

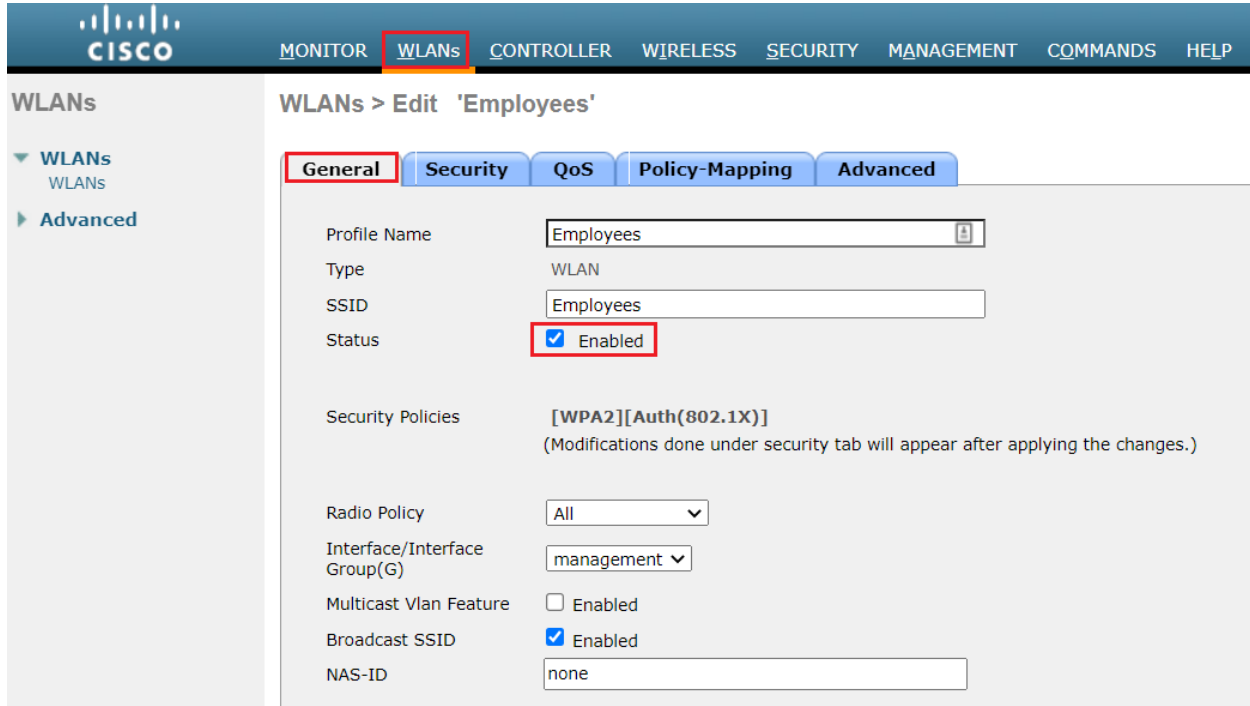
Click the **WLANs** menu from the controller GUI, and choose **Create New > Go**.



Choose WLAN for Type. Enter a **Profile Name** and a WLAN **SSID** of your choice, and click **Apply**.



Under the **General** tab, make sure that the **Enabled** option is checked for both **Status** and **Broadcast SSID**. Choose an interface for the WLAN. We use **management** for Interface.



Choose the **Security > Layer 2** Set Layer 2 Security: **WPA +WPA2** Parameters: WPA2 Policy-AES and Authentication Key Management: **802.1x**

The screenshot shows the Cisco WLAN configuration interface for the 'Employees' WLAN. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'Fast Transition' section has 'Fast Transition Over the DS' checked and 'Reassociation Timeout' set to 20 seconds. The 'Protected Management Frame' (PMF) is set to 'Disabled'. Under 'WPA+WPA2 Parameters', 'WPA2 Policy' is checked, and 'WPA2 Encryption' is set to 'AES'. Under 'Authentication Key Management', '802.1X' is checked and 'Enable' is selected.

Under **Security Tab > AAA Servers**. Authentication Servers: Enabled, Server1: 192.168.100.210 Cisco ISE IP address and same Accounting Servers. Apply Cisco ISE Default Settings: Enabled. Other options should remain at default values.

The screenshot shows the 'AAA Servers' sub-tab in the 'Security' configuration. The 'Apply Cisco ISE Default Settings' checkbox is checked. Under 'Authentication Servers', 'Enabled' is checked, and 'Server 1' is configured with IP: 192.168.100.210, Port: 1812. Under 'Accounting Servers', 'Enabled' is checked, and 'Server 1' is configured with IP: 192.168.100.210, Port: 1813. The 'EAP Parameters' section has 'Enable' unchecked.

Under **Advanced** tab, DHCP Addr. Assignment: **Required**. Other options should remain at default values. Make sure Allow AAA Override is **enabled**.

General **Security** **QoS** **Policy-Mapping** **Advanced**

Allow AAA Override ☒ Enabled

Coverage Hole Detection ☒ Enabled

Enable Session Timeout ☒ 1800
Session Timeout (secs)

Aironet IE ☒ Enabled

Diagnostic Channel [18](#) ☐ Enabled

Override Interface ACL IPv4 IPv6

Layer2 Acl

URL ACL

P2P Blocking Action

Client Exclusion [3](#) ☒ Enabled 180
Timeout Value (secs)

Maximum Allowed Clients [8](#)

Static IP Tunneling [11](#) ☐ Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

DHCP

DHCP Server ☐ Override

DHCP Addr. Assignment ☒ Required

OEAP

Split Tunnel ☐ Enabled

Management Frame Protection (MFP)

MFP Client Protection [4](#)

DTIM Period (in beacon intervals)

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

NAC

NAC State

Load Balancing and Band Select

Click **Apply** in order to save the configuration and finally, **Save Configuration**.

MONITOR **WLANs** **CONTROLLER** **WIRELESS** **SECURITY** **MANAGEMENT** [Ping](#) [Logout](#) [Refresh](#) [Home](#)

WLANs > Edit 'Employees'

[< Back](#) [Apply](#)

General **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name

Type

SSID

Status ☒ Enabled

Security Policies **[WPA2][Auth(802.1X)]**
(Modifications done under security tab will appear after applying the changes.)

Radio Policy

Interface/Interface Group(G)

Multicast Vlan Feature ☐ Enabled

Broadcast SSID ☒ Enabled