Security

802.1X on WLAN

- Description—WLAN should be using 802.1X security. There is no fix it button. Link to the WLAN page is provided. Day 0 default does not mandate an 802.1X.
- Status:
  - Selected—Enabled if at least one WLAN is using 802.1X
  - Unselected—Disabled

Rogue Policies

- Description—Policy should be at least High. Clicking **Fix it Now** sets the rogue detection security level to High.
- Status:
  - Selected—Policy is set to High or above

- Unselected—Policy is set to Custom.

- Set the rogue detection security level to High by entering this command:

```
(Cisco Controller) >config rogue detection security-level high
```

Rogue Threshold

- Description—Specifies the minimum RSSI value that rogues should have for APs to detect them and for the rogue entries to be created in the controller. Recommended value is –70 dBm. Clicking **Fix it Now** changes the minimum RSSI value that rogues should have to –80 dBm.
- Status:
  - Selected—Set to –80 dBm
  - Unselected—Set to less than –80 dBm
- CLI Option—Set the minimum RSSI value that rogues should have by entering this command:

```
(Cisco Controller) >config rogue detection min-rssi rssi-in-dBm
```

SSH/Telnet Access

- Description—SSH to the WLC should be enabled by default. Clicking **Fix it Now** enables SSH and disables Telnet to the WLC.
- Status:
  - Selected—SSH enabled; Telnet disabled
  - Unselected—SSH enabled and Telnet enabled OR SSH disabled and Telnet enabled
- CLI Option:
  - Enable SSH by entering this command:

```
(Cisco Controller) >config network ssh enable
```

  - Disable Telnet by entering this command:

```
(Cisco Controller) >config network telnet disable
```

Client Exclusion

- Description—Enables the WLC to exclude the clients from joining under specific conditions. Clicking **Fix it Now** enables client exclusion for all events.
- Status:
  - Selected—Client exclusion is enabled for all events

  - Unselected—Client exclusion is disabled for all events

- CLI Option—Enable client exclusion for all events by entering this command:

```
(Cisco Controller) >config wps client-exclusion all enable
```

Legacy IDS

- Description—Enables wireless IDS feature and 17 built-in signatures to avoid intrusion attacks. Clicking **Fix it Now** enables signature check.
- Status:
  - Selected—All standard signature check is enabled
  - Unselected—All standard signature check is disabled
- CLI Option—Enable signature check by entering this command:

```
(Cisco Controller) >config wps signature enable
```

Local Management Password Policies

- Description—Strong password policies should be enforced. Clicking **Fix it Now** enables the following strong password policies:
  - case-check—Checks the occurrence of same character thrice consecutively
  - consecutive-check—Checks the default values or its variants are being used
  - default-check—Checks either username or its reverse is being used
  - all-checks—Enables/disables all the strong password checks
  - position-check—Checks four-character range from old password
  - case-digit-check—Checks all four combinations to be present: lower, upper, digits, and special characters
- Status:
  - Selected—All strong password policies are enabled
  - Unselected—Some or no password policies are enabled
- CLI Option—Enable all strong password policies by entering this command:

```
(Cisco Controller) >config switchconfig strong-pwd all-checks enable
```

User Login Policies

- Description— The user login policies are provided to limit the number of concurrent logins of the local netusers of the controller. You can limit the number of concurrent logins, and the recommendation is greater than default of 0 (unlimited).
- Status:
  - Selected—Configured
  - Unselected—No user login policies are present
- CLI Option:
  - Verify the limit of the netusers by entering this command:

    ```
    (Cisco Controller) >show netuser summary
    ```

  - Configure user login policies by entering this command:

    ```
    (Cisco Controller) >config netuser maxUserLogin count
    ```

CPU ACLs

- Description—Control overall access to the WLC.
- Status:
  - Selected—Configured
  - Unselected—Not configured