Security

All best practices, except those that need manual configuration, are enabled by default in a Cisco Mobility Express network. These exceptions include NTP, WLAN with WPA2 or 802.1X, and high SSID counts.

- Client Exclusion, on page 1
- Legacy IDS, on page 2
- Local Management Password Policies, on page 2
- Minimum Rogue RSSI Threshold, on page 3
- Rogue Policies, on page 3
- SSH/Telnet Access, on page 4
- User Login Policies, on page 4
- WLAN with WPA2 or 802.1X, on page 4
- WLAN with WPA2 and AES Policy, on page 5

Client Exclusion

- Description—When the user fails to authenticate, the controller excludes the client. The client cannot connect to the network until the exclusion timer expires or is manually overridden by the administrator.

  Client exclusion detects authentication attempts made by a single device. When the device exceeds a maximum number of failures, that MAC address is not allowed to associate any longer to the controller.

  Client exclusion is enabled by default on the primary AP allowing it to exclude clients from joining the controller during the above 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—The Cisco Mobility Express controller performs WLAN IDS analysis using all the connected APs and reports detected attacks on to the virtual controller. The Wireless IDS analysis is complementary to any analysis that may otherwise be performed by a wired network IDS system. The embedded Wireless IDS capability of the Cisco Mobility Express controller analyzes 802.11- and Cisco Mobility Express controller-specific information that is not available to a wired network IDS system.

  Enables wireless IDS feature and 17 built-in signatures to avoid intrusion attacks.

- 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—You must enforce a strong password. The password policies allow enforcement of strong password checks on newly created passwords for additional management users of controller and access point. The following are the requirements enforced on the new password:
  - When the controller is upgraded from an old version, all the old passwords are maintained even though the passwords are weak. After the system upgrade, if the strong password checks are enabled, the same is enforced from that time and the strength of previously added passwords will not be checked or altered.
  - Depending on the settings done in the Password Policy page, the local management and access point user configuration is affected.

  Strong password policies should be enforced. They include:
  - 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
```

Minimum Rogue RSSI Threshold

- Description—This criterion normally indicates that unknown rogue APs are inside the facility perimeters, and can cause potential interference to the wireless network.

  This rule is not recommended for retail customers or venues that are shared by various tenants, where WiFi signals from all parties normally bleed into each other.

  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 –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
```

Rogue Policies

- Description—Rogue wireless devices are an ongoing threat to corporate wireless networks. Network owners need to do more than just scanning the unknown devices. They must be able to detect, disable, locate, and manage rogue/intruder threats automatically and in real time.

  Rogue APs can disrupt wireless LAN operations by hijacking legitimate clients and using plain text, denial-of-service attacks, or man-in-the-middle attacks. That is, a hacker can use a rogue AP to capture sensitive information, such as passwords and usernames. The hacker can then transmit a series of clear-to-send (CTS) frames, which mimics an AP informing a particular wireless LAN client adapter to transmit and instruct all others to wait. This scenario results in legitimate clients being unable to access the wireless LAN resources. Thus, wireless LAN service providers look for banning rogue APs from the air space.

  The best practice is to use rogue detection to minimize security risks, for example, in a corporate environment. However, there are certain scenarios in which rogue detection is not needed, for example, in OEAP deployment, open venues/stadium, citywide, and outdoors. Using outdoor mesh APs to detect rogues would provide little value while incurring resources to analyze. Finally, it is critical to evaluate (or avoid altogether) rogue auto-containment, as there are potential legal issues and liabilities if left to operate automatically.

  Policy should be at least High.

- Status:
  - Selected—Policy is set to High or above
  - Unselected—Policy is set to Low.

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

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

SSH/Telnet Access

- Description—SSH to the Cisco Mobility Express controller should be enabled by default. However, Telnet to the Cisco Mobility Express controller is disabled by default.
- 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
    ```

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
    ```

WLAN with WPA2 or 802.1X

- Description—WLAN should be using 802.1x or WPA2 security. You can enable this from the linked WLAN page. The default day 0 setting does not mandate configuring 802.1x.

- Status—If disabled, click **Manual Configuration** to specify the security setting of the WLAN.
  - Selected—Either 802.1x or WPA2 is enabled on at least one WLAN.
  - Unselected—Neither security is enabled on any WLAN.

WLAN with WPA2 and AES Policy

- Description—WPA2 with AES provides greater security compared to WPA with AES which has been deprecated.
- Status:
  - Selected—WLAN with WPA and AES policy is enabled on one or more WLANs.
  - Unselected—No WLAN with WPA2 and AES security policy.
- CLI Option—Use the following CLI to enable WPA2+AES:

```
(Cisco Controller) >config wlan security wpa enable wlan-id
```