Configuring a Fallback Policy with MAC Filtering and Web Authentication

Fallback Policy with MAC Filtering and Web Authentication

You can configure a fallback policy mechanism that combines Layer 2 and Layer 3 security. In a scenario where you have both MAC filtering and web authentication implemented, when a client tries to connect to a WLAN using the MAC filter (RADIUS server), if the client fails the authentication, you can configure the authentication to fall back to web authentication. When a client passes the MAC filter authentication, the web authentication is skipped and the client is connected to the WLAN. With this feature, you can avoid disassociations based on only a MAC filter authentication failure.

Restrictions

- MAC filtering does not support passthrough web-authentication. It supports only username and password for web-authentication.

Mobility is not supported for SSIDs with security type configured for Webauth on MAC filter failure.

This section contains the following subsections:

Configuring a Fallback Policy with MAC Filtering and Web Authentication (GUI)

Note Before configuring a fallback policy, you must have MAC filtering enabled.

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN for which you want to configure the fallback policy for web authentication. The WLANs > Edit page appears.

Step 3 Choose the **Security** and **Layer 3** tabs to open the WLANs > Edit (Security > Layer 3) page.

Step 4 From the Layer 3 Security drop-down list, choose **None.**

Step 5 Select the **Web Policy** check box.

Note The controller forwards DNS traffic to and from wireless clients prior to authentication.

The following options are displayed:

- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter Failure

Step 6 Click **On MAC Filter Failure**.

Step 7 Click **Apply** to commit your changes.

Step 8 Click **Save Configuration** to save your settings.

Configuring a Fallback Policy with MAC Filtering and Web Authentication (CLI)

Note Before configuring a fallback policy, you must have MAC filtering enabled.

Step 1 Enable or disable web authentication on a particular WLAN by entering this command:

config wlan security web-auth on-macfilter-failure *wlan-id*

Step 2 See the web authentication status by entering this command:

show wlan *wlan_id*

```
FT Over-The-Ds mode.............................. Enabled
CKIP ..................................... Disabled
   IP Security.................................... Disabled
   IP Security Passthru........................... Disabled
   Web Based Authentication....................... Enabled-On-MACFilter-Failure
        ACL.......................................... Unconfigured
        Web Authentication server precedence:
        1.............................................. local
        2.............................................. radius
```

```
3.............................................. ldap
```