MAC Authentication Bypass

MAC Authentication Bypass

You can configure the embedded wireless controller to authorize clients based on the client MAC address by using the MAC authentication bypass (MAB) feature.

When MAB is enabled, the embedded wireless controller uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. After detecting a client, the embedded wireless controller waits for a packet from the client. The embedded wireless controller sends the authentication server a RADIUS-access/request frame with a username and password based on the MAC address. If authorization succeeds, the embedded wireless controller grants the client access to the network. If authorization fails, the embedded wireless controller assigns the port to the guest WLAN, if one is configured.

Clients that were authorized with MAC authentication bypass can be re-authenticated. The re-authentication process is the same as that for clients that were authenticated. During re-authentication, the port remains in the previously assigned WLAN. If re-authentication is successful, the embedded wireless controller keeps the port in the same WLAN. If re-authentication fails, the embedded wireless controller assigns the port to the guest WLAN, if one is configured.

MAB Configuration Guidelines

- MAB configuration guidelines are the same as the 802.1x authentication guidelines.
- When MAB is disabled from a port after the port has been authorized with its MAC address, the port state is not affected.

- If the port is in the unauthorized state and the client MAC address is not in the authentication-server database, the port remains in the unauthorized state. However, if the client MAC address is added to the database, the switch can use MAC authentication bypass to re-authorize the port.
- If the port is in the authorized state, the port remains in this state until re-authorization occurs.
- You can configure a timeout period for hosts that are connected by MAB but are inactive. The valid range is from 1 to 65535, in seconds.

Note If wlan-profile-name is configured for a user, guest user authentication is allowed only from that WLAN.

If wlan-profile-name is not configured for a user, guest user authentication is allowed on any WLAN.

If you want the client to connect to SSID1, but not to SSID2 using mac-filtering, ensure that you configure **aaa-override** in the policy profile.

In the following example, when a client with MAC address 1122.3344.0001 tries to connect to a WLAN, the request is sent to the local RADIUS server, which checks the presence of the client MAC address in its attribute list (FILTER_1 and FILTER_2). If the client MAC address is listed in an attribute list (FILTER_1), the client is allowed to join the WLAN (WLAN_1) that is returned as *ssid attribute* from the RADIUS server. The client is rejected, if the client MAC address is not listed in the attribute list.

Local RADIUS Server Configuration

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"

!Username with the MAC address is added to the filter
username 1122.3344.0002 mac aaa attribute list FILTER_2

!
aaa attribute list FILTER_1
attribute type ssid "WLAN_1"
username 1122.3344.0001 mac aaa attribute list FILTER_1
```

Controller Configuration

```
! Sets authorization to the local radius server
aaa authorization network MLIST_MACFILTER local

!A WLAN with the SSID WLAN_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN_2 2 WLAN_2
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers

!WLAN with the SSID WLAN_1 is created and MAC filtering is set along with security parameters.
wlan WLAN_1 1 WLAN_1
mac-filtering MLIST_MACFILTER
no security wpa
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list WEBAUTH

! Policy profile to be associated with the above WLANs
```

```
wireless profile policy MAC_FILTER_POLICY
aaa-override
vlan 504
no shutdown
```

Configuring 802.11 Security for WLAN (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 Click **Add** to create WLANs.

The **Add WLAN** page is displayed.

Step 3 In the **Security** tab, you can configure the following:

- Layer2
- Layer3
- AAA

Step 4 In the **Layer2** tab, you can configure the following:

a) Choose the **Layer2 Security Mode** from the following options:

- None—No Layer 2 security.
- WPA + WPA2—Wi-Fi Protected Access.
- Static WEP—Static WEP encryption parameters.

b) Enable **MAC Filtering** if required. MAC Filtering is also known as MAC Authentication Bypass (MAB).

c) In the **Protected Management Frame** section, choose the **PMF** as *Disabled*, *Optional*, or *Required*. By default, the PMF is disabled.

d) In the **WPA Parameters** section, choose the following options, if required:

- WPA Policy
- WPA2 Policy
- WPA2 Encryption

e) Choose an option for **Auth Key Mgmt**.

f) Choose the appropriate status for **Fast Transition** between APs.

g) Check the **Over the DS** check box to enable Fast Transition over a distributed system.

h) Enter the **Reassociation Timeout** value, in seconds. This is the time after which a fast transition reassociation times out.

i) Click **Save & Apply to Device**.

Step 5 In the **Layer3** tab, you can configure the following:

a) Check the **Web Policy** check box to use the web policy.

b) Choose the required **Webauth Parameter Map** value from the drop-down list.

c) Choose the required **Authentication List** value from the drop down list.
d) In the **Show Advanced Settings** section, check the **On Mac Filter Failure** check box.
e) Enable the **Conditional Web Redirect** and **Splash Web Redirect**.
f) Choose the appropriate IPv4 and IPv6 ACLs from the drop-down lists.
g) Click **Save & Apply to Device**.

Step 6 In the **AAA** tab, you can configure the following:

a) Choose an authentication list from the drop-down.
b) Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN. Also, choose the required **EAP Profile Name** from the drop-down list.
c) Click **Save & Apply to Device**.

Configuring 802.11 Security for WLAN (CLI)

Follow the procedure below to configure 802.11 security for WLAN:

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id ssid* **Example:** `Device(config)# wlan ha-wlan-dot1x-test 3 ha-wlan-dot1x-test`	Configures the WLAN profile.
Step 2	**security dot1x authentication-list** *auth-list-name* **Example:** `Device(config-wlan)# security dot1x authentication-list default`	Enables security authentication list for dot1x security.
Step 3	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring AAA for External Authentication

Follow the procedure given below to configure AAA for external authentication.

Procedure

	Command or Action	Purpose
Step 1	**radius server** *server-name* **Example:**	Sets the radius server.

	Command or Action	Purpose
	`Device(config)# radius server ISE`	
Step 2	**address** {**ipv4** | **ipv6**}*radius-server-ip-address* **auth-port** *auth-port-no* **acct-port** *acct-port-no* **Example:** `Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813`	Specifies the radius server address.
Step 3	**key** *key* **Example:** `Device(config-radius-server)# key any123`	Sets the per-server encryption key.
Step 4	**exit** **Example:** `Device(config-locsvr-da-radius)# exit`	Returns to the configuration mode.
Step 5	**aaa local authentication default authorization default** **Example:** `Device(config)# aaa local authentication default authorization default`	Selects the default local authentication and authorization.
Step 6	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model. Enable new access control commands and functions.
Step 7	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Creates common session ID.
Step 8	**aaa authentication dot1x default group radius** **Example:** `Device(config)# aaa authentication dot1x default group radius`	Configures authentication for the default dot1x method. .
Step 9	**aaa authorization network default group radius** **Example:** `Device(config)# aaa authorization network default group radius`	Configures authorization for network services.
Step 10	**dot1x system-auth-control** **Example:** `Device(config)# dot1x system-auth-control`	Enables SysAuthControl.

Configuring AAA for Local Authentication (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **WLANs**.

Step 2 On the **Wireless Networks** page, click **Add**.

Step 3 In the **Add WLAN** window that is displayed, select **Security** > **AAA** .

Step 4 Select a value from the **Authentication List** drop-down.

Step 5 Check the **Local EAP Authentication** check box to enable local EAP authentication on the WLAN.

Step 6 Select a value from the **EAP Profile Name** drop-down.

Step 7 Click **Save & Apply to Device**.

Configuring AAA for Local Authentication (CLI)

Follow the procedure given below to configure AAA for local authentication.

Procedure

	Command or Action	Purpose
Step 1	**aaa authentication dot1x default local** **Example:** `Device(config)# aaa authentication dot1x default local`	Configures to use the default local RADIUS server.
Step 2	**aaa authorization network default local** **Example:** `Device(config)# aaa authorization network default local`	Configures authorization for network services.
Step 3	**aaa authorization credential-download default local** **Example:** `Device(config)# aaa authorization credential-download default local`	Configures default database to download credentials from local server.
Step 4	**username** *mac-address* **mac** **Example:** `Device(config)# username abcdabcdabcd mac`	For MAC filtering using username, use the **username** *abcdabcdabcd* **mac** command.
Step 5	**aaa local authentication default authorization default**	Configures the local authentication method list.

	Command or Action	Purpose
	Example: `Device(config)# aaa local authentication default authorization default`	
Step 6	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Creates a AAA authentication model. Enable new access control commands and functions.
Step 7	**aaa session-id common** **Example:** `Device(config)# aaa session-id common`	Creates common session ID.

Configuring MAB for Local Authentication

Follow the procedure given below to configure MAB for local authentication.

Before you begin

Configure AAA local authentication.

Configure the username for WLAN configuration (local authentication) using **username** *mac-address* **mac** command.

Note The mac-address must be in the following format: *abcdabcdabcd*

Procedure

	Command or Action	Purpose
Step 1	**wlan** *profile-name wlan-id* **Example:** `wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default`	Specifies the WLAN name and ID.
Step 2	**mac-filtering default** **Example:** `Device(config-wlan)# mac-filtering default`	Sets MAC filtering support for the WLAN.
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.

	Command or Action	Purpose
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 7	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.

Configuring MAB for External Authentication (GUI)

Before you begin

Configure AAA external authentication.

Procedure

Step 1 Choose **Configuration** > **Wireless** > **WLANs**.
Step 2 On the **Wireless Networks** page, click the name of the WLAN.
Step 3 In the **Edit WLAN** window, click the **Security** tab.
Step 4 In the **Layer2** tab, check the **MAC Filtering** check box to enable the feature.
Step 5 With MAC Filtering enabled, choose the **Authorization List** from the drop-down list.
Step 6 Save the configuration.

Configuring MAB for External Authentication (CLI)

Follow the procedure given below to configure MAB for external authentication.

Before you begin

Configure AAA external authentication.

Procedure

	Command or Action	Purpose
Step 1	**wlan** *wlan-name wlan-id ssid-name* **Example:** `wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius`	Specifies the WLAN name and ID.
Step 2	**mac-filtering** *list-name* **Example:** `Device(config-wlan)# mac-filtering ewlc-radius`	Sets the MAC filtering parameters. Here, *ewlc-radius* is an example for the *list-name*
Step 3	**no security wpa** **Example:** `Device(config-wlan)# no security wpa`	Disables WPA secuirty.
Step 4	**no security wpa akm dot1x** **Example:** `Device(config-wlan)# no security wpa akm dot1x`	Disables security AKM for dot1x.
Step 5	**no security wpa wpa2** **Example:** `Device(config-wlan)# no security wpa wpa2`	Disables WPA2 security.
Step 6	**mab request format attribute** {**1 groupsize** *size* **separator** *separator* [**lowercase** | **uppercase**] | **2** {**0** | **7** | **LINE**} **LINE** *password* | **32 vlan access-vlan**} **Example:** `Device(config)# mab request format attribute 1 groupsize 4 separator`	Optional. Configures the delimiter while using MAC filtering in a WLAN. Here, **1**- Specifies the username format used for MAB requests. **groupsize** *size*- Specifies the number of hex digits per group. The valid values range from 1 to 12. **separator** *separator*- Specifies how to separate groups. The separators are comma, semicolon, and full stop. **lowercase**- Specifies the username in lowercase format. **uppercase**- Specifies the username in uppercase format. **2**- Specifies the global password used for all the MAB requests. **0**- Specifies the unencrypted password.

	Command or Action	Purpose
		7- Specifies the hidden password. **LINE**- Specifies the encrypted or unencrypted password. *password*- LINE password. **32**- Specifies the NAS-Identifier attribute. **vlan**- Specifies a VLAN. **access-vlan**- Specifies the configured access VLAN.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `Device(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for AES.
Step 8	**no shutdown** **Example:** `Device(config-wlan)# no shutdown`	Enables the WLAN.