# MAC 認証バイパス



# MAC 認証バイパス

MAC 認証バイパス（MAB）機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するように 組み込みワイヤレスコントローラを設定できます。

MAB を有効にすると、 組み込みワイヤレスコントローラはクライアント ID として MAC アドレスを使用します。認証サーバーには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。クライアントの検出後、組み込みワイヤレスコントローラはクライアントからのパケットを待機します。 組み込みワイヤレスコントローラは、MAC アドレスに基づくユーザー名とパスワードを含む RADIUS アクセス/要求フレームを認証サーバーに送信します。認証が成功すると、 組み込みワイヤレスコントローラはクライアントにネットワークへのアクセス権を付与します。認証が失敗した場合、ゲスト WLAN が設定されていれば、 組み込みワイヤレスコントローラはゲスト WLAN にポートを割り当てます。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、認証されたクライアントの場合と同じです。再認証の間、ポートは前に割り当てられた WLAN のままです。再認証が成功すると、 組み込みワイヤレスコントローラは同じ WLAN でポートを保持します。再認証が失敗した場合、ゲスト WLAN が設定されていれば、 組み込みワイヤレスコントローラはゲスト WLAN にポートを割り当てます。

# MAB の設定に関する注意事項

- MAB の設定に関する注意事項は、802.1x 認証の注意事項と同じです。
- MAC アドレスで認可された後にポートで MAB を無効にしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバーデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAB によって接続されているにもかかわらず非アクティブなホストのタイムアウト時間を設定できます。有効な範囲は 1 ～ 65535 秒です。

（注） ユーザーに対して wlan-profile-name が設定されている場合、ゲストユーザー認証はその WLAN からのみ許可されます。

ユーザーに対して wlan-profile-name が設定されていない場合、すべての WLAN でゲストユーザー認証が許可されます。

クライアントを SSID1 に接続するが、MAC フィルタリングを使用して SSID2 には接続しない場合は、ポリシープロファイルで aaa-override を設定してください。

次の例では、MAC アドレスが 1122.3344.0001 のクライアントが WLAN に接続しようとすると、要求がローカル RADIUS サーバーに送信され、属性リスト（FILTER_1 および FILTER_2）にクライアントの MAC アドレスが存在するかどうかがチェックされます。クライアントの MAC アドレスが属性リスト（FILTER_1）にリストされている場合、クライアントは、RADIUS サーバーから ssid 属性として返される WLAN（WLAN_1）に接続できます。クライアントの MAC アドレスが属性リストにリストされていない場合、そのクライアントは拒否されます。

ローカル RADIUS サーバーの設定

```
!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
```

# WLAN の 802.11 セキュリティの設定（GUI）

### 手順

**ステップ 1** **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

**ステップ 2** [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

**ステップ 3** [Security] タブで次の設定を行えます。

- レイヤ 2
- Layer3
- AAA

**ステップ 4** [Layer2] タブで次の設定を行えます。

a) [Layer2 Security Mode] を次のオプションから選択します。

- [None]：レイヤ 2 セキュリティなし。
- [WPA + WPA2]：Wi-Fi Protected Access。
- Static WEP：静的 WEP 暗号化パラメータ。

b) 必要に応じて、[MAC Filtering] を有効にしますMAC フィルタリングは、MAC 認証バイパス（MAB）とも呼ばれます。

c) [Protected Management Frame] セクションの [PMF] で、[Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。
d) [WPA Parameters] セクションで、必要に応じて次のオプションを選択します。
   - WPA Policy
   - WPA2 Policy
   - WPA2 Encryption
e) [Auth Key Mgmt] のオプションを選択します。
f) AP 間の [Fast Transition] の適切なステータスを選択します。
g) 分散システム経由の高速移行を有効にするには、[Over the DS] チェック ボックスをオンにします。
h) [Reassociation Timeout] の値（秒単位）を入力します。これは、高速移行の再アソシエーションがタイムアウトするまでの時間です。
i) [Save & Apply to Device] をクリックします。

**ステップ 5** [Layer3] タブで次の設定を行えます。
a) Web ポリシーを使用するには、[Web Policy] チェック ボックスをオンにします。
b) 必要な [Webauth Parameter Map] 値をドロップダウンリストから選択します。
c) 必要な [Authentication List] 値をドロップダウンリストから選択します。
d) [Show Advanced Settings] セクションで、[On Mac Filter Failure] チェック ボックスをオンにします。
e) [Conditional Web Redirect] と [Splash Web Redirect] を有効にします。
f) ドロップダウンリストから適切な IPv4 および IPv6 ACL を選択します。
g) [Save & Apply to Device] をクリックします。

**ステップ 6** [AAA] タブで次の設定を行えます。
a) ドロップダウンから認証リストを選択します。
b) WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。また、必要な [EAP Profile Name] をドロップダウンリストから選択します。
c) [Save & Apply to Device] をクリックします。

# WLAN の 802.11 セキュリティの設定（CLI）

WLAN の 802.11 セキュリティを設定するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **wlan** *profile-name wlan-id ssid*<br>例：<br>`Device(config)# wlan ha-wlan-dot1x-test 3 ha-wlan-dot1x-test` | WLAN プロファイルを設定します。 |
| ステップ 2 | **security dot1x authentication-list** *auth-list-name*<br>例：<br>`Device(config-wlan)# security dot1x authentication-list default` | dot1x セキュリティ用のセキュリティ認証リストを有効にします。 |
| ステップ 3 | **no shutdown**<br>例：<br>`Device(config-wlan)# no shutdown` | WLAN をイネーブルにします。 |

# 外部認証用の AAA の設定

外部認証用に AAA を設定するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **radius server** *server-name*<br>例：<br>`Device(config)# radius server ISE` | Radius サーバーを設定します。 |
| ステップ 2 | **address** {**ipv4** \| **ipv6**}*radius-server-ip-address* **auth-port** *auth-port-no* **acct-port** *acct-port-no*<br>例：<br>`Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813` | Radius サーバーのアドレスを指定します。 |
| ステップ 3 | **key** *key*<br>例：<br>`Device(config-radius-server)# key any123` | サーバーごとの暗号キーを設定します。 |
| ステップ 4 | **exit**<br>例： | コンフィギュレーションモードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-locsvr-da-radius)# exit` | |
| ステップ 5 | **aaa local authentication default authorization default**<br>例：<br>`Device(config)# aaa local authentication default authorization default` | デフォルトのローカル認証および許可を選択します。 |
| ステップ 6 | **aaa new-model**<br>例：<br>`Device(config)# aaa new-model` | AAA 認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。 |
| ステップ 7 | **aaa session-id common**<br>例：<br>`Device(config)# aaa session-id common` | コモン セッション ID を作成します。 |
| ステップ 8 | **aaa authentication dot1x default group radius**<br>例：<br>`Device(config)# aaa authentication dot1x default group radius` | デフォルトの dot1x 方式の認証を設定します。<br>. |
| ステップ 9 | **aaa authorization network default group radius**<br>例：<br>`Device(config)# aaa authorization network default group radius` | ネットワークサービスに対する認証を設定します。 |
| ステップ 10 | **dot1x system-auth-control**<br>例：<br>`Device(config)# dot1x system-auth-control` | SysAuthControl を有効にします。 |

# ローカル認証用の AAA の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Wireless Networks] ページで [Add] をクリックします。

ステップ 3 表示される [Add WLAN] ウィンドウで、**[Security]** > **[AAA]** を選択します。

ステップ 4 [Authentication List] ドロップダウンから値を選択します。

**ステップ 5** WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。

**ステップ 6** [EAP Profile Name] ドロップダウンから値を選択します。

**ステップ 7** [Save & Apply to Device] をクリックします。

# ローカル認証用の AAA の設定（CLI）

ローカル認証用に AAA を設定するには、次の手順に従います。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **aaa authentication dot1x default local**<br>例：<br>`Device(config)# aaa authentication dot1x default local` | デフォルトのローカルRADIUSサーバーを使用するように設定します。 |
| **ステップ 2** | **aaa authorization network default local**<br>例：<br>`Device(config)# aaa authorization network default local` | ネットワークサービスに対する認証を設定します。 |
| **ステップ 3** | **aaa authorization credential-download default local**<br>例：<br>`Device(config)# aaa authorization credential-download default local` | ローカル サーバーからログイン情報をダウンロードするようにデフォルトデータベースを設定します。 |
| **ステップ 4** | **username** *mac-address***mac**<br>例：<br>`Device(config)# username abcdabcdabcd mac` | ユーザー名を使用したMACフィルタリングには、**username** *abcdabcdabcd* **mac** コマンドを使用します。 |
| **ステップ 5** | **aaa local authentication default authorization default**<br>例：<br>`Device(config)# aaa local authentication default authorization default` | ローカル認証方式リストを設定します。 |
| **ステップ 6** | **aaa new-model**<br>例：<br>`Device(config)# aaa new-model` | AAA 認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **aaa session-id common**<br>例：<br>`Device(config)# aaa session-id common` | コモン セッション ID を作成します。 |

# ローカル認証用の MAB の設定

ローカル認証用に MAB を設定するには、次の手順に従います。

### 始める前に

AAA ローカル認証を設定します。

**username** *mac-address* **mac** コマンドを使用して、WLAN 設定（ローカル認証）のユーザー名を設定します。

（注） MAC アドレスの形式は、abcdabcdabcd にする必要があります。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **wlan** *profile-name wlan-id*<br>例：<br>`wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default` | WLAN の名前と ID を指定します。 |
| ステップ 2 | **mac-filtering default**<br>例：<br>`Device(config-wlan)# mac-filtering default` | WLAN の MAC フィルタリング サポートを設定します。 |
| ステップ 3 | **no security wpa**<br>例：<br>`Device(config-wlan)# no security wpa` | WPA セキュリティを無効にします。 |
| ステップ 4 | **no security wpa akm dot1x**<br>例：<br>`Device(config-wlan)# no security wpa akm dot1x` | dot1x に対するセキュリティの AKM をディセーブルにします。 |
| ステップ 5 | **no security wpa wpa2**<br>例： | WPA2 セキュリティを無効にします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config-wlan)# no security wpa wpa2` | |
| ステップ 6 | **no security wpa wpa2 ciphers aes**<br>例：<br>`Device(config-wlan)# no security wpa wpa2 ciphers aes` | AES の WPA2 暗号化をディセーブルにします。 |
| ステップ 7 | **no shutdown**<br>例：<br>`Device(config-wlan)# no shutdown` | WLAN をイネーブルにします。 |

# 外部認証用の MAB の設定（GUI）

### 始める前に

AAA 外部認証を設定します。

### 手順

**ステップ 1** **[Configuration]** > **[Wireless]** > **[WLANs]** の順に選択します。
**ステップ 2** [Wireless Networks] ページで WLAN の名前をクリックします。
**ステップ 3** [Edit WLAN] ウィンドウで [Security] タブをクリックします。
**ステップ 4** [Layer2] タブで、[MAC Filtering] チェック ボックスをオンにして機能を有効にします。
**ステップ 5** MAC フィルタリングを有効にした状態で、ドロップダウンリストから [Authorization List] を選択します。
**ステップ 6** 設定を保存します。

# 外部認証用の MAB の設定（CLI）

外部認証用に MAB を設定するには、次の手順に従います。

### 始める前に

AAA 外部認証を設定します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **wlan** *wlan-name wlan-id ssid-name*<br>例：<br>`wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius` | WLAN の名前と ID を指定します。 |
| ステップ 2 | **mac-filtering** *list-name*<br>例：<br>`Device(config-wlan)# mac-filtering ewlc-radius` | MAC フィルタリング パラメータを設定します。ここで、ewlc-radius は list-name の例です |
| ステップ 3 | **no security wpa**<br>例：<br>`Device(config-wlan)# no security wpa` | WPA セキュリティを無効にします。 |
| ステップ 4 | **no security wpa akm dot1x**<br>例：<br>`Device(config-wlan)# no security wpa akm dot1x` | dot1x に対するセキュリティの AKM をディセーブルにします。 |
| ステップ 5 | **no security wpa wpa2**<br>例：<br>`Device(config-wlan)# no security wpa wpa2` | WPA2 セキュリティを無効にします。 |
| ステップ 6 | **mab request format attribute** {**1 groupsize** *size* **separator** *separator* [**lowercase** \| **uppercase**] \| **2** {**0** \| **7** \| **LINE**} **LINE** *password* \| **32 vlan access-vlan**}<br>例：<br>`Device(config)# mab request format attribute 1 groupsize 4 separator` | オプション。WLAN で MAC フィルタリングを使用する際のデリミタを設定します。<br>ここで、各変数は次のように定義されます。<br>**1**：MAB 要求に使用するユーザー名形式を指定します。<br>**groupsize** *size*：グループごとの 16 進数の桁数を指定します。有効な値の範囲は 1 ～ 12 です。<br>**separator** *separator*：グループを区切る方法を指定します。区切り文字は、コンマ、セミコロン、およびピリオドです。<br>**lowercase**：ユーザー名を小文字で指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | **uppercase**：ユーザー名を大文字で指定します。<br>**2**：すべてのMAB要求に使用するグローバルパスワードを指定します。<br>**0**：暗号化されていないパスワードを指定します。<br>**7**：非表示のパスワードを指定します。<br>**LINE**：暗号化されたパスワードまたは暗号化されていないパスワードを指定します。<br>*password*：回線パスワード。<br>**32**：NAS-Identifier 属性を指定します。<br>**vlan**：VLAN を指定します。<br>**access-vlan**：設定されたアクセス VLAN を指定します。 |
| ステップ 7 | **no security wpa wpa2 ciphers aes**<br>例：<br>`Device(config-wlan)# no security wpa wpa2 ciphers aes` | AES の WPA2 暗号化をディセーブルにします。 |
| ステップ 8 | **no shutdown**<br>例：<br>`Device(config-wlan)# no shutdown` | WLAN をイネーブルにします。 |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。