# 中央 Web 認証


- 中央 Web 認証について （1 ページ）
- ISE の設定方法 （2 ページ）
- コントローラでの中央 Web 認証の設定方法 （4 ページ）
- スリープ状態にあるクライアントの認証 （13 ページ）


## 中央 Web 認証について

中央 Web 認証では、Web ポータルとして機能する中央デバイス（この例では ISE）を配置することができます。通常のローカル Web 認証と比較した場合の主な相違点は、MAC フィルタリングまたは dot1x 認証に伴ってレイヤ 2 にシフトされることです。また、RADIUS サーバー（この例では ISE）が、スイッチに対して Web リダイレクションの必要性を指示する特別な属性を返す点も異なります。このソリューションにより、Web 認証を開始する際の遅延が解消されます。

クライアントステーションの MAC アドレスがグローバルに RADIUS サーバーに知られていない場合（ただし他の基準を使用することも可能）、サーバーはリダイレクション属性を返し、組み込みワイヤレスコントローラは（MAC フィルタリングを使用して）ステーションを認可しますが、Web トラフィックをポータルへリダイレクトするためのアクセスリストを配置します。

ユーザがゲスト ポータルへログインすると、クライアントの再認証が可能になり、認可変更（CoA）を使用する新しいレイヤ 2 MAC フィルタリングが行われます。これにより、ISE が Web 認証ユーザーだったことが ISE によって記憶され、ISE は、ネットワークにアクセスするために必要な許可属性を 組み込みワイヤレスコントローラにプッシュします。

## 中央 Web 認証の前提条件

- Cisco Identity Services Engine（ISE）

# ISE の設定方法

ISE を設定するには、次の手順に従います。

1. 認可プロファイルを作成します。
2. 認証ルールを作成します。
3. 認可ルールを作成します。

## 認可プロファイルの作成

**手順**

**ステップ 1** [Policy] をクリックし、[Policy Elements] をクリックします。

**ステップ 2** [Results] をクリックします。

**ステップ 3** [Authorization] を展開し、[Authorization Profiles] をクリックします。

**ステップ 4** [Add] をクリックして、中央 Web 認証用の新しい認可プロファイルを作成します。

**ステップ 5** [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

**ステップ 6** [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

**ステップ 7** [Web Redirection (CWA, MDM, NSP, CPP)] チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。

**ステップ 8** [ACL] フィールドに、リダイレクトするトラフィックを定義する ACL の名前を入力します。たとえば、「redirect」などと入力します。

**ステップ 9** [Value] フィールドで、デフォルト値またはカスタマイズされた値を選択します。

[Value] 属性は、ISE がデフォルトの Web ポータルを参照するか、または ISE 管理者が作成したカスタム Web ポータルを参照するかを定義します。

**ステップ 10** [**Save**] をクリックします。

## 認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順に従います。

**手順**

**ステップ 1** **[Policy]** > **[Authentication]** ページで、[Authentication] をクリックします。

**ステップ 2** 認証ルールの名前を入力します。たとえば、「MAB」と入力します。

**ステップ 3** [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。

**ステップ 4** [Compound condition] を選択し、[Wireless_MAB] を選択します

**ステップ 5** [and ...] の横にある矢印をクリックして、ルールをさらに展開します。

**ステップ 6** [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。

**ステップ 7** [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションを使用すると、MAC アドレスが不明な場合でもデバイスを認証できます。

**ステップ 8** [**Save**] をクリックします。

# 認可ルールの作成

認可ポリシーでは多数のルールを設定できます。このセクションでは [MAC not known] ルールが設定されています。

**手順**

**ステップ 1** [Policy] > [Authorization] をクリックします。

**ステップ 2** [Rule Name] フィールドに、名前を入力します。たとえば、「Mac not known」などと入力します。

**ステップ 3** [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

**ステップ 4** [Compound Conditions] を選択し、[Wireless_MAB] を選択します

**ステップ 5** 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

**ステップ 6** [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [AuthenticationStatus] を選択します。

**ステップ 7** [Equals] 演算子を選択します。

**ステップ 8** 右側のフィールドから、[UnknownUser] を選択します。

**ステップ 9** [Permissions] フィールドで、以前に作成した認可プロファイル名を選択します。

ISE は、ユーザー（または MAC）が不明の場合でも続行されます。

これで、不明なユーザーにログインページが表示されるようになりました。ただし、ユーザーが自分のログイン情報を入力すると、再び ISE の認証要求が表示されます。そのため、ユーザーがゲストユーザーである場合に満たされる条件で別のルールを設定する必要があります。たとえば、「UseridentityGroup Equals Guest」を使用している場合に、すべてのゲストがこのグループに属すると仮定します。

**ステップ 10** [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

**ステップ 11** [Compound Conditions] を選択し、新しい条件の作成を選択します。

新しいルールは「MAC not known」ルールの前に置く必要があります。

**ステップ 12** 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

**ステップ 13** [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [UseCase] を選択します。

**ステップ 14** [Equals] 演算子を選択します。

**ステップ 15** 右側のフィールドから、[GuestFlow] を選択します。

**ステップ 16** [Permissions] フィールドで、プラス（[+]）アイコンを選択してルールの結果を選択します。

[Standard] > [PermitAccess] オプションを選択するか、または必要な属性を返すカスタム プロファイルを作成できます。

ユーザがログイン ページで承認されると、レイヤ 2 認証の再起動の結果として、ISE により COA がトリガーされます。ユーザーがゲスト ユーザーとして識別されると、ユーザーが承認されます。

# コントローラでの中央 Web 認証の設定方法

コントローラで中央 Web 認証を設定するには、次の手順に従います。

1. WLAN を設定します。
2. ポリシー プロファイルを設定します。
3. リダイレクト ACL を設定します。
4. 中央 Web 認証用の AAA を設定します。
5. Flex プロファイルでリダイレクト ACL を設定します。

## WLAN の設定（GUI）

### 始める前に

リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

### 手順

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

**ステップ 2** [WLANs] ウィンドウで、WLAN の名前をクリックするか、[Add] をクリックして新規に作成します。

**ステップ 3** 表示される [Add/Edit WLAN] ウィンドウで、[General] タブをクリックして次のパラメータを設定します。

- [Profile Name]フィールドで、プロファイルの名前を入力または編集します。
- [SSID] フィールドで、SSID 名を入力または編集します。

  SSID 名には、最大 32 文字の英数字を使用できます。
- [WLAN ID] フィールドで、ID 番号を入力または編集します。有効な範囲は 1 ～ 512 です。
- [Radio Policy] ドロップダウンリストから、[802.11] 無線帯域を選択します。
- [Broadcast SSID] トグルボタンを使用して、ステータスを [Enabled] または [Disabled] に変更します。
- [Status] トグルボタンを使用して、ステータスを [Enabled] または [Disabled] に変更します。

**ステップ 4** [Security] タブ、[Layer 2] タブの順にクリックして、次のパラメータを設定します。

- [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。この設定により、レイヤ 2 セキュリティが無効になります。
- [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。
- 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。
- OWE を選択すると、Opportunistic Wireless Encryption（OWE）によって、AP 無線とワイヤレスクライアント間の無線暗号化によるデータの機密性が提供されます。OWE 移行モードは、一種の下位互換性を提供することを目的としています。
- 高速移行を選択すると、高速ローミングの IEEE 標準である 802.11r によって、対応するクライアントがターゲットアクセスポイントにローミングする前でも、新しい AP との最初のハンドシェイクが実行されるローミングの新しい概念が導入されます。この概念は高速移行と呼ばれます。
- WLAN で MAC フィルタリングを有効にするには、チェックボックスをオンにします。

**ステップ 5** [Save & Apply to Device] をクリックします。

# WLAN の設定（CLI）

（注） リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

WLAN の設定を完了後、変更がすべての AP にプッシュされていない場合、次の Syslog メッセージが表示されます。

*2021/01/06 16:20:00.597927186 {wncd_x_R0-4}{1}: [wlanmgr-db] [20583]: UUID: 0, ra: 0, TID: 0 (note): Unable to push WLAN config changes to all APs, cleanup required for WlanId: 2, profile: wlan1 state: Delete pending*

前述の Syslog メッセージが 6 分以上表示される場合は、コントローラをリロードします。

コントローラがリロードせず、まだ Syslog メッセージが表示されている場合は、アーカイブログ、wncd コアファイルを収集し、リンク（Support Case Manager）をクリックしてケースを提起します。

**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>`Device(config)# wlan wlanProfileName 1 ngwcSSID` | WLAN コンフィギュレーション サブモードを開始します。<br>**wlan-name** は、設定されている WLAN の名前です。<br>**wlan-id** はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 512 です。<br>**SSID-name** は、最大 32 文字の英数字からなる SSID 名です。<br>（注） すでにこのコマンドを設定している場合は、**wlan wlan-name** コマンドを入力します。 |
| **ステップ 2** | **mac-filtering** [*name*]<br>**例：**<br>`Device(config-wlan)# mac-filtering name` | WLAN での MAC フィルタリングを有効にします。<br>（注） 認証リストを事前に設定していない場合は、MAC フィルタリングの設定時にデフォルトの認証リストが仮定されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| 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 shutdown**<br>例：<br>`Device(config-wlan)# no shutdown` | WLAN をイネーブルにします。 |
| ステップ 5 | **end**<br>例：<br>`Device(config-wlan)# end` | 特権 EXEC モードに戻ります。 |

### 例

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

# ポリシー プロファイルの設定（CLI）

（注） AAA または ISE サーバーからのポリシーを適用するには、AAA オーバーライドが必要です。リダイレクト URL とリダイレクト ACL を ISE サーバーから受信すると、NAC を使用して中央 Web 認証（CWA）がトリガーされます。

クライアントが関連付けられるポリシープロファイルで、NAC と AAA オーバーライドの両方が使用可能である必要があります。

AP が他のどのポリシープロファイルにも関連付けられていない場合、デフォルト ポリシープロファイルが AP に関連付けられます。

### 手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **wireless profile policy default-policy-profile**<br>例：<br>`Device(config)# wireless profile policy default-policy-profile` | ポリシープロファイルを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **vlan vlan-id**<br>例：<br>`Device(config-wireless-policy)# vlan 41` | VLANをポリシープロファイルにマッピングします。vlan-id を指定しない場合は、デフォルトのネイティブの vlan 1 が適用されます。vlan-id の有効な範囲は 1 ～ 4096 です。<br>ポリシープロファイルに VLAN が設定されていない場合、管理 VLAN が適用されます。 |
| ステップ 3 | **aaa-override**<br>例：<br>`Device(config-wireless-policy)# aaa-override` | AAA サーバーまたは ISE サーバーから受信したポリシーを適用するようにAAAオーバーライドを設定します。 |
| ステップ 4 | **nac**<br>例：<br>`Device(config-wireless-policy)# nac` | ポリシープロファイルでネットワークアクセス コントロールを設定します。NAC は、中央 Web 認証（CWA）をトリガーするために使用されます。 |
| ステップ 5 | **no shutdown**<br>例：<br>`Device(config-wireless-policy)# no shutdown` | WLAN をイネーブルにします。 |
| ステップ 6 | **end**<br>例：<br>`Device(config-wireless-policy)# end` | 特権 EXEC モードに戻ります。 |

### 例

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

# ポリシー プロファイルの設定（GUI）

### 手順

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

**ステップ 2** [Policy Profile] ページで、[Add] をクリックします。

**ステップ 3** [Add Policy Profile] ウィンドウの [General] タブで、ポリシー プロファイルの名前と説明を入力します。

**ステップ 4** ポリシー プロファイルを有効にするには、[Status] を [Enabled] に設定します。

**ステップ 5** スライダを使用して、[Passive Client] と [Encrypted Traffic Analytics] を有効または無効にします。

**ステップ 6** （任意） [CTS Policy] セクションで、次について適切なステータスを選択します。

- [Inline Tagging]： 組み込みワイヤレスコントローラまたはアクセスポイントが送信元 SGT を認識するために使用するトランスポートメカニズム。
- [SGACL Enforcement]

**ステップ 7** デフォルトの **SGT** を指定します。有効な範囲は 2 ～ 65519 です。

**ステップ 8** [WLAN Switching Policy] セクションで、必要に応じて次を選択します。

- [Central Switching]
- [Central Authentication]
- Central DHCP
- [Central Association Enable]
- [Flex NAT/PAT]

**ステップ 9** [Save & Apply to Device] をクリックします。

# リダイレクト ACL の作成

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **ip access-list extended redirect**<br>**例**：<br>`Device(config)# ip access-list extended redirect` | ISE がリダイレクト ACL（**redirect** という名前）を使用するように設定されているため、HTTP および HTTPS ブラウジングは（他の ACL ごとの）認証なしでは機能しません。 |
| **ステップ 2** | **deny ip any host ISE-IP-add**<br>**例**：<br>`Device(config)# deny ip any host 123.123.134.112` | ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **deny ip host ISE-IP-add any**<br>例：<br>`Device(config)# deny ip host 123.123.134.112 any` | ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。<br>（注） このACLは、ローカルモードと flex モードの両方に適用できます。 |
| ステップ 4 | **permit TCP any any eq web address/port-number**<br>例：<br>HTTP の場合：<br>`Device(config)# permit TCP any any eq www`<br>`Device(config)# permit TCP any any eq 80`<br>例：<br>HTTPS の場合：<br>`Device(config)# permit TCP any any eq 443` | ISE ログイン ページへのすべての HTTP または HTTPS アクセスをリダイレクトします。HTTP ではポート番号 80 が使用され、HTTPS では ポート番号 443 が使用されます。<br>ACE が ISE へのトラフィックを許可するには、ISE を HTTP/HTTPS ACE の上に設定する必要があります。 |
| ステップ 5 | **end**<br>例：<br>`Device(config)# end` | 特権 EXEC モードに戻ります。 |

# 中央 Web 認証用の AAA の設定

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **aaa server radius dynamic-author**<br>例：<br>`Device(config)# aaa server radius dynamic-author` | 組み込みワイヤレスコントローラの認可変更（CoA）を設定します。 |
| ステップ 2 | **client ISE-IP-add server-key radius-shared-secret**<br>例：<br>`Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET` | RADIUS クライアントと RADIUS キーがデバイスと RADIUS クライアントの間で共有されるように指定します。<br>**ISE-IP-add** は RADIUS クライアントの IP アドレスです。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | **server-key** は RADIUS クライアントのサーバーキーです。<br>radius-shared-secret の内容は以下のとおりです。<br>• **0**：暗号化されていないキーを指定します。<br>• **6**：暗号化されたキーを指定します。<br>• **7**：「隠し」キーを指定します。<br>• **Word**：暗号化されていない（クリアテキスト）サーバー キー。<br>GUI で WSMA データを設定する場合、RADIUS 共有秘密は 240 文字を超えることはできません。<br>（注） これらのステップはすべて、AAA が設定されている場合にのみ機能します。詳細については、「AAA 認証の設定」を参照してください。 |

**例**

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 server-key 0 SECRET
Device(config-locsvr-da-radius)# end
```

# Flex プロファイルでのリダイレクト ACL の設定（GUI）

リダイレクト ACL の定義を FlexConnect プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホストされている FlexConnect プロファイルに設定する必要があります。アクセス ポイントがどの FlexConnect プロファイルでも設定されていない場合は、デフォルトの FlexConnect プロファイルが関連付けられます。

**手順**

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

**ステップ 2** [Flex Profile] ページで、 FlexConnect プロファイルの名前をクリックするか、[Add] をクリックして新しい FlexConnect プロファイルを作成します。

**ステップ 3** 表示される [Add/Edit Flex Profile] ウィンドウで、[Policy ACL] タブをクリックします。

**ステップ 4** [Add] をクリックして、ACL を FlexConnect プロファイルにマッピングします。

**ステップ 5** ACL 名を選択し、中央 Web 認証を有効にして、認証 URL フィルタを指定します。

**ステップ 6** [Save] をクリックします。

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

# Flex プロファイルでのリダイレクト ACL の設定（CLI）

リダイレクト ACL の定義を Flex プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホストされている Flex プロファイルに設定する必要があります。アクセス ポイントがどの Flex プロファイルでも設定されていない場合は、デフォルトの Flex プロファイルが関連付けられます。

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **wireless profile flex default-flex-profile**<br>例：<br>`Device(config)# wireless profile flex default-flex-profile` | 新しい flex ポリシーを作成します。デフォルトの flex プロファイル名は **default-flex-profile** です。 |
| **ステップ 2** | **acl-policy** *acl policy name*<br>例：<br>`Device(config-wireless-flex-profile)# acl-policy acl1` | ACL ポリシーを設定します。 |
| **ステップ 3** | **central-webauth**<br>例：<br>`Device(config-wireless-flex-profile-acl)# central-webauth` | 中央 Web 認証を設定します。 |
| **ステップ 4** | **end**<br>例：<br>`Device(config-wireless-flex-profile-acl)# end` | 特権 EXEC モードに戻ります。 |

# スリープ状態にあるクライアントの認証

## スリープ状態にあるクライアントの認証について

Web 認証に成功したゲスト アクセスを持つクライアントは、ログイン ページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は10～43200分、デフォルトは720分です。この期間は、WLANにマッピングされているWebAuthパラメータマップでも設定できます。スリープ状態にあるクライアントのタイマーは、アイドルタイムアウト、セッションタイムアウト、WLAN の無効化、AP の停止などのインスタンスが原因で有効になることに注意してください。

この機能は FlexConnect のローカル スイッチング、中央認証のシナリオでサポートされています。

⚠

**注意** スリープ モードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

### モビリティのシナリオ

次に、モビリティ シナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープ タイマーを適用できます。
- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティグループに2台の組み込みワイヤレスコントローラがあるとします。1台の組み込みワイヤレスコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方の 組み込みワイヤレスコントローラに関連付けられます。
- モビリティグループに3台の組み込みワイヤレスコントローラがあるとします。1台目の組み込みワイヤレスコントローラにアンカーされた2台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3台目の組み込みワイヤレスコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポートアンカーにアンカーされた同じまたは別のエクスポート外部 組み込みワイヤレスコントローラに関連付けられます。

# スリープ状態にあるクライアントの認証に関する制約事項

- スリープ クライアント機能は、WebAuth セキュリティが設定された WLAN に対してのみ動作します。
- スリープ状態にあるクライアントは WebAuth パラメータマップごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ 3 セキュリティが有効な WLAN でのみサポートされています。
- レイヤ 3 セキュリティでは、認証、パススルー、および On MAC Filter 失敗 Web ポリシーがサポートされています。条件付き Web リダイレクトとスプラッシュ ページ Web リダイレクト Web ポリシーはサポートされていません。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザー ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。

# スリープ状態のクライアントの認証の設定（GUI）

**手順**

**ステップ 1** **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

**ステップ 2** [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

**ステップ 3** [Sleeping Client Status] チェックボックスをオンにします。

**ステップ 4** [Update & Apply to Device] をクリックします。

# スリープ状態のクライアントの認証の設定（CLI）

**手順**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **[no] parameter-map type webauth** {*parameter-map-name* \| **global**}<br>例：<br>`Device(config)# parameter-map type webauth global` | パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **sleeping-client** [ **timeout** *time*]<br>例：<br>`Device(config-params-parameter-map)# sleeping-client timeout 100` | スリープ状態のクライアントのタイムアウトを100分に設定します。有効な範囲は 10 ～ 43200 分です。<br>（注） タイムアウト キーワードを使用しない場合、スリープ状態のクライアントにはデフォルトのタイムアウト値である720分が設定されます。 |
| ステップ 3 | **end** | parameter-map webauth コンフィギュレーションモードを終了し、特権EXECモードに戻ります。 |
| ステップ 4 | （任意） **show wireless client sleeping-client**<br>例：<br>`Device# show wireless client sleeping-client` | クライアントのMACアドレスと、それぞれのセッションの残り時間を表示します。 |
| ステップ 5 | （任意） **clear wireless client sleeping-client** [ **mac-address** *mac-addr*]<br>例：<br>`Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001` | • **clear wireless client sleeping-client**：スリープ状態のクライアントキャッシュからスリープ状態のクライアント エントリをすべて削除します。<br>• **clear wireless client sleeping-client mac-address** *mac-addr*：スリープ状態のクライアント キャッシュから特定の MAC エントリを削除します。 |