WLAN セキュリティ

レイヤ 2 セキュリティ

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN には、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーが設定されている必要があります。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
- Static WEP または 802.1X

（注）

- Static WEP と 802.1x はどちらも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるため、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、それらの両方を 使用できません。
- WLAN WEP は、1810w アクセス ポイントではサポートされません。

- WPA/WPA2

（注）

- 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（WPA）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。
- TKIP サポートが設定された WLAN は RM3000AC モジュールでは有効になりません。

注意事項と制約事項

- WLAN が暗号化キーなしでレイヤ 2 セキュリティ WEP で設定されている場合、次の XML メッセージが表示されます。

```
apf_xml_validate_vapStatus: Encryption mode 0 for static WEP does not match encryption
 mode 2 for dynamic WEP
Validation for node ptr_apfCfgData.apfVAPIDData.apfVapStatus failed, indices for
node are 11
```

- レイヤ 2 の保護が必要で、MAC スプーフィングを防止する場合は、Web 認証と WPA2-PSK や WPA2 dot1x などのレイヤ 2 セキュリティを組み合わせることをお勧めします。

認証

802.1X 動的キーおよび許可の設定（CLI）

コントローラでは、アクセス ポイント上で Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X Dynamic WEP キーを制御できます。また、WLAN の 802.1X ダイナミック キー設定をサポートしています。

（注） Lightweight アクセス ポイントとワイヤレス クライアントで LEAP を使用するには、CiscoSecure Access Control Server（ACS）を設定する際に RADIUS サーバ タイプとして [Cisco-Aironet] を選択することを確認します。

- 各 WLAN のセキュリティ設定を確認するには、次のコマンドを入力します。

  show wlan *wlan_id*

  新しい WLAN のデフォルトのセキュリティ設定は、ダイナミック キーが有効な 802.1X です。レイヤ 2 の堅牢なポリシーを維持するには、802.1X を WLAN 上で設定したままにします。

- 次のコマンドを入力して、802.1X 暗号化を無効または有効にします。

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

  802.1X 認証を有効にした後、コントローラから、ワイヤレス クライアントと認証サーバとの間で EAP 認証パケットが送信されます。このコマンドにより、すべての EAP タイプのパケットは、コントローラとの送受信が可能になります。

  （注） コントローラは、同じ WLAN で Web 認証と 802.1X 認証の両方を実行します。クライアントは、最初に 802.1x で認証されます。認証が成功すると、クライアントは、Web 認証クレデンシャルを提供する必要があります。Web 認証が成功すると、クライアントは RUN 状態に移行します。

- 次のコマンドを入力して、WLAN の 802.1X 暗号化レベルを変更します。

  config wlan security 802.1X encryption *wlan_id* **[0 | 40 | 104]**

  - Use the **0** option to specify no 802.1x encryption.
  - 40/64 ビット暗号化を指定するには、**40** オプションを使用します。
  - 104/128 ビット暗号化を指定するには、**104** オプションを使用します。（これは、デフォルトの暗号化設定です）。

RADIUS VSA

RADIUS VSA に関する情報

インターネット エンジニアリング タスク フォース（IETF）のドラフト標準では、ネットワーク アクセス サーバと RADIUS サーバ間でベンダー固有の属性（VSA）を使用してベンダー固有の情報を伝達する方法が規定されています。VSA を使用すれば、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。VSA は XML ファイル内で事前に定義されます。XML ファイルにベンダー固有の属性を追加する必要があり、この XML ファイルがコントローラにダウンロードされます。このサポートを有効にするためにコントローラ上で実施しな

ければならない設定はありません。ファイルには、XMLタグを指定するためのXMLスキーマで規定されている特定の形式で RADIUS 属性が含まれています。

定義されたベンダー固有の属性を含むXMLファイルはFTPサーバからダウンロードできます。ダウンロードしたファイルはフラッシュ メモリに保存され、複数のリブート プロセスを通して保持されます。ファイルは、ダウンロードが成功したときとコントローラが起動するたびに解析されます。XML ファイルは RADIUS サーバにアップロードして認証とアカウンティングに使用できます。コントローラは、これらの値を解析すると、そのファイルをベンダー固有の属性を保存するための別のデータ構造に保存します。また、指定された使用形式に基づいて、認証パケットとアカウンティングパケットのどちらかまたはその両方でこれらの属性値を使用します。ファイルにエラーが含まれている場合は、コントローラの解析が失敗して、属性が適用されません。ファイル内のエラーを修正するか、ファイルをFTPサーバからコントローラにダウンロードし直す必要があります。

RADIUS AVP リストの *XML* サンプル ファイル

参照用に、RADIUS AVP リストの XML サンプル ファイルを使用できます。サンプル XML ファイルには 2 個の属性のみが含まれていて、1 つは認証用、もうひとつはアカウンティング用です。RADIUS の属性と値のペアを追加することができますが、これらの属性と値のペアは、指定された形式で追加する必要があります。

（注） AVP のダウンロードでサポートされている WLAN の最大数は 32 です。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file edited by User1-->

<radiusFile>
<avpList SSID_PROF="test" incAuth="true" incAcct="false">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
<avpList SSID_PROF="test" incAcct="true">
        <radiusAttributes>
                <attributeName>Idle-Timeout</attributeName>
                <vendorId>9</vendorId>
                <attributeId>21</attributeId>
                <valueType>INTEGER</valueType>
                <attributeValue>100</attributeValue>
        </radiusAttributes>
        <radiusAttributes>
                <attributeName>remote-name</attributeName>
```

```
                <vendorId>9</vendorId>
                <attributeId>26</attributeId>
                <valueType>STRING</valueType>
                <attributeValue>TEST</attributeValue>
        </radiusAttributes>
</avpList>
</radiusFile>
```

RADIUS AVP リストのダウンロード（*GUI*）

手順

ステップ 1 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 2 [File Type] ドロップダウン リストから、[RADIUS AVP List] を選択します。

ステップ 3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- **SFTP**

ステップ 4 [IP Address] テキスト ボックスに、サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

ステップ 5 [File Path] テキスト ボックスに、RADIUS AVP リストのディレクトリ パスを入力します。

ステップ 6 [File Name] テキスト ボックスに、RADIUS AVP リストの名前を入力します。

ステップ 7 FTP サーバを使用している場合は、次の手順に従います。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。

b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 コントローラに RADIUS AVP リストをダウンロードするには、[Download] をクリックします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 9 **[Security]** > **[AAA]** > **[RADIUS]** > **[Downloaded AVP]** を選択して、[Download RADIUS AVP List] ページを開きます。

ステップ 10 [WLAN SSID Profile name] ドロップダウン リストから、WLAN SSID プロファイル名を選択します。

ステップ 11 AVP リストにマッピングされた RADIUS 認証属性を表示するには、[Auth AVP] タブをクリックします。

ステップ 12 AVP リストにマッピングされた RADIUS アカウンティング属性を表示するには、[Acct AVP] タブをクリックします。

RADIUS AVP リストのアップロード（*GUI*）

手順

ステップ 1 **[Commands]** > **[Upload File]** の順に選択して、[Upload File from Controller] ページを開きます。

ステップ 2 [File Type] ドロップダウン リストから、[RADIUS AVP List] を選択します。

ステップ 3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- **SFTP**

ステップ 4 [IP Address] テキスト ボックスに、サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

ステップ 5 [File Path] テキスト ボックスに、RADIUS AVP リストのディレクトリ パスを入力します。

ステップ 6 [File Name] テキスト ボックスに、RADIUS AVP リストの名前を入力します。

ステップ 7 FTP サーバを使用している場合は、次の手順に従います。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。

b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

ステップ 8 コントローラから RADIUS AVP リストをアップロードするには、[Upload] をクリックします。アップロードのステータスを示すメッセージが表示されます。

RADIUS AVP リストのアップロードおよびダウンロード（*CLI*）

手順

ステップ 1 コントローラ CLI にログインします。

ステップ 2 次のコマンドを入力して、FTP サーバからコントローラに XML ファイル形式の RADIUS AVP をダウンロードします。

transfer download datatype radius-avplist

ステップ 3 次のコマンドを使用して、コントローラから RADIUS サーバへ XML ファイルをアップロードします。

transfer upload datatype radius-avplist

ステップ 4 次のコマンドを使用して、VSA AVP を表示します。

show radius avp-list *ssid-profile-name*

ダウンロード可能な *RADIUS AVP* を使用した *RADIUS* アカウンティングに対するカスタム *NAS-ID*

ダウンロード可能な RADIUS AVP を使用した RADIUS アカウンティングに対するカスタム NAS-ID について

この機能は、WLAN ごとのカスタム アカウンティング目的で設定可能なカスタム NAS-ID の設定ニーズに対応します。Cisco WLC に XML ファイルをダウンロードするには、FTP（サーバ）方式を使用するか、または転送ダウンロード方式を使用できます。このファイルは再起動後も WLC に保持されます。

カスタム AVP は、アカウンティング メッセージの WLAN NAS-ID にのみ優先します。他の NAS-ID の優先順位には影響を与えません。

（注）

- グローバル WLAN NAS-ID は、アカウンティング メッセージでは使用されません。WLAN で NAS-ID（WLAN/インターフェイス/apgroup）が設定されていない場合は、システム名がデフォルトの NAS-ID として送信されます。
- AVP リストは、アップロードおよびダウンロードされた設定ファイルとしてのみ利用できます。GUI、CLI、または SNMP 方式を使用して、Cisco WLC の AVP リストを設定または変更することはできません。
- ダウンロードされた AVP リストがないか、WLAN 固有またはインターフェイス固有の NAS-ID が設定されていない場合、システム名がデフォルトの NAS-ID になります。
- XML ファイルがプライマリ コントローラにダウンロードされている間に、スタンバイ コントローラも AVP リストを受信します。

カスタム AVP ファイルの作成方法については、*WLC* 構成ガイド [英語] の「*RADIUS VSA*」セクションを参照してください。

以下は、NAS-ID でサポートされている値の型です（すべて大文字）。

- SYSNAME
- SYSIP
- SYSMAC
- APIP
- APNAME
- APMAC
- APETHMAC
- APGROUP
- FLEXGROUP
- SSID

- APLOCATION

（注） 新しい NAS 識別子 AVP では、8.6 から古いバージョンへのソフトウェア ダウングレードはサポートされていません。古いバージョンにダウングレードする場合は、次の手順を実行します。

1. 既存の RADIUS AVP 属性ファイルをアップロードします。
2. ファイルを編集して NAS 識別子 AVP を削除します。
3. コントローラをダウングレードします。
4. NAS 識別子 AVP を指定せずに、変更された RADIUS AVP ファイルをダウンロードします。

ダウンロード可能な RADIUS AVP を使用した RADIUS アカウンティングに対するカスタム NAS-ID の制約事項

- カスタム NAS-ID 文字列には、「:」を区切り文字として使用して、最小で 1 つの値の型、最大で 3 つの値の型を含める必要があります。
- ダウンロードした NAS-ID に同じ SSID プロファイルに対する複数のカスタム NAS-ID 構文がある場合、デフォルトでは、古い構文を上書きした後で、最新の構文が使用されます。
- ダウンロード可能な WLAN SSID プロファイルの最大数は 32 です。
- 構文から得られるカスタム NAS-ID のサポートされる最大長は 253 です。

カスタム NAS-ID AVP XML ファイルの設定

手順

ステップ 1 メモ帳を使用して XML ファイルを編集します。

ステップ 2 AVP を適用する WLAN プロファイル名で **SSID_PROF** タグを更新します。

ステップ 3 次のフィールドを更新します。

- **vendorId** タグは 0 に更新
- **attributeId** は 32 に更新
- **Valuetype** は「STRING」に更新
- **attributeValue** は属性タグ文字列に更新（区切り文字は「:」）

（注） **incAuth** または **incAcct** の値を True に設定する必要があります。カスタム NAS-ID は、認証パケットおよびアカウンティング パケットに対して更新されます。標準の **attributeID** 値の 32 のみがサポートされています。その他の値は、ベンダー属性として送信されます。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<radiusFile>
 <avpList SSID_PROF="DocTest_8500_OPEN" incAuth="true" incAcct="true">
  <radiusAttributes>
   <attributeName>SVR-Zip-Code</attributeName>
   <vendorId>0</vendorId>
   <attributeId>32</attributeId>
   <valueType>STRING</valueType>
   <attributeValue> SYSNAME:APNAME:APLOCATION </attributeValue>
  </radiusAttributes>
  <radiusAttributes>
   <attributeName>W2BW-NASId</attributeName>
   <vendorId>0</vendorId>
   <attributeId>32</attributeId>
   <valueType>STRING</valueType>
  <attributeValue>SYSNAME:APNAME:APLOCATION</attributeValue>
    </radiusAttributes>
    </avpList>
  </radiusFile>
```

ステップ 4 更新された AVP XML ファイルを WLC にダウンロードします。

ステップ 5 RADIUS でダウンロードが失敗した場合は、**debug option debug radiusavp-xml enable** を使用して、エラーの詳細を確認します。

NAS-ID AVP の削除（GUI）

手順

ステップ 1 テキスト エディタを使用して AVP XML ファイルを編集し、SSID_PROF 名を削除します。

ステップ 2 更新された NAS-ID AVP XML ファイルを Cisco WLC にダウンロードします。

ステップ 3 **[Security]** > **[RADIUS]** > **[Downloaded AVP]** の順に選択します。[DOWNLOADED RADIUS AVP LIST] ページの [Acct] タブに空のページが表示されます。

NAS-ID AVP が正常に削除されます。

（注） この手順では、選択した SSID プロファイルを削除します。XML AVP リスト ファイルに複数の AVP が記載されている場合は、削除手順を使用して削除しない限り、それらの AVP は機能し続けます。

カスタム NAS-ID の拡張設定の表示（GUI）

手順

ステップ 1 **[WLANs]** > **[WLAN ID]** > **[General]** を選択して、[WLAN] > [Edit] ページを開きます。

ステップ 2 [General] タブで、グレー表示の [NAS-ID] フィールドで値の型を確認します。

そのファイルのフォーマットの構文がダウンロードされていて、文字列が表示されているかどうかを確認します。

例：

ダウンロードされた NAS-ID 構文	アカウンティングおよび認証 NAS-ID のエンコードされたフォーマット	使用されている区切り記号
APIP:APNAME:SYSNAME	9.11.12.2:AP_BASEMENT_1:WLC_1	「:」コロン

ステップ 3 **[Security]** > **[RADIUS]** > **[Downloaded AVP]** > **[Acct AVP]** タブを選択して、[DOWNLOADED RADIUS AVP LIST] ページを開きます。

ステップ 4 ドロップダウン リストから、[Wlan SSID Profile Name] を選択します。

AVP の詳細が表示されます。

カスタム NAS-ID の拡張設定の表示（CLI）

手順

- 次のコマンドを入力して、NAS-ID のダウンロードされた AVP を表示します。

  show radius avp-list *profile-name*

- 次のコマンドを入力して、MAC アドレスごとのクライアントの詳細情報を表示します。

  show client detail*mac-addr*

- 次のコマンドを入力して、RADIUS パケットを表示します。

  debug aaa all enable

- 次のコマンドを入力して、ダウンロード エラーの原因を特定するためにデバッグ ログを有効にします。

  debug aaa avp-xml enable

RADIUS レルム

RADIUS レルムについて

モバイルクライアントがWLANにアソシエートするときに、RADIUS レルムが認証要求パケット内の EAP-AKA ID 応答要求の一部として受信されます。WLAN のネットワーク アクセス識別子（NAI）形式（EAP-AKA）は、*0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org* と

して指定できます。NAI 形式のレルムは @ 記号の後ろに示され、*wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org* のように指定されます。ベンダー固有の属性が MCC については 311、MNC については 480 ～ 489 として追加された場合、その NAI 形式は *0311480999999999@wlan.mnc480.mcc311.3gppnetwork.org* のように指定できます。

モバイル加入者の場合、コントローラは、デバイスから受信した NAI 形式のレルムが特定の標準に従っている場合にのみ、AAA サーバに認証要求を送信します。認証とは別に、アカウンティング要求もレルム フィルタリングに基づいて AAA サーバに送信する必要があります。

コントローラ上でレルム フィルタリングをサポートするには、RADIUS 上でレルムを設定する必要があります。ユーザが特定の SSID を使用して接続されている場合、RADIUS サーバ上で設定されたレルムに対して受信された NAI 形式を使用してユーザが認証および認可されます。

WLAN 上のレルム サポート

各 WLAN は NAI レルムをサポートするように設定されます。レルムが特定の SSID に対して有効になっている場合は、RADIUS サーバ上で設定されたレルムに対して EAP ID 応答で受信されたレルムを照合するためのルックアップが実施されます。

RADIUS サーバ上のレルム サポート

RADIUS サーバは、設定されたレルムに基づいて認証要求とアカウンティング要求をリダイレクトする必要があります。1 つの RADIUS サーバが認証とアカウンティングごとに最大 30 のレルムをサポートします。

- **認証用のレルム照合**：EAP 方式を使用した WPA2 dot1x（EAP AKA と同様）では、ユーザ名が EAP ID 応答の一部として受信されます。レルムは、ユーザ名から抽出され、RADIUS 認証サーバで設定されたレルムと照合されます。一致した場合は、認証要求が RADIUS サーバに転送されます。一致しなかった場合は、クライアントが認証解除されます。
- **アカウンティング用のレルム照合**：ユーザ名が Access Accept メッセージで受信されます。アカウンティング メッセージがトリガーされると、レルムがユーザ名から抽出され、RADIUS アカウンティング サーバ上で設定されたアカウンティング レルムと比較されます。一致した場合は、アカウンティング要求が RADIUS サーバに転送されます。一致しなかった場合は、アカウンティング要求が破棄されます。たとえば、レルムがコントローラ上で **cisco** として設定されている場合は、RADIUS サーバ上でユーザ名が **xyz@cisco** として認証されます。

（注） NAI レルムが WLAN 上で有効になっていても、レルムがユーザ名に含まれていない場合は、動作がデフォルトでルックアップなしに設定され、RADIUS サーバの通常の選択が使用されます。

（注） クライアントが高速再認証識別を使用すると、コントローラで対応する要求を正しいサーバに転送するために、認証サーバからレルム名が要求されます。

EAP-AKA をレルムと組み合わせて使用したとき、eap サーバがユーザ名部分とレルム部分の両方がある AT_NEXT_REAUTH_ID 属性で応答すると、高速再認証がサポートされます。レルムの目的は、受信コントローラが後続の高速再認証要求で正しいサーバをつかまえることです。たとえば EAP-AKA をサポートしているしているホスト apd サーバはレルム部分をサポートしません。したがって Cisco WLC は、この互換性がある eap サーバについてのみ、高速再認証をサポートしています。

RADIUS レルムの設定の前提条件

RADIUS 認証またはアカウンティング サーバは、レルムを追加する前に無効し、コントローラ上でレルムを追加した後に有効にする必要があります。

RADIUS レルムの設定に関する制約事項

- 1 つのコントローラに、最大 17 個の RADIUS 認証サーバおよびアカウンティング サーバを設定できます。
- 1 つの RADIUS 認証サーバおよびアカウンティング サーバに対して、設定できるレルムの合計数は 30 です。

WLAN でのレルムの設定（*GUI*）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

ステップ 4 WLAN でレルムを有効にするには、[RADIUS NAI-Realm] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

WLAN でのレルムの設定（*CLI*）

手順

ステップ 1 次のコマンドを入力して、WLAN でレルムを有効または無効にします。
config wlan*radius_server* **realm** {**enable** | **disable**} *wlan id*

ステップ 2 次のコマンドを入力して、 WLAN のレルムの設定を表示します。
show wlan *wlan-id*

RADIUS 認証サーバでのレルムの設定（*GUI*）

手順

ステップ 1 **[Security]** > **[AAA]** > **[RADIUS]** > **[Authentication]** を選択し、[RADIUS Authentication Servers > Edit] ページを開きます。

ステップ 2 [Realm List] リンクをクリックし、[Authentication Server Index] ページを開きます。

ステップ 3 [Realm Name] テキスト ボックスにレルム名を入力します。

ステップ 4 [Add] をクリックします。

RADIUS 認証サーバでのレルムの設定（*CLI*）

手順

ステップ 1 次のコマンドを入力して、RADIUS 認証サーバにレルムを追加します。
config radius auth realm add *radius_index realm_string*

ステップ 2 次のコマンドを入力して、RADIUS 認証サーバからレルムを削除します。
config radius auth realm delete *radius_index realm_string*

ステップ 3 次のコマンドを入力して、RADIUS 認証サーバの情報を表示します。
show radius auth detailed *radius_index*

RADIUS アカウンティング サーバでのレルムの設定（*GUI*）

手順

ステップ 1 **[Security]** > **[AAA]** > **[RADIUS]** > **[Accounting]** を選択し、[RADIUS Accounting Servers > Edit] ページを開きます。

ステップ 2 [Realm List] リンクをクリックし、[Accounting Server Index] ページを開きます。

ステップ 3 [Realm Name] テキスト ボックスにレルム名を入力します。

ステップ 4 [Add] をクリックします。

RADIUS アカウンティング サーバでのレルムの設定（*CLI*）

手順

ステップ 1 次のコマンドを入力して、RADIUS アカウンティング サーバにレルムを追加します。
config radius acct realm add *radius_index realm_string*

ステップ 2 次のコマンドを入力して、RADIUS アカウンティング サーバからレルムを削除します。
config radius acct realm delete *radius_index realm_string*

ステップ 3 次のコマンドを入力して、RADIUS アカウンティング サーバの情報を表示します。
show radius acct detailed *radius_index*

Identity ネットワー キング

Identity ネットワーキングについて

ほとんどの無線 LAN システムの場合、各 WLAN に静的なポリシーがあり、SSID が設定されているすべてのクライアントに適用されます。これは強力な方式ですが、クライアントに複数の Quality of Service（QoS）およびセキュリティ ポリシーを適用するには、そのクライアントに複数の SSID を設定する必要があるために、限界がありました。

これに対し、Cisco Wireless LAN ソリューションは Identity ネットワーキングをサポートしており、ネットワークが 1 つの SSID をアドバタイズできると同時に、ユーザ プロファイルに基づいて、個々のユーザに異なる QoS またはセキュリティ ポリシーを適用することができます。Identity ネットワーキングを使用して制御できるポリシーは次のとおりです。

- ACL：ACL 属性が RADIUS Access Accept で指定されている場合、システムは認証後に ACL 名をクライアント ステーションに適用します。これにより、インターフェイスに当てられているすべての ACL は上書きされます。
- VLAN：VLAN Interface-Name または VLAN-Tag が RADIUS Access Accept で指定されている場合、システムはクライアントを特定のインターフェイスに割り当てます。

（注） VLAN 機能は、MAC フィルタリング、802.1X、および WPA のみをサポートします。VLAN 機能では Web 認証または IPSec はサポートされません。

- トンネル属性。

（注） この項で後述する他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

オペレーティング システムのローカル MAC フィルタ データベースは、インターフェイス名を含むように拡張されました。これにより、クライアントを割り当てるインターフェイスをローカル MAC フィルタで指定できるようになりました。別の RADIUS サーバも使用できますが、その RADIUS サーバは [Security] メニューを使用して定義する必要があります。

Identity ネットワーキングで使用される *RADIUS* 属性

QoS-Level

この項では、Identity ネットワーキングで使用される RADIUS 属性について説明します。

この属性は、スイッチング ファブリック内、および無線経由のモバイル クライアントのトラフィックに適用される QoS レベルを示しています。この例は、QoS-Level 属性フォーマットの要約を示しています。テキスト ボックスは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           QoS Level                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – 3 オクテット：
  - 3 – Bronze（バックグラウンド）
  - 0 - Silver（ベストエフォート）
  - 1 – Gold（ビデオ）
  - 2 – Platinum（音声）

ACL-Name

この属性は、クライアントに適用される ACL 名を示します。ACL-Name 属性形式の要約を次に示します。テキスト ボックスは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – クライアントに対して使用する ACL の名前を含む文字列

Interface Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。Interface-Name 属性形式の要約を次に示します。テキスト ボックスは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Interface Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – クライアントが割り当てられるインターフェイスの名前を含む文字列

（注） この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

グループ化

この属性は、特定のトンネル セッションのグループ ID を示し、Tunnel-Private-Group-ID 属性とも呼ばれます。

この属性は、トンネルの発信側が、特定の接続からグループを事前に判別できる場合は Access-Request パケットに含めることができ、このトンネル セッションを特定のプライベート グループに属するものとして処理する場合は Access-Accept パケットに含める必要があります。プライベート グループは、トンネル セッションを特定のユーザのグループと関連付けるために使用できます。たとえば、未登録の IP アドレスが特定のインターフェイスを通過するようにするルーティングを容易にするために使用できます。Start と Stop のいずれかの値を持つ Acct-Status-Type 属性を含み、かつトンネル セッションに関連する Accounting-Request パケットには、プライベート グループを含める必要があります。

Tunnel-Private-Group-ID 属性形式の要約を次に示します。テキスト ボックスは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 81（Tunnel-Private-Group-ID 用）
- Length – >= 3
- Tag：Tag テキスト ボックスは、長さが 1 オクテットで、同じパケット内で同じトンネルを示す属性をグループ化するために使用されます。Tag テキスト ボックスの値が 0x00 より大きく、0x1F 以下である場合、その値は（いくつかの選択肢のうち）この属性が関連しているトンネルを示すと解釈されます。Tag テキスト ボックスが 0x1F より大きい場合、その値は後続の String テキスト ボックスの最初のバイトであると解釈されます。
- String：これは必須のテキスト ボックスです。グループはこの String テキスト ボックスによって表されます。グループ ID の形式に制約はありません。

（注） この項の他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

トンネル属性

RFC 2868 では、認証と許可に使用される RADIUS トンネル属性が定義されています。RFC2867 では、アカウンティングに使用されるトンネル属性が定義されています。IEEE 802.1X Authenticator がトンネリングをサポートしている場合は、認証の結果としてサプリカントに対して強制的なトンネルを設定できます。

これは特に、認証の結果に基づいて IEEE8021Q で定義されている特定の VLAN にポートを配置できるようにする場合に適しています。たとえば、この設定を使用すると、ワイヤレス ホストがキャンパス ネットワーク内を移動するときに同じ VLAN 上にとどまれるようになります。

RADIUS サーバは、一般的に、Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。ただし IEEE 802.1X Authenticator も、Access- Request 内にトンネル属性を

含めることによって、サプリカントに割り当てる VLAN に関するヒントを示すことができます。

VLAN 割り当てのために、次のトンネル属性が使用されます。

- Tunnel-Type=VLAN（13）
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

VLAN ID は、1 ～ 4094（両端の値を含む）の 12 ビットの値です。RFC 2868 で定義されているように、IEEE 802.1X で使用される Tunnel-Private-Group-ID は文字列型であるため、VLAN ID の整数値は文字列としてエンコードされます。

トンネル属性が送信されるときは、Tag テキスト ボックスに値が含まれている必要があります。RFC 2868 の第 3.1 項には次のように明記されています。

- Tag テキスト ボックスは長さが 1 オクテットであり、同じパケット内で同じトンネルを示す属性をグループ化するために使用されます。このテキストボックスの有効な値は、0x01 ～ 0x1F（両端の値を含む）です。Tag テキスト ボックスが使用されない場合、値はゼロ（0x00）でなければなりません。
- Tunnel-Client-Endpoint、Tunnel-Server-Endpoint、Tunnel-Private-Group-ID、Tunnel-Assignment-ID、Tunnel-Client-Auth-ID、または Tunnel-Server-Auth-ID 属性（ただし Tunnel-Type、Tunnel-Medium-Type、Tunnel-Password、Tunnel-Preference は含まない）で使用する場合、0x1F より大きい Tag テキスト ボックスは、次のテキスト ボックスの最初のオクテットであると解釈されます。
- 代替トンネルタイプが指定されていない場合（たとえば、トンネリングはサポートしているが VLAN はサポートしていない IEEE 802.1X Authenticator の場合）、トンネル属性は 1 つのトンネルのみを指定する必要があります。したがって、VLANID を指定することだけが目的の場合、すべてのトンネル属性の Tag テキスト ボックスをゼロ（0x00）に設定する必要があります。代替トンネル タイプが提供される場合は、0x01 ～ 0x1F のタグ値を選択する必要があります。

AAA オーバーライド

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

IPv6 ACL の AAA Override

Cisco Identity Services Engine（ISE）、ACS などの一元化された AAA サーバによるアクセス コントロールのサポートのために、AAA Override 属性を使用して各クライアントについて IPv6 ACL をプロビジョニングできます。この機能を使用するには、IPv6 ACL をコントローラで設定し、AAA Override 機能をイネーブルにして WLAN を設定する必要があります。ACL がコン

トローラで事前に設定されていない場合、クライアントは認証解除されます。IPv6 ACL の実際の名前付き AAA 属性は、IPv4 ベースの ACL をプロビジョニングするために使用される *Airespace ACL-Name* 属性に似た ***Airespace-IPv6-ACL-Name*** です。AAA 属性が返すコンテンツは、コントローラで設定された IPv6 ACL の名前に一致する文字列になるはずです。

（注） リリース 7.5 から、アップストリーム AAA Override のレート制限値はダウンストリーム AAA Override のレート制限値と同じになりました。

AAA Override の制約事項

- AAA Override のためにクライアントが新しいインターフェイスに移動したあと、そのインターフェイスに ACL を適用しても、クライアントが再認証されるまで ACL は有効になりません。この問題を回避するには、インターフェイス上ですでに設定済みの ACL にすべてのクライアントが接続するように、ACL を適用してから WLAN を有効にします。あるいは、クライアントが再認証されるように、インターフェイスを適用したあとで WLAN を一旦無効にし、再び有効にします。
- AAA サーバから返された ACL がコントローラ上にないか、 ACL が間違った名前で設定されている場合、クライアントは認証されません。
- FlexConnect のローカル スイッチングを使用すると、マルチキャストは SSID がマッピングされた VLAN にのみ転送され、上書きされた VLAN には転送されません。したがって、IPv6 は、マルチキャスト トラフィックが不正な VLAN から転送されるため、正しく動作しません。
- インターフェイス グループが WLAN にマッピングされ、クライアントがその WLAN に接続した場合、クライアントはラウンドロビン方式で IP アドレスを取得しません。インターフェイス グループによる AAA Override はサポートされています。
- AAA Override を許可する設定の多くは、RADIUS サーバで実行されます。RADIUS サーバでは、コントローラに返すようにする上書きプロパティで、Access Control Server（ACS）を設定する必要があります。
- コントローラでは、GUI または CLI を使用して、Allow AAA Override 設定パラメータを有効にします。このパラメータを有効にすることにより、コントローラで RADIUS サーバから返される属性を受け入れるようになります。次にコントローラはそれらの属性をクライアントに適用します。
- レイヤ 2 認証中に AAA Override を有効にすると、ローカル ポリシーは適用されず、Override が優先されます。
- Cisco TrustSec セキュリティ グループのタグは、WLAN で AAA ocerride を有効にするまで適用されません。

正しい *QoS* 値を取得するための *RADIUS* サーバ ディクショナリ ファイルの更新

Steel-Belted RADIUS（SBR）、FreeRadius、または同等の RADIUS サーバを使用している場合、AAA Override 機能を有効化した後、クライアントが正しい QoS 値を取得できないことがあります。ディクショナリ ファイルの編集を可能にするこれらのサーバについて、正しい QoS 値（Silver = 0、Gold = 1、Platinum = 2、Bronze = 3）を反映させてファイルを更新する必要があります。RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。

（注） この問題は、Cisco Secure Access Control Server（ACS）には適用されません。

RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。

1. SBR サービス（または他の RADIUS サービス）を停止します。
2. 次のテキストを、`ciscowlan.dct` として `Radius_Install_Directory\Service` フォルダに保存します。

```
##############################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
##############################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level          Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze     3
VALUE Aire-QoS-Level Silver     0
VALUE Aire-QoS-Level Gold       1
VALUE Aire-QoS-Level Platinum   2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

##############################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
##############################################################################
```

3. （同じディレクトリにある）dictiona.dcm ファイルを開いて、「@ciscowlan.dct.」行を追加します。
4. dictiona.dcm ファイルを保存して閉じます。
5. （同じディレクトリにある）vendor.ini ファイルを開いて、次のテキストを追加します。

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id              =
```

6. vendor.ini ファイルを保存して閉じます。
7. SBR サービス（または他の RADIUS サービス）を起動します。
8. SBR アドミニストレータ（または他の RADIUS アドミニストレータ）を起動します。
9. RADIUS クライアントを追加します（まだ追加されていない場合）。[Make/Model] ドロップダウン リストから [Cisco WLAN Controller] を選択します。

AAA Override の設定（*GUI*）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 設定する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Allow AAA Override] チェックボックスをオンにして AAA Override を有効にするか、オフにしてこの機能を無効にします。デフォルト値は [disabled] です。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

AAA オーバーライドの設定（*CLI*）

手順

- 次のコマンドを入力して、WLAN 上の AAA を介したユーザ ポリシーのオーバーライドを設定します。

  config wlan aaa-override {**enable** | **disable**} *wlan-id*

  wlan-id には 1 ～ 16 の値を入力します。

- 次のコマンドを入力して、802.1X AAA インタラクションのデバッグを設定します。

debug dot1x aaa {**enable** | **disable**}

- 次のコマンドを入力して、AAA QoS オーバーライドのデバッグを設定します。
  debug ap aaaqos-dump {**enable** | **disable**}

WLAN ごとの RADIUS 送信元

WLAN ごとの *RADIUS* 送信元サポートの前提条件

- コントローラは選択されたインターフェイスのみからトラフィックを受信するので、認証サーバ（RADIUS）の新しいIDをフィルタする適切なルールを実行する必要があります。

WLAN ごとの *RADIUS* 送信元サポートの制約事項

WLAN ごとの *RADIUS* 送信元サポートについて

コントローラ の動的インターフェイスのいずれかを介してアクセス可能な VLAN 上に設定済みの RADIUS サーバが存在しない場合は、コントローラ がその管理インターフェイスの IP アドレスから RADIUS トラフィックを送信します。RADIUS サーバにコントローラ の動的インターフェイスを介して到達可能な場合は、その RADIUS サーバへの RADIUS 要求は、対応する動的インターフェイスを介してコントローラから取得されます。

デフォルトでは、コントローラ から取得された RADIUS パケットによって、そのパケットの送信元 IP アドレス（トポロジに応じて管理または動的）に関係なく、NAS-IP-Address 属性が管理インターフェイスの IP アドレスの属性に設定されます。

WLAN 単位の RADIUS 送信元サポート（RADIUS サーバ上書きインターフェイス）が有効になっている場合は、送信元のインターフェイスを反映するように、NAS-IP-Address 属性がコントローラ によって上書きされます。また、それに応じて、RADIUS 属性が Identity に一致するように変更されます。この機能は、各 WLAN が別個のレイヤ 3 Identity を持つ可能性がある場合に、WLAN ごとの RADIUS トラフィックでコントローラ を効果的に仮想化します。この機能は、ACS ネットワーク アクセス制限、およびネットワーク アクセス プロファイルと統合する展開に役立ちます。

WLAN をフィルタ処理するには、RFC 3580 で APMAC:SSID 形式に設定された callStationID を使用します。また、NAS-IP-Address 属性を使用することで、認証サーバ上のフィルタリングを WLAN ごとの送信元インターフェイス上にまで拡張できます。

アドレスの送信元として WLAN ごとの動的インターフェイスを用いる管理インターフェイスなどを使用するいくつかの WLAN および通常の RADIUS トラフィックの送信元と、WLAN ごとの RADIUS 送信元サポートを組み合わせることができます。

WLAN ごとの *RADIUS* 送信元サポートの設定（*GUI*）

始める前に

WLAN がディセーブル状態になっていることを確認します。設定の完了後、WLAN を有効にできます。

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 [WLAN ID] をクリックします。

ステップ 3 [Security] タブをクリックして、[AAA Servers] タブをクリックします。

ステップ 4 [RADIUS Server Overwrite interface] チェックボックスをオンにし、WLAN ごとの RADIUS ソース サポートを有効にします。

（注） 有効にすると、コントローラは、WLAN 上のすべての RADIUS 関連トラフィックのアイデンティティおよび送信元として、そのWLANの設定で指定されているインターフェイスを使用します。無効にすると、コントローラは、NAS-IP-Address 属性のアイデンティティとして管理インターフェイスを使用します。RADIUS サーバが直接接続された動的インターフェイスにある場合、RADIUS トラフィックはそのインターフェイスから送信されます。それ以外の場合は、管理 IP アドレスが使用されます。いずれのケースでも、機能が有効でない限り、NAS-IP-Address 属性は管理インターフェイスのままとなります。

ステップ 5 RADIUS パケット ルーティング用のインターフェイスとして、[Interface Priority] ドロップダウン リストから、[AP Group] または [WLAN] を選択します。

ステップ 6 RADIUS サーバ アカウンティングに対する [Interim Interval] が有効な範囲内にあることを確認します。

ステップ 7 設定を保存します。

WLAN ごとの *RADIUS* 送信元サポートの設定（*CLI*）

手順

ステップ 1 **config wlan disable** *wlan-id* コマンドを入力して、WLAN を無効にします。

ステップ 2 次のコマンドを入力して、WLAN ごとのRADIUS送信元サポートを有効または無効にします。

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan-id*

（注） 有効にすると、コントローラは、WLAN 上のすべての RADIUS 関連トラフィックのアイデンティティおよび送信元として、そのWLANの設定で指定されているインターフェイスを使用します。無効にすると、コントローラは、NAS-IP-Address 属性のアイデンティティとして管理インターフェイスを使用します。RADIUS サーバが直接接続された動的インターフェイスにある場合、RADIUS トラフィックはそのインターフェイスから送信されます。それ以外の場合は、管理 IP アドレスが使用されます。いずれのケースでも、機能が有効でない限り、NAS-IP-Address 属性は管理インターフェイスのままとなります。

ステップ 3 次のコマンドを入力して、RADIUS パケット ルーティング用の AP グループのインターフェイスまたは WLAN のインターフェイスを有効にします。

- AP グループのインターフェイス：**config wlan radius_server overwrite-interface apgroup** *wlan-id*
- WLAN のインターフェイス：**config wlan radius_server overwrite-interface wlan** *wlan-id*

（注） 有効な WLAN ID の範囲は 1 ～ 16 です。

ステップ 4 **config wlan enable** *wlan-id* コマンドを入力して、WLAN を有効にします。

（注） CiscoSecure ACS を使用して、RADIUS サーバ側で要求をフィルタリングできます。要求は、ネットワーク アクセス制限ルールを介して、NAS-IP-Address 属性によってフィルタリング（受け入れまたは拒否）できます。使用されるフィルタリングは、CLI/DNIS フィルタリングです。

WLAN ごとの *RADIUS* 送信元サポートのステータスのモニタリング（*CLI*）

機能が有効または無効かどうかを確認するには、次のコマンドを入力します。

show wlan *wlan-id*

例

次の例は、WLAN ごとの RADIUS 送信元サポートが WLAN 1 で有効であることを示しています。

show wlan *1*

次のような情報が表示されます。

```
WLAN Identifier................................ 4
Profile Name................................... example
Network Name (SSID)............................ example
Status......................................... Enabled
MAC Filtering.................................. Disabled
Broadcast SSID................................. Enabled
AAA Policy Override............................ Disabled
Network Admission Control
...
Radius Servers
   Authentication............................... Global Servers
   Accounting................................... Global Servers
   Overwrite Sending Interface.................. Enabled
Local EAP Authentication....................... Disabled
```

LDAP

LDAP の概要

LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）をLDAPサーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとして LDAP を使用する場合があります。

（注） リリース 8.0 以降では、IPv6 を使用してコントローラの LDAP サーバを設定することもできます。

LDAP Servers のフォールバック

LDAP サーバは認証用に WLAN に設定されます。フォールバック動作が行われるようにするには、少なくとも 2 台の LDAP サーバでそれらを設定する必要があります。WLAN ごとにフォール バック動作が行われるように、最大 3 台の LDAP サーバを設定できます。サーバは認証の優先順位で表示されます。最初の LDAP サーバが応答しない場合、コントローラは次の LDAP サーバに切替えます。2 番目の LDAP サーバが応答しない場合、コントローラは、3 番目の LDAP サーバに再度切替えます。

LDAP バックエンドデータベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、EAP-FAST/EAP-GTC、および PEAPv0/MSCHAPv2 もサポートされますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。

Cisco ワイヤレス LAN コントローラは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカル EAP 認証をサポートしています。Novell の eDirectory に対するローカル EAP 認証をコントローラに設定する方法の詳細については、次の URL にある『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。
http://www.cisco.com/en/US/products/ps6366/products_white_paper09186a0080b4cd24.shtml

LDAP の設定（*GUI*）

手順

ステップ 1 [Security] > [AAA] > [LDAP] の順に選択して、[LDAP Servers] ページを開きます。

- 既存の LDAP サーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 2 次のいずれかの操作を行います。

- 既存の LDAP サーバを編集するには、そのサーバのインデックス番号をクリックします。[LDAP Servers > Edit] ページが表示されます。
- LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。新しいサーバを追加している場合は、[Server Index (Priority)] ドロップダウン リストから数字を選択し、その他の設定済み LDAP サーバに対してこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラが最初のサーバに

接続できない場合、リスト内の2番目のサーバへの接続を試行する、というようになります。

ステップ 3 新しいサーバを追加している場合は、[Server IP Address] テキスト ボックスに LDAP サーバの IP アドレスを入力します。

（注） リリース 8.0 以降では、IPv6 を使用してコントローラの LDAP サーバを設定することもできます。

ステップ 4 新しいサーバを追加している場合は、[Port Number] テキスト ボックスに LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ～ 65535 で、デフォルト値は 389 です。

（注） Cisco WLC では、LDAP ポート 389 のみがサポートされます。他のポートは、LDAP 用としてサポートされません。

ステップ 5 [Server Mode（via TLS）] ドロップダウン リストから [Disabled] を選択し、TCP を使用して LDAP サーバと Cisco WLC 間の LDAP 接続（セキュア トンネルなし）を確立します。または [Enabled] を選択し、TLS を使用してセキュア LDAP 接続を確立します。

ステップ 6 [Enable Server Status] チェックボックスをオンにしてこの LDAP サーバを有効にするか、オフにして無効にします。デフォルト値は [disabled] です。

ステップ 7 [Simple Bind] ドロップダウン リストから [Anonymous] または [Authenticated] を選択して、LDAP サーバ用のローカル認証バインド方式を指定します。[Anonymous] 方式では、LDAP サーバへの匿名アクセスが可能です。[Authenticated] 方式では、ユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルトでは [Anonymous] になっています。

ステップ 8 前の手順で [Authenticated] を選択した場合は、次の手順に従ってください。

a) [Bind Username] テキスト ボックスに、LDAP サーバのローカル認証に使用されるユーザ名を入力します。ユーザ名には、最大 80 文字を使用できます。

（注） ユーザ名が「cn=」（小文字）で始まる場合、コントローラはユーザ名に完全な LDAP データベース パスが含まれていると見なし、ユーザベース DN を付加しません。この指定により、認証済みのバインドユーザをユーザ ベース DN の外に置くことができます。

b) [Bind Username] テキスト ボックスに、LDAP サーバのローカル認証に使用されるユーザ名を入力します。ユーザ名には、最大 80 文字を使用できます。

ステップ 9 [User Base DN] テキスト ボックスに、全ユーザのリストが含まれた、LDAP サーバ内のサブツリーの識別名（DN）を入力します。たとえば、ou=organizational unit、.ou=next organizational unit、o=corporation.com のようになります。ユーザを含むツリーがベース DN である場合は、次を入力します。

o=*corporation*.com

または

dc=*corporation***,dc=com**

ステップ 10 [User Attribute] テキスト ボックスに、ユーザ名が含まれたユーザ レコード内の属性の名前を入力します。この属性はディレクトリ サーバから取得できます。

ステップ 11 [User Object Type] テキスト ボックスに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクト タイプと共有する値があります。

ステップ 12 [Server Timeout] テキスト ボックスに、再送信の間隔を秒単位で入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 13 [Apply] をクリックして、変更を確定します。

ステップ 14 [Save Configuration] をクリックして、変更を保存します。

ステップ 15 次の手順を実行して、LDAP をローカル EAP 認証用の優先バックエンド データベース サーバとして指定します。

a) [Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます。

b) [LOCAL] を強調表示して、[<] をクリックし、それを左の [User Credentials] ボックスに移動します。

c) [LDAP] を強調表示して、[>] をクリックし、それを右の [User Credentials] ボックスに移動します。右側の [User Credentials] ボックスの上部に表示されるデータベースは、ユーザの資格情報を取得する際に使用されます。

（注） [LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカルユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d) [Apply] をクリックして、変更を確定します。

e) [Save Configuration] をクリックして、変更を保存します。

ステップ 16 （オプション）次の手順を実行して、特定の LDAP サーバを WLAN に割り当てます。

a) [WLANs] を選択して、[WLANs] ページを開きます。

b) 必要な WLAN の ID 番号をクリックします。

c) [WLANs > Edit] ページが表示されたら [Security] > [AAA Servers] タブを選択し、[WLANs > Edit]（[Security > AAA Servers]）ページを開きます。

d) [LDAP Servers] ドロップダウン リストから、この WLAN で使用する LDAP サーバを選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位に従って試行されます。

（注） これらの LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。

e) [Apply] をクリックして、変更を確定します。

f) [Save Configuration] をクリックして、変更を保存します。

ステップ 17 次の手順を実行して、LDAP サーバ フォールバックの動作を指定します。

a) [WLAN] > [AAA Server] を選択して、[Fallback Parameters] ページを開きます。

b) [LDAP Servers] ドロップダウン リストから、コントローラが管理ユーザを認しようとする際の優先順位に従って、LDAP サーバを選択します。認証順序はサーバから開始します。

c) [Security] > [AAA] > [LDAP] の順に選択して、コントローラに設定されたグローバル LDAP サーバのリストを表示します。

LDAP の設定（*CLI*）

手順

- 次のコマンドを入力して、LDAP サーバを設定します。
  - **config ldap add** *index server_ip_address port# user_base user_attr user_type* **secure**：セキュア LDAP 用の LDAP サーバを追加します。
  - **config ldap delete** *index*：以前追加された LDAP サーバを削除します。
  - **config ldap** {**enable** | **disable**} *index*：LDAP サーバを有効または無効にします。
  - **config ldap security-mode enable** *index*：既存のコマンドとともにインデックスを使用して LDAP サーバを有効にします。
  - **config ldap simple-bind** {**anonymous** *index* | **authenticated** *index* **username** *username* **password** *password*}：LDAP サーバのローカル認証バインド方式を指定します。匿名方式では LDAP サーバへの匿名アクセスが可能です。一方、認可方式ではユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルト値は [anonymous] です。ユーザ名には、最大 80 文字を使用できます。

    ユーザ名が「cn=」（小文字）で始まる場合、コントローラはユーザ名に完全な LDAP データベース パスが含まれていると見なし、ユーザベース DN を付加しません。この指定により、認証済みのバインド ユーザをユーザ ベース DN の外に置くことができます。
  - **config ldap retransmit-timeout** *index timeout*：LDAP サーバの再送信間隔の秒数を設定します。
- 次のコマンドを入力して、LDAP を優先バックエンド データベース サーバとして指定します。

  config local-auth user-credentials ldap

  config local-auth user-credentials ldap local command を入力すると、ローカル EAP が LDAP バックエンドデータベースを使用してクライアントの認証を試行し、LDAP サーバが到達不能な場合にローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap command** を入力すると、ローカル EAP がローカル ユーザ データベースだけを使用して認証を試みます。LDAP バックエンド データベースへのフェールオーバーは行われません。
- （オプション）次のコマンドを入力して、特定の LDAP サーバを WLAN に割り当てます。

- **config wlan ldap add** *wlan_id server_index*：設定済みの LDAP サーバを WLAN にリンクします。

  このコマンドで指定される LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。

- **config wlan ldap delete** *wlan_id* {*all* | *index*}：特定の LDAP サーバ、または設定済みのすべての LDAP サーバを WLAN から削除します。

• 次のコマンドを入力して、設定済みの LDAP サーバに関連する情報を表示します。

- **show ldap summary**：設定された LDAP サーバの概要を表示します。

```
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4           389     No
2    10.10.20.22       389     Yes

Idx      Server Address      Port     Enabled  Secure
---      --------------      -----    ------  -------
1         2.3.1.4            389       No       No
2         2.3.1.5            389       Yes      No
```

- **show ldap** *index*：詳細な LDAP サーバ情報を表示します。次のような情報が表示されます。

```
Server Index..................................... 2
Address.......................................... 10.10.20.22
Port............................................. 389
Enabled.......................................... Yes
User DN.......................................
ou=active,ou=employees,ou=people,
             o=cisco.com
User Attribute................................... uid
User Type........................................ Person
Retransmit Timeout............................... 2 seconds
Bind Method ..................................... Authenticated
Bind Username................................ user1

Controller# show ldap 1
Server Index..................................... 1
Address.......................................... 9.1.0.100
Port............................................. 389
Server State..................................... Disabled
User DN.......................................... user1
User Attribute................................... user
User Type........................................ user
Retransmit Timeout............................... 2 seconds
Secure (via TLS)................................. Disabled
Bind Method ..................................... Anonymous
```

- **show ldap statistics**：LDAP サーバの統計情報を表示します。

```
Server Index..................................... 1
Server statistics:
  Initialized OK................................. 0
  Initialization failed.......................... 0
  Initialization retries......................... 0
  Closed OK...................................... 0
```

```
Request statistics:
  Received..................................... 0
  Sent......................................... 0
  OK........................................... 0
  Success...................................... 0
  Authentication failed........................ 0
  Server not found............................. 0
  No received attributes....................... 0
  No passed username........................... 0
  Not connected to server...................... 0
  Internal error............................... 0
  Retries...................................... 0

Server Index................................... 2
..
```

- **show wlan** *wlan_id*：WLAN に適用される LDAP サーバを表示します。

- 次のコマンドを入力して、コントローラがLDAPサーバに到達できることを確認します。
  ping *server_ip_address*
- 次のコマンドを入力して、変更を保存します。
  save config
- 次のコマンドを入力して、LDAP のデバッグを有効または無効にします。
  debug aaa ldap {enable | disable}

ローカル EAP

ローカル *EAP* について

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンドシステムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証をサポートします。

（注） LDAP バックエンドデータベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。

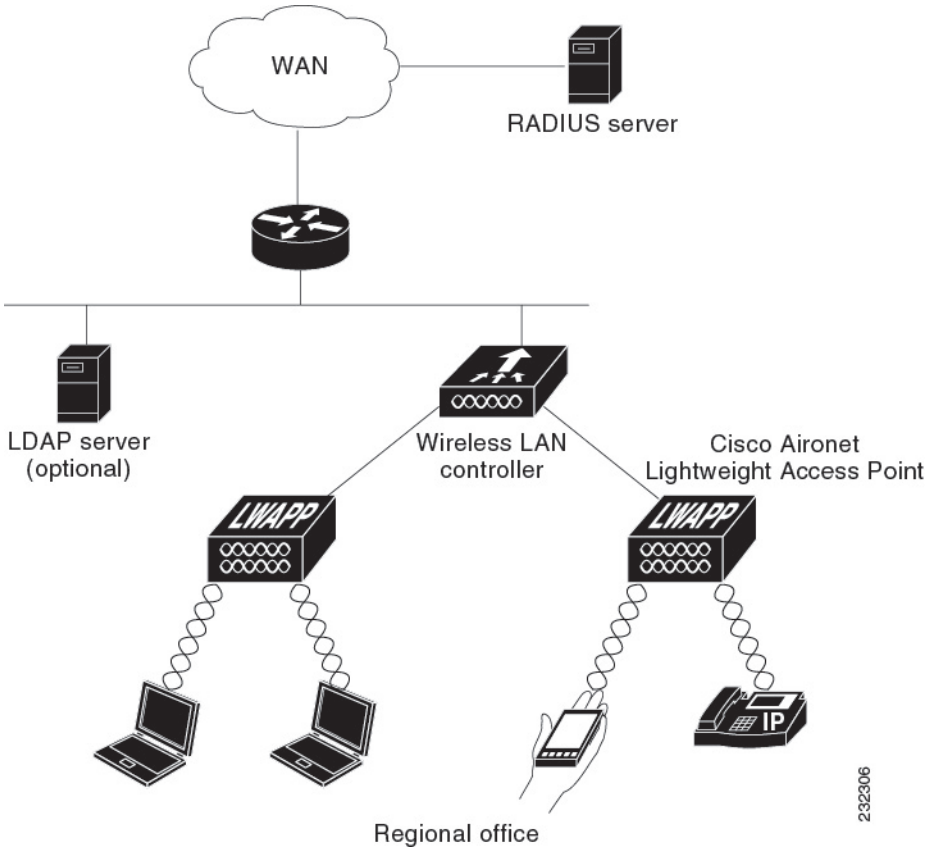
（注） Cisco ワイヤレス LAN コントローラは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカル EAP 認証をサポートしています。Novell の eDirectory に対するローカル EAP 認証をコントローラに設定する方法の詳細については、次の URL にある『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。
http://www.cisco.com/en/US/products/ps6366/products_white_paper09186a0080b4cd24.shtml

（注） 第 2 レベルの階層（CA + 中間 CA + デバイス）の証明書を使用したローカル認証はサポートされていません。

コントローラ上で RADIUS サーバが設定されている場合は、コントローラはまず RADIUS サーバを使用してワイヤレスクライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番めの RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番めの RADIUS サーバを試行し、次に 4 番めの RADIUS サーバ、その次にローカル EAP を試行します。コントローラで外部 RADIUS サーバを使用したクライアント認証を行いたくない場合は、次の CLI コマンドを示された順序どおりに入力します。

- **config wlan disable** *wlan_id*
- **config wlan radius_server auth disable** *wlan_id*
- **config wlan enable** *wlan_id*

図 *1* : ローカル *EAP* の例



関連トピック

デバイスの証明書のダウンロード

ローカル *EAP* の制約事項

- 8.6 以降のリリースでは、RC4 または 3DES 暗号化タイプを必要とするレガシー クライアントは、ローカル EAP 認証ではサポートされません。

ローカル *EAP* の設定（*GUI*）

始める前に

（注） EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA; 認証局）の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。

手順

ステップ 1 上記に示したいずれかの EAP タイプを使用するようにローカル EAP を設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。

ステップ 2 コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。

ステップ 3 コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。

ステップ 4 次の手順を実行して、ユーザの資格情報をバックエンド データベース サーバから取得する順序を指定します。

a) [Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます。

b) ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を決定します。たとえば、LDAP データベースがローカルユーザデータベースよりも優先されるようにすることも、または LDAP データベースがまったく考慮されないようにすることもできます。

c) 優先順位を決定したら、目的のデータベースを強調表示します。次に、左と右の矢印および [Up] ボタンと [Down] ボタンを使用して、目的のデータベースを右側の [User Credentials] ボックスの上部に移動します。

（注） [LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカルユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d) [Apply] をクリックして、変更を確定します。

ステップ 5 次の手順を実行して、ローカル EAP タイマーの値を指定します。

a) [Security] > [Local EAP] > [General] の順に選択して、[General] ページを開きます。

b) [Local Auth Active Timeout] テキスト ボックスに、設定済み RADIUS サーバのペアによる認証が失敗した後に、コントローラがローカル EAP を使用してワイヤレス クライアントを認証する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。

ステップ 6 次のように Advanced EAP パラメータの値を指定します。

a) [Security] > [Advanced EAP] を選択します。

b) [Identity Request Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を送信する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。

c) [Identity Request Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。

d) [Dynamic WEP Key Index] テキスト ボックスに、Dynamic Wired Equivalent Privacy（WEP）に使用するキーインデックスを入力します。デフォルト値は 0 で、これはキーインデックス 1 に相当します。有効な値は 0 ～ 3（キー インデックス 1 ～ 4）です。

e) [Request Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を送信する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。

f) [Request Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。

g) [Max-Login Ignore Identity Response] ドロップダウン リストから [Enable] を選択して、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限します。同じコントローラ上の異なるデバイス（PDA、ノートパソコン、IP フォンなど）から最大 8 台までログインできます。デフォルト値はイネーブルです。

h) [EAPOL-Key Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を入力します。有効な値の範囲は 1 ～ 5 秒で、デフォルトの設定は 1 秒です。

（注） コントローラとアクセス ポイントが WAN リンクによって分離されている場合、デフォルト タイムアウト値の 1 秒では不十分な場合があります。

i) [EAPOL-Key Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。

j) [Apply] をクリックして、変更を確定します。

ステップ 7 次の手順を実行して、ワイヤレスクライアントでサポートされる EAP 認証タイプを指定する、ローカル EAP プロファイルを作成します。

a) [Security] > [Local EAP] > [Profiles] の順に選択して、[Local EAP Profiles] ページを開きます。

このページでは、これまでに設定されたすべてのローカル EAP プロファイルが表示され、その EAP タイプを指定します。最大 16 個のローカル EAP プロファイルを作成できます。

（注） 既存のプロファイルを削除するには、そのプロファイルの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

b) [New] をクリックして、[Local EAP Profiles > New] ページを開きます。

c) [Profile Name] テキスト ボックスに新しいプロファイルの名前を入力し、[Apply] をクリックします。

（注） プロファイル名には最大 63 文字の英数字を入力できます。スペースは含めないでください。

d) [Local EAP Profiles] ページが再度表示されたら、新しいプロファイルの名前をクリックします。[Local EAP Profiles > Edit] ページが表示されます。

e) [LEAP]、[EAP-FAST]、[EAP-TLS]、または [PEAP] チェックボックスをオンにし、ローカル認証に使用できる EAP タイプを指定します。

（注） プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、PEAPv1/GTC など）を選択する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注） [PEAP] チェックボックスをオンにすると、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

f) EAP-FAST を選択し、コントローラ上のデバイス証明書を認証に使用する場合は、[Local Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにしておきます。これはデフォルトの設定です。

（注） デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このオプションは EAP-FAST にのみ適用されます。

g) EAP-FAST を選択し、ワイヤレス クライアントが認証のためデバイス証明書をコントローラに送信するよう設定するには、[Client Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにしておきます。これはデフォルトの設定です。

（注） クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このオプションは EAP-FAST にのみ適用されます。

h) 証明書を使用する EAP-FAST、EAP-TLS、または PEAP を選択する場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。[Cisco] または [Vendor] を [Certificate Issuer] ドロップダウン リストから選択してください。デフォルトの設定は、[Cisco] になっています。

i) 証明書を使用する EAP-FAST または EAP-TLS を選択し、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証する場合は、[Check Against CA Certificates] チェックボックスをオンにします。デフォルト設定はイネーブルです。

j) 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信する証明書の共通名（CN）をコントローラに設定されているローカル ネット ユーザと照合して検証する場合は、[Verify Certificate CN Identity] チェックボックスをオンにします。デフォルト設定では無効になっています。

k) 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信するデバイス証明書が現在有効であり、期限切れでないことをコントローラで検証されるようにする場合は、

[Check Certificate Date Validity] チェックボックスをオンにします。デフォルト設定はイネーブルです。

（注） 証明書の日付の有効性が、コントローラに設定された現在のUTC（GMT）時間と照合されます。タイムゾーンのオフセットは無視されます。

l) [Apply] をクリックして、変更を確定します。

ステップ 8 EAP-FAST プロファイルを作成した場合、EAP-FAST パラメータを設定する手順は、次のとおりです。

a) [Security] > [Local EAP] > [EAP-FAST Parameters] の順に選択して、[EAP-FAST Method Parameters] ページを開きます。

b) [Server Key] テキスト ボックスおよび [Confirm Server Key] フィールドに、PAC の暗号化と暗号化解除に使用するキー（16 進数文字）を入力します。

c) [Time to Live for the PAC] テキスト ボックスに、PAC の有効日数を入力します。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。

d) [Authority ID] テキスト ボックスに、ローカル EAP-FAST サーバの認証局 ID を 16 進数文字で入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。

e) [Authority ID Information] テキスト ボックスに、ローカル EAP-FAST サーバの Authority ID をテキスト形式で入力します。

f) 匿名プロビジョニングを有効にするには、[Anonymous Provision] チェックボックスをオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にする場合、PAC は手動でプロビジョニングされる必要があります。デフォルト設定はイネーブルです。

（注） ローカル証明書またはクライアント証明書、あるいはその両方を必要とし、すべての EAP-FAST クライアントで証明書が使用されるよう強制する場合は、[Anonymous Provision] チェックボックスをオフにしてください。

g) [Apply] をクリックして、変更を確定します。

ステップ 9 次の手順を実行して、WLAN 上でローカル EAP を有効にします。

a) [WLANs] を選択して、[WLANs] ページを開きます。

b) 必要な WLAN の ID 番号をクリックします。

c) [WLANs > Edit] ページが表示されたら [Security] > [AAA Servers] タブを選択し、[WLANs > Edit]（[Security > AAA Servers]）ページを開きます。

d) この WLAN に対して RADIUS アカウンティングおよび認証を無効にするには、RADIUS 認証サーバおよびアカウンティング サーバの [Enabled] チェックボックスをオフにします。

e) [Local EAP Authentication] チェックボックスをオンにして、この WLAN に対してローカル EAP を有効にします。

f) [EAP Profile Name] ドロップダウン リストから、この WLAN に使用する EAP プロファイルを選択します。

g) 必要に応じて、[LDAP Servers] ドロップダウン リストから、この WLAN でローカル EAP と共に使用する LDAP サーバを選択します。

h) [Apply] をクリックして、変更を確定します。

ステップ 10 次の手順を実行して、WLAN で EAP パラメータを有効にします。

a) [WLANs] を選択して、[WLANs] ページを開きます。

b) 必要な WLAN の ID 番号をクリックします。

c) [WLANs > Edit] ページが表示されたら [Security] > [AAA Servers] タブを選択し、[WLANs > Edit]（[Security > AAA Servers]）ページを開きます。

d) この WLAN に対して EAP パラメータを設定するには、[Enable] チェックボックスをオンにします。

e) [EAPOL Key Timeout (200 to 5000 millisec)] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の試行時間を入力します（ミリ秒単位）。有効な範囲は 200 ～ 5000 ミリ秒で、デフォルト値は 1000 ミリ秒です。

f) [EAPOL Key Retries (0 to 4)] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の最大試行回数を入力します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。

g) [Identity Request Timeout (1 to 120 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を送信する際の試行時間を入力します（秒単位）。有効な範囲は 1 ～ 120 秒で、デフォルト値は 30 秒です。

h) [Identity Request Retries (1 to 20 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 2 回です。

i) [Request Timeout (1 to 120 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を送信する際の試行時間を入力します（秒単位）。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。

j) [Request Retries (1 to 20 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 2 回です。

k) [Apply] をクリックして、変更を確定します。

ステップ 11 [Save Configuration] をクリックして、変更を保存します。

ローカル *EAP* の設定（*CLI*）

始める前に

（注） EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は認証に証明書を使用し、EAP-FAST は証明書または PACb のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA; 認証局）の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。

手順

ステップ 1 上記に示したいずれかの EAP タイプを使用するようにローカル EAP を設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。

ステップ 2 コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。

ステップ 3 コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。

ステップ 4 次のコマンドを入力して、ローカルまたはLDAPデータベースからユーザの資格情報を取得する順位を指定します。

config local-auth user-credentials {*local* | *ldap*}

（注） **config local-auth user-credentials ldap local** コマンドを入力すると、ローカル EAP が LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが到達不能な場合はローカルユーザデータベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap command** を入力すると、ローカル EAP がローカル ユーザ データベースだけを使用して認証を試みます。LDAP バックエンドデータベースへのフェールオーバーは行われません。

ステップ 5 次のコマンドを入力して、ローカル EAP タイマーの値を指定します。

- **config local-auth active-timeout** *timeout*：設定された RADIUS サーバのペアで障害が発生してから、コントローラがローカル EAP を使用してワイヤレス クライアントの認証を試みるまでの時間（秒単位）を指定します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。
- **config advanced eap identity-request-timeout** *timeout*：コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求の送信を試みる時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config advanced eap identity-request-retries** *retries*：コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求の再送信を試みる最大回数を指定します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。
- **config advanced eap key-index** *index*：ダイナミック Wired Equivalent Privacy（WEP）に使用するキー インデックスを指定します。デフォルト値は 0 で、これはキー インデックス 1 に相当します。有効な値は 0 ～ 3（キー インデックス 1 ～ 4）です。
- **config advanced eap request-timeout** *timeout*：コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求の送信を試みる時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config advanced eap request-retries** *retries*：コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求の再送信を試みる最大回数を指定します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。

- **config advanced eap eapol-key-timeout** *timeout*：コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーの送信を試みる時間（秒単位）を指定します。有効な値の範囲は 1 ～ 5 秒で、デフォルトの設定は 1 秒です。

  （注） コントローラとアクセス ポイントが WAN リンクによって分離されている場合、デフォルト タイムアウト値の 1 秒では不十分な場合があります。

- **config advanced eap eapol-key-retries** *retries*：コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーの送信を試みる最大回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}：有効になっている場合、このコマンドは 802.1x 認証経由で同じユーザ名のコントローラに接続可能なデバイスの数に対して設定されている制限を無視します。ディセーブルにすると、このコマンドは、コントローラに同じユーザ名で接続できるデバイスの数を制限します。これは Web 認証ユーザには適用されません。同じコントローラ上の異なるデバイス（PDA、ノートパソコン、IP フォンなど）から最大 8 台までログインできます。デフォルト値はイネーブルです。**config netuser maxUserLogin** コマンドを使用して、同じユーザ名ごとのデバイスの最大数の制限を設定します。

ステップ 6 次のコマンドを入力して、WLAN でローカル EAP タイマーの値を指定します。

- **config wlan security eap-params {enable | disable}** *wlan_id*：SSID 固有の EAP タイムアウトまたは再試行を有効または無効にするように指定します。デフォルト値は [disabled] です。
- **config wlan security eap-params eapol-key-timeout** *timeout wlan_id*：コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーの送信を試みる時間（ミリ秒単位）を指定します。有効な範囲は 200 ～ 5000 ミリ秒で、デフォルト設定は 1000 ミリ秒です。
- **config wlan security eap-params eapol-key-retries** *retries wlan_id*：コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーの送信を試みる最大回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。
- **config wlan security eap-params identity-request-timeout** *timeout wlan_id*：コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求の送信を試みる時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config wlan security eap-params identity-request-retries** *retries wlan_id*：コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求の再送信を試みる最大回数を指定します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 2 回です。
- **config wlan security eap-params request-timeout** *timeout wlan_id*：コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求の送信を試みる時間（秒単位）を指定します。有効な範囲は 1 ～ 120 秒で、デフォルトの設定は 30 秒です。
- **config wlan security eap-params request-retries** *retries wlan_id*：コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求の再送信を試みる最大回数を指定します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 2 回です。

ステップ 7 次のコマンドを入力して、ローカル EAP プロファイルを作成します。

config local-auth eap-profile add *profile_name*

（注） プロファイル名にスペースを含めないでください。

（注） ローカル EAP プロファイルを削除するには、**config local-auth eap-profile delete** *profile_name* コマンドを入力します。

ステップ 8 次のコマンドを入力して、ローカル EAP プロファイルに EAP 方式を追加します。

config local-auth eap-profile method add *method profile_name*

サポートされている方式は leap、fast、tls、および peap です。

（注） peap を選択する場合、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

（注） プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC など）でプロファイルを作成する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注） ローカル EAP プロファイルから EAP メソッドを削除するには、**config local-auth eap-profile method delete** *method profile_name* コマンドを入力します。

ステップ 9 EAP-FAST プロファイルを作成した場合は、次のコマンドを入力して EAP-FAST パラメータを設定します。

config local-auth method fast *?*

ここで、*?* は、次のいずれかを示します。

- **anon-prov** {**enable**|**disable**}：匿名プロビジョニングを許可するようにコントローラを設定します。これにより、PAC プロビジョニング中に、PAC のないクライアントに自動的に PAC が送信されます。
- **authority-id** *auth_id*：ローカル EAP-FAST サーバの Authority ID を指定します。
- **pac-ttl** *days*：PAC の有効日数を指定します。
- **server-key** *key*：PAC の暗号化または復号化に使用されるサーバ キーを指定します。

ステップ 10 次のコマンドを入力して、プロファイルごとに証明書パラメータを設定します。

- **config local-auth eap-profile method fast local-cert** {**enable** | **disable**} *profile_name*：認証にコントローラ上のデバイス証明書が必要かどうかを指定します。

  （注） デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile method fast client-cert** {**enable** | **disable**} *profile_name*：ワイヤレスクライアントが認証を受けるために、デバイス証明書をコントローラに送信する必要があるかどうかを指定します。

  （注） クライアント証明書はLEAPまたはPEAPと共に使用されず、EAP-TLSには必須であるため、このコマンドはEAP-FASTにのみ適用されます。

- **config local-auth eap-profile cert-issuer** {**cisco** | **vendor**} *profile_name*：証明書を使用するEAP-FAST、EAP-TLS、またはPEAPを指定した場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。
- **config local-auth eap-profile cert-verify ca-issuer** {**enable** | **disable**} *profile_name*：証明書を使用するEAP-FASTまたはEAP-TLSを選択した場合は、クライアントから受信する証明書をコントローラ上のCA証明書と照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify cn-verify** {**enable** | **disable**} *profile_name*：証明書を使用するEAP-FASTまたはEAP-TLSが選択した場合は、受信した証明書の共通名（CN）をコントローラ上のCA証明書のCNと照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify date-valid** {**enable** | **disable**} *profile_name*：証明書を使用するEAP-FASTまたはEAP-TLSを選択した場合は、受信したデバイス証明書が有効で期限切れになっていないことをコントローラで検証するかどうかを指定します。

ステップ 11 次のコマンドを入力して、ローカルEAPを有効にし、EAPプロファイルをWLANに接続します。

config wlan local-auth enable *profile_name wlan_id*

（注） WLANのローカルEAPを無効にするには、**config wlan local-auth disable** *wlan_id* コマンドを入力します。

ステップ 12 次のコマンドを入力して、変更を保存します。

save config

ステップ 13 次のコマンドを入力して、ローカルEAPに関連する情報を表示します。

- **show local-auth config**—コントローラ上のローカルEAP設定を表示します。

```
User credentials database search order:
   Primary ..................................... Local DB

Timer:
    Active timeout .............................. 300

Configured EAP profiles:
   Name ........................................ fast-cert
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. Yes
       Client certificate required ............. Yes
     Enabled methods ........................... fast
```

```
      Configured on WLANs ....................... 1

    Name ......................................... tls
      Certificate issuer ........................ vendor
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No
      Enabled methods ........................... tls
      Configured on WLANs ....................... 2

EAP Method configuration:
   EAP-FAST:
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Accept client on auth prov ................ No
      Authority ID .............................. 436973636f00000000000000000000
      Authority Information ..................... Cisco A-ID
```

- **show local-auth statistics**：ローカル EAP 統計情報を表示します。
- **show local-auth certificates**：ローカル EAP に使用可能な証明書を表示します。
- **show local-auth user-credentials**コントローラがローカルデータベースまたはLDAPデータベースからユーザ クレデンシャルを取得するときに使用する優先順位を表示します。
- **show advanced eap**：ローカル EAP のタイマー値を表示します。

```
EAP-Identity-Request Timeout (seconds)........... 1
EAP-Identity-Request Max Retries................. 20
EAP Key-Index for Dynamic WEP.................... 0
EAP Max-Login Ignore Identity Response........... enable
EAP-Request Timeout (seconds).................... 20
EAP-Request Max Retries.......................... 20
EAPOL-Key Timeout (seconds)...................... 1
EAPOL-Key Max Retries........................ 2
```

- **show ap stats wlan** *Cisco_AP*：各 WLAN の特定のアクセス ポイントの EAP タイムアウトと障害カウンタを表示します。
- **show client detail** *client_mac*：特定の関連クライアントの EAP タイムアウトと障害カウンタを表示します。これらの統計は、クライアントアソシエーションの問題のトラブルシューティングを行う際に有用です。

```
...
Client Statistics:
      Number of Bytes Received................... 10
      Number of Bytes Sent....................... 10
      Number of Packets Received................. 2
      Number of Packets Sent..................... 2
      Number of EAP Id Request Msg Timeouts...... 0
      Number of EAP Id Request Msg Failures...... 0
      Number of EAP Request Msg Timeouts......... 2
      Number of EAP Request Msg Failures......... 1
      Number of EAP Key Msg Timeouts............. 0
      Number of EAP Key Msg Failures............. 0
      Number of Policy Errors.................... 0
```

```
Radio Signal Strength Indicator............ Unavailable
Signal to Noise Ratio...................... Unavailable
```

- **show wlan** *wlan_id*：特定の WLAN のローカル EAP のステータスを表示します。

ステップ 14 （オプション）次のコマンドを入力して、ローカル EAP セッションのトラブルシューティングを行います。

- **debug aaa local-auth eap method** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}：ローカル EAP 方式のデバッグを有効または無効にします。
- **debug aaa local-auth eap framework** {**all** | **errors** | **events** | **packets** | **sm**} {*enable* | *disable*}：ローカル EAP フレームワークのデバッグを有効または無効にします。

  （注） 上記の 2 つのコマンドでは、**sm** とはステート マシンを指します。

- **clear stats local-auth**：ローカル EAP カウンタをクリアします。
- **clear stats ap wlan** *Cisco_AP*：各 WLAN の特定のアクセス ポイントの EAP タイムアウトと障害カウンタをクリアします。

```
WLAN      1
   EAP Id Request Msg Timeouts................... 0
   EAP Id Request Msg Timeouts Failures.......... 0
   EAP Request Msg Timeouts...................... 2
   EAP Request Msg Timeouts Failures............. 1
   EAP Key Msg Timeouts.......................... 0
   EAP Key Msg Timeouts Failures................. 0
WLAN      2
   EAP Id Request Msg Timeouts................... 1
   EAP Id Request Msg Timeouts Failures.......... 0
   EAP Request Msg Timeouts...................... 0
   EAP Request Msg Timeouts Failures............. 0
   EAP Key Msg Timeouts.......................... 3
EAP Key Msg Timeouts Failures............. 1
```

MAC フィルタリング

WLAN の MAC フィルタ リング

WLAN の MAC フィルタリングについて

クライアント認可または管理者認可に MAC フィルタリングを使用する場合は、WLAN レベルで先に有効にしておく必要があります。任意の WLAN でローカル MAC アドレス フィルタリングを使用する予定がある場合は、この項のコマンドを使用して WLAN の MAC フィルタリングを設定します。

MAC フィルタリングの制限

- MAC フィルタはゲスト LAN 用に設定できません。
- 中央認証およびスイッチング：外部 RADIUS が WLAN 用に設定されている場合は、MAC 認証が MAC フィルタリングより優先されます。

- ローカル認証およびスイッチング：MAC フィルタリングがローカル認証でサポートされていない場合は、MAC 認証が機能しません。
- インターフェイス マッピングとプロファイルの優先順位：任意の WLAN/インターフェイスに設定された WLAN の MAC フィルタリングには、トラフィックが適切に動作するようプロファイル名が必要で、その後にインターフェイス名が続く必要があります。

MAC フィルタリングの有効化

WLAN 上で MAC フィルタリングを有効にするには、次のコマンドを使用します。

- MAC フィルタリングを有効にするには、**config wlan mac-filtering enable** *wlan_id* コマンドを入力します。
- WLAN の MAC フィルタリングが有効になっていることを確認するには、**show wlan** コマンドを入力します。

MAC フィルタリングを有効にすると、WLAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。追加されていない MAC アドレスは、WLAN への接続が許可されません。

クライアントが初めて WLAN にアソシエートしようとする場合、クライアントは AAA サーバからの MAC アドレスにより認証されます。認証が成功すると、クライアントは DHCP サーバから IP アドレスを取得して、WLAN に接続されます。

クライアントが同じ AP または別の AP にローミングまたはアソシエーション要求を送信したときに、まだ WLAN に接続されていれば、クライアントは AAA サーバに再認証されません。

クライアントが WLAN に接続されていない場合は、クライアントは AAA サーバから認証される必要があります。

ローカル *MAC* フィルタ

ローカル MAC フィルタについて

コントローラには MAC フィルタリング機能が組み込まれています。これは、RADIUS authorization サーバで提供されるものとよく似ています。

ローカル MAC フィルタの設定に関する前提条件

WLAN で AAA を有効にして、インターフェイス名を上書きする必要があります。

ローカル MAC フィルタの設定（CLI）

- コントローラに MAC フィルタ エントリを作成するには、**config macfilter add** *mac_addr wlan_id* [*interface_name*] [*description*] [*IP_addr*] コマンドを入力します。

  次のパラメータはオプションです。

  - *mac_addr*：クライアントの MAC アドレス。
  - *wlan_id*：クライアントがアソシエートしている WLAN ID。
  - *interface_name*：インターフェイスの名前。このインターフェイス名は WLAN に設定されたインターフェイスを上書きするために使用されます。

- *description*：インターフェイスの簡単な説明。二重引用符で囲みます（たとえば、"Interface1"）。
- *IP_addr*：上記の mac addr 値で指定される MAC アドレスを持つパッシブ クライアントに使用される IP アドレス。

- **config macfilter add** コマンドで IP アドレスが割り当てられていない場合に、既存の MAC フィルタ エントリに IP アドレスを割り当てるには、**config macfilter ip-address** *mac_addr IP_addr* コマンドを入力します。
- **show macfilter** コマンドを入力して、MAC アドレスが WLAN に割り当てられていることを確認します。

（注） ISE NAC WLAN では、MAC 認証要求は常に外部 RADIUS サーバに送信されます。MAC 認証は、ローカルデータベースと照合して検証されません。この機能はCSCvh85830に対する修正によりリリース 8.5、8.7、8.8 以降のリリースに適用されます。

以前はMAC フィルタリングを設定した場合、コントローラはまず RADIUS サーバを使用してワイヤレス クライアントを認証しようとしました。ローカル MAC フィルタリングが試行されたのは、RADIUS サーバがタイムアウトしたか、またはRADIUS サーバが設定されていなかったために RADIUS サーバが検出されなかった場合のみです。

802.1x への *MAC* 認証フェールオーバー

802.1X 認証への MAC 認証フェールオーバーの設定

クライアントに対する Static WEP による MAC 認証が失敗したときに、802.1X 認証を開始するようにコントローラを設定できます。RADIUS サーバが、クライアントを認証解除する代わりにクライアントからのアクセス要求を拒否した場合、コントローラは 802.1X 認証を受けることをクライアントに強制できます。クライアントが 802.1X 認証にも失敗した場合、クライアントは認証解除されます。

MAC認証が成功し、クライアントが802.1X認証を要求する場合、クライアントがデータ トラフィックの送信を許可されるには、802.1X 認証をパスする必要があります。クライアントが 802.1X 認証を選択しない場合、クライアントが MAC 認証にパスすれば、クライアントは認証を宣言されます。

（注） MAC が失敗した場合の **WPA2 + 802.1X + WebAuth with WebAuth** と WLAN はサポートされていません。

802.1X 認証への MAC 認証フェールオーバーの設定（GUI）

手順

ステップ 1 **[WLANs]** > **[WLAN ID]**を選択して、[WLANs > Edit] ページを開きます。

ステップ 2 [Security] タブで、[Layer 2] タブをクリックします。

ステップ 3 [MAC Filtering] チェックボックスをオンにします。

ステップ 4 [Mac Auth or Dot1x] チェックボックスをオンにします。

802.1X 認証への MAC 認証フェールオーバーの設定（CLI）

手順

802.1X 認証への MAC 認証フェールオーバーを設定するには、次のコマンドを入力します。

config wlan security 802.1X on-macfilter-failure {**enable** | **disable**} *wlan-id*

802.11w の設定

802.11w の制約事項

- Cisco の従来の管理フレーム保護は 7.4 リリースで実装されている 802.11w 標準には関連しません。
- 802.11w 標準は、Cisco WLC リリース 7.5 以降のすべての 802.11n 対応 AP でサポートされています。
- 802.11w 標準は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラではサポートされていません。
- 802.11w はオープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。

802.11w に関する情報

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。認証/認証解除、アソシエーション/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、AP を選択し、ネットワーク サービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータ トラフィックとは異なり、これらのフレームは、すべてのクライアントによって解釈されることが必要であり、したがってオープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディ

アを保護するために偽造を防止することが必要になります。たとえば、攻撃者はクライアントと AP の間のセッションを切断するために、AP から管理フレームをスプーフィングする可能性があります。

管理フレーム保護のための 802.11w 標準が 7.4 リリースに実装されています。

802.11w プロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。これらには、ディスアソシエーション、認証解除、ロバスト アクション フレームが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトル管理
- QoS
- DLS
- ブロック ACK
- 無線測定
- 高速 BSS 移行
- SA クエリ
- 保護されたデュアル パブリック アクション
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

- ディスアソシエーション フレームと認証解除フレームに対して、（MIC 情報要素を含めることにより）AP の暗号保護によるクライアント保護が追加されます。これによって、DoS 攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間と SA クエリーの手順から構成されるセキュリティ アソシエーション（SA）ティア ダウン保護メカニズムを追加することによって、インフラストラクチャの保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

802.11w の設定（GUI）

手順

ステップ 1 [WLANs] > [WLAN ID] の順に選択して、[WLANs > Edit] ページを開きます。

ステップ 2 [Security] タブで、[Layer 2] セキュリティ タブを選択します。

ステップ 3 [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。

802.11w IGTK キーはフォーウェイ ハンドシェークを使用して生成されます。つまり、レイヤ 2 で WPA2 セキュリティ用に設定された WLAN でのみ使用できます。

（注） WPA2 は必須であり、暗号化タイプは AES である必要があります。TKIP は無効です。

ステップ 4 ドロップダウン リストから PMF 状態を選択します。

次のオプションを使用できます。

- [Disabled]：WLAN での 802.11w MFP 保護を無効にします。
- [Optional]：クライアントが 802.11w をサポートしている場合に使用します。
- [Required]：802.11w をサポートしていないクライアントが WLAN とアソシエートできないようにします。

ステップ 5 PMF 状態を [Optional] または [Required] のいずれかとして選択する場合、次を行います。

a) [Comeback Timer] ボックスに、Association Comeback の間隔をミリ秒単位で入力します。これは、有効なセキュリティ アソシエーションの後に、アクセス ポイントがクライアントと再度アソシエーションする期間です。

b) [SA Query Timeout] ボックスに、Security Association（SA）クエリーがタイム アウトするまでの最大時間を入力します。

ステップ 6 [Authentication Key Management] セクションで、次の手順を実行します。

a) [PMF 802.1X] チェックボックスをオンまたはオフにして、管理フレームを保護するために 802.1X 認証を設定します。

b) [PMF PSK] チェックボックスをオンまたはオフにして、PMF 用に事前共有されているキーを設定します。PSK フォーマットには ASCII または 16 進数のいずれかを選択し、PSK を入力します。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Save Configuration] をクリックします。

802.11w の設定（CLI）

手順

- 次のコマンドを入力して、PMF の 802.1X 認証を設定します。

  config wlan security wpa akm pmf 802.1x {**enable** | **disable**} *wlan-id*

- 次のコマンドを入力して、PMF の事前共有キーのサポートを設定します。

  config wlan security wpa akm pmf psk {**enable** | **disable**} *wlan-id*

- 完了しない場合、次のコマンドを入力して、WLAN の事前共有キーを設定します。

  config wlan security wpa akm psk set-key {*ascii* | *hex*} *psk wlan-id*

- 次のコマンドを入力して、保護された管理フレームを設定します。

  config wlan security pmf {**disable** | **optional** | **required**} *wlan-id*

- 次のコマンドを入力して、Association Comeback の時間設定を構成します。

  config wlan security pmf association-comeback *timeout-in-seconds wlan-id*

- 次のコマンドを入力して、SA クエリー リトライ タイムアウト設定を構成します。

  config wlan security pmf saquery-retrytimeout *timeout-in-milliseconds wlan-id*

- 次のコマンドを入力して、WLAN の 802.11w 設定ステータスを表示します。

  show wlan *wlan-id*

- 次のコマンドを入力して、PMF のデバッグを設定します。

  debug pmf events {**enable** | **disable**}

高速安全ローミング

802.11r の高速移行

802.11R 高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP 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、高速移行（FT）と呼ばれるローミングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key（PTK）計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- Over-the-Air
- Over-the-DS（分散システム）

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN 設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

リリース 8.0 から、WPAv2 WLAN でもある 802.11r WLAN を作成できます。以前のリリースでは、802.11r の WLAN と通常のセキュリティ用にそれぞれ個別の WLAN を作成する必要がありました。802.11r WLAN が非 802.11r アソシエーションを受け入れることができるため、非 802.11r クライアントが 802.11r WLAN 対応 WLAN に接続できるようになりました。混合モードまたは 802.11r 接続をサポートしないクライアントは、非 802.11r WLAN に接続できます。FT PSK 以降を設定すると、PSK を混合モードで WLAN を結合できる PSK だけ結合できるクライアントを定義します。

クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクションフレームで実行されてから、コントローラ によって送信されます。

図 *2 : Over the Air* クライアントのローミングの設定時のメッセージ交換

この図は、Over the Air クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

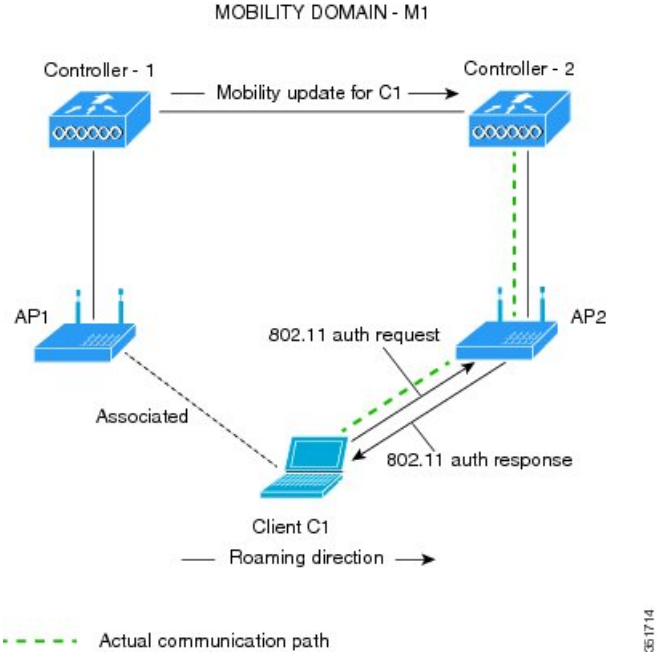
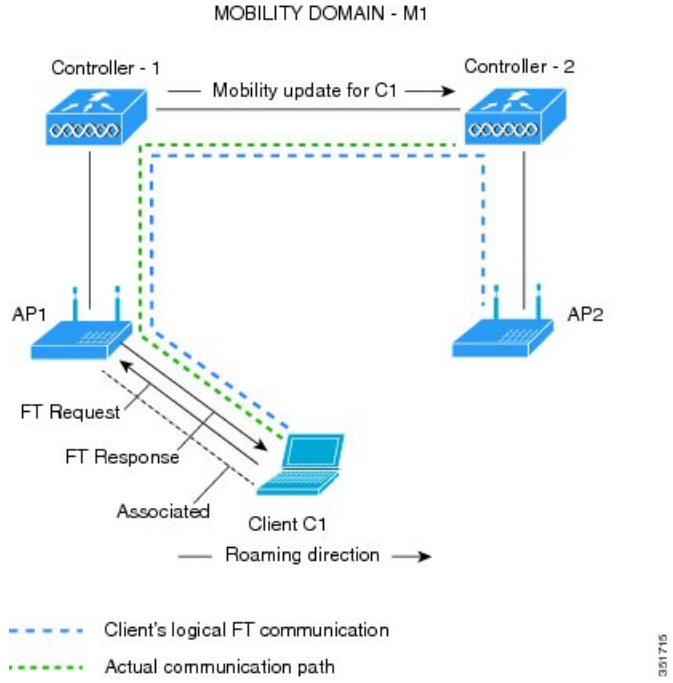


図 3 : *Over the DS* クライアントのローミングの設定時にメッセージが交換されます

この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。



802.11R 高速移行の制約事項

- この機能はメッシュ アクセス ポイントでサポートされていません。
- 8.1 以前のリリースでは、この機能は FlexConnect モードのアクセス ポイントでサポートされていません。リリース 8.2 では、この制約がなくなります。
- FlexConnect モードの AP では、次の事項を考慮します。
  - 802.11R 高速移行は、ローカルで集中的に切り替わる WLAN でサポートされています。
  - この機能は、ローカル認証が有効になっている WLAN ではサポートされません。
  - 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
  - 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。
  - ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。
  - AP が同じ FlexConnect グループに存在する場合のみ、802.11r 高速ローミングは機能します。

- クライアントがスタンドアロンモードのOver-the-DS事前認証を使用する場合、802.11r高速ローミングはサポートされません。
- EAP LEAP方式はサポートされません。 WANリンク遅延は、最大2秒間にアソシエーション時間を抑制します。
- スタンドアロンAPからクライアントへのサービスは、セッションタイマーが切れるまでサポートされます。
- TSpecは802.11r高速ローミングではサポートされません。したがって、RIC IEの処理はサポートされません。
- WANリンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。Cisco WLCは、Over-the-AirおよびOver-the-DS DS方式の両方をローミングする間、802.11r高速移行の認証要求を処理します。
- この機能は、オープンでWPA2設定のWLANでサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE内の追加AKMを認識しない場合、802.11rが有効にされているWLANにアソシエートできません。この制限のため、クライアントは、WLANにアソシエーション要求を送信できません。ただし、これらのクライアントは、非802.11r WLANとアソシエートできます。802.11r対応クライアントは、802.11rと802.11iの両方の認証キー管理スイートが有効にされているWLANの802.11iクライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい802.11r AKMで動作するようにするか、またはアップグレードすることです。そうすることで、レガシークライアントは、802.11r対応WLANと正常にアソシエートできます。

  もう1つの回避策は、同じ名前で異なるセキュリティ設定（FTおよび非FT）の2つのSSIDを持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、Cisco WLCでは、異なるAPと最大3つの高速移行ハンドシェイクが可能です。
- 非802.11r対応デバイスはFT対応WLANにアソシエートできなくなります。
- 802.11r FT + PMFはお勧めしません。
- 802.11r FT Over-the-Airローミングは FlexConnect導入にお勧めします。
- デフォルトのFlexGroupシナリオでは、高速ローミングはサポートされていません。
- CSCvk64674の修正の一環として、802.11r高速移行のアダプティブ モードはオープンWLANに対してはサポートされていません。つまり、WLANのレイヤ2セキュリティとして[None]を選択する場合は、802.11r高速移行のアダプティブ モードを無効にする必要があります。無効にしないと、WLANを有効にできません。

802.11r の Fast Transition の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ウィンドウを開きます。

ステップ 2 WLAN ID をクリックして、[WLANs > Edit] ウィンドウを開きます。

ステップ 3 [Security] > [Layer 2] タブを選択します。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。

Fast Transition の認証キー管理パラメータが表示されます。

ステップ 5 [Fast Transition] ドロップダウン リストから、WLAN の Fast Transition を選択します。

ステップ 6 [Over the DS] チェックボックスをオンまたはオフにして、分散システム経由の Fast Transition を有効または無効にします。

このオプションは、Fast Transition を有効にしたとき、または Fast Transition が適応型の場合のみ指定できます。

802.11r Fast Transition を使用するには、over-the-air および over-the-ds を無効にする必要があります。

ステップ 7 [Reassociation Timeout] フィールドに、AP へのクライアントの再関連付けの試行がタイムアウトになる秒数を入力します。有効範囲は 1 ～ 100 秒です。

（注） このオプションは、高速移行を有効にした場合だけ使用できます。

ステップ 8 [Authentication Key Management] で、[FT 802.1X] または [FT PSK] を選択します。キーを有効または無効にするには、対応するチェックボックスをオンまたはオフにします。[FT PSK] チェックボックスをオンにした場合は、[PSK Format] ドロップダウン リストから [ASCII] または [Hex] を選択して、キー値を入力します。

（注） 適応型 Fast Transition が有効な場合、802.1X および PSK AKM のみ使用できます。

ステップ 9 [WPA gtk-randomize State] ドロップダウン リストで [Enable] または [Disable] を選択して、Wi-Fi Protected Access (WPA) group temporal key (GTK) randomize state を設定します。

ステップ 10 [Apply] をクリックして設定値を保存します。

802.11r Fast Transition の設定（CLI）

802.11r 対応 WLAN は、ワイヤレス クライアント デバイスに高速ローミングを実現します。ただし、802.11r が WLAN で有効になっており、ビーコンおよびプローブ RSN IE で Fast Transition（FT）および非 FT AKM をアドバタイズしている場合、不正に実装されている一部のデバイスは RSN IE の FT/WPA2 認証キー管理（AKM）を認識できず、参加に失敗します。その結果、顧客は SSID で 802.11r を有効にすることはできません。

これに対処するため、シスコ無線インフラストラクチャは適応型 802.11r 機能を導入しています。FT モードが適応型に設定されている場合、WLAN は 802.11i 対応 WLAN で 802.11r モビリティ ドメイン ID をアドバタイズします。Apple iOS10 クライアント デバイスは 80211i/WPA2 WLAN の MDIE の存在を特定し、独自のハンドシェイクをして 802.11r の関連付けを確立します。クライアントが 802.11r の関連付けを正常に完了すると、標準 802.11r 対応 WLAN で FT ローミングを行うことができるようになります。

FT 適応型は選択された Apple iOS10 デバイスのみに適用できます。他のすべてのクライアントは引き続き WLAN で 802.11i に関連付けられます。

手順

ステップ 1 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft** {**adaptive** | **enable** | **disable**} *wlan-id* コマンドを使用します。

Fast Transition 適応型オプションは新しい WLAN を、シスコ ワイヤレス コントローラ（WLC）、リリース 8.3 以降から作成する場合、デフォルトで有効になります。ただし、既存の WLAN は以前のリリースからリリース 8.3 へ Cisco WLC をアップグレードする場合に現在の設定を保持します。

クライアント デバイスがある WLAN から別の WLAN にスムーズに切り替えることができるよう、高速 SSID 機能を有効にします。。

ステップ 2 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft over-the-ds** {**enable** | **disable**} *wlan-id* コマンドを使用します。

クライアント デバイスは通常、機能が WLAN でアドバタイズされている場合 fast transition over-the-ds を優先します。クライアントに fast transition over-the-air を強制的に実行させるには、fast transition over-the-ds を無効にします。

ステップ 3 事前共有キー（PSK）を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft psk** {**enable** | **disable**} *wlan-id* コマンドを使用します。

デフォルトで、PSK を使用した認証キー管理は無効です。

ステップ 4 PSK を使用した適応型の認証キー管理を有効または無効にするには、**config wlan security wpa akm psk** {**enable** | **disable**} *wlan-id* コマンドを使用します。

ステップ 5 802.1x を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-802.1X** {**enable** | **disable**} *wlan-id* コマンドを使用します。

デフォルトでは、802.1X を使用した認証キー管理は有効です。

ステップ 6 802.1x を使用した適応型の認証キー管理を有効または無効にするには、**config wlan security wpa akm 802.1x** {**enable** | **disable**} *wlan-id* コマンドを使用します。

（注） 適応型 Fast Transition が有効な場合、802.1X および PSK AKM のみ使用できます。

ステップ 7 802.11r Fast Transition の再アソシエーション タイムアウトを有効または無効にするには、**config wlan security ft reassociation-timeout** *timeout-in-seconds wlan-id* コマンドを使用します。

有効範囲は 1 ～ 100 秒です。再アソシエーション タイムアウトのデフォルト値は 20 秒です。

ステップ 8 WLAN の高速移行の設定を表示するには、**show wlan** *wlan-id* コマンドを使用します。

ステップ 9 クライアントの高速移行の設定を表示するには、**show client detail** *client-mac* コマンドを使用します。

（注） このコマンドは、接続済みまたは接続中のクライアント ステーション（STA）にのみ該当します。

ステップ 10 高速移行イベントのデバッグを有効または無効にするには、**debug ft events** {**enable** | **disable**} コマンドを使用します。

次のタスク

- 無効にされている場合、tech support コマンド出力および xml config は Fast Transition 情報を表示しません。
- 有効にされている場合、tech support コマンド出力および xml config は Adaptive 802.11r 情報を表示します。
- 現在の Cisco WLC 設定の包括的なビューを表示するには、[show run-config all] コマンドを使用します。
- Fast Transition 適応型モードはリリース 8.3 以前のリリースではサポートされておらず、Fast Transition 適応型 WLAN は、Cisco WLC がリリース 8.3 から以前のリリースにダウングレードされている場合デフォルトで fast transition disable になり、Fast Transition 適応型設定は無効になります。

802.11r BSS Fast Transition のトラブルシューティング

症状	解決策
非 802.11r レガシー クライアントはすでに接続していません。	WLAN で FT が有効であるかどうかを確認します。その場合、非 FT WLAN が作成される必要があります。
WLAN を設定する場合、FT 設定オプションは表示されません。	WPA2 が使用されているかどうかを確認します（802.1x/PSK）。FT は WPA2 SSID およびオープン SSID だけでサポートされます。
802.11r クライアントは、新しいコントローラにレイヤ 2 のローミングを実行するときに、再認証されると想定されます。	コントローラの GUI で、[WLANs] > [WLAN Name] > [Security] > [Layer 2] と移動して、再認証タイムアウトがデフォルトの 20 よりも小さくなっているかどうかを確認します。

Sticky Key Caching

Sticky Key Caching について

コントローラは Sticky Key Caching（SKC）をサポートします。Sticky Key Caching により、クライアントは、アソシエートする AP ごとに異なる PMKID を受信し、保存します。AP も、クライアントに発行される PMKID のデータベースを維持します。

SKC では、クライアントは Pairwise Master Key Security Association（PMKSA）に対してそれぞれの Pairwise Master Key ID（PMKID）を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。SKC の場合、PMKSA はクライアントが保存する AP のキャッシュごとであり、新しい AP の BSSID に基づいて事前に計算されます。

Sticky Key Caching の制約事項

- コントローラは、クライアントあたり最大 8 つの AP の SKC をサポートします。クライアントがセッションあたり 8 以上の AP にローミングする場合、クライアントのローミング時に、古い AP は削除され、新しくキャッシュされたエントリが保存されます。大規模な展開に SKC を使用しないことを推奨します。
- SKC は、WPA2 が有効になっている WLAN でのみ動作します。
- SKC は、モビリティ グループのアクセス コントローラでは機能しません。
- SKC はローカル モードの AP でのみ動作します。

Sticky Key Caching の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 2 次のコマンドを入力して、sticky key caching を有効にします。

config wlan security wpa wpa2 cache sticky enable *wlan_id*

デフォルトでは、SKC は無効で opportunistic key caching（OKC）が有効になっています。

（注） SKC は、WPA2 が有効になっている WLAN でのみ動作します。

SKC が有効かどうかを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 2
Profile Name..................................... new
Network Name (SSID).............................. new
Status........................................... Disabled
```

```
MAC Filtering..................................... Disabled
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys............................... Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE)............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
      Auth Key Management
         802.1x.................................. Disabled
         PSK..................................... Enabled
         CCKM.................................... Disabled
         FT(802.11r)............................. Disabled
         FT-PSK(802.11r)......................... Disabled
     SKC Cache Support......................... Enabled
      FT Reassociation Timeout................... 20
      FT Over-The-Air mode....................... Enabled
      FT Over-The-Ds mode........................ Enabled
CCKM tsf Tolerance............................... 1000
   Wi-Fi Direct policy configured................ Disabled
   EAP-Passthrough............................... Disabled
```

ステップ 3 WLAN を有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

ステップ 4 次のコマンドを入力して、設定を保存します。

save config

暗号化

Static WEP 用 WLAN

Static WEP 用 WLAN について

Static WEP キーをサポートするために、最大 4 つの WLAN を設定できます。Static WEP 用 WLAN を設定する場合は、次のガイドラインに従ってください。

- Static WEP をレイヤ 2 セキュリティ ポリシーとして設定する場合、他のセキュリティ ポリシーは指定できません。つまり、Web 認証を設定できません。ただし、Static WEP をレイヤ 2 セキュリティ ポリシーとして設定する場合は、Web 認証を設定できます。

WPA1 と *WPA2*

Wi-Fi 保護アクセス（WPA または WPA1）および WPA2 は、無線 LAN システム用のデータ保護とアクセス コントロールを提供する Wi-Fi Alliance の規格ベースのセキュリティ ソリューションです。WPA1 は、IEEE 802.11i 規格に準拠していますが、規格の承認前に実装されたも

のです。これに対して、WPA2 は、承認された IEEE 802.11i 規格が Wi-Fi Alliance によって実装されています。

WPA1 のデフォルトでは、データの保護に Temporal Key Integrity Protocol（TKIP）および Message Integrity Check（MIC）が使用されますが、WPA2 では Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用したより強力な Advanced Encryption Standard 暗号化アルゴリズム（AES-CCMP）が使用されます。WPA1 および WPA2 のデフォルトでは、両方とも 802.1X を使用して認証キー管理を行います。ただし、次のオプションも使用できます。

- 802.1X：IEEE によって定義された無線 LAN セキュリティの規格。802.1X for 802.11、または単に 802.1X と呼ばれます。802.1X をサポートするアクセス ポイントは、無線ネットワークを介して通信を行う相手となるワイヤレスクライアントおよび認証サーバ（RADIUS サーバなど）との間のインターフェイスとして機能します。[802.1X] が選択されている場合は、802.1X クライアントのみがサポートされます。

- PSK：PSK（WPA 事前共有キーまたは WPA パスフレーズとも呼ばれます）を選択した場合は、事前共有キー（またはパスフレーズ）を設定する必要があります。このキーは、クライアントと認証サーバの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。

- CCKM：Cisco Centralized Key Management（CCKM）では、迅速なキーの再生成技術を使用しています。この技術を使用すると、クライアントは、通常 150 ミリ秒（ms）以下で、コントローラを経由せずにあるアクセス ポイントから別のアクセス ポイントにローミングできます。CCKM により、クライアントが新しいアクセス ポイントと相互に認証を行い、再アソシエーション時に新しいセッションキーを取得するために必要な時間が短縮されます。CCKM の迅速かつ安全なローミングでは、無線 VoIP、Enterprise Resource Planning（ERP）、Citrix ベースのソリューションなどの時間依存型のアプリケーションにおいて、認識できるほどの遅延は発生しません。CCKM は、CCXv4 に準拠する機能です。CCKM が選択されている場合は、CCKM クライアントのみがサポートされます。

  CCKM を有効にすると、アクセス ポイントの動作は、高速ローミングのコントローラと次の点で異なります。

  - クライアントから送信されるアソシエーション要求の Robust Secure Network Information Element（RSN IE）で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合、コントローラは完全な認証を行いません。代わりに、コントローラは PMKID を検証し、フォーウェイハンドシェイクをします。

  - クライアントから送信されるアソシエーション要求の RSN IE で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合でも、AP は完全な認証を行います。CCKM が RSN IE で有効になっている場合、このアクセスポイントではアソシエーション要求と一緒に送信される PMKID は使用されません。

- 802.1X+CCKM：通常の動作状態の間、802.1X が有効になっているクライアントは、主要な RADIUS サーバとの通信を含む完全な 802.1X 認証を実行することにより、新しいアクセス ポイントとの相互認証を行います。ただし、802.1X および CCKM の迅速で安全なローミング用に WLAN を設定した場合、CCKM が有効になっているクライアントは、

RADIUS サーバに対して再認証せずに、あるアクセス ポイントから別のアクセス ポイントに安全にローミングを行います。このオプションが選択されている場合、CCKM クライアントと非CCKM クライアントの両方がサポートされるため、802.1X+CCKM はオプションの CCKM と見なされます。

単一の WLAN では、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM のクライアントに接続を許可できます。このような WLAN のアクセス ポイントはいずれも、ビーコンとプローブ応答で WPA1、WPA2、および 802.1X/PSK/CCKM/ 802.1X+CCKM 情報要素をアドバタイズします。WPA1 または WPA2、あるいは両方を有効にした場合は、データ トラフィックを保護するために設計された 1 つまたは 2 つの暗号方式（暗号化アルゴリズム）を有効にすることもできます。具体的には、WPA1 または WPA2、あるいはその両方に対して、AES または TKIP、またはその両方を有効にすることができます。TKIP は WPA1 のデフォルト値で、AES は WPA2 のデフォルト値です。

Static WEP の設定の制約事項

- OEAP 600 シリーズはクライアントの高速ローミングをサポートしません。デュアル モードの音声クライアントは、OEAP602 アクセス ポイントの 2 つのスペクトラム間をローミングするときに、コール品質が低下します。音声デバイスは 2.4 GHz または 5.0 GHz の 1 帯域にのみ接続するように設定することをお勧めします。
- Cisco WLC ソフトウェアは、CCX バージョン 1 ～ 5 をサポートしています。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラは、クライアント データベースにクライアントの CCX バージョンを格納し、これを使用してクライアントの機能を制限します。CCKM を使用するには、クライアントで CCXv4 または v5 をサポートする必要があります。CCX の詳細については、「Cisco Client Extensions の設定」の項を参照してください。
- 複数の VLAN クライアントが WGB でサポートされる統合アーキテクチャでは、WEP 暗号化が WGB で有効である場合、暗号化の暗号スイートおよび WEP キーをグローバルに設定する必要があります。設定しない場合、有線 VLAN クライアントのマルチキャスト トラフィックが失敗します。

WPA1+WPA2 の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit]（[Security] > [Layer 2]）ページを開きます。

ステップ 4 [Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択します。

ステップ 5 [WPA+WPA2 Parameters] で、[WPA Policy] チェックボックスをオンにして WPA1 を有効にするか、[WPA2 Policy] チェックボックスをオンにして WPA2 を有効にするか、または両方のチェックボックスをオンにして WPA1 と WPA2 を両方とも有効にします。

（注） WPA1 および WPA2 のデフォルト値は、両方とも無効になっています。WPA1 と WPA2 を両方とも無効のままにすると、アクセス ポイントは、ステップ 7 で選択する認証キー管理方式に対してのみ情報要素をビーコンおよびプローブ応答でアドバタイズします。

ステップ 6 AES データ暗号化を有効にする場合は **[WPA2 Policy-AES]** チェックボックスをオンにし。

（注） Wi-Fi Alliance（WFA）のガイダンスによれば、WPA/TKIP はセカンダリ インターフェイス（CLI）上でしか設定できません。以前に保存した TKIP 設定はすべてアップグレード時に保存されるため、CLI で表示できます。これにより、WPA/TKIP のみをサポートする Wi-Fi クライアントを使用しているお客様が、AES をサポートするデバイスへの移行を計画することができます。

ステップ 7 [Auth Key Mgmt] ドロップダウン リストから、[802.1X]、[CCKM]、[PSK]、または [802.1X+CCKM] のいずれかのキー管理方式を選択します。

（注） Cisco の OEAP 600 では、CCKM はサポートされていません。802.1X または PSK を選択する必要があります。

（注） Cisco OEAP 600 の場合、TKIP および AES セキュリティ暗号化の設定は、WPA と WPA2 で同一であることが必要です。

ステップ 8 ステップ 7 で [PSK] を選択した場合は、[PSK Format] ドロップダウン リストから [ASCII] または [HEX] を選択し、空のテキスト ボックスに事前共有キーを入力します。WPA の事前共有キーには、8 ～ 63 文字の ASCII テキスト、または 64 桁の 16 進数文字が含まれている必要があります。

（注） PSK パラメータは、設定専用パラメータです。PSK キーに設定された値は、セキュリティ上の理由からユーザには表示されません。たとえば、PSK キーを設定するときに、キー形式として [HEX] を選択した場合に、あとでこの WLAN のパラメータを表示すると、表示される値はデフォルト値になります。デフォルトは ASCII です。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

WPA1+WPA2 の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 2 次のコマンドを入力して、WLAN の WPA を有効または無効にします。

config wlan security wpa {**enable** | **disable**} *wlan_id*

ステップ 3 次のコマンドを入力して、WLAN の WPA1 を有効または無効にします。

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

ステップ 4 WLAN の WPA2 を有効または無効にするには、次のコマンドを入力します。

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

ステップ 5 WPA1 または WPA2 に対して AES または TKIP データ暗号化を有効または無効にするには、次のコマンドを入力します。

- **config wlan security wpa wpa1 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*
- **config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。

（注） リリース 8.0 から、スタンドアロン暗号化方式として TKIP を設定できなくなりました。TKIP は、AES 暗号化方式でのみ使用できます。

（注） CLI を使用してのみ TKIP 暗号化を有効または無効にできます。GUI での TKIP 暗号化の設定はサポートされていません。

WGB に VLAN 設定がある場合、たとえば **encryption vlan 80 mode ciphers tkip** など、特定の VLAN に対して暗号化方式モードとキーを設定する必要があります。その後に、次の **encryption mode ciphers tkip** コマンドを入力して、マルチキャストインターフェイス上の暗号化方式モードをグローバルに設定する必要があります。

ステップ 6 802.1X、PSK、または CCKM 認証キー管理を有効または無効にするには、次のコマンドを入力します。

config wlan security wpa akm {**802.1X** | **psk** | **cckm**} {**enable** | disable} *wlan_id*

デフォルト値は 802.1X です。

ステップ 7 ステップ *6* で PSK を有効にした場合は、次のコマンドを入力して事前共有キーを指定します。

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA の事前共有キーには、8 ～ 63 文字の ASCII テキスト、または 64 桁の 16 進数文字が含まれている必要があります。

ステップ 8 高速移行に対して認証キー管理スイートを有効または無効にするには、次のコマンドを入力します。

config wlan security wpa akm ft {**802.1X** | **psk**} {**enable** | **disable**} *wlan_id*

（注） AKM スイートとして PSK または高速移行 PSK を選択できます。

ステップ 9 AP とクライアント間のグループの一時的キー（GTK）のランダム化を有効または無効にするには、次のコマンドを入力します。

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

ステップ 10 802.1X 認証キー管理で WPA2、または CCKM 認証キー管理で WPA1 または WPA2 を有効にした場合、必要に応じて、PMK キャッシュ ライフタイム タイマーを使用して、クライアントで

の再認証をトリガーします。タイマーは、AAA サーバから受信したタイムアウト値または WLAN のセッション タイムアウト設定に基づきます。タイマーが切れるまでに残されている時間を確認するには、次のコマンドを入力します。

show pmk-cache all

802.1X 認証キー管理で WPA2 を有効にした場合、コントローラは opportunistic PMKID キャッシュと sticky（non-opportunistic）PMKID キャッシュの両方をサポートします。sticky PMKID キャッシュ（SKC）で、クライアントは、アソシエートする AP ごとに異なる、複数の PMKID を保存します。opportunistic PMKID キャッシュ（OKC）は、クライアントあたり 1 つの PMKID だけを保存します。デフォルトで、コントローラは OKC をサポートします。

ステップ 11 WLAN を有効にするには、次のコマンドを入力します。

config wlan enablewlan_id

ステップ 12 次のコマンドを入力して、設定を保存します。

save config

CKIP

CKIP について

Cisco Key Integrity Protocol（CKIP）は、IEEE 802.11 メディアを暗号化するためのシスコ独自のセキュリティ プロトコルです。CKIP では、インフラストラクチャ モードでの 802.11 セキュリティを強化するために、キーの置換、メッセージの整合性チェック（MIC）、およびメッセージ シーケンス番号が使用されています。ソフトウェア リリース 4.0 以降では、静的キーを使用した CKIP をサポートしています。この機能を正常に動作させるには、WLAN に対して Aironet 情報要素（IE）を有効にする必要があります。

Lightweight アクセス ポイントは、ビーコンおよびプローブ応答パケットに Aironet IE を追加し、CKIP ネゴシエーション ビット（キー置換およびマルチモジュラ ハッシュ メッセージ整合性チェック [MMH MIC]）の一方または両方を設定することにより、CKIP のサポートをアドバタイズします。キー置換は、基本の暗号キーおよび現在の初期ベクトル（IV）を使用して新しいキーを作成するデータ暗号化技術です。MMH MIC では、ハッシュ関数を使用してメッセージ整合性コードを計算することにより、暗号化されたパケットでのパケット改ざん攻撃を回避します。

WLAN で指定された CKIP の設定は、アソシエートを試みるすべてのクライアントに必須です。WLAN で CKIP のキー置換および MMH MIC の両方が設定されている場合、クライアントは両方をサポートする必要があります。WLAN がこれらの機能の 1 つだけに設定されている場合は、クライアントではその CKIP 機能だけをサポートする必要があります。

CKIP では、5 バイトおよび 13 バイトの暗号キーは 16 バイトのキーに拡張される必要があります。キーを拡張するためのアルゴリズムは、アクセス ポイントで発生します。キーは、長さが 16 バイトに達するまで、そのキー自体に繰り返し追加されます。Lightweight アクセス ポイントはすべて CKIP をサポートしています。

（注） CKIP は Static WEP での使用についてのみサポートされています。Dynamic WEP での使用はサポートされていません。したがって、Dynamic WEP で CKIP を使用するように設定された無線クライアントは、CKIP 用に設定されている WLAN にアソシエートできません。CKIP なしで Dynamic WEP を使用する（安全性がより低い）か、または TKIP または AES で WPA/WPA2 を使用する（安全性がより高い）ことを推奨します。

CKIP の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Aironet IE] チェックボックスをオンにして、この WLAN に対する Aironet IE を有効にし、[Apply] をクリックします。

ステップ 5 [General] タブを選択します。

ステップ 6 [Status] チェックボックスがオンになっている場合は、これをオフにしてこの WLAN を無効にし、[Apply] をクリックします。

ステップ 7 [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit]（[Security] > [Layer 2]）ページを開きます。

ステップ 8 [Layer 2 Security] ドロップダウン リストから [CKIP] を選択します。

ステップ 9 [CKIP Parameters] で、[Key Size] ドロップダウン リストから CKIP 暗号キーの長さを選択します。その範囲は、[Not Set]、[40 bits]、または [104 bits] です。デフォルトは、[Not Set] です。

ステップ 10 [Key Index] ドロップダウン リストからこのキーに割り当てる番号を選択します。キーは、最高 4 つまで設定できます。

ステップ 11 [Key Format] ドロップダウン リストから、[ASCII] または [HEX] を選択し、[Encryption Key] テキスト ボックスに暗号化キーを入力します。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。

ステップ 12 この WLAN に対して **MMH MIC** データ保護を有効にする場合は、[MMH Mode] チェックボックスをオンにします。デフォルト値では無効（またはオフ）になっています。

ステップ 13 この形式の CKIP データ保護を有効にする場合は、[Key Permutation] チェックボックスをオンにします。デフォルト値では無効（またはオフ）になっています。

ステップ 14 [Apply] をクリックして、変更を確定します。

ステップ 15 [General] タブを選択します。

ステップ 16 [Status] チェックボックスをオンにして、この WLAN を有効にします。

ステップ 17 [Apply] をクリックして、変更を確定します。

ステップ 18 [Save Configuration] をクリックして、変更を保存します。

CKIP の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 2 この WLAN の Aironet IE を有効にするには、次のコマンドを入力します。

config wlan ccx aironet-ie enable *wlan_id*

ステップ 3 WLAN の CKIP を有効または無効にするには、次のコマンドを入力します。

config wlan security ckip {**enable** | **disable**\\ *wlan_id*

ステップ 4 WLAN に対して CKIP 暗号化キーを指定するには、次のコマンドを入力します。

config wlan security ckip akm psk set-key *wlan_id*{**40** |**104**} {**hex** |**ascii**\\キー *key_index*

ステップ 5 WLAN に対して CKIP MMH MIC を有効または無効にするには、次のコマンドを入力します。

config wlan security ckip mmh-mic {**enable** | **disable**\\ *wlan_id*

ステップ 6 WLAN に対して CKIP キー置換を有効または無効にするには、次のコマンドを入力します。

config wlan security ckip kp {**enable** | **disable**} *wlan_id*

ステップ 7 WLAN を有効にするには、次のコマンドを入力します。

config wlan enablewlan_id

ステップ 8 次のコマンドを入力して、設定を保存します。

save config

Identity PSK

Identity PSK について

この機能は、ネットワークに接続するデバイス数の増加に対応する簡単でセキュアな方法を提供するように設計されています。Internet of Things（IoT）クライアントなどの一部のデバイスは、802.1 x セキュリティプロトコルに対応していないことがあります。それらのデバイスは、PSK 認証メカニズムを使用してネットワークに接続できます。

すべてのクライアントが同じキーを使用していて、そのキーが不正ユーザと共有されている場合、セキュリティ違反が発生します。

IPSK 機能を使用すると、管理者は同じ SSID で WPA-PSK プロトコルベースの一意な事前共有キーを設定できます。この事前共有キーは、個人またはユーザのグループに発行して、それぞれのデバイスを簡単かつ安全にネットワークに接続できるようにします。これは、ネットワークに接続しているその他の事前共有キーを持つデバイスに影響を与えずに、一連のデバイスを特定および管理するのにも役立ちます。これらのキーは、認証に関するルールを指定して設定でき、ネットワークに適切なレベルのアクセスを提供できます。

以下は、クライアントの認証に使用される AAA RADIUS サーバ キーです。

Cisco ISE の設定マニュアルについては、Cisco ISE 2.2 管理者ガイド [英語] を参照してください。

Identity PSK の前提条件

RADIUS サーバは、MAC フィルタリング認証要求に対する応答で、次の Cisco AV ペアを返すように設定する必要があります。

- psk-mode=ascii
- psk=cisco123

キーの長さは、ASCII の場合は 8 ～ 63 文字、16 進数の場合は 64 文字にする必要があります。RADIUS サーバに設定されているキーが長さの要件を満たしていない場合、WLAN に設定されている PSK を使用してクライアントを認証できます。

Identity PSK の設定（GUI）

手順

ステップ 1 [WLAN] を選択して、[WLAN] ページを開きます。

ステップ 2 新しい WLAN を作成するか、既存の WLAN をクリックします。

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

ステップ 4 **[Security]** > **[Layer 2]** タブを選択します。

ステップ 5 [Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択します。

ステップ 6 [MAC Filtering] チェックボックスをオンにします。

ステップ 7 [Authentication Key Management] で [PSK Enable] チェックボックスをオンにします。

ステップ 8 **[Security]** > **[AAA Servers]** タブを選択します。

ステップ 9 [Authentication Servers Enabled] チェックボックスをオンにします。

ステップ 10 ドロップダウンリストから、[Server IP address and port number] を選択します。

RADIUS サーバが設定されていない場合は、グローバル リストから RADIUS サーバが選択されます。

ステップ 11 [Advanced] タブを選択します。

ステップ 12 [Allow AAA Override Enabled] チェックボックスをオンにして、AAA オーバーライドを有効にします。デフォルト値は [disabled] です。

ステップ 13　[Apply] をクリックします。

Identity PSK の設定（CLI）

手順

- 次コマンドを入力して、MAC フィルタリングを有効にします。
  config wlan mac-filtering enable *wlan-id*
- 次のコマンドを入力して、WLAN で AAA オーバーライドを有効にします。
  config wlan aaa-override enable *wlan-id*
- 次のコマンドを入力して、WLAN で RADIUS 認証を有効にします。
  config wlan radius_server auth enable *wlan-id*
- 次のコマンドを入力して、WLAN で PSK サポートを有効にします。
  config wlan security wpa akm psk enable *wlan-id*
- 次のコマンドを入力して、PSK 事前共有キーを設定します。
  config wlan security wpa akm psk set-key *ascii/hex psk-key wlan-id*

レイヤ 3 セキュリティ

Web 認証を使用したレイヤ 3 セキュリティの設定

WLAN の Web 認証を設定するための前提条件

- HTTP/HTTPS Web 認証リダイレクションを開始するには、HTTP URL または HTTPS URL を使用します。
- CPU ACL が HTTP / HTTPS トラフィックをブロックするように設定されている場合、正常な Web ログイン認証の後に、リダイレクション ページでエラーが発生する可能性があります。
- Web 認証を有効にする前に、すべてのプロキシ サーバがポート 53 以外のポートに対して設定されていることを確認してください。
- WLAN の Web 認証を有効にする場合、コントローラがワイヤレス クライアントで送受信されるトラフィックを転送することを示すメッセージが認証前に表示されます。DNS トラフィックを規制し、DNS トンネリング攻撃を検出および予防するために、ゲスト VLAN の背後にファイアウォールまたは侵入検知システム（IDS）を設置することをお勧めします。
- Web 認証が WLAN で有効になっており、さらに、CPU ACL のルールもある場合、クライアント ベースの Web 認証ルールは、クライアントが非認証である限り優先されます

（webAuth_Reqd ステート）。クライアントが RUN 状態になると、CPU ACL ルールが適用されます。したがって、コントローラで CPU ACL ルールが有効である場合、次の状況で、仮想インターフェイス IP に対する allow ルール（任意の方向）が必要なります。

- CPU ACL で、両方向とも allow ACL ルールが設定されていない。
- allow ALL ルールが設定されているが、優先順位が高いポート 443 または 80 に対する DENY ルールも設定されている。

- 仮想 IP に対する allow ルールは、TCP プロトコルおよびポート 80（secureweb が無効な場合）またはポート 443（secureweb が有効な場合）に設定します。このプロセスは、仮想インターフェイス IP アドレスへのクライアントのアクセスを許可し、CPU ACL ルールが設定されている場合に正常認証をポストするために必要です。

WLAN の Web 認証の設定に関する制約事項

- Web 認証はレイヤ 2 セキュリティ ポリシー（オープン認証、オープン認証 + WEP、WPA-PSK）でのみサポートされています。7.4 リリースでは、Web 認証での 802.1X の使用がサポートされています。
- Web 認証のユーザ名フィールドでの特殊文字はサポートされていません。
- クライアントが WebAuth SSID に接続したときに、事前認証 ACL が VPN ユーザを許可するように設定されていると、クライアントは数分ごとに SSID との接続を解除されます。Webauth SSID の接続には、Web ページでの認証が必要です。

  Web 認証ユーザ セクションの **[WLANs] > [Security] > [AAA servers] > [Authentication priority]** で次の ID ストアを選択して、Web 認証ユーザを認証できます。

  - Local
  - RADIUS
  - LDAP

  複数の ID ストアを選択すると、コントローラはユーザの認証が成功するまで、リストの各 ID ストアを指定された順序で上から下までチェックします。コントローラがリストの最後に達しても ID ストアのいずれかに未認証のユーザが残っている場合、認証は失敗します。

Web 認証について

コントローラで VPN パススルーが有効になっていない場合に限り、WLAN では Web 認証を使用できます。Web 認証は、セットアップも使用方法も簡単で、SSL とともに使用することで WLAN 全体のセキュリティを向上させることができます。

802.1x と Web 認証の使用

WLAN で 802.1x と一緒に Web 認証を使用する場合は、3 種類のタイマーがアクティブになります。これらのタイマーは、AAA サーバから受信したタイムアウト値または WLAN セッション タイムアウトに基づきます。

- セッション タイマー：再認証を要求する WLAN 用に設定されたクライアント セッション タイムアウト。このタイマーは、Web 認証の成功後に起動します。
- 再認証タイマー：WPA1 用のクライアント再認証をトリガーするために使用されるタイマー。
- PMK キャッシュ タイマー：WPA2 用のクライアント再認証をトリガーするために使用されるキャッシュ ライフタイム タイマー。

このセクションでは、WLAN が 802.1x と一緒に Web 認証を使用するように設定されている場合に、クライアントで発生する可能性のある 2 つのシナリオについて説明します。

1 つのコントローラにアソシエートされたクライアント：このシナリオでは、再認証または PMK キャッシュ タイマーの有効期限が切れると、クライアントが再認証を行い、再認証/PMK キャッシュ タイマーを更新し、実行状態を維持します。クライアント セッション タイマー（ST）の有効期限が切れると、再認証/PMK キャッシュ タイマーがまだ有効であっても、クライアントが認証解除されます。

コントローラ間のクライアント ローミング：このシナリオでは、クライアントがローミングしてから、外部コントローラが L2 認証をトリガーし、アンカー コントローラが L3 認証をトリガーします。802.1x 再認証/PMK タイマーは外部コントローラ上で動作し、クライアント セッションタイマーはアンカーコントローラ上で動作します。再認証/PMK タイマーの有効期限が切れると、802.1x クライアント再認証が実施され、クライアントが実行状態になります。クライアントは、クライアント セッション タイマーの有効期限が切れたときにのみ認証解除されます。

セッション タイムアウトは、認証のタイプ（AAA またはローカル）とユーザの人数によって異なります。

- AAA ユーザの AAA オーバーライドが有効になっている場合は、セッション タイムアウトが RADIUS サーバから受信されます。
- AAA ユーザの AAA オーバーライドが無効になっている場合は、セッション タイムアウトが対応する WLAN から取得されます。
- ローカル認証が使用されている場合は、802.1x 再認証/PMK キャッシュ タイマーが WLAN ST 値になり、Web 認証ローカルユーザの残りのライフタイムが ST として設定されます。

（注） 802.1x と Web 認証の両方を同じユーザに使用することも、別々のユーザに使用することもできます。

Web 認証の設定

Web 認証の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Web 認証を設定する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Web Policy] チェックボックスをオンにします。

ステップ 5 [Authentication] オプションが選択されていることを確認します。

ステップ 6 [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして設定を保存します。

Web 認証の設定（CLI）

手順

ステップ 1 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。

config wlan security web-auth {**enable** | **disable**} *wlan_id*

ステップ 2 Web 認証ポリシーのタイマーが切れたときにゲスト ユーザの IP アドレスを解放して、ゲスト ユーザが 3 分間 IP アドレスを取得しないようにするには、次のコマンドを入力します。

config wlan webauth-exclude *wlan_id*{**enable** |**disable**}

デフォルト値は [disabled] です。コントローラに内部 DHCP スコープを設定するときに、このコマンドを適用できます。デフォルトでは、ゲスト ユーザは、Web 認証のタイマーが切れた場合、別のゲスト ユーザがその IP アドレスを取得する前に、ただちに同じ IP アドレスに再アソシエートできます。ゲスト ユーザの数が多い場合、または DHCP プールの IP アドレスが限れられている場合、一部のゲストユーザが IP アドレスを取得できなくなる可能性があります。

ゲスト WLAN でこの機能を有効にした場合、Web 認証ポリシーのタイマーが切れると、ゲスト ユーザの IP アドレスが解放され、このゲスト ユーザは 3 分間 IP アドレスの取得から除外されます。その IP アドレスは、別のゲスト ユーザが使用できます。3 分経つと、除外されていたゲスト ユーザは、可能であれば、再アソシエートし、IP アドレスを取得できるようになります。

ステップ 3 次のコマンドを入力して、Web 認証のステータスを表示します。

show wlan *wlan_id*

デフォルトの Web 認証ログイン ページの選択

デフォルトの Web 認証ログイン ページについて

内部コントローラの Web サーバによって処理されるカスタムの webauth bundle を使用する場合は、ページに 5 つを超える要素（HTML、CSS、イメージなど）を含めることはできません。これは、内部コントローラの Web サーバが実装する DoS 保護メカニズムにより、各クライアントが開く同時 TCP 接続が負荷に応じて最大 5 つに制限されるためです。ページに多くの要素が含まれていて、ブラウザによる DoS 保護の処理方法によっては、ページのロードが遅くなることがある場合、一部のブラウザでは、同時に 5 つを超える TCP セッションが開かれようとします。

ユーザが SSLv2 専用に設定されているブラウザを使用して Web ページに接続するのを防止する場合は、**config network secureweb cipher-option sslv2 disable command** を入力して、Web 認証に対して SSLv2 を無効化できます。このコマンドを使用すると、ユーザは、SSLv3 以降のリリースなどのよりセキュアなプロトコルを使用するように設定したブラウザを使用しなければなりません。デフォルト値は [disabled] です。

（注） Cisco TAC はカスタム Web 認証バンドルを作成する責任を負いません。

複雑なカスタムの Web 認証モジュールが存在する場合は、コントローラ上の外部 Web 認証設定を使用して、完全なログイン ページが外部 Web サーバでホストされるようにすることを推奨します。

デフォルトの Web 認証ログイン ページの選択（GUI）

手順

ステップ 1 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login Page] を開きます。

ステップ 2 [Web Authentication Type] ドロップダウン リストから [Internal (Default)] を選択します。

ステップ 3 デフォルトの Web 認証ログイン ページをそのまま使用する場合、ステップ 8 に進みます。デフォルトのログイン ページを変更する場合は、ステップ 4 に進みます。

ステップ 4 デフォルト ページの右上に表示されている Cisco ロゴを非表示にするには、[Cisco Logo] の [Hide] オプションを選択します。表示する場合は、**[Show]** オプションをクリックします。

ステップ 5 ログイン後にユーザを特定の URL（会社の URL など）にダイレクトさせる場合、[Redirect URL After Login] テキスト ボックスに必要な URL を入力します。最大 254 文字を入力することができます。

ステップ 6 ログイン ページで独自のヘッドラインを作成する場合、[Headline] テキスト ボックスに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。

ステップ 7 ログイン ページで独自のメッセージを作成する場合、[Message] テキスト ボックスに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。

ステップ 8 [Apply] をクリックして、変更を確定します。

ステップ 9 [Preview] をクリックして、Web 認証ログイン ページを表示します。

ステップ 10 ログイン ページの内容と外観に満足したら、[Save Configuration] をクリックして変更を保存します。納得いかない場合は、納得する結果を得られるように必要に応じて上記手順を繰り返します。

デフォルトの Web 認証ログイン ページの選択（CLI）

手順

ステップ 1 次のコマンドを入力して、デフォルトの Web 認証タイプを指定します。

config custom-web webauth_type internal

ステップ 2 デフォルトの Web 認証ログイン ページをそのまま使用する場合、ステップ 7 に進みますデフォルトのログイン ページを変更する場合は、ステップ 3 に進みます。

ステップ 3 デフォルトのログイン ページの右上に表示されている Cisco ロゴの表示/非表示を切り替えるには、次のコマンドを入力します。

config custom-web weblogo {**enable** | **disable**}

ステップ 4 ユーザをログイン後に特定の URL（会社の URL など）に転送させる場合、次のコマンドを入力します。

config custom-web redirecturl *url*

URL には最大 130 文字を入力することができます。リダイレクト先をデフォルトの設定に戻すには、**clear redirecturl** コマンドを入力します。

ステップ 5 ログイン ページで独自のヘッドラインを作成する場合、次のコマンドを入力します。

config custom-web webtitle *title*

最大 130 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。ヘッドラインをデフォルトの設定にリセットするには、**clear webtitle** コマンドを入力します。

ステップ 6 ログイン ページで独自のメッセージを作成する場合、次のコマンドを入力します。

config custom-web webmessage *message*

最大 130 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。メッセージをデフォルトの設定にリセットするには、**clear webmessage** コマンドを入力します。

ステップ 7 [web authentication logout] ポップアップ ウィンドウを有効または無効にするには、次のコマンドを入力します。

config custom-web logout-popup {**enable** | **disable**}

ステップ 8 **save config** コマンドを入力して、設定を保存します。

ステップ 9 次の手順で独自のロゴを Web 認証ログイン ページにインポートします。

1. Trivial File Transfer Protocol（TFTP）サーバがダウンロードのために使用可能であることを確認します。TFTP サーバをセットアップするときには、次のガイドラインに従ってください。
   - サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
   - ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
   - サードパーティの TFTP サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。
2. 次のコマンドを入力して、コントローラが TFTP サーバと通信可能であることを確認します。

   ping ip-address
3. TFTP サーバのデフォルト ディレクトリにロゴ ファイル（.jpg、.gif、または .png 形式）を移動します。ファイル サイズは 30 キロビット以内です。うまく収まるようにするには、ロゴは、横 180 ピクセル X 縦 360 ピクセル前後の大きさにします。
4. 次のコマンドを入力して、ダウンロード モードを指定します。

   transfer download mode tftp
5. 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

   transfer download datatype image
6. 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。

   transfer download serverip *tftp-server-ip-address*

   （注） TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

7. 次のコマンドを入力して、ダウンロード パスを指定します。

   transfer download path *absolute-tftp-server-path-to-file*

8. 次のコマンドを入力して、ダウンロードするファイルを指定します。

   transfer download filename {*filename.jpg* | *filename.gif* | *filename.png*}

9. 次のコマンドを入力して、更新した設定を表示し、プロンプトに *y* と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

   transfer download start

10. 次のコマンドを入力して、設定を保存します。

    save config

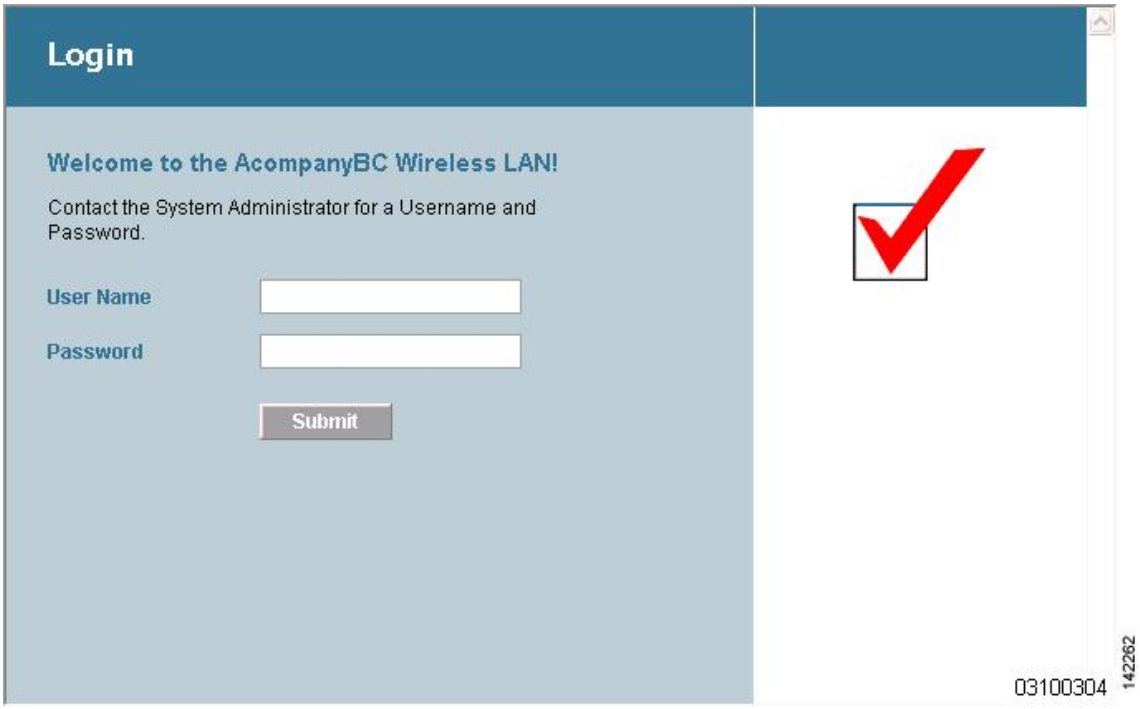
    （注） Web 認証ログイン ページからこのロゴを削除する場合は、**clear webimage** コマンドを入力します。

ステップ 10 「Web 認証ログイン ページの設定の確認（CLI） （81 ページ）」の項の指示に従って、設定を確認します。

例：変更されたデフォルトの Web 認証ログイン ページの例

図 *4*：変更されたデフォルトの *Web* 認証ログイン ページの例

次の図に、変更されたデフォルトの Web 認証ログイン ページの例を示します。



このログイン ページは、次の CLI コマンドを使用して作成されました。

- **config custom-web weblogo** *disable*
- **config custom-web webtitle** *AcompanyBC* ワイヤレス *LAN* の概要
- **config custom-web webmessage** ユーザ名とパスワードについては、システム管理者にお問い合わせください。
- **transfer download** *start*
- **config custom-web redirecturl** *url*

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの使用

カスタマイズされた Web 認証ログイン ページについて

Web 認証ログイン ページをカスタマイズして、外部 Web サーバにリダイレクトすることができます。この機能を有効にすると、ユーザは、外部 Web サーバ上のカスタマイズされたログイン ページへダイレクトされます。

外部 Web サーバに対して、WLAN 上で事前認証アクセス コントロール リスト（ACL）を設定し、[WLANs] > [Edit] ページの [Layer 3 Security] > [Web Policy] で、WLAN 事前認証 ACL としてこの ACL を選択する必要があります。

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択（GUI）

手順

ステップ 1 **[Security]** > **[Web Auth]** > **[Web Login Page]** の順に選択して、[Web Login] ページを開きます。

ステップ 2 [Web Authentication Type] ドロップダウン リストから [External (Redirect to external server)] を選択します。

ステップ 3 [Redirect URL after login] テキスト ボックスに、ログイン後にユーザをリダイレクトさせる URL を入力します。

たとえば、会社の URL を入力すると、ユーザがログインした後にその URL へ転送されます。254 文字以内で指定します。デフォルトで、ユーザは、ログイン ページが表示される前にユーザのブラウザに入力された URL にリダイレクトされます。最大 252 文字を入力することができます。

ステップ 4 [External Webauth URL] テキスト ボックスに、外部 Web 認証に使用する URL を入力します。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択（CLI）

手順

ステップ 1 次のコマンドを入力して、Web 認証タイプを指定します。

config custom-web webauth_type external

ステップ 2 次のコマンドを入力して、Web サーバ上でカスタマイズされた Web 認証ログイン ページの URL を指定します。

config custom-web ext-webauth-url *url*

URL には最大 252 文字を入力することができます。

ステップ 3 次のコマンドを入力して、Web サーバの IP アドレスを指定します。

config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

ステップ 4 **save config** コマンドを入力して、設定を保存します。

ステップ 5 「Web 認証ログイン ページの設定の確認（CLI）（81 ページ）」の項の指示に従って、設定を確認します。

例：カスタマイズされた Web 認証ログイン ページの作成

この項では、カスタマイズされた Web 認証ログイン ページの作成について説明します。作成後は、外部 Web サーバからアクセスできるようになります。

Web 認証ログイン ページのテンプレートを次に示します。カスタマイズされたページを作成する際に、モデルとして使用できます。

（注） カスタマイズされた Web 認証ログイン ページを作成する場合は、シスコのガイドラインに従うことをお勧めします。Google Chrome または Mozilla Firefox ブラウザの最新バージョンにアップグレードした場合は、Web 認証バンドルの *login.html* ファイルに次の行が含まれていることを確認します。

```
<body onload="loadAction();">
```

この問題の詳細については、 CSCvj17640 を参照してください。

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<title>Web Authentication</title>
<script>

function submitAction(){
 var link = document.location.href;
 var searchString = "redirect=";
```

```
 var equalIndex = link.indexOf(searchString);
 var redirectUrl = "";

 if (document.forms[0].action == "") {
  var url = window.location.href;
  var args = new Object();
  var query = location.search.substring(1);
  var pairs = query.split("&");
  for(var i=0;i<pairs.length;i++){
  var pos = pairs[i].indexOf('=');
   if(pos == -1) continue;
    var argname = pairs[i].substring(0,pos);
    var value = pairs[i].substring(pos+1);
    args[argname] = unescape(value);
  }
   document.forms[0].action = args.switch_url;
  }

      if(equalIndex >= 0) {
  equalIndex += searchString.length;
  redirectUrl = "";
  redirectUrl += link.substring(equalIndex);
  }
  if(redirectUrl.length > 255)
  redirectUrl = redirectUrl.substring(0,255);
  document.forms[0].redirect_url.value = redirectUrl;
  document.forms[0].buttonClicked.value = 4;
        document.forms[0].submit();
}

 function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
//alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");

      }
      else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username
 is already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
```

```
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25" MAXLENGTH="63"
 VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password" name="password" SIZE="25"
MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

ユーザのインターネット ブラウザがカスタマイズされたログイン ページにリダイレクトされるときに、次のパラメータが URL に追加されます。

- **ap_mac**：無線ユーザがアソシエートされているアクセス ポイントの MAC アドレス。
- **switch_url**：ユーザ クレデンシャルをポストするコントローラの URL。
- **redirect**：認証に成功した後、ユーザがリダイレクトされる URL。
- **statusCode**：コントローラの Web 認証サーバから返されるステータス コード。
- **wlan**：無線ユーザがアソシエートされている WLAN SSID。

使用できるステータス コードは、次のとおりです。

- ステータス コード 1：「You are already logged in. No further action is required on your part.」
- ステータス コード 2：「You are not configured to authenticate against web portal. No further action is required on your part.」
- ステータス コード 3：「The username specified cannot be used at this time. Perhaps the username is already logged into the system?」
- ステータス コード 4：「You have been excluded.」
- ステータス コード 5：「The User Name and Password combination you have entered is invalid. Please try again.」

（注） 詳細については、http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html [英語] にある『*External Web Authentication with Wireless LAN Controllers Configuration Example*』を参照してください。

カスタマイズされた Web 認証ログイン ページのダウンロード

Web 認証ログイン ページに使用するページやイメージ ファイルを .tar ファイルに圧縮してコントローラへダウンロードできます。これらのファイルは、webauth bundle と呼ばれています。ファイルの最大許容サイズは、非圧縮の状態で 1 MB です。.tar ファイルがローカル TFTP サーバからダウンロードされる際、コントローラのファイル システムに、展開済みファイルとして取り込まれます。

ログイン ページ例を Cisco Prime Infrastructure からダウンロードし、カスタマイズされたログイン ページの開始点として利用できます。詳細については、Cisco Prime Infrastructure のドキュメントを参照してください。

（注） webauth bundle を GNU に準拠していない .tar 圧縮アプリケーションでロードすると、コントローラでこのバンドル内のファイルを解凍できないため、「Extracting error」および「TFTP transfer failed」というエラー メッセージが表示されます。そのため、webauth bundle の .tar ファイルを圧縮する場合は、GNU 標準に準拠したアプリケーション（PicoZip など）を使用することをお勧めします。

（注） 設定のバックアップには、webauth bundle や外部ライセンスなど、ダウンロードしてコントローラに格納した付加的なファイルやコンポーネントは含まれないため、このようなファイルやコンポーネントの外部バックアップ コピーは手動で保存する必要があります。

（注） カスタマイズされた webauth bundle に異なる要素が 4 つ以上含まれる場合は、コントローラ上の TCP レート制限ポリシーが原因で発生するページの読み込み上の問題を防ぐために、外部サーバを使用してください。

カスタマイズされた Web 認証ログイン ページのダウンロードの前提条件

- ログイン ページの名前を `login.html` とします。コントローラは、この名前に基づいて Web 認証 URL を作成します。webauth bundle の展開後にこのファイルが見つからない場合、bundle は破棄され、エラー メッセージが表示されます。
- ユーザ名とパスワードの両方に入力テキスト ボックスを提供する。
- リダイレクト先の URL を元の URL から抽出後、非表示入力アイテムとして保持する。
- 元の URL からアクション URL を抽出して、ページに設定する。
- リターン ステータス コードをデコードするスクリプトを提供する。
- メインページで使用されているすべてのパス（たとえば、イメージを参照するパス）を確認する。
- バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

カスタマイズされた Web 認証ログイン ページのダウンロード（GUI）

手順

ステップ 1 ログイン ページが含まれる .tar ファイルをサーバのデフォルトディレクトリに移動します。

ステップ 2 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 3 [File Type] ドロップダウン リストから、[Webauth Bundle] を選択します。

ステップ 4 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- **TFTP**
- **FTP**
- **SFTP**（7.4 以降のリリースで利用可能）

ステップ 5 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。

ステップ 6 TFTP サーバを使用している場合は、コントローラによる .tar ファイルのダウンロードの最大試行回数を [Maximum Retries] テキスト ボックスに入力します。

指定できる範囲は 1 ～ 254 です。

デフォルトは 10 です。

ステップ 7 TFTP サーバを使用している場合は、コントローラによる *.tar ファイルのダウンロード試行がタイムアウトするまでの時間（秒数）を [Timeout] テキスト ボックスに入力します。

指定できる範囲は 1 ～ 254 秒です。

デフォルトは 6 秒です。

ステップ 8 [File Path] テキスト ボックスに、ダウンロードする .tar ファイルのパスを入力します。デフォルト値は「/」です。

ステップ 9 [File Name] テキスト ボックスに、ダウンロードする .tar ファイルの名前を入力します。

ステップ 10 FTP サーバを使用している場合は、次の手順に従います。

1. [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
2. [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
3. [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 11 [Download] をクリックして、.tar ファイルをコントローラへダウンロードします。

ステップ 12 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。

ステップ 13 [Web Authentication Type] ドロップダウン リストから [Customized (Downloaded)] を選択します。

ステップ 14 [Apply] をクリックします。

ステップ 15 [Preview] をクリックして、カスタマイズされた Web 認証ログイン ページを表示します。

ステップ 16 ログイン ページの内容と外観に満足したら、[Save Configuration] をクリックします。

カスタマイズされた Web 認証ログイン ページのダウンロード（CLI）

手順

ステップ 1 ログイン ページが含まれる .tar ファイルをサーバのデフォルトディレクトリに移動します。

ステップ 2 次のコマンドを入力して、ダウンロード モードを指定します。

transfer download mode {**tftp** | **ftp** | **sftp**}

ステップ 3 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer download datatype webauthbundle

ステップ 4 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。

transfer download serverip *tftp-server-ip-address.*

（注） TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

ステップ 5 次のコマンドを入力して、ダウンロード パスを指定します。

transfer download path *absolute-tftp-server-path-to-file*

ステップ 6 次のコマンドを入力して、ダウンロードするファイルを指定します。

transfer download filename *filename.tar*

ステップ 7 次のコマンドを入力して、更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

transfer download start

ステップ 8 次のコマンドを入力して、Web 認証タイプを指定します。

config custom-web webauth_type *customized*

ステップ 9 **save config** コマンドを入力して、設定を保存します。

例：カスタマイズされた Web 認証ログイン ページ

図 5：カスタマイズされた *Web* 認証ログイン ページの例

次の図に、カスタマイズされた Web 認証ログイン ページの例を示します。

Web 認証ログイン ページの設定の確認（CLI）

次のコマンドを入力して、Web 認証ログイン ページに対する変更内容を確認します。

show custom-web

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当てについて

ユーザに対して、WLAN ごとに異なる Web 認証ログイン ページ、ログイン失敗ページ、ログアウト ページを表示できます。この機能を使用すると、ゲスト ユーザや組織内のさまざまな

部署の従業員など、さまざまなネットワーク ユーザに対し、ユーザ固有の Web 認証ページを表示できます。

すべての Web 認証タイプ（[Internal]、[External]、[Customized]）で異なるログイン ページを使用できます。ただし、Web 認証タイプで [Customized] を選んだ場合に限り、異なるログイン失敗ページとログアウト ページを指定できます。

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Web ログイン ページ、ログイン失敗ページ、またはログアウト ページを割り当てる WLAN の ID 番号をクリックします。

ステップ 3 [Security] > [Layer 3] の順に選択します。

ステップ 4 [Web Policy] と [Authentication] が選択されていることを確認します。

ステップ 5 グローバル認証設定 Web 認証ページを無効にするには、[Override Global Config] チェックボックスをオンにします。

ステップ 6 [Web Auth Type] ドロップダウン リストが表示されたら、次のオプションのいずれかを選択して、無線ゲスト ユーザ用の Web 認証ページを定義します。

- [Internal]：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- [Customized]：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン リストが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。

  （注） これらのオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- [External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

  [WLANs > Edit]（[Security] > [AAA Servers]）ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 7 ステップ 6 で Web 認証タイプとして [External] を選択した場合は、[AAA Servers] を選択して、ドロップダウン リストから最大 3 つの RADIUS サーバおよび LDAP サーバを選択します。

（注） RADIUS および LDAP の外部サーバは、[WLANs > Edit]（[Security] > [AAA Servers]）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 8 次の手順で、Web 認証で接続するサーバの優先順位を指定します。

（注） デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

1. [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類（[Local]、[Radius]、[LDAP]）を強調表示します。
2. 希望のサーバ タイプがボックスの先頭になるまで、[Up] および [Down] をクリックします。
3. [<] 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。
4. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て（CLI）

手順

ステップ 1 次のコマンドを入力して、Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる WLAN の ID 番号を決定します。

show wlan summary

ステップ 2 カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに無線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して Web 認証ページのファイル名および表示する WLAN を指定します。

- **config wlan custom-web login-page** *page_name wlan_id*：特定の WLAN のカスタマイズされたログイン ページを定義します。
- **config wlan custom-web loginfailure-page** *page_name wlan_id*：特定の *WLAN* のカスタマイズされたログイン失敗ページを定義します。

  （注） コントローラのデフォルト ログイン失敗ページを使用するには、**config wlan custom-web loginfailure-page none** *wlan_id* コマンドを入力します。

- **config wlan custom-web logout-page** *page_name wlan_id*：特定の WLAN のカスタマイズされたログアウト ページを定義します。

（注） コントローラのデフォルト ログアウト ページを使用するには、**config wlan custom-web logout-page none** *wlan_id* コマンドを入力します。

ステップ 3 次のコマンドを入力して外部サーバの URL を指定することにより、Web ログイン ページにアクセスする前に無線ゲスト ユーザを外部サーバにリダイレクトします。

config wlan custom-web ext-webauth-url*ext_web_url wlan_id*

ステップ 4 次のコマンドを入力して、Web 認証サーバの接続順序を定義します。

config wlan security web-auth server-precedence*wlan_id*{**local** |**ldap** |**radius**} {**local** |**ldap** |**radius**} {**local** |**ldap** |**radius**}

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

（注） すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらを設定できます。

ステップ 5 次のコマンドを入力して、無線ゲスト ユーザ用の Web 認証ページを定義します。

config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

値は次のとおりです。

- **internal** コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** は、ステップ *2* で設定したカスタム Web ログイン ページを表示します。

  （注） ログイン失敗ページとログアウトページは常にカスタマイズされているため、ステップ *5* で Web 認証タイプを定義する必要はありません。

- **external** は、ステップ *3.* で設定した URL にユーザをリダイレクトします。

ステップ 6 次のコマンドを入力して、グローバル カスタム Web 設定ではなく、WLAN 固有のカスタム Web 設定を使用します。

config wlan custom-web global disable *wlan_id*

（注） **config wlan custom-web global enable** *wlan_id* コマンドを入力すると、カスタム Web 認証の設定がグローバル レベルで使用されます。

ステップ 7 次のコマンドを入力して、変更を保存します。

save config

Web 認証プロキシ

Web 認証プロキシについて

この機能を使用すると、ブラウザで手動 Web プロキシが有効になっているクライアントに対し、コントローラによる認証を強化することができます。ユーザのブラウザで、ポート番号 8080 または 3128 を使用して手動プロキシが設定されている場合、クライアントが URL を要求すると、コントローラは応答の Web ページで、プロキシ設定が自動的に検出されるようにインターネットのプロキシ設定を変更するようユーザに要求します。これにより、ブラウザの手動プロキシ設定情報が失われることはなくなります。ユーザはこの設定を有効にしたあと、Web 認証ポリシーを通じてネットワークにアクセスできます。この機能がポート 8080 および 3128 に提供されるのは、それらのポートが Web プロキシ サーバで最も一般的に使用されているからです。

（注） Web 認証プロキシのリダイレクト ポートは CPU ACL でブロックされません。Web 認証プロキシ設定の中で、ポート 8080、3128、および 1 つのランダムなポートをブロックするように CPU ACL が設定されていても、これらのポートはブロックされません。これは、クライアントが webauth_req 状態でない限り、Web 認証ルールは CPU ACL ルールよりも優先されるからです。

Web ブラウザに設定できる 3 種類のインターネット設定を次に示します。

- 自動検出
- システム プロキシ
- 手動

手動プロキシ サーバ設定では、ブラウザはプロキシ サーバの IP アドレスとポートを使用します。この設定がブラウザで有効になっている場合、ワイヤレス クライアントは、設定されたポート上の宛先プロキシ サーバの IP アドレスと通信します。Web 認証シナリオでは、コントローラはこのようなプロキシポートをリッスンしないので、クライアントはコントローラとの TCP 接続を確立できません。ユーザは、認証用のログイン ページを表示できず、ネットワークにアクセスすることはできません。

ワイヤレス クライアントは、Web 認証された WLAN に入ると、URL にアクセスしようとします。クライアントのブラウザに手動プロキシが設定されている場合、クライアントから発信されるすべての Web トラフィックは、ブラウザに設定されたプロキシ IP およびポートに送信されます。

- TCP 接続は、クライアントと、コントローラがプロキシとして動作しているプロキシサーバの IP アドレスの間で確立されます。
- クライアントは DHCP 応答を処理し、コントローラから JavaScript ファイルを取得します。このスクリプトによって、そのセッションに関するクライアントのプロキシ設定はすべて無効になります。

（注） 外部クライアントに対しては、コントローラはログインページを現状のまま（JavaScipt なしで）送信します。

- プロキシ設定をバイパスする要求。そのあと、コントローラは Web リダイレクション、ログイン、認証を実行できます。
- クライアントがネットワークから出て独自のネットワークに戻った場合は、DHCP が更新され、クライアントはブラウザに設定された以前のプロキシ設定を引き続き使用します。
- 外部 DHCP サーバで Web 認証プロキシを使用する場合、該当するスコープの DHCP サーバで DHCP オプション 252 を設定する必要があります。オプション 252 の値の形式は http://<virtual ip>/proxy.js です。内部の DHCP サーバでは、追加設定は必要ありません。

（注） FIPS モードでセキュアな Web 認証を設定する場合は、ブラウザに Mozilla Firefox を使用することをお勧めします。

- HTTPS への Web 認証リダイレトが有効になっている場合は、クライアントの HTTPS 要求と HTTP 要求の両方が HTTPS Web 認証にリダイレクトされます。

（注） この拡張機能は、リリース 8.0 で導入されました。

Web 認証プロキシの設定（GUI）

手順

ステップ 1 [Controller] > [General] の順に選択します。

ステップ 2 [WebAuth Proxy Redirection Mode] ドロップダウン リストから、[Enabled] または [Disabled] を選択します。

ステップ 3 [WebAuth Proxy Redirection Port] テキスト ボックスに、Web 認証プロキシのポート番号を入力します。

このテキスト ボックスでは、コントローラが Web 認証プロキシ リダイレクションを実行するためにリッスンするポート番号を指定します。デフォルトでは、80、8080、および 3128 の 3 つのポートが想定されています。これら以外の値に Web 認証リダイレクション ポートを設定した場合は、その値を指定してください。

ステップ 4 [Apply] をクリックします。

Web 認証プロキシの設定（CLI）

手順

- 次のコマンドを入力して、Web 認証プロキシ リダイレクションを有効にします。
  config network web-auth proxy-redirect {**enable** | **disable**}
- 次のコマンドを入力して、クライアントに対してセキュア Web（HTTPS）認証を設定します。
  config network web-auth secureweb {**enable** | **disable**}
  デフォルトでは、クライアントのセキュア Web（HTTPS）認証は有効になっています。

（注） **config network web-auth secureweb disable** コマンドを使用してクライアントのセキュア Web（HTTPS）認証を禁止するように設定した場合、Cisco WLC をリブートして変更を適用する必要があります。

- 次のコマンドを入力して、Web 認証ポート番号を設定します。
  config network web-auth port *port-number*
  このパラメータでは、コントローラが Web 認証プロキシ リダイレクションを実行するためにリッスンするポート番号を指定します。デフォルトでは、80、8080、および 3128 の 3 つのポートが想定されています。これら以外の値に Web 認証リダイレクション ポートを設定した場合は、その値を指定してください。
- 次のコマンドを入力して、Web 認証クライアントのための安全なリダイレクション（HTTPS）を設定します。
  config network web-auth https-redirect {**enable** | **disable**}
- 次のいずれかのコマンドを入力して、Web認証プロキシ設定の現在のステータスを表示します。
  - **show network summary**
  - **show running-config**

キャプティブ ポータル バイパス

キャプティブ バイパスについて

WISPr は、ユーザが異なるワイヤレス サービス プロバイダー間をローミングできるようにするドラフト プロトコルです。一部のデバイス（Apple iOS デバイスなど）には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これにより、ユーザがインターネットにアクセスするために、自身の認証情報を提供することが可

能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアント デバイス（Apple IOS デバイス）は、WISPr 要求をコントローラに送信します。コントローラはユーザ エージェントの詳細をチェックし、コントローラでの Web 認証代行受信により HTTP 要求をトリガーします。ユーザエージェントによって提供される IOS バージョンおよびブラウザの詳細の確認後に、コントローラによってクライアントはキャプティブ ポータル設定のバイパスを許可され、インターネットにアクセスできます。

（注） IOS7 用キャプティブ ポータル バイパスは、Cisco ワイヤレス LAN コントローラ リリース 7.6 でのみサポートされています。

このHTTP要求は、他のページ要求がワイヤレスクライアントによって実行されると、コントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web認証がいずれかのコントローラ スプラッシュ ページ機能で使用されていると（設定された RADIUS サーバが URL を指定）、WISPr 要求が非常に短い間隔で発信されるので、スプラッシュ ページが表示されることはなく、いずれかのクエリーが指定のサーバに到達できるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュ ページ表示プロセスが中断されます。そして、デバイスによってページ要求が処理され、スプラッシュ ページ機能は中断されます。

たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple IOS バージョン 6 以前の場合はhttp://www.apple.com/library/test/success.html、および Apple IOS バージョン 7 以降の場合は複数の該当するターゲット URL に送られます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされたと見なされ、Apple の Captive Network Assistant（CNA）が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。コントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr 検出プロセスをバイパスするようにコントローラを設定できるようになりました。それによって、ユーザが、ユーザ コンテキストでスプラッシュ ページ ロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

キャプティブ バイパスの設定（CLI）

キャプティブ バイパスを設定するには、次のコマンドを使用します。

- **config network web-auth captive-bypass {enable | disable}**：ネットワーク レベルでのキャプティブ ポータルのバイパスに対するコントローラのサポートを有効または無効にします。
- **show network summary**：WISPr プロトコル検出機能のステータスを表示します。

WLAN ごとの Captive Network Assistant のバイパス設定（GUI）

手順

ステップ 1 WLC の Web UI にログインします。

ステップ 2 WLAN では、次の 2 つのオプションのいずれかを選択します。

a) ドロップダウン リストから [Create New] を選択して新しい WLAN を作成し、[Go] をクリックします。

[WLANs] > **[New]** ページが表示されます。

b) Captive Network Assistant バイパス機能を設定する WLAN の ID 番号をクリックします。

[WLANs] > **[Edit]** ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Layer 3 Security] ドロップダウン リストから次のいずれかを選択します。

- [None]：グローバルな Captive Network Assistant バイパスの設定が適用されます。
- [Enable]：この特定の WLAN に対する Captive Network Assistant バイパスが有効になります。
- [Disable]：この特定の WLAN に対する Captive Network Assistant バイパスが無効になります。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

WLAN ごとの Captive Network Assistant バイパスの設定（CLI）

手順

有効、無効、または次のコマンドを入力して、グローバル キャプティブ ネットワークアシスタント バイパス WLAN あたりを有効化します。

config wlan security web-auth captive-bypass {**none | enable | disable**} *wlan-id*

Web 認証への MAC 認証フォールバック

MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーについて

レイヤ 2 およびレイヤ 3 セキュリティを組み合わせたフォールバック ポリシー メカニズムを設定できます。MAC フィルタリングおよび Web 認証の両方が設定されているシナリオで、MAC フィルタ（RADIUS サーバ）を使用して WLAN への接続を試行する場合、クライアントが認証に失敗すると、Web 認証にフォール バックできるように認証を設定できます。クライアントが MAC フィルタ認証をパスすると、Web 認証が省略され、クライアントは WLAN に接続されます。この機能を使用して、MAC フィルタ認証エラーのみに基づいたアソシエーション解除を回避できます。

制約事項

- モビリティは、MAC フィルタの失敗時に Webauth に設定されるセキュリティ タイプの SSID ではサポートされません。
- MAC フィルタリングはパススルー Web 認証をサポートしていません。Web 認証用のユーザ名とパスワードのみサポートしています。

モビリティは、MAC フィルタの失敗時に Webauth に設定されるセキュリティ タイプの SSID ではサポートされません。

MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定（GUI）

（注） フォールバック ポリシーを設定する前に、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 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Web 認証に対してフォールバック ポリシーを設定する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 4 [Layer 3 Security] ドロップダウン リストから、[None] を選択します。

ステップ 5 [Web Policy] チェックボックスをオンにします。

（注） コントローラは、認証前にワイヤレス クライアントで送受信される DNS トラフィックを転送します。

次のオプションが表示されます。

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

ステップ 6 [On MAC Filter Failure] をクリックします。

ステップ 7 [Apply] をクリックして、変更を確定します。

ステップ 8 [Save Configuration] をクリックして設定を保存します。

MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定（CLI）

（注） フォールバック ポリシーを設定する前に、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 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。

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

ステップ 2 Web 認証ステータスを表示するには、次のコマンドを入力します。

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
```

8021.x 認証を使用した Web リダイレクト

802.1X 認証を使用した Web リダイレクトについて

802.1X 認証が正常に完了した後に、ユーザを特定の Web ページにリダイレクトするように WLAN を設定できます。Web リダイレクトを設定して、ユーザにネットワークへの部分的または全面的なアクセス権を与えることができます。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。RADIUS サーバ上で、リダイレクト先のページとリダイレクトが発生する条件を指定できます。条件には、ユーザのパスワードの有効期限が近づいている場合、または使用を継続するためにユーザが料金を支払う必要がある場合などがあります。

RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。さらにサーバから Cisco AV ペア「url-redirect-acl」も返された場合は、指定されたアクセス コントロール リスト（ACL）が、そのクライアントの事前認証 ACL としてインストールされます。クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。

指定された URL（たとえば、パスワードの変更、請求書の支払い）でクライアントが特定の操作を完了すると、クライアントの再認証が必要になります。RADIUS サーバから「url-redirect」が返されない場合、クライアントは完全に認証されたものと見なされ、トラフィックを渡すことを許可されます。

（注） 条件付き Web リダイレクト機能は、802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上で条件付き Web リダイレクトを設定できます。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークに完全にアクセスできます。リダイレクト ページは RADIUS サーバで指定でき、対応する ACL が「url-redirect acl」でこのサーバにアクセスできるようにします。RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。クライアントは、この段階で完全に認証され、RADIUS サーバが「url-redirect」を返さなくても、トラフィックを渡すことができます。

（注） スプラッシュ ページ Web リダイレクト機能は、802.1x キー管理を使用する 802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。事前共有キー管理は、レイヤ 2 セキュリティ方式ではサポートされません。

ワイヤレス クライアントで実行するバック エンド アプリケーションがあり、通信に HTTP または HTTPS ポートを使用したとします。実際の Web ページが開く前にアプリケーションが通信を開始すると、リダイレクト機能が Web パススルーで機能しません。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上でスプラッシュ ページ Web リダイレクトを設定できます。

RADIUS サーバの設定（GUI）

（注） 次の手順は、CiscoSecure ACS 固有の手順ですが、その他の RADIUS サーバでも同様の手順を使用します。

手順

ステップ 1 CiscoSecure ACS メイン メニューから、[Group Setup] を選択します。

ステップ 2 [Edit Settings] をクリックします。

ステップ 3 [Jump To] ドロップダウン リストから [RADIUS (Cisco IOS/PIX 6.0)] を選択します。

ステップ 4 [[009\001] cisco-av-pair] チェックボックスをオンにします。

ステップ 5 [[009\001] cisco-av-pair] 編集ボックスに次の Cisco AV ペアを入力して、ユーザをリダイレクトする URL を指定するか、条件付 Web リダイレクトを設定する場合は、ダイレクトが発生する条件をそれぞれ指定します。

url-redirect=http://**url**

url-redirect-acl=**acl_name**

Web リダイレクトの設定

Web リダイレクトの設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 必要な WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit]（[Security] > [Layer 2]）ページを開きます。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[802.1X] または [WPA+WPA2] を選択します。

ステップ 5 802.1X または WPA+WPA2 に対して任意の追加パラメータを設定します。

ステップ 6 [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

ステップ 7 [Layer 3 Security] ドロップダウン リストから、[None] を選択します。

ステップ 8 [Web Policy] チェックボックスをオンにします。

ステップ 9 条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを有効化するオプションとして、[Conditional Web Redirect] または [Splash Page Web Redirect] のいずれかを選択します。デフォルトでは、両方のパラメータが無効になっています。

ステップ 10 ユーザをコントローラ外部のサイトにリダイレクトする場合、[Preauthentication ACL] ドロップダウン リストから RADIUS サーバ上で設定された ACL を選択します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

Web リダイレクトの設定（CLI）

手順

ステップ 1 条件付き Web リダイレクトを有効または無効にするには、次のコマンドを入力します。

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

ステップ 2 スプラッシュ ページ Web リダイレクトを有効または無効にするには、次のコマンドを入力します。

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

ステップ 3 次のコマンドを入力して、設定を保存します。

save config

ステップ 4 特定の WLAN の Web リダイレクト機能のステータスを表示するには、次のコマンドを入力します。

show wlan *wlan_id*

以下に類似した情報が表示されます。

```
WLAN Identifier................................ 1
Profile Name................................... test
Network Name (SSID)............................ test
...
Web Based Authentication....................... Disabled
Web-Passthrough................................ Disabled
Conditional Web Redirect....................... Disabled
Splash-Page Web Redirect....................... Enabled
```

. . .

WLAN ごとのアカウンティング サーバの無効化（GUI）

（注） アカウンティングサーバを無効にすると、すべてのアカウンティング動作が無効となり、コントローラが WLAN に対するデフォルトの RADIUS サーバにフォールバックしなくなります。

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 変更する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Security] タブおよび [AAA Servers] タブを選択して、[WLANs > Edit]（[Security] > [AAA Servers]）ページを開きます。

ステップ 4 [Accounting Servers] の [Enabled] チェックボックスをオフにします。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

WLAN ごとのカバレッジ ホールの検出の無効化

（注） カバレッジ ホールの検出は、コントローラでグローバルに有効になっています。

（注） WLAN ごとにカバレッジ ホールの検出を無効にできます。WLAN でカバレッジ ホールの検出を無効にした場合、カバレッジ ホールの警告はコントローラに送信されますが、カバレッジ ホールを解消するためのそれ以外の処理は行われません。この機能については、ゲストのネットワーク接続時間は短く、モビリティが高いと考えられるようなゲスト WLAN に有用です。

WLAN 上のカバレッジ ホールの検出の無効化（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 変更する WLAN のプロファイル名をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを表示します。

ステップ 4 [Coverage Hole Detection Enabled] チェックボックスをオフにします。

（注） OEAP 600 シリーズ アクセス ポイントでは、カバレッジ ホールの検出はサポートされません。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

WLAN 上のカバレッジ ホールの検出の無効化（CLI）

手順

ステップ 1 カバレッジ ホールの検出を無効にするには、次のコマンドを入力します。

config wlan chd *wlan-id* **disable**

（注） OEAP 600 シリーズ アクセス ポイントでは、カバレッジ ホールの検出はサポートされません。

ステップ 2 次のコマンドを入力して、設定を保存します。

save config

ステップ 3 特定の WLAN のカバレッジ ホールの検出ステータスを表示するには、次のコマンドを入力します。

show wlan *wlan-id*

以下に類似した情報が表示されます。

```
WLAN Identifier................................. 2
Profile Name.................................... wlan2
Network Name (SSID)............................. 2
. . .
CHD per WLAN................................. Disabled
```

中央 Web 認証

中央 Web 認証（CWA）の Web 認証は Cisco ISE サーバで行われます。Cisco ISE サーバの Web ポータルでは、クライアントにログイン ページが表示されます。Cisco ISE サーバで資格情報が検証されると、クライアントがプロビジョニングされます。認可変更（CoA）が適用されるまで、クライアントは POSTURE _REQD 状態です。資格情報と ACL が Cisco ISE サーバから送信されます。

（注） CWA と MAC のフィルタリング設定シナリオでは、事前認証や事後認証中に VLAN で変更が発生すると、関連付け解除要求がクライアントに送信され、クライアントは強制的にもう一度 DHCP を通過させられます。

NAC アウトオブバンド統合

NAC アウトオブバンド統合について

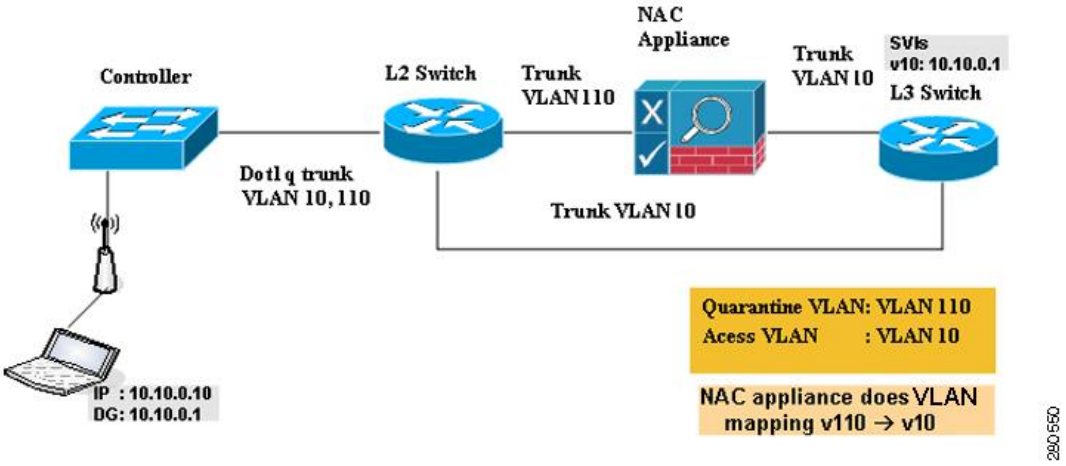
Cisco Clean Access（CCA）とも呼ばれる Cisco NAC アプライアンスはネットワーク アドミッション制御（NAC）製品です。この製品を使用して、ネットワーク管理者は、ユーザをネットワークに許可する前に、有線、無線、およびリモート ユーザおよびマシンを認証、許可、評価、修正できます。NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。

NAC アプライアンスは、インバンド モードとアウトオブバンド モードの 2 つのモードで利用できます。顧客は、必要に応じて特定の種類のアクセスを対象にし、2 つのモードを展開できます（例：無線ユーザをサポートする場合はインバンド、有線ユーザをサポートする場合はアウトオブバンド）。

コントローラ上に NAC アウトオブバンド機能を実装するには、WLAN またはゲスト LAN 上で NAC のサポートを有効にしてから、この WLAN またはゲスト LAN を、検疫 VLAN（信頼できない VLAN）およびアクセス VLAN（信頼できる VLAN）で設定されたインターフェイスにマッピングする必要があります。クライアントは、アソシエートしてレイヤ 2 認証を完了すると、アクセス VLAN サブネットから IP アドレスを取得しますが、クライアントの状態は Quarantine となります。NAC アウトオブバンド機能の導入中は、コントローラが接続されたレイヤ 2 スイッチと NAC アプライアンスとの間でのみ検疫 VLAN が許可されること、および NAC アプライアンスが一意の検疫 - アクセス VLAN マッピングで設定されていることを確認します。クライアントのトラフィックは、NAC アプライアンスにトランクされた検疫 VLAN に渡されます。ポスチャ検証が終了すると、クライアントは修復のための処置を実行するように促されます。クリーニングが完了すると、NAC アプライアンスはコントローラを更新してクライアントの状態を Quarantine から Access へ変更します。

図 *6 : NAC* アウト オブ バンド統合の例

コントローラとスイッチとの間のリンクをトランクとして設定することにより、隔離 VLAN（110）とアクセス VLAN（10）を有効にしています。レイヤ 2 スイッチ上では、検疫トラフィックが NAC アプライアンスにトランクされ、アクセス VLAN トラフィックがレイヤ 3 スイッチに直接送信されます。NAC アプライアンス上の検疫 VLAN に到達するトラフィックは、静的なマッピング設定に基づいてアクセス VLAN にマップされます。



NAC アウトオブバンドの前提条件

- NAC アウトオブバンド統合には、CCA のソフトウェア リリース 4.5 以降が必要です。
- NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ 上で設定されているインターフェイスごとに一意の隔離 VLAN を設定する必要があります。たとえば、コントローラ 1 で 110 という隔離 VLAN を設定し、コントローラ 2 で 120 という隔離 VLAN を設定します。ただし、2 つの WLAN またはゲスト LAN が、コントローラのダイナミック インターフェイスとして同一の VLAN を使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つのときは、同じ隔離 VLAN を使用する必要があります。NAC アプライアンスは、一意の検疫 - アクセス VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッション タイムアウトを設定し、WLAN でのセッションの失効が NAC アプライアンスでの失効より大きいことを確認します。
- オープン WLAN でセッション タイムアウトが設定されると、Quarantine 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラ から認証解除されるため、ポスチャ検証を再度実行する必要があります。
- レイヤ 2 およびレイヤ 3 認証はすべて、検疫 VLAN で実行されます。外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP トラフィックを許可するとともに、検疫 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。

（注） 設定手順については、http://www.cisco.com/c/en/us/support/security/nac-appliance-clean-access/products-installation-and-configuration-guides-list.html で『Cisco NAC appliance configuration guides』を参照してください。

- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。複数の NAC アプライアンスの導入を必要とする場合があります。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。複数の NAC アプライアンスの導入を必要とする場合があります。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンド モードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータ パス内になければなりません。インバンド モードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが NAC 適用ポイントを通過する必要があります。コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンド モードで NAC アプライアンスと統合できます。この場合、NAC アプライアンスは、クライアントが解析およびクリーニングされるまでデータ パスに保持されます。アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。

NAC アウトオブバンドの制限

- NAC アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンド モードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータ パス内になければなりません。インバンド モードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが NAC 適用ポイントを通過する必要があります。コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンド モードで NAC アプライアンスと統合できます。この場合、NAC アプライアンスは、クライアントが解析およびクリーニングされるまでデータ パスに保持されます。アウトオブバンド モードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。

- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカル スイッチングを行うように設定されている WLAN での使用はサポートされていません。

NAC アウトオブバンド統合の設定（GUI）

手順

ステップ 1 次の手順で、動的インターフェイスに対して検疫 VLAN を設定します。

a) [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

b) [New] をクリックして、新たに動的インターフェイスを作成します。

c) [Interface Name] テキスト ボックスに、「quarantine」など、このインターフェイスの名前を入力します。

d) [VLAN ID] テキスト ボックスに、アクセス VLAN ID としてゼロ以外の値（「10」など）を入力します。

e) [Apply] をクリックして、変更を確定します。[Interfaces > Edit] ページが表示されます。

f) [Quarantine] チェックボックスをオンにして、隔離 VLAN ID としてゼロ以外の値（「110」など）を入力します。

（注） ネットワーク全体で一意の検疫 VLAN を設定することを推奨します。同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセス インターフェイスが同じサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、同じ検疫 VLAN を保持する必要があります。同じモビリティ グループ内に複数のコントローラが設定されており、すべてのコントローラのアクセスインターフェイスが別々のサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、別々の検疫 VLAN を保持する必要があります。

g) このインターフェイスの残りのテキスト ボックス（IP アドレス、ネットマスク、デフォルト ゲートウェイなど）を設定します。

h) [Apply] をクリックして変更内容を保存します。

ステップ 2 次の手順で、WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定します。

a) [WLANs] を選択して、[WLANs] ページを開きます。

b) 必要な WLAN またはゲスト LAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。

c) [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

d) この WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定するには、[NAC State] チェックボックスをオンにします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ（デフォルト値）のままとします。

e) [Apply] をクリックして、変更を確定します。

ステップ 3 次の手順で、特定のアクセス ポイント グループに対して NAC アウトオブバンドのサポートを設定します。

a) [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
b) 目的のアクセス ポイント グループの名前をクリックします。
c) [WLANs] タブを選択して、[AP Groups > Edit]（[WLANs]）ページを開きます。
d) [Add New] をクリックして、このアクセス ポイント グループに WLAN を割り当てます。[Add New] のセクションがページ上部に表示されます。
e) [WLAN SSID] ドロップダウン リストから、この WLAN の SSID を選択します。
f) [Interface Name] ドロップダウン リストから、アクセス ポイント グループをマップするインターフェイスを選択します。NAC アウトオブバンドのサポートを有効にする場合は、検疫 VLAN を選択します。
g) このアクセス ポイント グループに対して NAC アウトオブバンドのサポートを有効にするには、[NAC State] チェックボックスをオンにします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ（デフォルト値）のままとします。
h) [Add] をクリックして、この WLAN をアクセス ポイント グループに追加します。この WLAN が、このアクセス ポイント グループに割り当てられている WLAN のリストに表示されます。

（注） この WLAN をアクセス ポイント グループから削除する場合は、カーソルをこの WLAN の青のドロップダウン矢印の上に置いて、[Remove] を選択します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ステップ 5 次の手順で、クライアントの現在の状態（Quarantine または Access）を表示します。

a) [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
b) 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。NAC 状態が、[Security Information] のセクションに表示されます。

（注） クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。

NAC アウトオブバンド統合の設定（CLI）

手順

ステップ 1 動的インターフェイスに対して検疫 VLAN を設定するには、次のコマンドを入力します。

config interface quarantine vlan *interface_name vlan_id*

（注） コントローラ上のインターフェイスごとに一意の検疫 VLAN を設定する必要があります。

インターフェイスで検疫 VLAN を無効にするには、VLAN ID に *0* を入力します。

ステップ 2 WLAN またはゲスト LAN に対して NAC アウトオブバンド サポートを有効または無効にするには、次のコマンドを入力します。

config {**wlan** | **guest-lan**} **nac** {**enable** | **disable**} {*wlan_id* | *guest_lan_id*}

ステップ 3 特定のアクセス ポイント グループに対して NAC アウトオブバンド サポートを有効または無効にするには、次のコマンドを入力します。

config wlan apgroup nac {**enable** | **disable**} *group_name wlan_id*

ステップ 4 次のコマンドを入力して、変更を保存します。

save config

ステップ 5 NAC 状態など、WLAN またはゲスト LAN の構成を表示するには、次のコマンドを入力します。

show { **wlan** *wlan_ id* | **guest-lan** *guest_lan_id*}

以下に類似した情報が表示されます。

```
WLAN Identifier................................. 1
Profile Name.................................... wlan
Network Name (SSID)............................. wlan
Status.......................................... Disabled
MAC Filtering................................... Disabled
Broadcast SSID.................................. Enabled
AAA Policy Override............................. Disabled
Network Admission Control

  NAC-State..................................... Enabled
  Quarantine VLAN............................ 110
...
```

ステップ 6 クライアントの現在の状態（Quarantine または Access）を表示するには、次のコマンドを入力します。

show client detailed *client_mac*

以下に類似した情報が表示されます。

```
Client’s NAC state................................ QUARANTINE
```

（注） クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。

ISE NAC

ISE NAC サポートについて

Cisco Identity Services Engine（ISE）は、次世代のコンテキストベース アクセス コントロール ソリューションで、Cisco Secure Access Control System（ACS）と Cisco Network Admission Control（NAC）の機能を 1 つの統合されたプラットフォームで提供します。

Cisco Wireless Release 7.0.116.0 では、Cisco ISE を導入しました。Cisco ISE は、展開したネットワークに高度なセキュリティを提供します。ISE は、コントローラ上で設定できる認証サーバです。ISE NAC 対応の WLAN 上の Cisco WLC にクライアントを関連付けると、コントローラは Cisco ISE サーバに要求を転送します。

（注） ISE NAC は、以前は RADIUS NAC と呼ばれていました。

Cisco ISE サーバはデータベースでユーザを検証し、認証が完了すると、URL と事前認証 ACL がクライアントに送信されます。このときクライアントは Posture Required 状態になり、ISE サーバから返された URL にリダイレクトされます。

（注） Cisco ISE サーバから返された URL にキーワード **cwa** が含まれている場合、クライアントは中央 Web 認証（CWA）状態になります。

クライアントの NAC エージェントによって、ポスチャ検証プロセスがトリガーされます。Cisco ISE サーバによるポスチャ検証が完了すると、クライアントは RUN 状態になります。

（注） リリース 7.2.110.0 では、ISE NAC サポートによる FlexConnect ローカル スイッチングが追加されました。これには、リリース 7.0 およびリリース 7.2.103.0 ではサポートしていません。7.2.110.0 以降のリリースからリリース 7.2.103.0 またはリリース 7.0 にダウングレードする場合、ISE NAC を機能させるために WLAN を再設定する必要があります。

デバイス登録

デバイス登録を行うと、RADIUS NAC を使用して WLAN の新しいデバイスの認証とプロビジョニングを行えるようになります。デバイスを WLAN に登録すると、そのデバイスは、設定されている ACL に基づいてネットワークを使用できます。

中央 Web 認証

中央 Web 認証（CWA）の Web 認証は Cisco ISE サーバで行われます。Cisco ISE サーバの Web ポータルでは、クライアントにログイン ページが表示されます。Cisco ISE サーバで資格情報が検証されると、クライアントがプロビジョニングされます。認可変更（CoA）が適用されるまで、クライアントは POSTURE _REQD 状態です。資格情報と ACL が Cisco ISE サーバから送信されます。

（注） CWA と MAC のフィルタリング設定シナリオでは、事前認証や事後認証中に VLAN で変更が発生すると、関連付け解除要求がクライアントに送信され、クライアントは強制的にもう一度 DHCP を通過させられます。

ローカル Web 認証

ローカル Web 認証は、RADIUS NAC でサポートされていません。

次の表に、一般的な ISE でのデバイス登録、CWA、および LWA の有効な組み合わせを示します。

表 *1 : ISE* ネットワーク認証フロー

WLAN の設定	CWA	LWA	デバイス登録
RADIUS NAC 対応	○	×	○
L2 なし	×	PSK、Static WEP、CKIP	×
L3 なし	該当なし	内部/外部	該当なし
MAC フィルタリング対応	○	×	○

ISE NAC サポートのガイドラインと制約事項

ガイドライン

- 認証またはアカウンティング RADIUS サーバに障害が発生した場合、認証またはアカウンティング サーバのリスト内の該当するサーバが起動しなくなります。これにより、クライアント認証およびアカウンティングが同じ IP 認証サーバおよびアカウンティング サーバで発生します。ただし、認証サーバおよびアカウンティング サーバを連携させる場合、RADIUS サーバの設定時にこれらのサーバを同じ順序で追加する必要があります。
- クライアントがある WLAN から別の WLAN へ移動し、アイドル タイムアウトが発生する前に元の WLAN に戻った場合、Cisco WLC はそのクライアントの監査セッション ID を保持しています。その結果、アイドル タイムアウト セッションの期限が切れる前にクライアントが Cisco WLC と関連付けられると、それらのクライアントはただちに RUN 状態に

なります。セッションがタイムアウトしてから、クライアントが Cisco WLC に再度割り当てられているかどうかが検証されます。

- WLAN が 2 つあり、WLAN 1 が Cisco WLC（WLC1）、WLAN 2 が別の Cisco WLC（WLC2）に設定されていて、両方で ISE NAC が有効になっている場合、クライアントは WLC1 に最初に接続し、ポスチャ検証後に RUN 状態になります。次にこのクライアントは、WLC2 に移動するとします。WLC1 内のこのクライアントに対する PMK の期限が切れる前に、クライアントが WLC1 に再接続した場合、このクライアントに対するポスチャ検証は省略されます。クライアントはポスチャ検証を省略してただちに RUN 状態になります。これは、Cisco WLC が Cisco ISE にすでに認識されているクライアントの古い監査セッション ID を保持しているためです。
- ワイヤレス ネットワークに ISE NAC を導入する場合は、プライマリおよびセカンダリ Cisco ISE サーバを設定しないでください。代わりに、2 つの Cisco ISE サーバ間にハイ アベイラビリティ（HA）を設定することをお勧めします。プライマリおよびセカンダリ ISE を設定すると、クライアントが RUN 状態に移行する前に、ポスチャ検証が必要になります。HA が設定されていると、クライアントはフォールバック Cisco ISE サーバで自動的に RUN 状態に移行します。
- アクティブなネットワーク内で AAA サーバ インデックスを入れ替えないでください。クライアントが切断され、RADIUS サーバへの再接続が必要になる可能性があります。それによって、ISE サーバ ログにログ メッセージが追加される場合があります。
- ISE NAC を使用するには、WLAN 上で AAA オーバーライドを有効にします。
- WLAN 上で WPA および WPA2 または dot1X を有効にする必要があります。これは、レイヤ 2 セキュリティの PSK の場合でも必要です。
- 低速なローミング中に、クライアントのポスチャ検証が行われます。
- AAA の url-redirect-acl および url-redirect 属性を AAA サーバが要求する場合、AAA Override 機能をコントローラで有効にする必要があります。

制約事項

- ISE NAC 対応の WLAN は、オープン認証と MAC フィルタリングのみサポートしています。
- ISE NAC WLAN では、MAC 認証要求は常に外部 RADIUS サーバに送信されます。MAC 認証は、ローカルデータベースと照合して検証されません。この機能は CSCvh85830 に対する修正によりリリース 8.5、8.7、8.8 以降のリリースに適用されます。
- 設定されたアカウンティング サーバが認証（Cisco ISE）サーバと異なっている場合、ISE NAC は機能しません。Cisco ISE 機能を使用する場合は、認証およびアカウンティング サーバと同じサーバを設定する必要があります。Cisco ISE を Cisco ACS 機能専用にする場合は、アカウンティング サーバを柔軟に設定できます。
- ISE NAC が設定されたコントローラ ソフトウェアは、サービス ポートでの CoA をサポートしません。

- ゲストのトンネリング モビリティは、ISE NAC 対応の WLAN でのみサポートされます。
- VLAN Select はサポートされません。
- ワークグループ ブリッジはサポートされません。
- AP Group over NAC は ISE NAC ではサポートされません。
- ISE NAC を有効にすると、RADIUS サーバの上書きインターフェイスはサポートされません。
- リモート LAN（RLAN）はサポートされません。
- コントローラが別のモビリティ ドメインに属している場合、監査セッション ID はモビリティ ドメイン間でサポートされません。

ISE NAC サポートの設定（GUI）

手順

ステップ 1 [WLANs] を選択します。

ステップ 2 [WLAN ID] をクリックします。

[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [NAC State] ドロップダウン リストで、次のオプションから選択します。

- **None**
- [SNMP NAC]：WLAN に SNMP NAC を使用します。
- **[ISE NAC]**：WLAN に ISE NAC を使用します。

（注） WLAN 上で ISE NAC を使用すると、AAA オーバーライドが自動的に有効になります。

ステップ 5 設定を保存します。

ISE NAC サポートの設定（CLI）

次のコマンドを入力します。

config wlan nac radius {**enable** | **disable**} *wlan_id*

WPA/WPA2-PSK WLAN での ISE NAC の有効化

WPA と WPA2-PSK WLAN における ISE NAC の有効化について

WLAN で、ISE NAC および WPA と WPA2-PSK の両方を有効にすることができます。

この拡張機能は、リリース 8.3 で導入しました。リリース 8.3 以前は、同じ WLAN 上でこれら両方の設定を有効にすることはできませんでした。

使用例としては、デバイス オンボーディングのための、Cisco WLC 上の PSK による Web リダイレクトがあります。たとえば、SSID と PSK を使用するオンボード デバイスが、中央 Web 認証（CWA）で Cisco ISE に MAC アドレスを送信し、登録されているかどうかを確認します。

ワークフロー

ISE NAC と合わせて PSK をサポートするには、AAA サーバとの通信リンクを支援するために MAC フィルタリングを有効にして、リダイレクト URL と事前認証 ACL を取得する必要があります。サポート対象の WLAN 設定は、WPA と WPA-2 PSK + MAC フィルタリング + ISE NAC です。

1. クライアントはレイヤ 2 認証方式（PSK と WLAN 作成時に作成したクレデンシャル）で WLAN に参加します。
2. Cisco WLC は MAC フィルタリングが有効になっているかどうかを AAA サーバで確認します。有効であれば、AAA サーバはリダイレクト URL と事前認証 ACL を提供します。クライアントは Web 認証（CWA）状態に移行します。
3. クライアントはリダイレクト URL にログインし、利用できるクレデンシャルで認証します。CoA が AAA サーバから Cisco WLC に送信されます。
4. CoA の一環として、Cisco WLC は UNSPECIFIED を理由に、30 秒の再接続タイマーを開始して、クライアントに DISSOC のトリガーをかけます。
5. 最終的な認証は、最終 VLAN や最終 ACL など最終的な承認結果が戻る MAC 認証です。
6. クライアントがレイヤ 2 認証により MK と GTK を生成して再び参加することを想定して、無線暗号化リンクの Cisco WLC は AAA サーバに対する ACCESS REQ と、Cisco WLC が VLAN の変更や AAA サーバのその他の拡張属性を指定した ACCESS RESP を送信します。この属性の適用により、クライアントはラン状態に移行します。

その他の参考資料

- 『Web Authentication on WLAN Controller—』http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc17
- 『Central Web Authentication on the WLC and ISE Configuration Example—』http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

WPA/WPA2-PSK WLAN での ISE NAC の有効化（GUI）

手順

ステップ 1 Cisco WLC の設定：

a) 認可変更（CoA）が有効な状態の Cisco WLC に Cisco ISE を RADIUS サーバとして追加します。

b) レイヤ 2 セキュリティ タイプを [WPA+WPA2] に設定し、MAC フィルタリングを有効な状態にし、認証キー管理を [PSK] に設定し、NAC 状態を [ISE NAC] に設定した WLAN を設定します。

1. [WLANs] を選択して、WLAN ID をクリックします。
2. [WLANs > Edit] ページで、**[Security]** > **[Layer 2]** タブをクリックします。
3. レイヤ 2 セキュリティを [WPA+WPA2] に設定します。
4. [MAC Filtering] を有効にします。
5. [Authentication Key Management] で、[PSK] を有効にし、PSK フォーマットを設定します。
6. [Advanced] タブで、[NAC State] を [ISE NAC] に設定します。

c) Cisco ISE サーバのみと通信するために事前認証 ACL を作成します。ACL を作成する方法については、（アクセス コントロール リストの設定の章に設定されるリンク）を参照してください。

（注）
- ISE トラフィックに加えて、DNS、DNS を許可するよう指定する DHCP、およびリダイレクト ACL の DHCP トラフィックなどその他の必要なトラフィックを許可します。
- AP が FlexConnect モードの場合、事前認証 ACL は該当しません。認証されていないクライアントにアクセスできるようにするために、FlexConnect ACL が使用できます。

ステップ 2 Cisco ISE の設定：

a) Cisco WLC が Cisco ISE にあることを確認します。

b) 認証プロファイルを追加します。

c) 認証プロファイルを追加します。

d) 事前認証ポリシーを追加します。

e) 認証ポリシーを追加します。

（注）
1. 最初のインスタンスでは、ユーザが SSID に関連付けられており、中央 Web 認証プロファイルが返されています（不明な MAC アドレス：したがって、リダイレクションするようユーザを設定する必要があります）。
2. 2 番目のインスタンスでは、この設定でデフォルト ルール（内部ユーザ）と一致するよう、ユーザが Web ポータルで認証されています（要件に合わせて設定可能です）。認証部分が中央 Web 認証プロファイルと再度一致しないことが重要です。そうしないと、リダイレクション ループになります。

Cisco ISE の手順については、http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html#anc6 を参照してください。

ローカル ネットワーク ユーザ

コントローラ上のローカル ネットワーク ユーザについて

コントローラ上のローカル ユーザ データベースに、ローカル ネットワーク ユーザを追加することができます。ローカル ユーザ データベースには、すべてのローカル ネットワーク ユーザの資格情報（ユーザ名とパスワード）が保存されます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。

（注） コントローラはクライアント情報をまず RADIUS 認証サーバに渡します。クライアント情報が RADIUS データベースのエントリに一致しない場合、RADIUS 認証サーバは認証失敗メッセージで応答します。RADIUS 認証サーバが応答しない場合は、ローカル ユーザ データベースにクエリーが送信されます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

コントローラに対するローカル ネットワーク ユーザの設定（GUI）

手順

ステップ 1 [Security] > [AAA] > [Local Net Users] の順に選択して、[Local Net Users] ページを開きます。

（注） 既存のユーザを削除するには、そのユーザの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

管理者がローカル ネットワーク ユーザのクレデンシャルを変更すると、そのユーザは WLAN から関連付けを解除されます。ここでは、クレデンシャルは、そのユーザのパスワードまたは WLAN プロファイルの変更を指します。

ステップ 2 次のいずれかの操作を行います。

- 既存のローカル ネットワーク ユーザを編集するには、そのユーザのユーザ名をクリックします。[Local Net Users] > [Edit] ページが表示されます。
- ローカル ネットワーク ユーザを追加するには、[New] をクリックします。[Local Net Users > New] ページが表示されます。

ステップ 3 新しいユーザを追加している場合は、[User Name] テキスト ボックスにローカル ユーザのユーザ名を入力します。最大 49 文字の英数字を入力できます。

（注） ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

ステップ 4 [Password] および [Confirm Password] テキスト ボックスに、ローカル ユーザのパスワードを入力します。最大 49 文字の英数字を入力できます。

ステップ 5 新しいユーザを追加している場合、そのユーザがローカルネットワークにアクセスできる時間を制限するには、[Guest User] チェックボックスをオンにします。デフォルト設定は選択されていません。

ステップ 6 新しいユーザを追加していて、[Guest User] チェックボックスをオンにした場合は、[Lifetime] テキスト ボックスに、ゲスト ユーザ アカウントをアクティブにしておく時間（秒単位）を入力します。有効な範囲は 60 ～ 2,592,000（30 日間）秒（両端の値を含む）で、デフォルトの設定は 86,400 秒です。

ステップ 7 新しいユーザを追加していて、[Guest User] チェックボックスをオンにした場合、そのゲスト ユーザに QoS ロールを割り当てるには、[Guest User Role] チェックボックスをオンにします。デフォルト設定は選択されていません。

（注） ゲスト ユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

ステップ 8 新しいユーザを追加していて、[Guest User Role] チェックボックスをオンにした場合は、そのゲスト ユーザに割り当てる QoS ロールを [Role] ドロップダウン リストから選択します。

ステップ 9 [WLAN Profile] ドロップダウン リストから、ローカル ユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である [Any WLAN] を選択すると、ユーザは設定済みのどの WLAN にもアクセスできるようになります。

（注） ネットワーク ユーザに関連付けられている WLAN を削除しようとすると、システムが、WLAN 自体を削除する前に WLAN に関連付けられたすべてのネットワーク ユーザを削除するように指示するプロンプトを表示します。

ステップ 10 [Description] テキスト ボックスに、ローカル ユーザを説明するタイトル（「ユーザ 1」など）を入力します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

コントローラに対するローカル ネットワーク ユーザの設定（CLI）

手順

- 次のコマンドを入力して、ローカル ネットワーク ユーザを設定します。
  - **config netuser add** *username password* **wlan** *wlan_id userType* **permanent description** *description*：コントローラ上のローカル ユーザ データベースに永久ユーザを追加します。
  - **config netuser add** *username password* {**wlan | guestlan**} {*wlan_id* | *guest_lan_id*} **userType guestlifetime** *seconds* **description** *description*：コントローラのローカル ユーザ データベースに WLAN または有線ゲスト LAN 上のゲスト ユーザを追加します。

（注） 永久ユーザまたはゲスト ユーザをコントローラからローカル ユーザ データベースに追加する代わりに、RADIUS サーバ上にユーザに対するエントリを作成して Web 認証が実行される WLAN に対して RADIUS 認証を有効にするよう選択できます。

- **config netuser delete** {**username** *username* | **wlan-id** *wlan-id*}
  - *username*：コントローラ上のローカル ユーザ データベースからユーザを削除します。

    （注） ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

  - *wlan-id*：WLAN ID に関連付けられたネットワーク ユーザをすべて削除します。

    （注） ネットワーク ユーザに関連付けられている WLAN を削除すると、システムは、先に WLAN に関連付けられているすべてのネットワーク ユーザを削除するように指示するプロンプトを表示します。ネットワーク ユーザを削除した後に、WLAN を削除できます。

- 次のコマンドを入力して、コントローラに設定されたローカル ネットワーク ユーザに関する情報を表示します。
  - **show netuser detail** *username*：ローカル ユーザ データベース内の特定のユーザの設定を表示します。
  - **show netuser summary**：ローカル ユーザ データベース内のすべてのユーザの一覧を表示します。
- 次のコマンドを入力して、変更を保存します。

  save config

クライアント除外ポリシー

クライアント除外ポリシーの設定（GUI）

手順

ステップ 1 **[Security]** > **[Wireless Protection Policies]** > **[Client Exclusion Policies]** を選択して、[Client Exclusion Policies] ページを開きます。

ステップ 2 指定された条件について、コントローラがクライアントを除外するように設定するには、次のチェックボックスのいずれかをオンにします。各除外ポリシーのデフォルトは有効です。

- [Excessive 802.11 Association Failures]：クライアントは、802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.11 Authentication Failures]：クライアントは、802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.1X Authentication Failures]：クライアントは、802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [IP Theft or IP Reuse]：IP アドレスが他のデバイスにすでに割り当てられている場合、クライアントは除外されます。
- [Excessive Web Authentication Failures]：クライアントは、Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。

ステップ 3 設定を保存します。

クライアント除外ポリシーの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、802.11 アソシエーションを 5 回連続して失敗したあと、6 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion 802.11-assoc {**enable** | **disable**}

ステップ 2 次のコマンドを入力して、802.11 認証を 5 回連続して失敗したあと、6 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion 802.11-auth {**enable** | **disable**}

ステップ 3 次のコマンドを入力して、802.1X 認証を 3 回連続して失敗したあと、4 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion 802.1x-auth {**enable** | **disable**}

ステップ 4 次のコマンドを入力して、RADIUS サーバとの 802.1X 認証で最大失敗試行回数に達するクライアントを除外するようコントローラを設定します。

config wps client-exclusion 802.1x-auth max-1x-aaa-fail-attempts

802.1X 認証の最大失敗試行回数は 1 ～ 3 の範囲で設定できます。デフォルト値は 3 です。

ステップ 5 次のコマンドを入力して、IP アドレスが別のデバイスにすでに割り当てられている場合に、コントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion ip-theft {**enable** | **disable**}

ステップ 6 次のコマンドを入力して、Web 認証を 3 回連続して失敗したあと、4 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion web-auth {**enable** | **disable**}

ステップ 7 次のコマンドを入力して、上記のすべての理由でコントローラがクライアントを除外する設定を有効または無効にします。

config wps client-exclusion all {**enable** | **disable**}

ステップ 8 次のコマンドを使用して、クライアント除外エントリを追加または削除します。

config exclusionlist {**add** *mac-addr description* | **delete** *mac-addr* | **description** *mac-addr description*}

ステップ 9 次のコマンドを入力して、変更を保存します。

save config

ステップ 10 次のコマンドを入力して、動的に除外されたクライアントのリストを表示します。

show exclusionlist

以下に類似した情報が表示されます。

```
Dynamically Disabled Clients
----------------------------
  MAC Address             Exclusion Reason        Time Remaining (in secs)
  -----------             ----------------        ------------------------
```

```
00:40:96:b4:82:55         802.1X Failure           51
```

ステップ 11 次のコマンドを入力して、AP でローカルに除外された FlexConnect クライアントのリストを表示します。

show flexconnect client exclusion-list

以下に類似した情報が表示されます。

```
cisco-ap#show flexconnect client exclusion-list
Client Exclusion List:
     Excluded Mac life    Type
8E:BB:02:65:55:AA    0  static
A0:B4:35:B1:AG:55    0  static
E8:02:FH:C4:6A:11   35 dynamic
```

ステップ 12 次のコマンドを入力して、クライアント除外ポリシー構成の設定を表示します。

show wps summary

以下に類似した情報が表示されます。

```
Auto-Immune
 Auto-Immune..................................... Disabled

Client Exclusion Policy
  Excessive 802.11-association failures.......... Enabled
  Excessive 802.11-authentication failures....... Enabled
  Excessive 802.1x-authentication................ Enabled
  IP-theft....................................... Enabled
  Excessive Web authentication failure........... Enabled
  Maximum 802.1x-AAA failure attempts............ 3

Signature Policy
  Signature Processing........................ Enabled
```

Wi-Fi Direct クライアント ポリシー

Wi-Fi Direct クライアント ポリシーについて

Wi-Fi Direct 対応のデバイスは迅速な相互接続が可能で、印刷、同期、データ共有などのタスクを効率的に実行できます。Wi-Fi Direct デバイスは、複数のピアツーピア（P2P）デバイスおよびインフラストラクチャ無線 LAN（WLAN）に同時にアソシエートしている場合があります。コントローラ を使用して、Wi-Fi Direct クライアント ポリシーを WLAN 単位で設定できます。その際、Wi-Fi デバイスとインフラストラクチャ WLAN のアソシエーションを許可または禁止するか、WLAN に対して Wi-Fi Direct クライアント ポリシーをすべて無効にすることができます。

Wi-Fi Direct クライアント ポリシーの制限

- Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。
- FlexConnect モードの Cisco AP は（中央認証や中央スイッチングの場合でも）サポートされていません。
- 混合 AP モードの導入環境（一部の AP がFlexConnect モードで、一部の AP がローカル モード）で、この機能を有効化することはお勧めできません。このようなタイプの導入は、FlexConnect モードではサポートもテストもされていません。
- WLAN クライアントに適用されるポリシーが無効の場合、クライアントは「クライアント QoS ポリシー障害」という項目理由のため除外されます。

Wi-Fi Direct クライアント ポリシーの設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 Wi-Fi Direct クライアント ポリシーを設定する WLAN の WLAN ID をクリックします。[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Wi-Fi Direct Clients Policy] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [Disabled]：クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します。
- [Allow]：Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します。
- [Not-Allow]：Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します。
- [Xconnect-Not-Allow]：AP による、Wi-Fi Direct オプションが有効になっているクライアントのアソシエーションの許可を有効にしますが、クライアント（Wi-Fi 標準に従って動作する場合）は、ピアツーピア接続を差し控えます。

ステップ 5 設定を保存します。

Wi-Fi Direct クライアント ポリシーの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、WLAN に Wi-Fi Direct クライアント ポリシーを設定します。

config wlan wifidirect {**allow** | **disable** | **not-allow**} *wlan-id*

このコマンドの構文は次のとおりです。

- **allow**—Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します。
- **disable**—クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します。
- **not-allow**—Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します。
- **xconnect-not-allow**—AP による、Wi-Fi Direct オプションが有効になっているクライアントのアソシエーションの許可を有効にしますが、クライアント（Wi-Fi 標準に従って動作する場合）は、ピアツーピア接続を差し控えます。
- *wlan-id*：WLAN ID。

ステップ 2 次のコマンドを入力して、設定を保存します。

save config

Wi-Fi Direct クライアント ポリシーの監視とトラブルシューティング（CLI）

手順

- 次のコマンドを入力して、Wi-Fi Direct クライアント ポリシーの監視およびトラブルシューティングを行います。
  - **show wlan wifidirect** *wlan-id*：WLAN の Wi-Fi Direct クライアント ポリシーのステータスを表示します。
  - **show client wifiDirect-stats**：Wi-Fi Direct クライアント ポリシーが有効になっている場合に、アソシエートされたクライアントの総数と拒否されたクライアントの数を表示します。

AP 無線あたりの WLAN ごとのクライアント数の制限

AP 無線あたりの WLAN ごとのクライアント数の制限（GUI）

- ローカル モードの AP では、Cisco WLC はすべてのクライアントの関連付け要求を検証します。Cisco WLC は、設定された制限数に達した場合、クライアント関連付け要求をドロップします。

- FlexConnect モードの AP では、接続モード（ローカルまたは中央スイッチング、ローカルまたは中央認証）およびスタンドアロンモード（ローカルスイッチング、ローカル認証）の両方に対して、AP は認証または再関連付けフェーズでクライアント アドミッションを検証します。

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 [WLAN ID] をクリックします。

ステップ 3 [WLANs > Edit] ページで [Advanced] タブをクリックします。

ステップ 4 [Maximum Allowed Clients] フィールドに、WLAN への参加を許可されるクライアントの最大数を入力します。

（注） 値として 0 を入力すると、WLAN への参加を許可するクライアントの数を制限しないことになります。

ステップ 5 **最大許容クライアントあたり AP 無線**] フィールドには、AP の無線あたりの WLAN への参加を許可できるクライアントの最大数を入力します。

有効な範囲は 1 ～ 200 クライアントです。

ステップ 6 設定を保存します。

AP 無線あたりの WLAN ごとのクライアント数の制限（CLI）

- ローカル モードの AP では、Cisco WLC はすべてのクライアントの関連付け要求を検証します。Cisco WLC は、設定された制限数に達した場合、クライアント関連付け要求をドロップします。
- FlexConnect モードの AP では、接続モード（ローカルまたは中央スイッチング、ローカルまたは中央認証）およびスタンドアロンモード（ローカルスイッチング、ローカル認証）の両方に対して、AP は認証または再関連付けフェーズでクライアント アドミッションを検証します。

手順

ステップ 1 次のコマンドを入力して、AP 無線ごとに WLAN への参加を許可できるクライアントの最大数を設定します。

config wlan max-radio-clients *max-clients wlan-id*

ステップ 2 次のコマンドを入力して、クライアント情報を表示します。

- Cisco WLC コンソールの場合：**show client summary**

- Cisco Wave 2 AP コンソールの場合：**show dot11 clients**

ステップ 3 次のコマンドを入力して、Cisco Wave 2 AP コンソールのデバッグを有効にします。

- 802.11 イベント レベルのデバッグを有効にする場合：**debug dot11 events**
- 802.11 情報レベルのデバッグを有効にする場合：**debug dot11 info**

ピアツーピア ブロック

ピアツーピア ブロッキングについて

ピアツーピアブロッキングは個別のWLANに対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがコントローラ内でローカルにブリッジされたり、コントローラによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

WLAN ごとに、ピアツーピア設定がコントローラによって FlexConnect AP にプッシュされます。4.2 以前のコントローラのソフトウェア リリースでは、ピアツーピア ブロッキングはすべての WLAN 上のすべてのクライアントにグローバルに適用され、それによって同じ VLAN 上の2つのクライアント間のトラフィックが、コントローラでブリッジされるのではなく、アップストリームVLANに転送されていました。この動作の結果、スイッチはパケットを受け取ったのと同じポートからパケットを転送しないため、通常アップストリームスイッチでトラフィックがドロップされます。

IPSK タグを使用したピアツーピア ブロッキング

トラフィックは VLAN 全体でブリッジされないため、P2P ブロッキングは適用されません。IPSK ベースのピア ブロッキングは例外で、IPSK タグが一致する場合、VLAN 間のクライアントトラフィックは上流に位置するスイッチに転送され、一致しない場合はドロップされます。

拡張機能は、コントローラで [Allow Private Group] が有効になっている中央スイッチングおよび Flex + ローカル スイッチングの IPv4 および IPv6 プロトコルでサポートされています。

表 *2 : IPSK* タグのトラフィック フロー

WLAN P2P 設定	IPSK 送信元デバイスのタグ	IPSK 接続先デバイスのタグ	トラフィック ブリッジングの決定	結果
Drop	いずれか（Any）	いずれか（Any）	ブロック	この設定では、すべての P2P トラフィックがドロップされます。
Disable	いずれか（Any）	いずれか（Any）	許可	この設定では、すべての P2P トラフィックがブリッジされます。
Up Stream	いずれか（Any）	いずれか（Any）	転送	この設定では、すべての P2P トラフィックがネクスト ホップ スイッチに転送されます。
Allow Private Group	T1	T2	ブロック	この設定で、クライアントが異なる VLAN にある場合でも、異なるタグ値（T1 と T2）を持つ P2P トラフィックがドロップされます。
Allow Private Group	T	T	許可	この設定では、同じタグ値（T）を持つ P2P トラフィックがブリッジされます。 クライアントが異なる VLAN にある場合、トラフィックは上流に位置するスイッチに転送されます。

ピアツーピア ブロッキングの制約事項

- シスコ コントローラと AP がサポートしている、IPSK タグ ベースの P2P はブロック機能は次のとおりです。
  - シスコ コントローラ：3504、5520、8540 シリーズ コントローラ
  - Cisco AP：1800、2800、3800 シリーズ AP。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- FlexConnect では、特定の FlexConnect AP または AP のサブセットのみにソリューションのピアツーピア ブロッキング設定を適用することはできません。これは、SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチングのクライアントに対応するシスコ コントローラではピアツーピア アップストリーム転送がサポートされます。しかし、これは FlexConnect ソリューションでサポートされません。これはピア ツー ピア ドロップとして処理され、クライアント パケットはドロップされます。
- 中央スイッチングのクライアントに対応するシスコ コントローラでは、別々の AP に関連付けられたクライアントに対するピアツーピア ブロッキングがサポートされます。ただし、このソリューションでは、同一の AP に接続するクライアントだけがターゲットとなります。FlexConnect ACL は、この制限の回避策として使用できます。

ピアツーピア ブロッキングの設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 ピアツーピア ブロッキングを設定する WLAN の ID 番号をクリックします。

ステップ 3 [Advanced] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

ステップ 4 [P2P Blocking] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [Disabled]：ピアツーピア ブロッキングを無効にして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。これはデフォルト値です。

  （注） コントローラ内の VLAN でトラフィックがブリッジされることはありません。

- [Drop]：コントローラでパケットを破棄するようにします。
- [Forward-UpStream]：パケットがアップストリーム VLAN に転送されるようにします。これらのパケットに対して行われる動作は、コントローラよりも上流にあるデバイスにより決定されます。

（注） FlexConnect ローカル スイッチングに設定された WLAN でピアツーピア ブロッキングを有効にするには、[P2P Blocking] ドロップダウン リストから [Drop] を選択し、[FlexConnect Local Switching] チェックボックスをオンにします。

- [Allow-Private-Group]：PSK クライアントだけに適用されます。トラフィック転送の判断は、送信元と宛先のクライアント デバイスに関連付けられている IPSK タグに基づいて行われます。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

ピアツーピア ブロッキングの設定（CLI）

手順

ステップ 1 WLAN のピアツーピア ブロッキングを設定するには、次のコマンドを入力します。

config wlan peer-blocking {**disable** | **drop** | **forward-upstream** | **allow-private-group**} *wlan_id*

（注） **Allow-private-group** は PSK クライアントだけに適用されます。

ステップ 2 次のコマンドを入力して、変更を保存します。

save config

ステップ 3 次のコマンドを入力して、WLAN のピアツーピア ブロッキングのステータスを参照します。

show wlan *wlan_id*

以下に類似した情報が表示されます。

```
WLAN Identifier................................ 1
Profile Name................................... test
Network Name (SSID)............................ test
Status......................................... Enabled
...
...
...
Peer-to-Peer Blocking Action................... Disabled
Radio Policy................................... All
Local EAP Authentication..................... Disabled
```

ステップ 4 次のコマンドを入力して、クライアントに関連付けられている IPSK タグを確認します。

show client summary ipsk-tag

ローカル ポリシー

ローカル ポリシーについて

コントローラは、HTTP、 DHCP などのプロトコルに基づいてデバイスのプロファイリングを実行して、クライアントを識別できます。デバイスベースのポリシーを設定し、ネットワークにユーザごとまたはデバイスごとのポリシーを適用できます。コントローラは、ユーザごとまたはデバイスごとのエンドポイント、およびデバイスごとに適用できるポリシーに基づく統計情報を表示します。設定できるポリシーの最大数は 64 です。

ポリシーは、次の属性に基づいて定義されます。

- ユーザ グループまたはユーザ ロール
- Windows クライアント、スマートフォン、タブレットなどのデバイス タイプ
- SSID（Service Set Identifier）
- エンドポイントが接続されているアクセス ポイント グループに基づく場所
- 時刻
- クライアントが接続されている EAP 方式をチェックするための拡張認証プロトコル（EAP）タイプ。

これらのポリシー属性が一致する場合は、次のアクションを定義できます。

- 仮想ローカル エリア ネットワーク（VLAN）
- アクセス コントロール リスト（ACL）
- Quality of Service（QoS）レベル
- セッション タイムアウト値
- スリープ状態にあるクライアントのタイムアウト値
- AAA サーバに定義されたローカル ポリシー属性に基づいて、AVC プロファイル、ロール、またはその両方を選択します。

  次に、AAA サーバに定義された AVC プロファイルとロールの組み合わせに基づいて適用されるローカル ポリシーによる別の方法を示します。

  - AVC プロファイルとロールの両方が AAA サーバから取得される場合、次のオプションを使用できます。
    - AAA Override が有効である場合、AVC プロファイルは優先順位付けされて適用されます。
    - AAA Override が無効である場合、ロール マッチングが適用されます。

- ロールのみを AAA サーバから取得してロール マッチングを行う場合、次のオプションを使用できます。
  - プロファイルがポリシー内で定義されている場合、ロールポリシーが適用されます。
  - プロファイルがポリシーで定義されていない場合、WLAN で定義された AVC プロファイルが適用されます。
- AVC プロファイルのみを AAA サーバから取得する場合、次のオプションを使用できます。
  - AAA Override が有効である場合、AAA サーバから受け取った AVC プロファイルが適用されます。
  - AAA Override が無効である場合、WLAN で定義された AVC プロファイルが適用されます。

ローカル ポリシー分類の制約事項

- AAA Override が有効で、AAA 属性が AAA サーバのロール タイプ以外である場合、設定されたポリシーのアクションは適用されません。AAA Override 属性が優先されます。
- WLAN では、ローカル プロファイルが有効になっている場合、RADIUS プロファイルは許可されません。
- クライアント プロファイルではコントローラの既存のプロファイルが使用されます。
- カスタム プロファイルを作成することはできません。
- ワークグループ ブリッジ（WGB）の背後の有線クライアントはプロファイルされず、ポリシー アクションは実行されません。
- ポリシープロファイルと一致する最初のポリシールールのみが優先されます。各ポリシープロファイルには、ポリシーとの一致に使用されるポリシールールが関連付けられています。
- 最大 64 のポリシーを設定することができ、これらのポリシーを WLAN ごとに最大 16 設定できます。
- レイヤ 2 認証またはレイヤ 3 認証の完了後、またはデバイスが HTTP トラフィックを送信して、デバイスがプロファイルされた場合、ポリシー アクションが実行されます。したがって、プロファイルおよびポリシーアクションはクライアントごとに複数回実行されます。
- VLAN、ACL、Session Timeout および QoS のみがポリシー アクション属性としてサポートされます。
- プロファイルは、IPv4 クライアントでのみ行われます。

- モビリティ グループのすべてのコントローラについて、ローカル ポリシー設定に同じ一致基準属性とアクション属性が必要です。これ以外の場合、コントローラ間でローミングが発生すると、ローカル ポリシー設定は無効になります。
- ローカル ポリシーがデバイス タイプ ポリシーの一致に設定されており、ゲスト アンカーが有効になっている WLAN 上で設定されている場合、ローカル ポリシーの AVC プロファイル名は、アンカーでは適用されません。

表 *3 : Cisco Identity Services Engine（ISE）とコントローラでのプロファイル サポートの違い*

ISE	コントローラ
RADIUS プローブ、DHCP プローブ、HTTP およびクライアント タイプの識別に使用するその他のプロトコルを使用したプロファイルをサポートします。	MAC OUI、DHCP、および HTTP ベースのプロファイルをサポートします。
ポリシー アクションの複数の異なる属性をサポートし、各属性を選択するためのインターフェイスがあります。	ポリシーアクション属性として VLAN、ACL、Session-Timeout および QoS をサポートします。
ユーザ定義属性によるプロファイル ルールのカスタマイズをサポートします。	デフォルトのプロファイルルールのみをサポートします。

ローカル ポリシーの設定（GUI）

手順

ステップ 1 **[Security]** > **[Local Policies]** を選択します。

ステップ 2 新しいポリシーを作成するには、[New] をクリックします。

ステップ 3 ポリシー名を入力し、[Apply] をクリックします。

ステップ 4 [Policy List] ページで、設定するポリシー名をクリックします。

ステップ 5 [Policy > Edit] ページで、次の手順を実行します。

a) [Match Criteria] 領域で、[Match Role String] の値を入力します。これはユーザのユーザ タイプまたはユーザ グループです（たとえば、学生、教員など）。

b) [Match EAP Type] ドロップダウン リストから、クライアントが使用する EAP 認証方式を選択します。

c) [Device Type] ドロップダウン リストから、デバイス タイプを選択します。

d) ポリシーのデバイス リストにデバイス タイプを追加するには、[Add] をクリックします。

選択したデバイス タイプは、[Device List] に表示されます。

e) [Action] 領域で、適用させるポリシーを指定します。[IPv4 ACL] ドロップダウン リストから、ポリシーの IPv4 ACL を選択します。

f) ポリシーに関連付ける必要がある **VLAN ID** を入力します。

g) [QoS Policy] ドロップダウン リストから、適用する QoS ポリシーを選択します。

h) [Session Timeout] の値を入力します。これは、クライアントに再認証を強制するまでの最大時間（秒単位）です。

i) [Sleeping Client Timeout] の値を入力します。これはスリープ状態にあるクライアントのタイムアウトです。

スリープ状態にあるクライアントとは、Web認証に成功したゲストアクセスを持つクライアントであり、スリープおよび再起動のためにログインページからの別の認証プロセスを必要としません。

このスリープ状態のクライアントタイムアウト設定は、WLAN固有のスリープ状態のクライアント タイムアウト設定に優先します。

j) [AVC Profile] ドロップダウン リストから、AAA に定義されたロールに基づいて適用される AVC プロファイルを選択します。

k) [Active Hours] 領域の [Day] ドロップダウン リストから、ポリシーをアクティブにする曜日を選択します。

l) ポリシーの**開始時間**と**終了時間**を入力します。

m) [Add] をクリックします。

指定した曜日および開始時刻と終了時刻が表示されます。

n) [Apply] をクリックします。

次のタスク

次の手順に従って、作成したローカル ポリシーを WLAN に適用します。

1. [WLANs] を選択します。
2. 対応する WLAN ID をクリックします。

   [**WLANs > Edit**] ページが表示されます。
3. [Policy-Mapping] タブをクリックします。
4. ポリシーの**プライオリティ インデックス**を入力します。
5. [Local Policy] ドロップダウン リストから、WLAN に適用させるポリシーを選択します。
6. [Add] をクリックします。

   選択したプライオリティ インデックスおよびポリシーが表示されます。WLAN に対して最大 16 のポリシーを適用できます。

ローカル ポリシーの設定（CLI）

手順

- 次のコマンドを入力して、ローカル ポリシーを作成または削除します。

  config policy *policy-name* {**create** | **delete**}

- 次のコマンドを入力して、ポリシーに一致タイプを設定します。
  - **config policy** *policy-name* **match device-type** {**add** | **delete**} *device-type*
  - **config policy** *policy-name* **match eap-type** {**add** | **delete**} {**eap-fast** | **eap-tls** | **leap** | **peap**}
  - **config policy** *policy-name* **match role** {*role-name* | *none*}

- 次のコマンドを入力して、ポリシーの一部として実行させるアクションを設定します。
  - ポリシーに対する ACL アクション：**config policy** *policy-name* **action acl** {**enable** | **disable**} *acl-name*
  - QoS 平均データ レート：**config policy** *policy-name* **action average-data-rate** {**enable** | **disable**} *rate*
  - QoS 平均リアルタイム データ レート：**config policy** *policy-name* **action average-realtime-rate** {**enable** | **disable**} *rate*
  - QoS バースト データ レート：**config policy** *policy-name* **action burst-data-rate** {**enable** | **disable**} *rate*
  - QoS バースト リアルタイム データ レート：**config policy** *policy-name* **action burst-realtime-rate** {**enable** | **disable**} *rate*
  - QoS アクション：**config policy** *policy-name* **action qos** {**enable** | **disable**} {**bronze** | **gold** | **platinum** | **silver**}
  - セッション タイムアウト アクション：**config policy** *policy-name* **action session-timeout** {**enable** | **disable**} *timeout-in-seconds*
  - スリープ状態にあるクライアントのタイムアウト アクション：**config policy** *policy-name* **action sleeping-client-timeout** {**enable** | **disable**} *timeout-in-hours*
  - AVC プロファイルの有効化：**config policy** *policy-name* **action avc-profile-name enable** *avc-profile-name*
  - AVC プロファイルの無効化：**config policy** *policy-name* **action avc-profile-name disable**
  - VLAN アクション：**config policy** *policy-name* **action vlan** {**enable** | **disable**} *vlan-id*

（注） バースト データ レートを設定する前に平均データ レートを設定してください。

- 次のコマンドを入力して、ポリシーのアクティブ タイムを設定します。

  config policy *policy-name* **active** {**add** | **delete**} **hours start-time end-time days** {*mon* | *tue* | *wed* | *thu* | *fri* | *sat* | *sun* | *daily* | *weekdays*}

- 次のコマンドを入力して、WLAN にローカル ポリシーを適用します。

  config wlan policy {**add** | **delete**} *priority-index policy-name wlan-id*

- 次のコマンドを入力して、HTTP、DHCP、またはそれらの両方に基づいて、WLAN に対してローカル モードでクライアント プロファイルを有効または無効にします。

  config wlan profiling local {**dhcp** | **http** | **all**} {**enable** | **disable**} *wlan-id*

- 次のコマンドを入力して、WLAN の AP グループにローカル ポリシーを適用します。

  config wlan apgroup policy {**add** | **delete**} *priority-index policy-name ap-group-name wlan-id*

- 次のコマンドを入力して、ポリシーに関する情報を表示します。

  show policy {**summary** | *policy-name*} **statistics**

- 次のコマンドを入力して、ローカル デバイス分類プロファイルの概要を表示します。

  show profiling policy summary

- 次のコマンドを入力して、特定のデバイス タイプのライアントをすべて表示します。

  show client wlan *wlan-id* **device-type** *device-type*

- 次のコマンドを入力して、RADIUS サーバおよびコントローラによって行われたプロファイルを含むクライアントのプロファイル ステータスを表示します。

  show wlan *wlan-id*

- 次のコマンドを入力して、AP グループに関するポリシーの詳細を表示します。

  show wlan apgroups

- 次のコマンドを入力して、ポリシーのデバッグ タスクを設定します。

  debug policy {**error** | **event**} {**enable** | **disable**}

組織の一意の ID リストの更新

組織の一意の ID リストの更新（GUI）

手順

ステップ 1 サーバ上のデフォルト ディレクトリに、http://standards.ieee.org/develop/regauth/oui/oui.txt から入手できる最新の OUI リストをコピーします。

ステップ 2 **[Commands]** > **[Download File]** を選択します。

[Controller] ページへのダウンロード ファイルが表示されます。

ステップ 3 **[File Type]** ドロップダウン リストから、**[OUI Update]** を選択します。

ステップ 4 **[Transfer Mode]** ドロップダウン リストから、サーバ タイプを選択します。

サーバの詳細が同じページに表示されます。

ステップ 5 [Download] をクリックします。

ステップ 6 ダウンロードが完了したら、**[Commands]** > **[Reboot]** を選択して Cisco WLC をリブートします。

ステップ 7 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。

ステップ 8 [OK] をクリックします。

組織の一意の ID リストの更新（CLI）

手順

ステップ 1 サーバ上のデフォルトディレクトリに、http://standards.ieee.org/develop/regauth/oui/oui.txt から入手できる最新の OUI リストをコピーします。

ステップ 2 次のコマンドを入力して、サーバ タイプを指定します。

transfer download mode {tftp | ftp | sftp}

ステップ 3 次のコマンドを入力して、ファイルのタイプを指定します。

transfer download datatype oui-update

ステップ 4 次のコマンドを入力して、ファイルのダウンロードを開始します。

transfer download start

（注） 画面上の指示に従って、ダウンロード プロセスを完了します。

ステップ 5 次のコマンドを入力して、Cisco WLC をリブートします。

reset system

ステップ 6 次のコマンドを入力して、更新された OUI リストを確認します。

show profiling oui-string summary

（注） OUI アップデートのための HA サポート：OUI アップデートがスタンバイ コントローラにも適用されるように、OUI ファイルをアクティブ コントローラにダウンロードしている間、HA リンクがアップ状態になっている必要があります。

デバイス プロファイル リストの更新

デバイス プロファイル リストの更新（GUI）

手順

ステップ 1 サーバ上のデフォルト ディレクトリに、最新のデバイス プロファイル リスト ファイルをコピーします。

ステップ 2 **[Commands]** > **[Download File]** を選択します。

[Controller] ページへのダウンロード ファイルが表示されます。

ステップ 3 **[From the File Type]** ドロップダウン リストから、**[Device Profile]** を選択します。

ステップ 4 **[Transfer Mode]** ドロップダウン リストから、サーバ タイプを選択します。

サーバの詳細が同じページに表示されます。

ステップ 5 [Download] をクリックします。

ステップ 6 ダウンロードが完了したら、**[Commands]** > **[Reboot]** を選択して Cisco WLC をリブートします。

ステップ 7 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。

ステップ 8 [OK] をクリックします。

デバイス プロファイル リストの更新（CLI）

手順

ステップ 1 サーバ上のデフォルト ディレクトリに、最新のデバイス プロファイル リスト ファイルをコピーします。

ステップ 2 次のコマンドを入力して、サーバ タイプを指定します。

transfer download mode {**tftp** | **ftp** | **sftp**}

ステップ 3 次のコマンドを入力して、ファイルのタイプを指定します。

transfer download datatype device-profile

ステップ 4 次のコマンドを入力して、ファイル名を指定します。

transfer download filename *device_profile-xml-file*

ステップ 5 次のコマンドを入力して、ファイルのダウンロードを開始します。

transfer download start

（注） 画面上の指示に従って、ダウンロード プロセスを完了します。

ステップ 6 次のコマンドを入力して、Cisco WLC をリブートします。

reset system

ステップ 7 次のコマンドを入力して、更新された OUI リストを確認します。

show profiling policy summary

有線ゲスト アクセス

有線ゲスト アクセスについて

有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスからまたは会議室の特定のポートを介して利用することもできます。無線ゲストユーザアカウントのように、有線ゲストアクセスポートがLobby Ambassador機能を使用するネットワークに追加されます。

有線ゲストアクセスは、スタンドアロン設定または、アンカーコントローラと外部コントローラの両方を使用するデュアルコントローラ設定で設定できます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

有線ゲスト アクセス ポートは最初、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセス トラフィック用の VLAN インターフェイスで設定されているスイッチ ポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

（注） 2 つのコントローラが展開されるとき、有線ゲストアクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

（注） QoS ロールと帯域幅コントラクトを設定することにより、ネットワーク内の有線ゲスト ユーザに割り当てられている帯域幅の量を指定できます。

基本的なピアツーピア WLAN ACL を作成して有線ゲスト WLAN に適用できます。これはピアツーピア トラフィックをブロックしないので、ゲスト ユーザは互いに通信できます。

有線ゲストのアクセスを設定するための前提条件

無線ネットワーク上で有線ゲストアクセスを設定するには、次の手順を実行する必要があります。

1. 有線ゲスト ユーザ アクセス用の動的インターフェイス（VLAN）を設定します。
2. ゲスト ユーザ アクセス用の有線 LAN を作成します。
3. コントローラを設定します。

4. アンカーコントローラを設定します（別のコントローラでトラフィックを終端する場合）。
5. ゲスト LAN 用のセキュリティを設定します。
6. 設定を確認します。

有線ゲストのアクセスの設定に関する制限

- 有線ゲスト アクセス インターフェイスは、タグ付きである必要があります。
- 有線ゲスト アクセス ポートは、外部コントローラと同じレイヤ 2 ネットワークになければなりません。
- コントローラ上で、最大 5 つの有線ゲスト アクセス LAN を設定できます。また、有線ゲスト アクセス LAN では、複数のアンカーがサポートされます。
- 有線ゲスト アクセス クライアントに対して、レイヤ 3 Web 認証と Web パススルーがサポートされています。レイヤ 2 セキュリティはサポートされていません。
- 予期しない結果が生じる場合があるため、有線ゲスト VLAN を複数の外部コントローラにトランクしないでください。
- コントローラは、有線クライアントの認証時に RADIUS サーバに対して設定された callStationIDType パラメータを使用せずに、callStationIDType パラメータに設定されているシステム MAC アドレスを使用します。

有線ゲスト アクセスの設定（GUI）

手順

ステップ 1 有線ゲスト ユーザ アクセス用の動的インターフェイスを作成するために、[Controller] > [Interfaces] の順に選択します。[Interfaces] ページが表示されます。

ステップ 2 [New] をクリックして、[Interfaces > New] ページを開きます。

ステップ 3 新しいインターフェイスの名前と VLAN ID を入力します。

ステップ 4 [Apply] をクリックして、変更を確定します。

ステップ 5 [Port Number] テキスト ボックスに、有効なポート番号を入力します。0 ～ 25（両端の値を含む）の数値を入力できます。

ステップ 6 [Guest LAN] チェックボックスをオンにします。

ステップ 7 [Apply] をクリックして、変更を確定します。

ステップ 8 ゲスト ユーザ アクセス用に有線 LAN を作成するために、[WLANs] を選択します。

ステップ 9 [WLANs] ページで、ドロップダウン リストから [Create New] を選択して、[Go] をクリックします。**[WLANs > New]** ページが表示されます。

ステップ 10 [Type] ドロップダウン リストから、[Guest LAN] を選択します。

ステップ 11 [Profile Name] テキスト ボックスに、ゲスト LAN を識別する名前を入力します。スペースを使用しないでください。

ステップ 12 [WLAN ID] ドロップダウン リストから、このゲスト LAN の ID 番号を選択します。

（注） 最大 5 つのゲスト LAN を作成できるので、[WLAN ID] オプションは 1 ～ 5（両端の値を含む）です。

ステップ 13 [Apply] をクリックして、変更を確定します。

ステップ 14 [Status] パラメータの [Enabled] チェックボックスをオンにします。

ステップ 15 Web 認証（[Web-Auth]）は、デフォルトのセキュリティ ポリシーです。Web パススルーに変更する場合は、ステップ *16* とステップ *17* を完了してから [Security] タブを選択します。

ステップ 16 [Ingress Interface] ドロップダウン リストから、ステップ *3* で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 17 [Egress Interface] ドロップダウン リストから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィックのコントローラから送信されるパスを提供します。

ステップ 18 認証方式を変更する（たとえば、Web 認証から Web パススルーへ）場合、[Security] > [Layer 3] の順に選択します。[WLANs > Edit]（[Security] > [Layer 3]）ページが表示されます。

ステップ 19 [Layer 3 Security] ドロップダウン リストから、次のいずれかを選択します。

- [None]：**レイヤ 3 セキュリティが無効になっています。**
- [Web Authentication]：無線ネットワークに接続する際に、ユーザにユーザ名とパスワードの入力を求めます。これはデフォルト値です。
- [Web Passthrough]：ユーザがユーザ名とパスワードを入力せずに、ネットワークにアクセスすることを許可します。

（注） ゲスト有線 VLAN にはレイヤ 3 ゲートウェイが存在しないようにしてください。コントローラによる Web 認証がバイパスされるためです。

ステップ 20 [Web Passthrough] オプションを選択すると、[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メールアドレスの入力を求める場合は、このチェックボックスをオンにします。

ステップ 21 [Web Login Page] に設定されているグローバル認証設定を無効にするには、[Override Global Config] チェックボックスをオンにします。

ステップ 22 [Web Auth Type] ドロップダウン リストが表示されたら、次のオプションのいずれかを選択して、有線ゲスト ユーザ用の Web 認証ページを定義します。

- [Internal]：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- [Customized]：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン リストが表示されます。3 つのオプ

ションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。

（注） これらのオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- [External]：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

  [WLANs > Edit]（[Security] > [AAA Servers]）ページで、外部認証を行う特定の RADIUS サーバまたはLDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 23 ステップ *22* で Web 認証タイプとして [External] を選択した場合は、[Security] > [AAA Servers] を選択して、ドロップダウン リストから最大 3 つの RADIUS サーバおよび LDAP サーバを選択します。

（注） 認証と LDAP サーバの設定には、IPv4 アドレスと IPv6 アドレスの両方を使用できます。

（注） RADIUS および LDAP の外部サーバは、[WLANs > Edit]（[Security] > [AAA Servers]）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 24 次の手順で、Web 認証で接続するサーバの優先順位を指定します。

（注） デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

1. [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類（[Local]、[Radius]、[LDAP]）を強調表示します。
2. 希望のサーバ タイプがボックスの先頭になるまで、[Up] および [Down] をクリックします。
3. [<] 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。
4. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 25 [Apply] をクリックします。

ステップ 26 [Save Configuration] をクリックします。

ステップ 27 2 番めの（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

有線ゲスト アクセスの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、有線ゲストユーザのアクセス用の動的インターフェイス（VLAN）を作成します。

config interface create *interface_name vlan_id*

ステップ 2 リンク集約トランクが設定されていない場合、次のコマンドを入力して、物理ポートをインターフェイスにマッピングします。

config interface port *interface_name primary_port* {*secondary_port*}

ステップ 3 次のコマンドを入力して、ゲスト LAN VLAN を有効または無効にします。

config interface guest-lan *interface_name* {**enable | disable**}

この VLAN は、ステップ *5* で作成した入力インターフェイスに後でアソシエートされます。

ステップ 4 有線クライアント トラフィック用の有線 LAN を作成して、インターフェイスにアソシエートさせるには、次のコマンドを入力します。

config guest-lan create *guest_lan_id interface_name*

ゲスト LAN ID は、1 ～ 5（両端の値を含む）にする必要があります。

（注） 有線ゲスト LAN を削除するには、 **config guest-lan delete** *guest_lan_id* コマンドを入力します。

ステップ 5 レイヤ 2 アクセス スイッチ経由で、有線ゲスト クライアントとコントローラ間のパスを提供する有線ゲストVLANの入力インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan ingress-interface *guest_lan_id interface_name*

ステップ 6 コントローラから有線ゲスト トラフィックを送信するように出力インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan interface *guest_lan_id interface_name*

（注） 有線ゲスト トラフィックが別のコントローラで終端する場合は、終点の（アンカー）コントローラに対してステップ *4* とステップ *6* を繰り返し、起点の（外部）コントローラに対してステップ *1* からステップ *5* を繰り返します。また、両方のコントローラに対して**config mobility group anchor add** { **guest-lan** *guest_lan_id* | **wlan** *wlan_id}* *IP_address* コマンドを設定します。

ステップ 7 有線ゲスト LAN のセキュリティ ポリシーを設定するには、次のコマンドを入力します。

config guest-lan security {**web-auth enable guest_lan_id | web-passthrough enable** *guest_lan_id*}

（注） Web 認証はデフォルト設定です。

ステップ 8 有線ゲスト LAN を有効または無効にするには、次のコマンドを入力します。

config guest-lan {enable | disable} *guest_lan_id*

ステップ 9 カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに有線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して、Web 認証ページのファイル名および表示するゲスト LAN を指定します。

- **config guest-lan custom-web login-page** *page_name guest_lan_id*：*Web* ログイン ページを定義します。
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id*：[Web login failure] ページを定義します。

  （注） コントローラのデフォルト ログイン失敗ページを使用するには、**config guest-lan custom-web loginfailure-page none** *guest_lan_id* コマンドを入力します。

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*：[Web logout] ページを定義します。

  （注） コントローラのデフォルト ログアウト ページを使用するには、**config guest-lan custom-web logout-page none** *guest_lan_id* コマンドを入力します。

ステップ 10 有線ゲスト ユーザが Web ログイン ページにアクセスする前に有線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

ステップ 11 ローカル（コントローラ）または外部（RADIUS、LDAP）の Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

config wlan security web-auth server-precedence*wlan_id***{local |ldap |radius} {local |ldap |radius} {local |ldap |radius}**

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

（注） すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページまたは [LDAP Servers] ページでこれらを設定できます。

ステップ 12 有線ゲスト ユーザ用の Web ログイン ページを定義するには、次のコマンドを入力します。

config guest-lan custom-web webauth-type {internal | customized | external} *guest_lan_id*

値は次のとおりです。

- **internal** コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** では、ステップ *9* で設定したカスタム Web ページ（ログイン ページ、ログイン失敗ページ、またはログアウト ページ）が表示されます。
- **external** は、ステップ *10* で設定した URL にユーザをリダイレクトします。

ステップ 13 グローバル カスタム Web 設定ではなく、ゲスト LAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

config guest-lan custom-web global disable *guest_lan_id*

（注） **config guest-lan custom-web global enable** *guest_lan_id* コマンドを入力すると、カスタム Web 認証の設定がグローバル レベルで使用されます。

ステップ 14 次のコマンドを入力して、変更を保存します。

save config

（注） 設定された Web 認証ページの情報は、**show run-config** コマンドと **show running-config** コマンドの両方に表示されます。

ステップ 15 次のコマンドを入力して、特定のゲスト LAN に対するカスタマイズ Web 認証設定を表示します。

show custom-web {all | guest-lan guest_lan_id}

（注） 内部の Web 認証が設定されていると、Web Authentication Type は、外部（コントローラ レベル）またはカスタマイズ（WLAN プロファイル レベル）ではなく内部として表示されます。

ステップ 16 次のコマンドを入力して、ローカル インターフェイスの要約を表示します。

show interface summary

（注） この例の有線ゲスト LAN のインターフェイス名は、*wired-guest*、VLAN ID は 236 です。

次のコマンドを入力して、詳細なインターフェイス情報を表示します。

show interface detailed *interface_name*

ステップ 17 次のコマンドを入力して、特定の有線ゲスト LAN の設定を表示します。

show guest-lan *guest_lan_id*

（注） **show guest-lan summary** コマンドを入力して、コントローラに設定されているすべての有線ゲスト LAN を表示します。

ステップ 18 次のコマンドを入力して、アクティブな有線ゲスト LAN クライアントを表示します。

show client summary guest-lan

ステップ 19 次のコマンドを入力して、特定のクライアントの詳細情報を表示します。

show client detail *client_mac*

IPv6 クライアントのゲスト アクセスのサポート

クライアントが認証されるまで、クライアントは WebAuth 状態です。コントローラは、この状態の IPv4 トラフィックと IPv6 トラフィックの両方を代行受信し、コントローラの仮想 IP アドレスにリダイレクトします。認証されると、ユーザの MAC アドレスが RUN 状態に移行し、IPv4 トラフィックと IPv6 トラフィックの両方が通過を許可されます。

IPv6 専用クライアントのリダイレクションをサポートするために、コントローラは、コントローラに設定された IPv4 仮想アドレスに基づいて IPv6 仮想アドレスを自動的に作成します。仮想 IPv6 アドレスは、[::ffff:<仮想 IPv4 アドレス>] という表記法に従います。たとえば、仮想 IP アドレス 192.0.2.1 は、[::ffff:192.0.2.1] に変換されます。IPv6 キャプティブ ポータルが表示されるためには、ユーザは、DNSv6（AAAA）レコードを返す、IPv6 に解決できる DNS エントリ（ipv6.google.com など）を要求する必要があります。

ポリシーの適用とクォータの管理

クライアントの継続的なセッションを中断することなく、Platinum、Gold、Bronze、または Silver、および 802.11 クライアントのアップストリームとダウンストリームの TCP または UDP データ レートを含む動的な QoS ポリシーをシームレスに適用できます。これにより、クライアントとネットワークの関連付けを解除する必要がなくなります。この機能は、すべての認証方式（802.1 X、PSK、Web 認証など）でサポートされています。

AP は、帯域幅の使用状況を含むクライアントの統計情報を定期的にコントローラに送信します。クライアントのデータの使用率を含む中間アカウンティング メッセージは、設定された間隔で AAA サーバに送信されます。AAA サーバは、各クライアントのデータ使用に関する情報を蓄積し、クライアントがデータの上限量を使い果たした場合、認可変更（CoA）メッセージをコントローラに送信します。CoA ハンドシェイクに成功すると、コントローラは新しいポリシーを適用して、AP に送信します。

ポリシーの適用とクォータの管理の制約事項

- 次のモードがサポートされています。
  - 中央スイッチング、ローカルおよびブリッジ モード
  - ローカル スイッチング Flexconnect および Flex + ブリッジ モード
- この機能は、Cisco ISE ではサポートされていません。

クォータの管理とポリシーの適用の設定（GUI）

手順

ステップ 1 **[WLANs]** > **[WLAN ID]** > **[Advanced]** タブを選択します。

ステップ 2 [Allow AAA Override] チェックボックスをオンにして、AAA オーバーライドを有効にします。

ステップ 3 **[Security]** > **[RADIUS]** > **[Authentication]** タブを選択します。

[New] をクリックして新しい RADIUS サーバを追加するか、既存のサーバの [Server Index] をクリックします。

ステップ 4 [Server Status] ドロップダウン リストから [Enabled] を選択してこの RADIUS サーバを有効にするか、[Disabled] を選択して無効にします。

デフォルト値はイネーブルです。

ステップ 5 [Support for CoA] ドロップダウン リストから [Enable] を選択します。

ステップ 6 設定を保存します。

コントローラでのクォータの管理とポリシーの適用の表示（CLI）

手順

- 次のコマンドを入力して、MAC アドレスを使用しているクライアントの詳細を表示します。

  show client detail *client-mac-addr*

コントローラでのクォータの管理とポリシーの適用のデバッグ（CLI）

手順

- このコマンドを入力して AAA イベントをデバッグします。

  debug aaa events {**enable | disable**}

- このコマンドを入力して、AAA の詳細をデバッグします。

  Debug aaa detail {**enable | disable**}

- 次のコマンドを入力して、クライアントの MAC アドレスでクライアントをデバッグします。

  debug client *client-mac-addr*

AP でのクォータの管理とポリシーの適用の表示（CLI）

手順

- 次のコマンドを入力して、FlexConnect クライアントの AAA オーバーライド ステータスを表示します。

  show flexconnect client aaa-override

- 次のコマンドを入力して、レート制限値を表示します。

  show rate-limit {**bssid | client | wlan**}

AP でのクォータの管理とポリシーの適用のデバッグ（CLI）

手順

- 次のコマンドを入力して、CAPWAP クライアント ペイロードをデバッグします。

  debug capwap client payload

- このコマンドを入力して 802.11 クライアントをデバッグします。

  debug dot11 client