ISEを使用したWLCでのFlexConnect APによるCWAの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[ネットワーク図](#)
[WLC の設定](#)
[ISE の設定](#)
[許可プロファイルの作成](#)
[認証ルールの作成](#)
[許可ルールの作成](#)
[IP 更新の有効化（オプション）](#)
[Traffic flow](#)
[確認](#)

概要

このドキュメントでは、ローカル スイッチング モードで Identity Services Engine（ISE）を搭載したワイヤレス LAN コントローラ（WLC）上の FlexConnect アクセス ポイント（AP）を使用した中央 Web 認証を設定する方法について説明します。

重要な注：現時点では、このシナリオではFlexAPでのローカル認証はサポートされていません。

このシリーズの他のドキュメント

- [スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例](#)
- [WLC と ISE での中央 Web 認証の設定例](#)

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine（ISE）リリース 1.2.1
- ワイヤレス LAN コントローラ ソフトウェア リリース バージョン 7.4.100.0

設定

ワイヤレス LAN コントローラ（WLC）の中央 Web 認証を設定するには複数の方法があります。最初の方法は、ローカル Web 認証です。この認証では、WLC で HTTP トラフィックを内部サーバまたは外部サーバにリダイレクトし、そこでユーザは認証のための入力を求められます。WLC では、次にクレデンシャル（資格情報）を取得して（外部サーバの場合は HTTP GET リクエストによって送り返される）、RADIUS 認証を行います。ゲストユーザの場合は、外部サーバ(Identity Service Engine(ISE)やNACゲストサーバ(NGS)など)が必要です。これは、ポータルがデバイス登録やセルフプロビジョニングなどの機能を提供するためです。このプロセスには、次のステップがあります。

1. ユーザが Web 認証 SSID に関連付けられます。
2. ユーザが自分のブラウザを開きます。
3. URL を入力するとすぐに、WLC によってゲスト ポータル（ISE や NGS など）にリダイレクトされます。
4. ポータルで認証します。
5. ゲスト ポータルは WLC にリダイレクトして入力されたクレデンシャルを戻します。
6. WLC で、RADIUS によってゲスト ユーザを認証します。
7. WLC が元の URL にリダイレクトします。

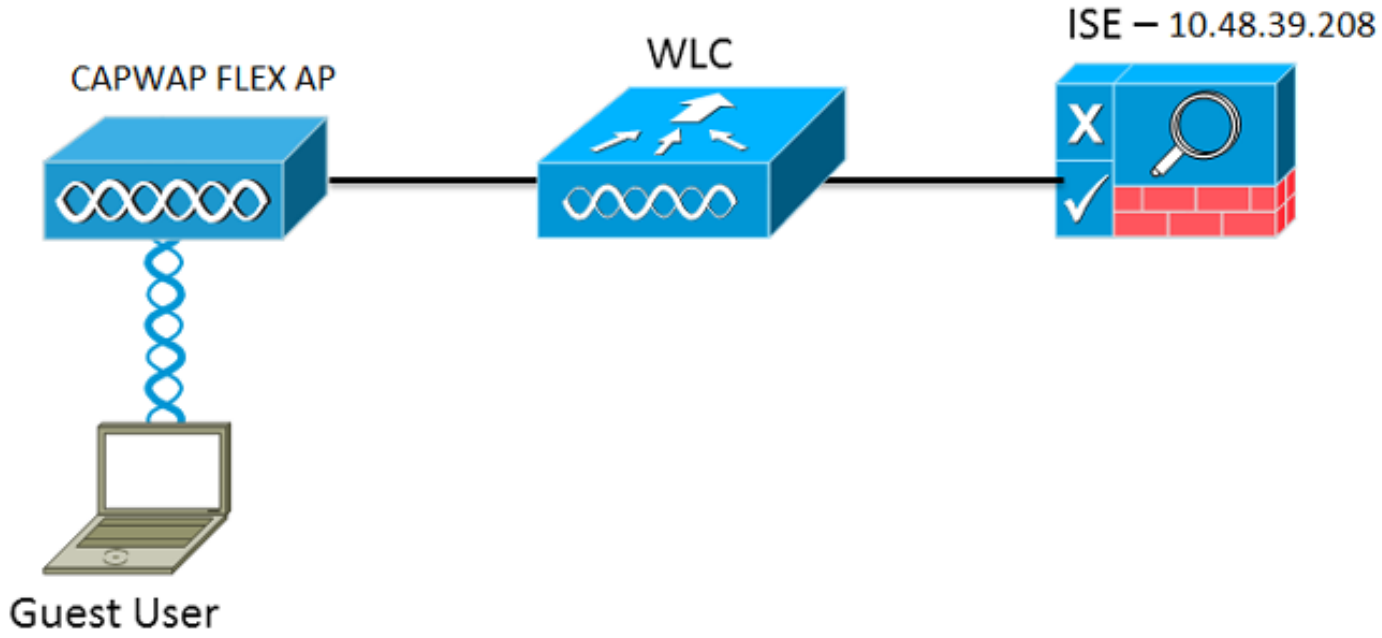
このプロセスには、多くのリダイレクトが含まれています。新しいアプローチは、ISE（1.1 よりも後のバージョン）および WLC（7.2 よりも後のバージョン）で機能する中央 Web 認証を使用することです。このプロセスには、次のステップがあります。

1. ユーザが Web 認証 SSID に関連付けられます。
2. ユーザが自分のブラウザを開きます。
3. WLC はゲストのポータルにリダイレクトします。
4. ポータルで認証します。
5. ISE では、そのユーザが有効であることをコントローラに示すために RADIUS 認可変更（CoA - UDP ポート 1700）を送信し、最後にアクセス コントロール リスト（ACL）などの RADIUS 属性をプッシュします。
6. ユーザは元の URL の再試行を促されます。

この項では、WLC および ISE に中央 Web 認証を設定するために必要な手順について説明します。

ネットワーク図

この設定では、次のネットワーク設定を使用します。

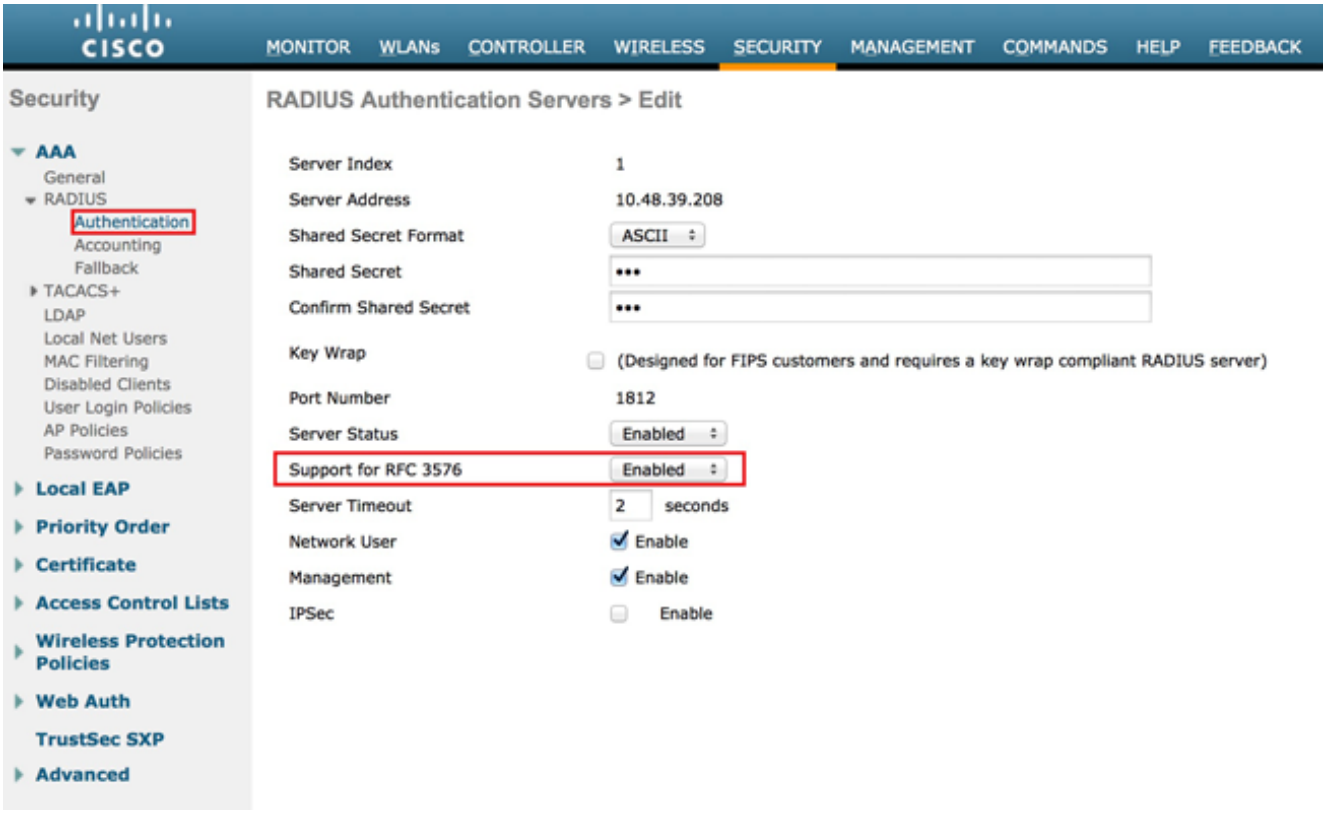


WLC の設定

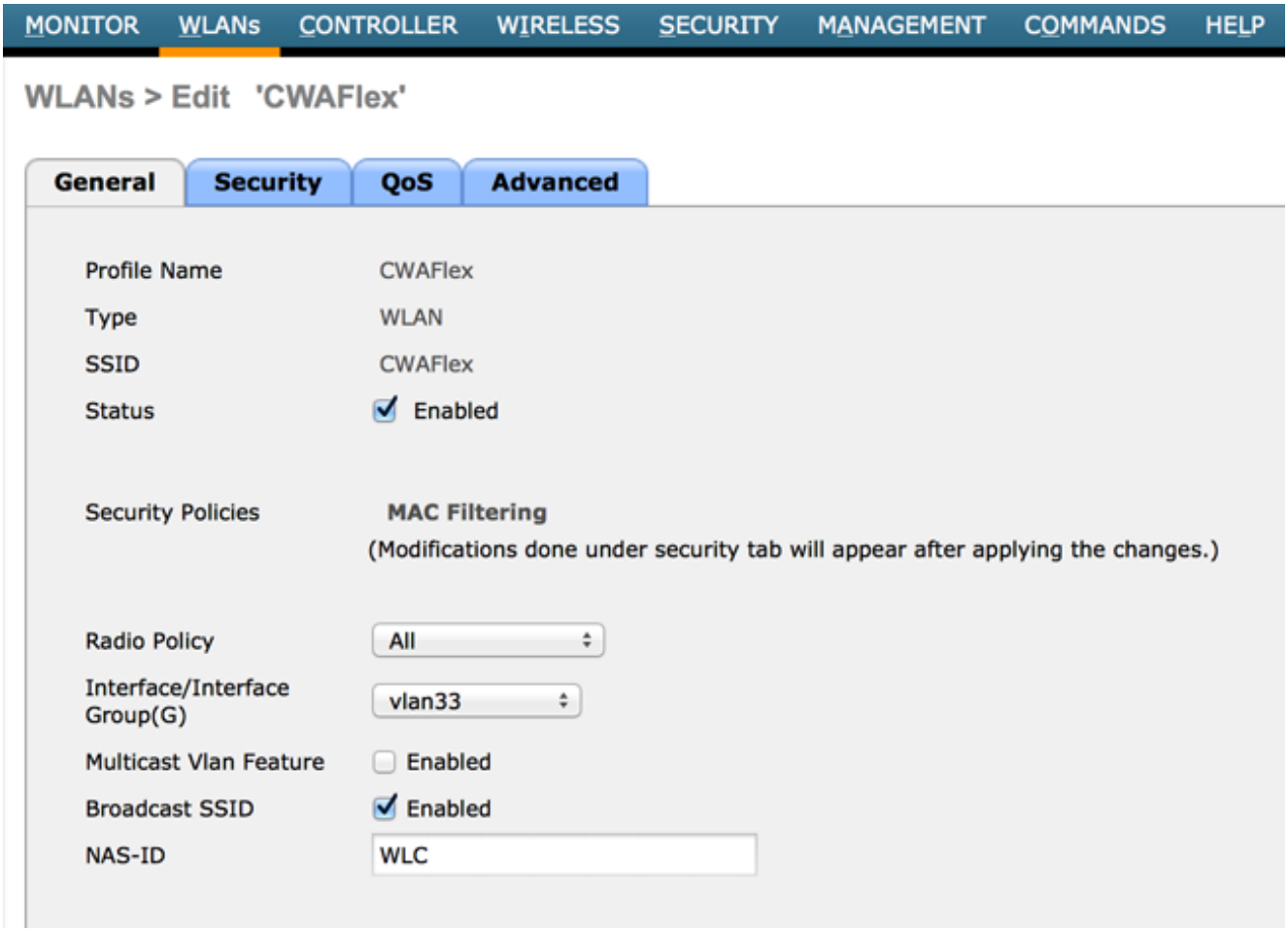
WLC の設定は比較的簡単です。「トリック」は、ISEからダイナミック認証URLを取得するために使用されます (スイッチと同じ) 。 (CoAを使用するため、セッションIDがURLの一部であるため、セッションを作成する必要があります。) MAC フィルタリングを使用するように SSID を設定し、MAC アドレスが見つからない場合でも Access-Accept メッセージを返し、その結果すべてのユーザにリダイレクション URL を送信するように ISE を設定します。

また、RADIUS のネットワーク アドミッション コントロール (NAC) と、AAA オーバーライドを有効にする必要もあります。RADIUS NAC を使用すると、ユーザが認証済みで、ネットワークにアクセスできることを示す CoA 要求を ISE が送信できます。また、RADIUS NAC は、ISE がポスチャ結果に基づいてユーザ プロファイルを変更するポスチャ アセスメントにも使用されます。

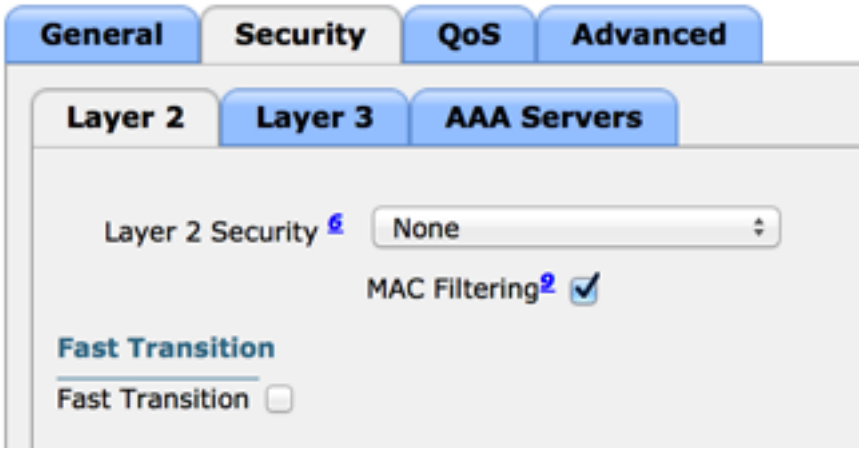
1. RADIUS サーバで RFC3576 (CoA) が有効 (デフォルト) になっていることを確認します。



2. 新規 WLAN を作成してください。次の例では、*CWAFlex*という名前の新しいWLANを作成し、それをvlan33に割り当てます（アクセスポイントがローカルスイッチングモードであるため、大きな影響はありません）。

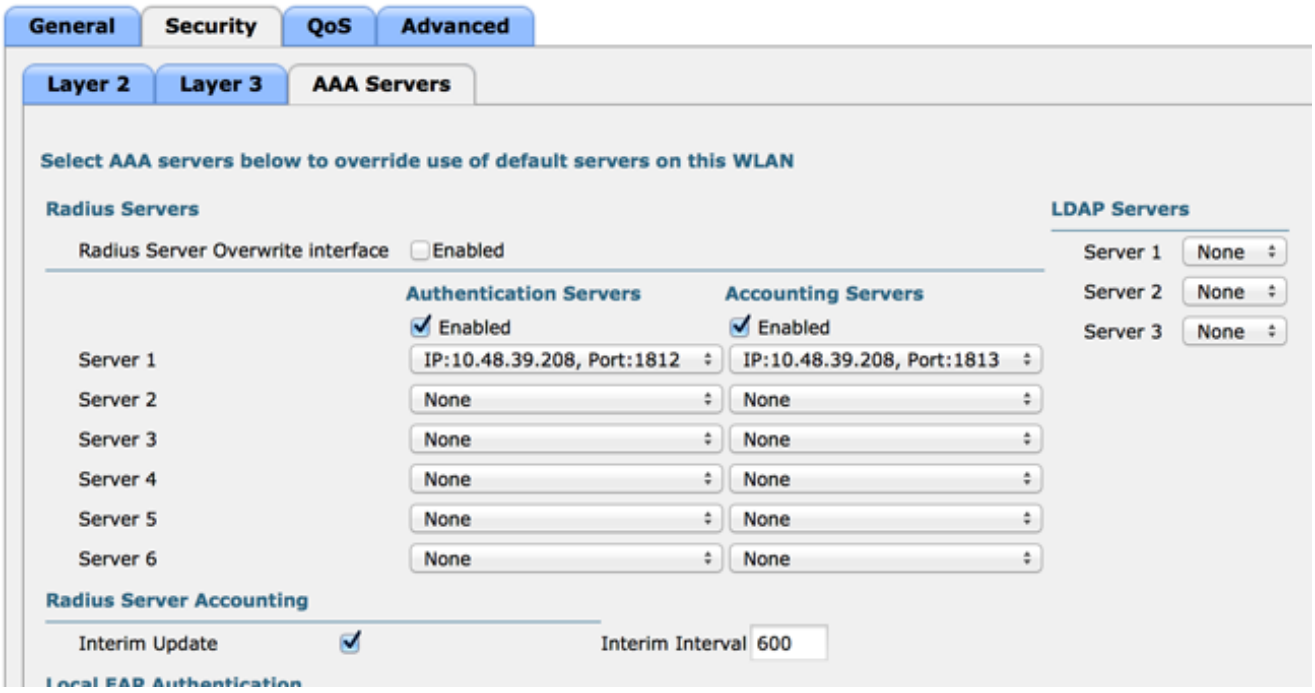


3. [Security] タブで、MAC フィルタリングをレイヤ 2 セキュリティとして有効にします。

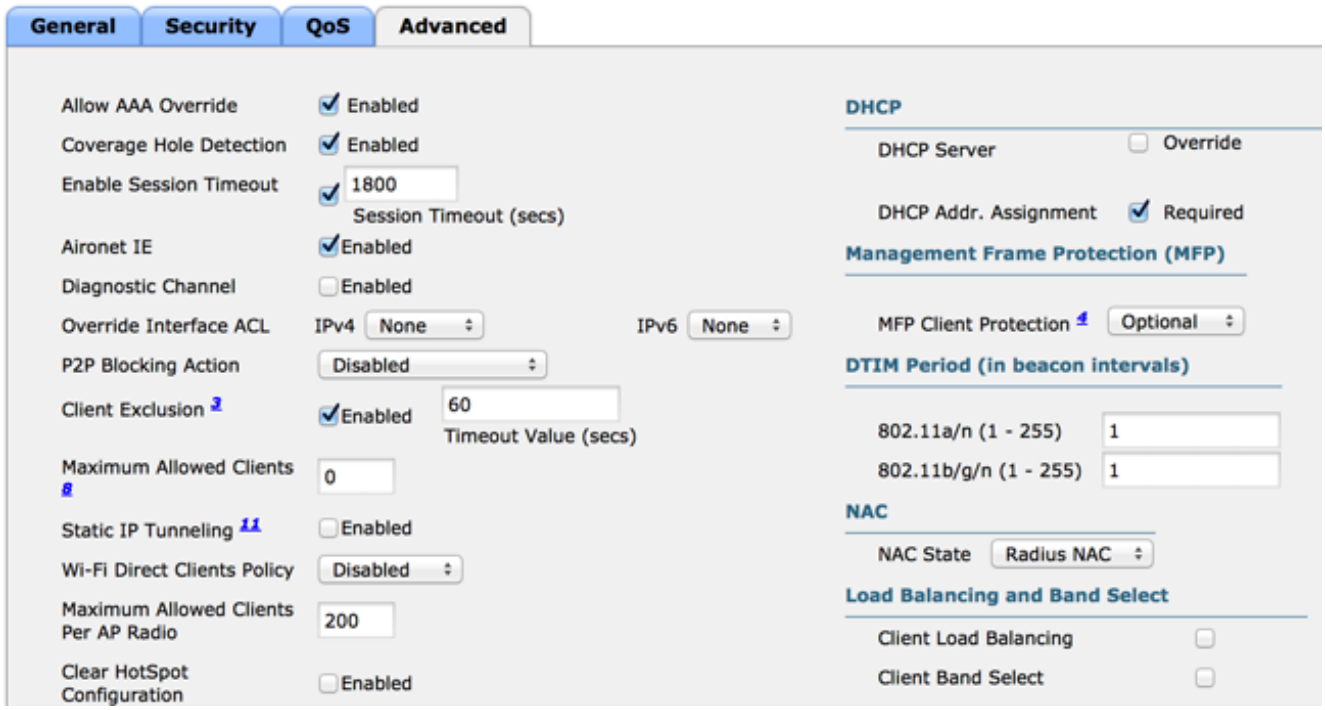


4. [Layer 3] タブで、セキュリティが無効であることを確認します（Web 認証がレイヤ 3 で有効にされると、中央 Web 認証ではなく、ローカル Web 認証が有効になります）。

5. [AAA Servers] タブで、ISE サーバを WLAN の RADIUS サーバとして選択します。オプションで、ISE に関する詳細情報を得るためにアカウンティング用に ISE サーバを選択できます。



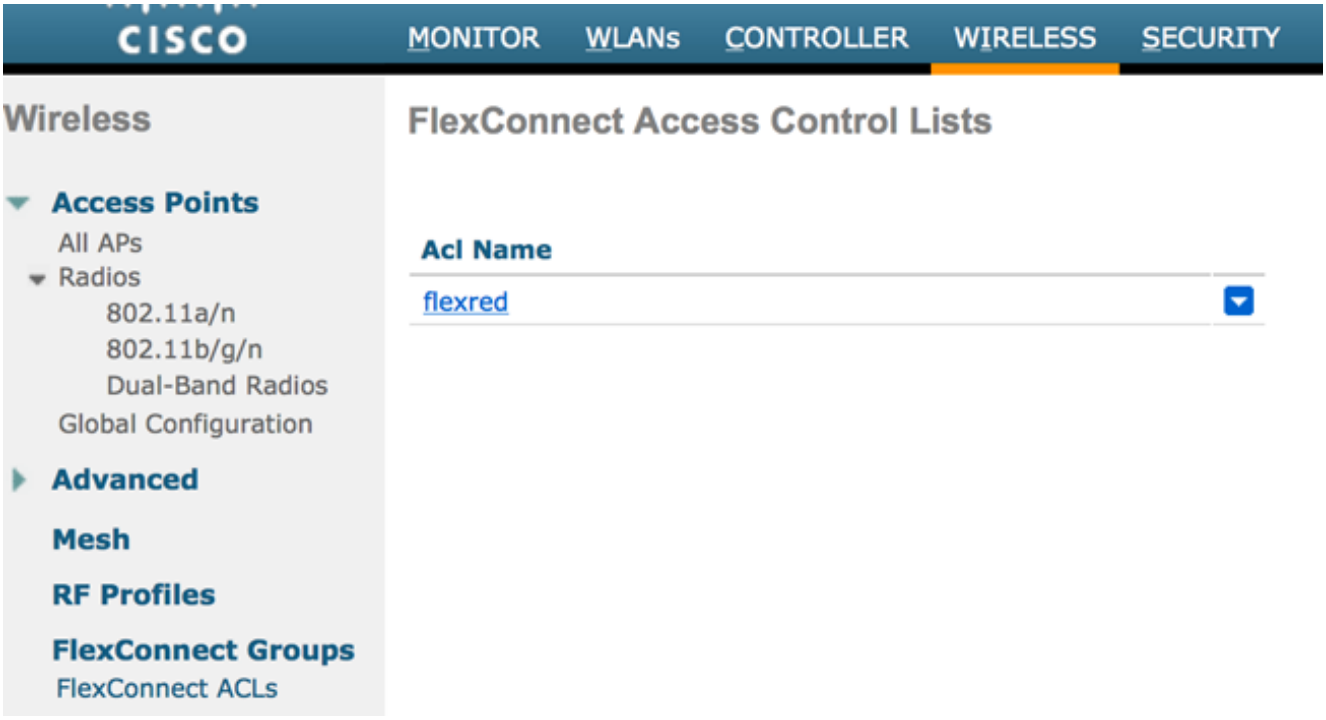
6. [Advanced] タブで、[Allow AAA Override] がオンで [NAC State] に対して [Radius NAC] が選択されていることを確認します。



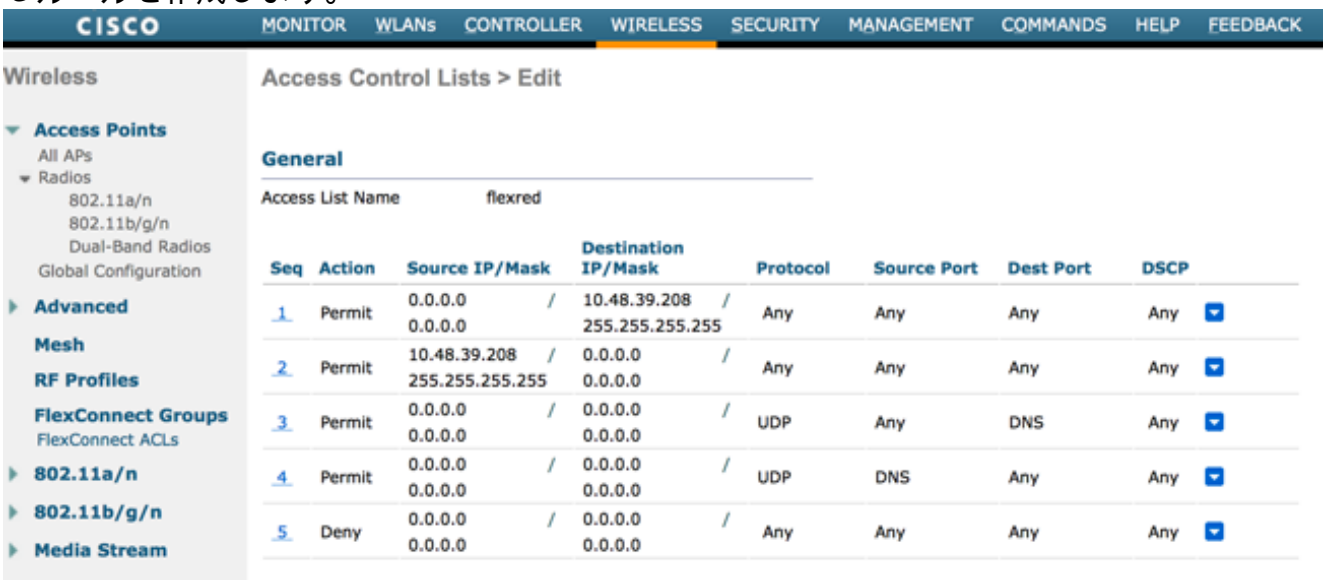
7. リダイレクト ACL を作成します。

この ACL は ISE の Access-Accept メッセージで参照され、リダイレクトすべきトラフィック（ACL によって拒否される）、およびリダイレクトすべきでないトラフィック（ACL によって許可される）を定義します。基本的には、DNS および ISE との間でやり取りされるトラフィックを許可する必要があります。 **注**:FlexConnect APの問題は、通常のACLとは別にFlexConnect ACLを作成する必要があることです。この問題はCisco Bug CSCue68065に記載されており、リリース7.5で修正されています。WLC 7.5以降では、FlexACLのみが必要で、標準ACLは必要ありません。WLC では、ISE によって返されるリダイレクト ACL が標準 ACL であると想定します。ただし、そのように機能することを保証するには、

FlexConnect ACL と同じ ACL が適用される必要があります。
次の例では、flexred という名前の FlexConnect ACL の作成方法を示しています。

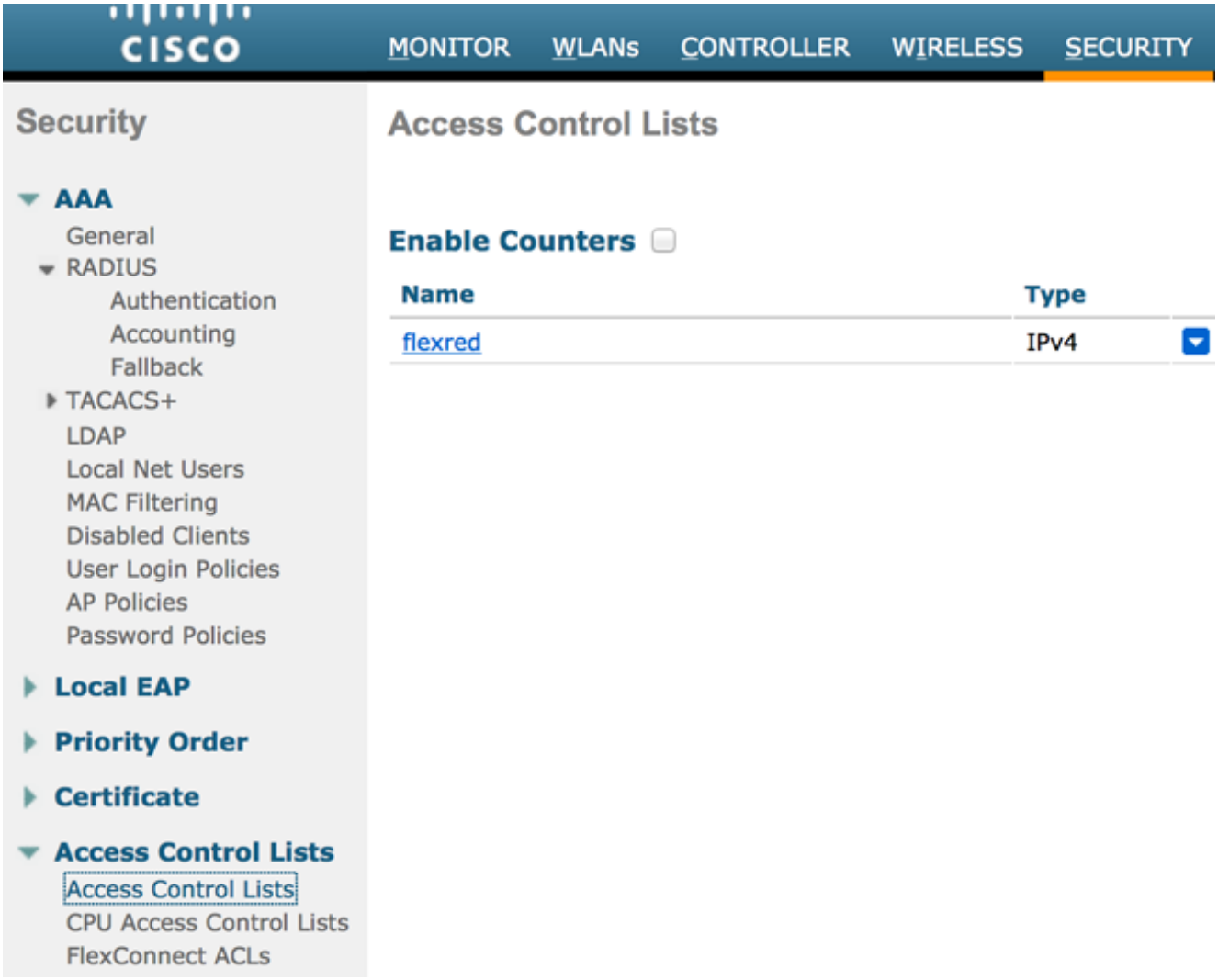


ISE へのトラフィックと同様に DNS トラフィックを許可し、残りのトラフィックを拒否するルールを作成します。



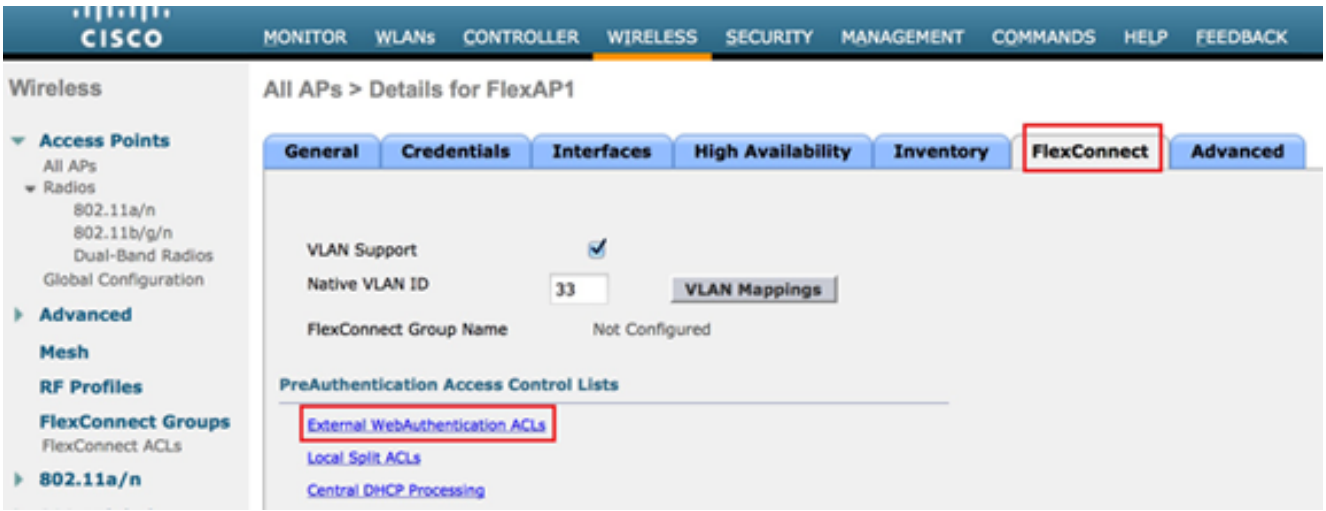
最大限のセキュリティが必要な場合は、ISEに対してポート8443のみを許可できます（ポスチャリングを行う場合は、8905,8906,8909,8910などの一般的なポスチャポートを追加する必要があります）。

（CSCue68065 が原因でバージョン 7.5 よりも前のコードについてのみ）[Security] > [Access Control Lists] を選択して、同じ名前の同一の ACL を作成します。



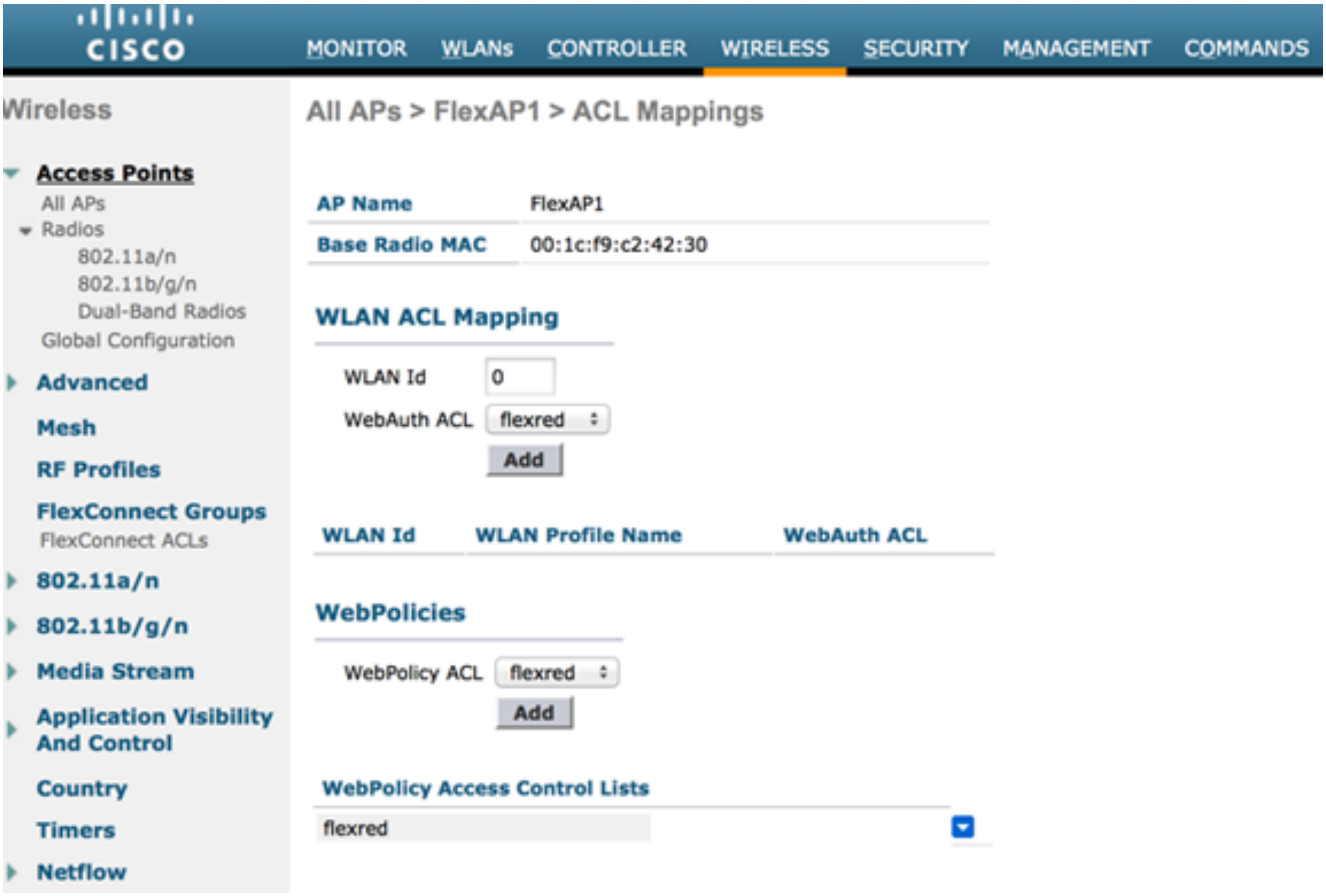
特定の FlexConnect AP を用意します。より大規模な導入の場合、通常は FlexConnect グループを使用し、拡張性の理由から、次の項目を AP 単位で実行しないことに注意してください。

[Wireless] をクリックして、特定のアクセス ポイントを選択します。[FlexConnect] **タブをクリックし、[External Webauthentication ACLs]** をクリックします（バージョン 7.4 よりも前は、このオプションの名前は *web policies* でした）。



Web ポリシー領域に ACL（この例では *flexred という名前*）を追加します。これにより、こ

の ACL がアクセス ポイントに事前にプッシュされます。この ACL はまだ適用されていませんが、必要な場合に適用できるように、ACL の内容が AP に提供されます。



WLC の設定はこれで完了しました。

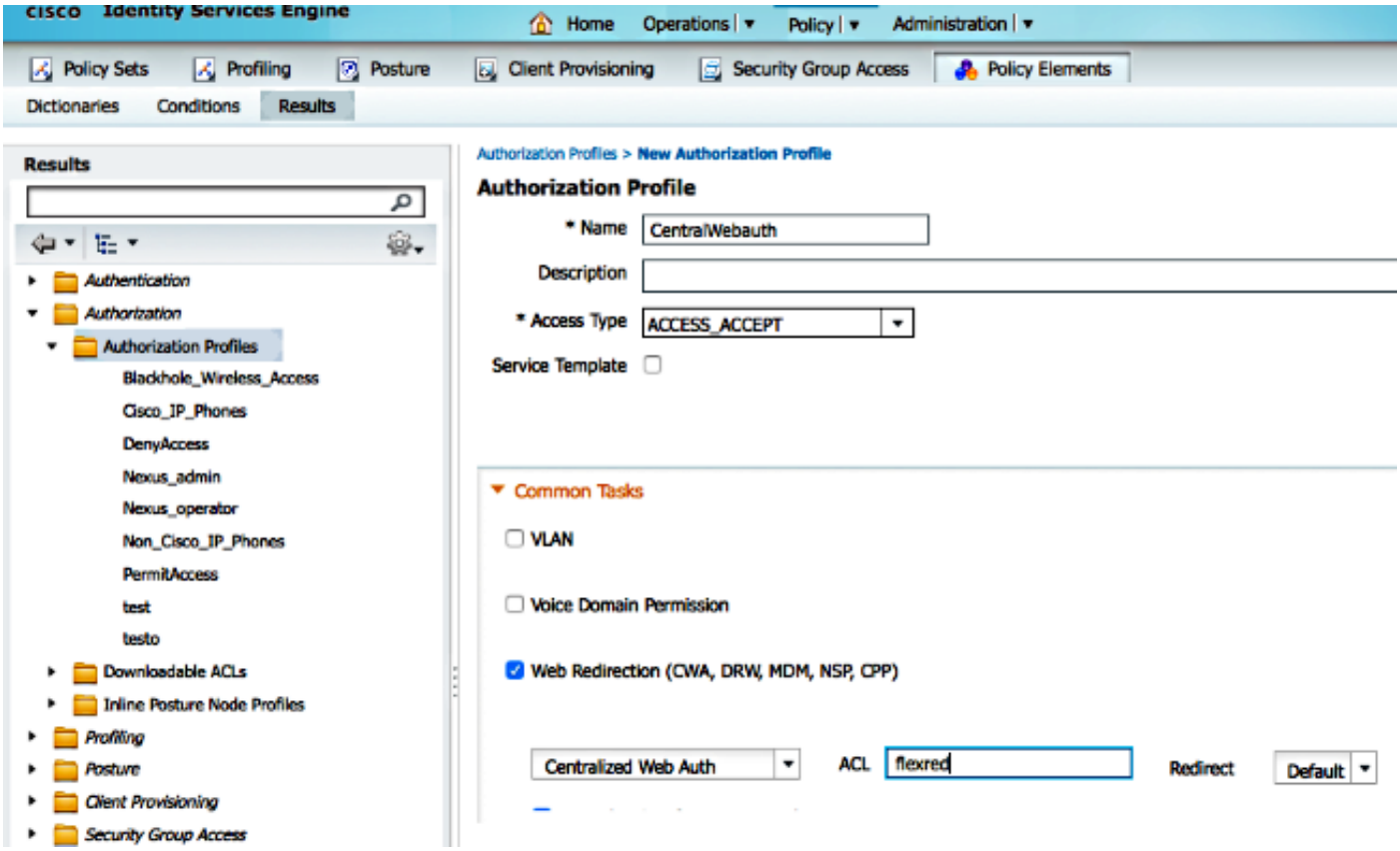
ISE の設定

許可プロファイルの作成

許可プロファイルを作成するには、次の手順を実行します。

1. [Policy] をクリックして、[Policy Elements] をクリックします。
2. [Results] をクリックします。
3. [Authorization] を展開して、[Authorization profile] をクリックします。
4. [Add] ボタンをクリックして、中央 webauth の新しい許可プロファイルを作成します。
5. [Name] フィールドに、プロファイルの名前を入力します。この例では「*CentralWebauth*」という名前を使用します。
6. [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。
7. [Web Authentication] **チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。**
8. [ACL] フィールドに、リダイレクトされるトラフィックを定義する WLC 上の ACL の名前を入力します。この例では、*flexred* を使用します。
9. [Redirect] ドロップダウン リストで [Default] を選択します。

[Redirect] 属性は、ISE がデフォルトの Web ポータルと ISE 管理者が作成したカスタム Web ポータルのいずれを参照するかを定義します。たとえば、この例の *flexred ACL* では、*クライアントから任意の宛先への HTTP トラフィックのリダイレクトをトリガーします。*

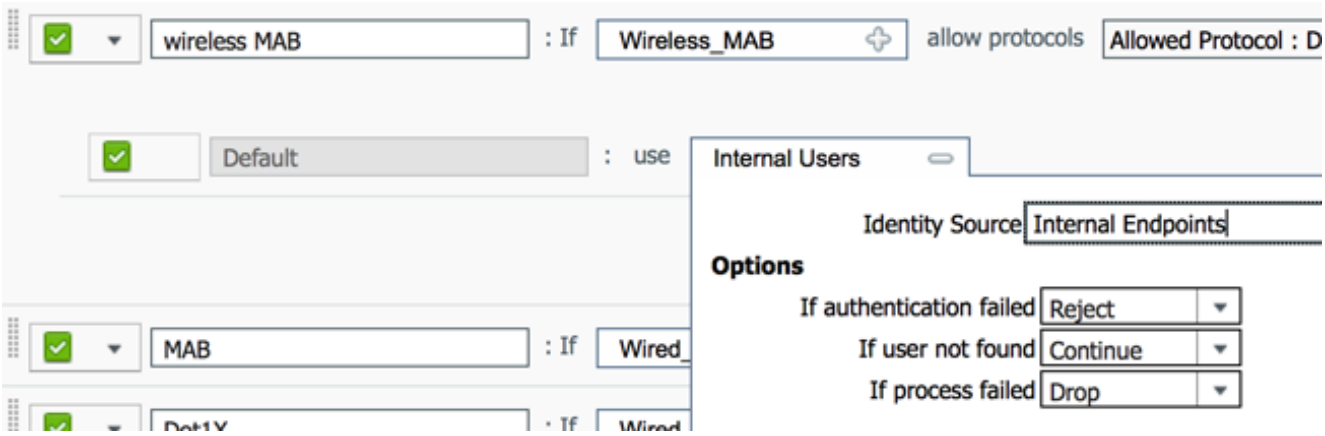


認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順を実行します。

1. [Policy] メニューで [Authentication] をクリックします。 この図は、認証ポリシー ルールの設定方法の例を示します。この例では、MAC フィルタリングの検出時にトリガーされるルールが設定されています。

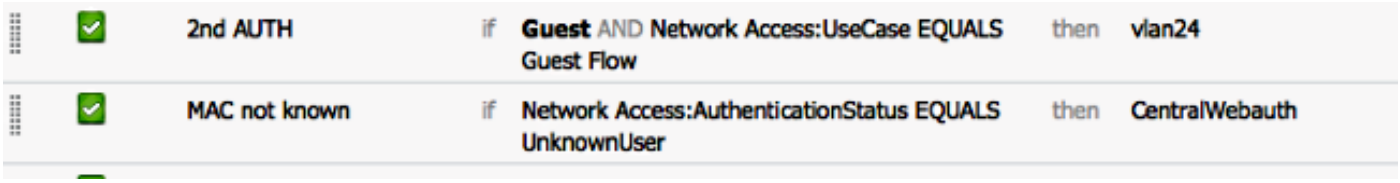
2. 認証ルールの名前を入力します。この例では *Wireless mab* を使用しています。
3. [If] 条件フィールドで、プラス ([+]) アイコンをクリックします。
4. [Compound condition] を選択してから、[Wireless_MAB] を選択します。
5. 許可されるプロトコルとして [Default network access] を選択します。
6. ルールをさらに展開するには、[and ...] **の横にある矢印をクリックします。**
7. [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。
8. [If user not found] ドロップダウン リストから [Continue] を選択します。



このオプションにより、MAC アドレスが不明な場合でも、webauth によってデバイスが認証済みとなります。Dot1x クライアントはクレデンシャルを使用して認証できるので、この設定で考慮する必要はありません。

許可ルールの作成

ここでは、許可ポリシーでいくつかのルールを設定します。PCが関連付けられると、MACフィルタリングが実行されます。MACアドレスが不明であると想定され、webauthとACLが返されます。この [MAC not known] *のルールは、次の画像に示され、このセクションで設定されます。*



許可ルールを作成するには、次の手順を実行します。

1. 新しいルールを作成し、名前を入力します。この例では、「*MAC not known*」という名前を使用します。
2. 条件フィールドでプラス ([+]) アイコンをクリックして、新しい条件を作成します。
3. [expression] ドロップダウン リストを展開します。
4. [Network Access] を選択し、展開します。
5. [AuthenticationStatus] をクリックし、[Equals] 演算子を選択します。
6. 右側のフィールドで [UnknownUser] を選択します。
7. [General Authorization] ページの [then] という単語の右側のフィールドで、[CentralWebauth] (**許可プロファイル**) を選択します。この手順により、ユーザ (または MAC アドレス) が不明でも、ISE を続行することができます。不明なユーザには、ここで [Login] ページが表示されます。ただし、ユーザがクレデンシャルを入力すると、ISEで認証要求が再度表示されます。したがって、ユーザがゲストユーザの場合に満たす条件を使用して、別のルールを設定する必要があります。この例では、[If UseridentityGroup equals Guest] を使用し、すべてのゲストがこのグループに属すると想定されています。
8. [MAC not known] ルールの末尾にあるアクション ボタンをクリックして、上で説明した新しいルールを挿入します。**注：この**新しいルールは、*MAC not known*ルールの前に来ることが非常に重要です。

9. 名前フィールドに、「**2nd AUTH**」と入力します。
10. 条件として ID グループを選択します。この例では、[Guest] を選択します。

11. 条件フィールドでプラス ([+]) アイコンをクリックして、新しい条件を作成します。

12. [Network Access] を選択し、[UseCase] をクリックします。

13. 演算子として [Equals] を選択します。

14. 右のオペランドとして [GuestFlow] を選択します。これは、Web ページでログインしたばかりで、認可変更 (ルールのゲスト フローの部分) の後に戻ってきたユーザを捕捉することを意味し、これはゲスト ID グループに属している場合にのみ実行されます。

15. 許可ページで [then] の隣にあるプラス ([+]) アイコンをクリックし、ルールの結果を選択します。

    この例では、事前設定されたプロファイル(vlan34)が割り当てられています。この設定は、このドキュメントでは示されていません。

    [Permit Access] オプションを選択するか、カスタム プロファイルを作成し、VLAN または任意の属性に戻ることができます。

重要な注意：ISEバージョン1.3では、Web認証のタイプによっては、「ゲストフロー」ユースケースが発生しない場合があります。この場合、認可ルールには、唯一の使用可能な条件としてゲスト ユーザ グループを含める必要があります。

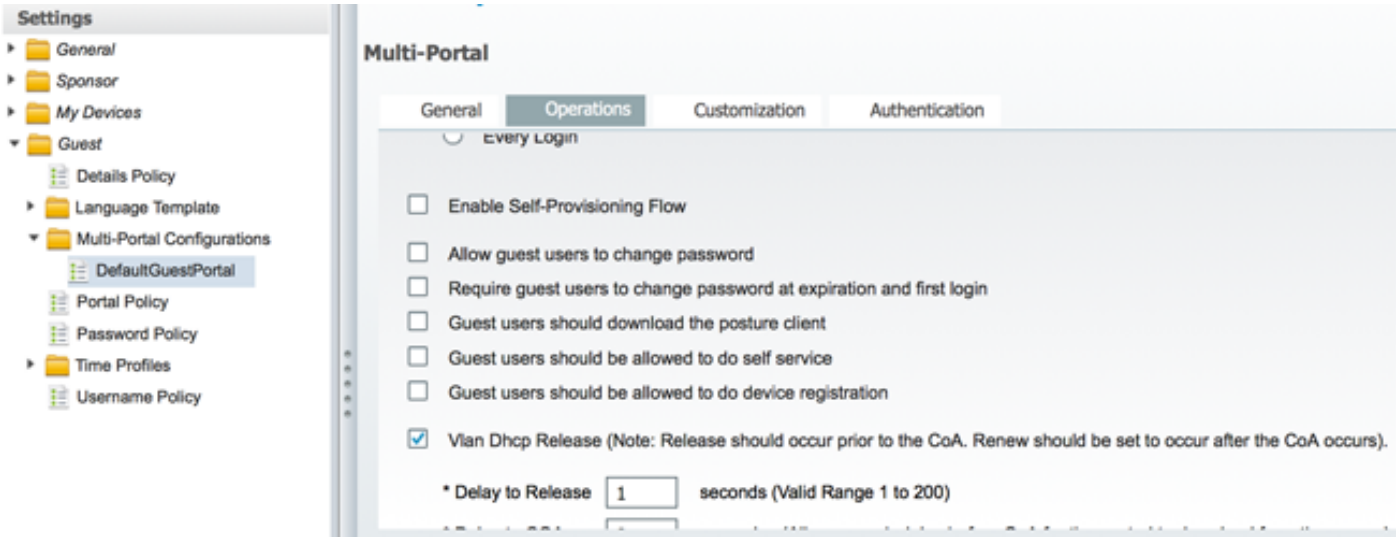
IP 更新の有効化 (オプション)

VLAN を割り当てる場合、最後のステップとして、クライアント PC 用の IP アドレスを更新します。このステップは、Windows クライアント用のゲスト ポータルによって実行できます。前の手順で、*2nd AUTH* ルールに VLAN を設定していない場合は、このステップを省略できます。

FlexConnect AP では、VLAN が AP 自体に事前に存在している必要があることに注意してください。したがって、VLAN が事前に存在しない場合、AP 自体、または作成する新規 VLAN に ACL をなにも適用しない Flex グループに VLAN-ACL マッピングを作成することができます。これにより、VLAN が実際に作成されます (その VLAN に ACL なしで) 。

VLAN を割り当てた場合は、次の手順を実行し、IP 更新を有効にします。

1. [Administration] をクリックして、[Guest Management] をクリックします。
2. [Setting] をクリックします。
3. [Guest] を展開してから、[Multi-Portal Configuration] を展開します。
4. [DefaultGuestPortal] または作成したカスタム ポータルの名前をクリックします。
5. [VLAN DHCP Release] **チェックボックスをオンにします。注：このオプション**は、Windowsクライアントに対してのみ機能します。



Traffic flow

このシナリオでは、どのトラフィックがどこに送信されるかを理解することが難しいように思われる可能性があります。再確認のために以下に簡単にまとめます。

- クライアントが無線で SSID のアソシエーション要求を送信します。
- WLC が ISE を使用して MAC フィルタリング認証を処理します（WLC がリダイレクト属性を受信する場合）。
- クライアントが、MAC フィルタリングの完了後にアソシエーション応答を受信します。
- クライアントがDHCP要求を送信し、DHCP要求が **ローカル** リモートサイトのIPアドレスを取得するために、アクセスポイントによってスイッチングされます。
- Central_webauth状態では、リダイレクトACLで拒否するようにマークされたトラフィック（HTTPが一般的）は次のとおりです。 **中心に** 交換された.したがって、リダイレクションを実行するのはAPではなくWLCです。たとえば、クライアントからWebサイトを要求されると、APはCAPWAPにカプセル化されたWLCにこれを送信し、WLCはそのWebサイトのIPアドレスをスプーフィングしてISEにリダイレクトします。
- クライアントが ISE のリダイレクト URL にリダイレクトされます。これは **ローカル** 再びスイッチされる（FlexRedirect ACLの[permit]にヒットするため）。
- 一度 RUN 状態になると、トラフィックはローカルにスイッチされます。

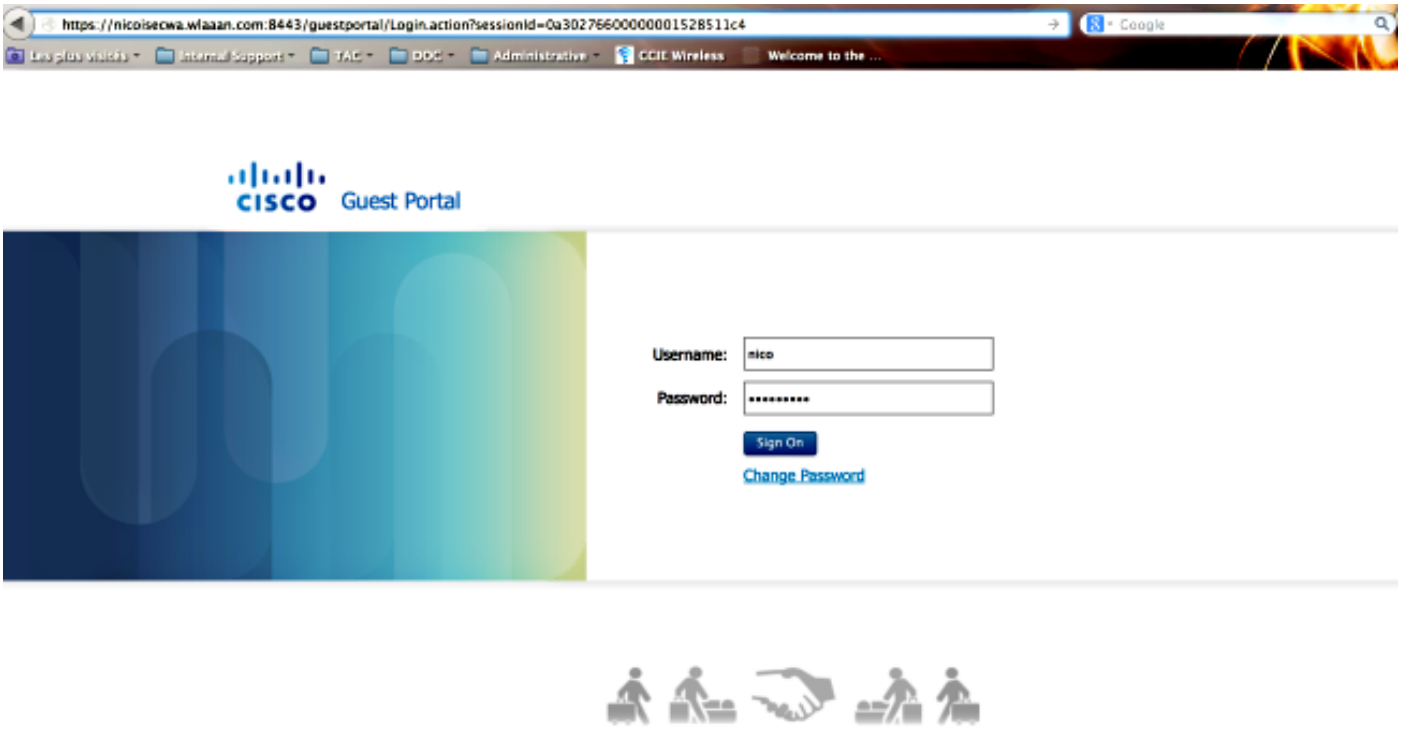
確認

ユーザが SSID に関連付けられると、認可が [ISE] ページに表示されます。

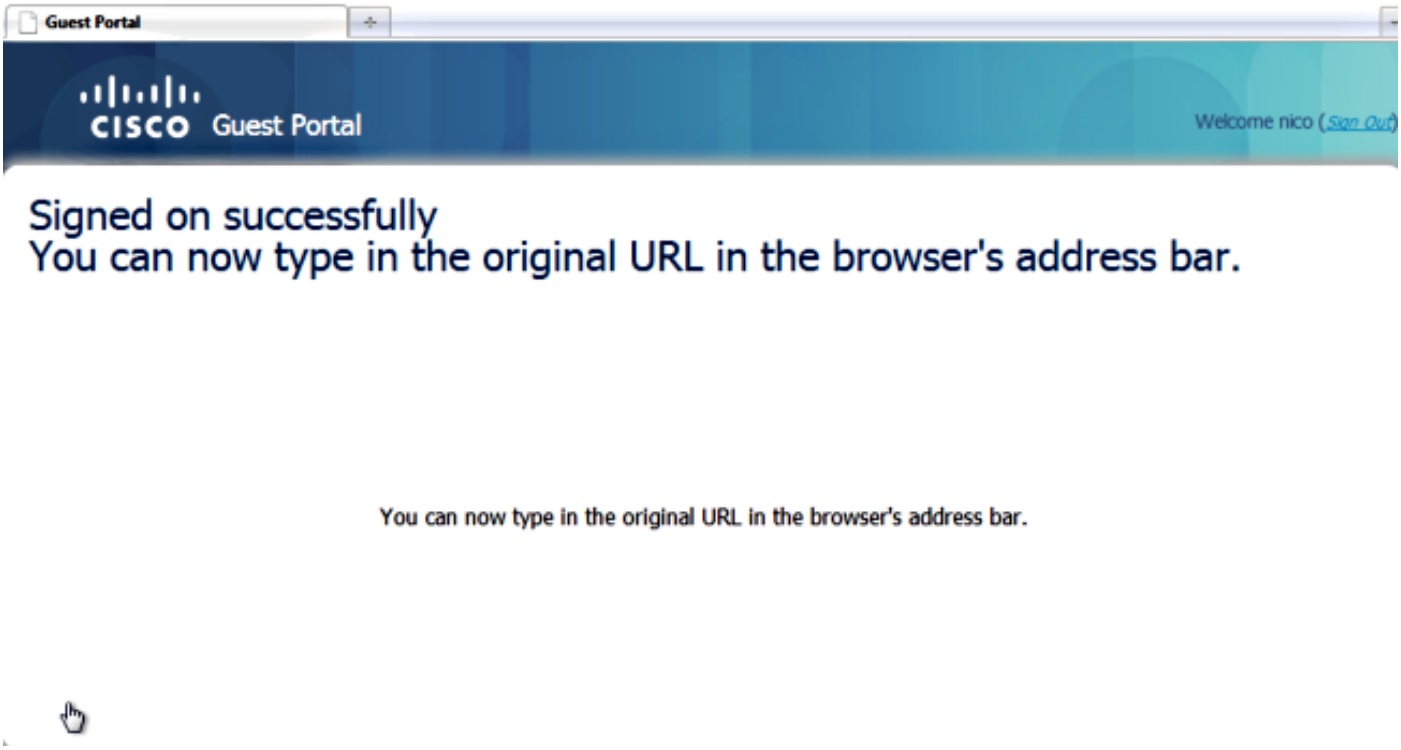
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

CWA 属性を返す MAC アドレスのフィルタリング認証を下から上に確認できます。次にユーザ名を使用したポータルのログインです。その次に、ISE が WLC に CoA を送信し、最後の認証は WLC 側のレイヤ 2 の MAC フィルタリング認証ですが、ISE はクライアントとユーザ名を記憶していて、この例で設定した必要な VLAN を適用します。

クライアントで任意のアドレスを開くと、そのブラウザが ISE にリダイレクトされます。ドメイン ネーム システム（DNS）が正しく設定されていることを確認します。



ユーザがポリシーを受け入れるとネットワーク アクセスが許可されます。



コントローラでは、ポリシー マネージャの状態と RADIUS NAC の状態が *POSTURE_REQD* から *RUN* に変わります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。