

ISEを使用したWLCでのFlexConnect APによるCWAの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[WLC の設定](#)

[ISE 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](#)

[関連情報](#)

はじめに

このドキュメントでは、ローカルスイッチングモードのWLC ISE上のFlexConnect APで中央Web認証を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

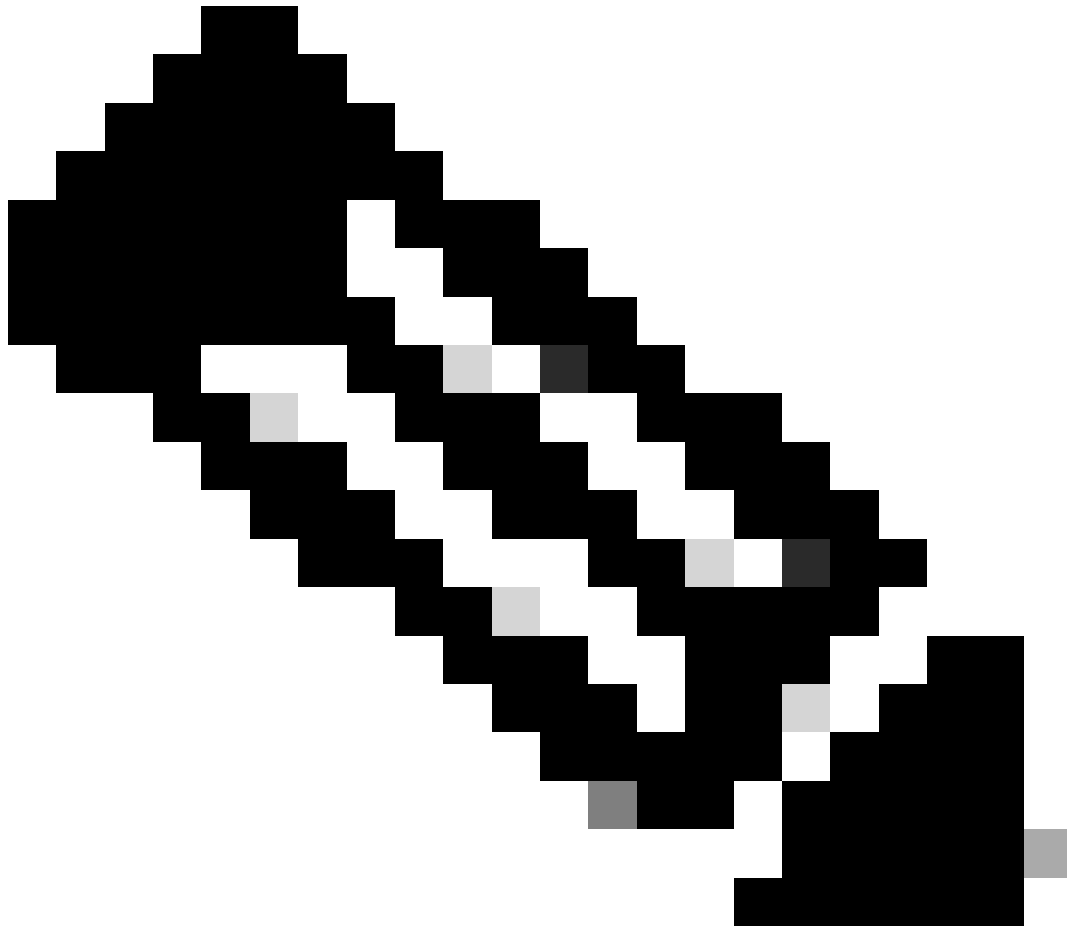
使用するコンポーネント

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(WLC)ソフトウェア、リリースバージョン – 7.4.100.0
- アクセスポイント(AP)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していません。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明



注：現時点では、FlexAPでのローカル認証はこのシナリオで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](#)

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、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、外部サーバ (Identity Service Engine (ISE) または NAC ゲストサーバ (NGS) など) が必要です。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。

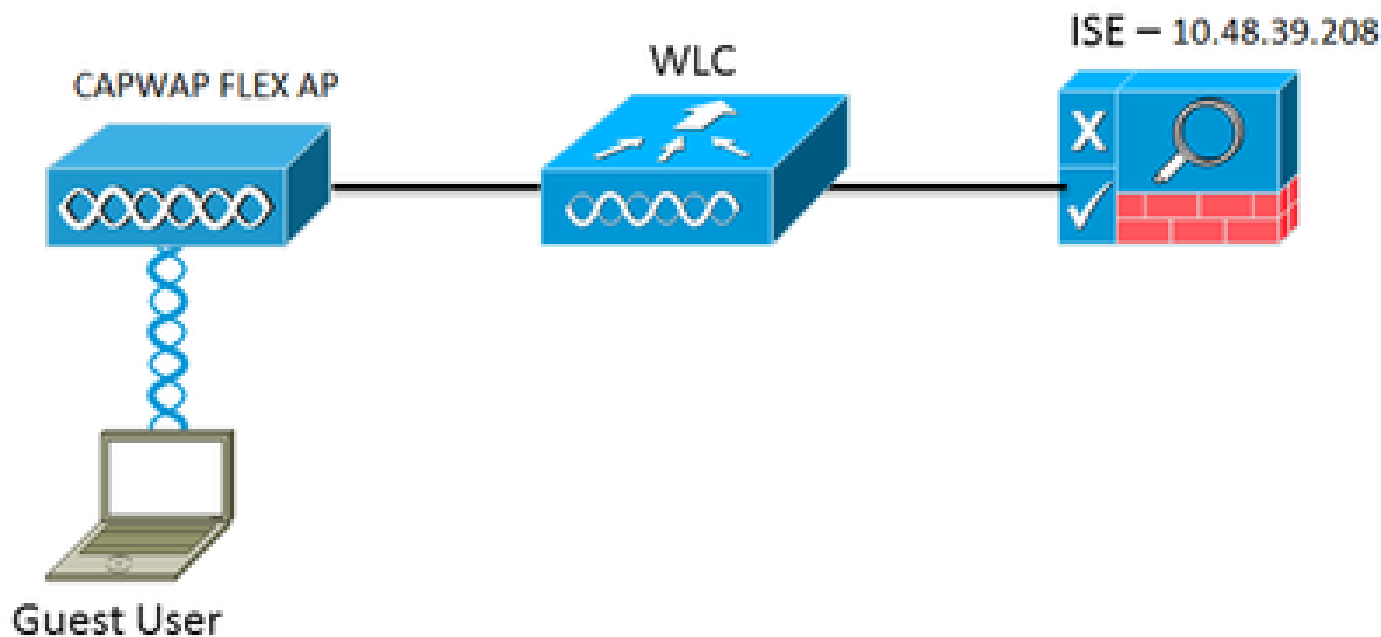
このプロセスには、多くのリダイレクトが含まれています。新しいアプローチは、ISE (1.1 よりも後のバージョン) および WLC (7.2 よりも後のバージョン) で機能する中央 Web 認証を使用することです。このプロセスには、次のステップがあります。

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。



ネットワーク構成

WLC の設定

WLC の設定は比較的簡単です。ISEからダイナミックな認証URLを取得するために、(スイッチ上と同じように) テクニックを使用します (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SSION 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。

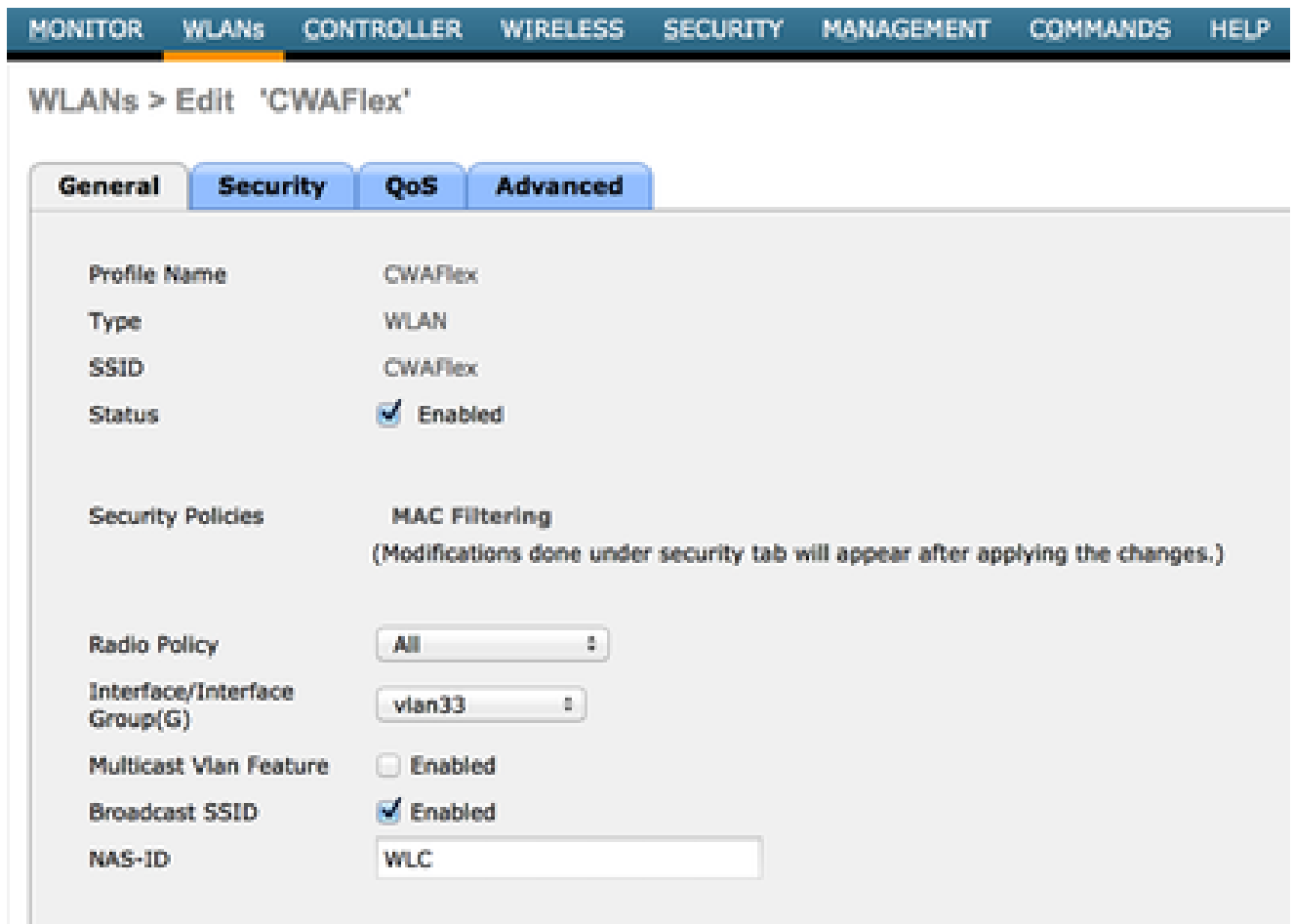
1. RADIUS サーバで RFC3576 (CoA) が有効 (デフォルト) になっていることを確認します

The screenshot shows the Cisco configuration page for RADIUS Authentication Servers. The left sidebar contains a navigation menu with 'Authentication' highlighted under the 'RADIUS' section. The main content area is titled 'RADIUS Authentication Servers > Edit' and lists various configuration parameters:

- Server Index: 1
- Server Address: 10.48.39.208
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled** (highlighted with a red box)
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

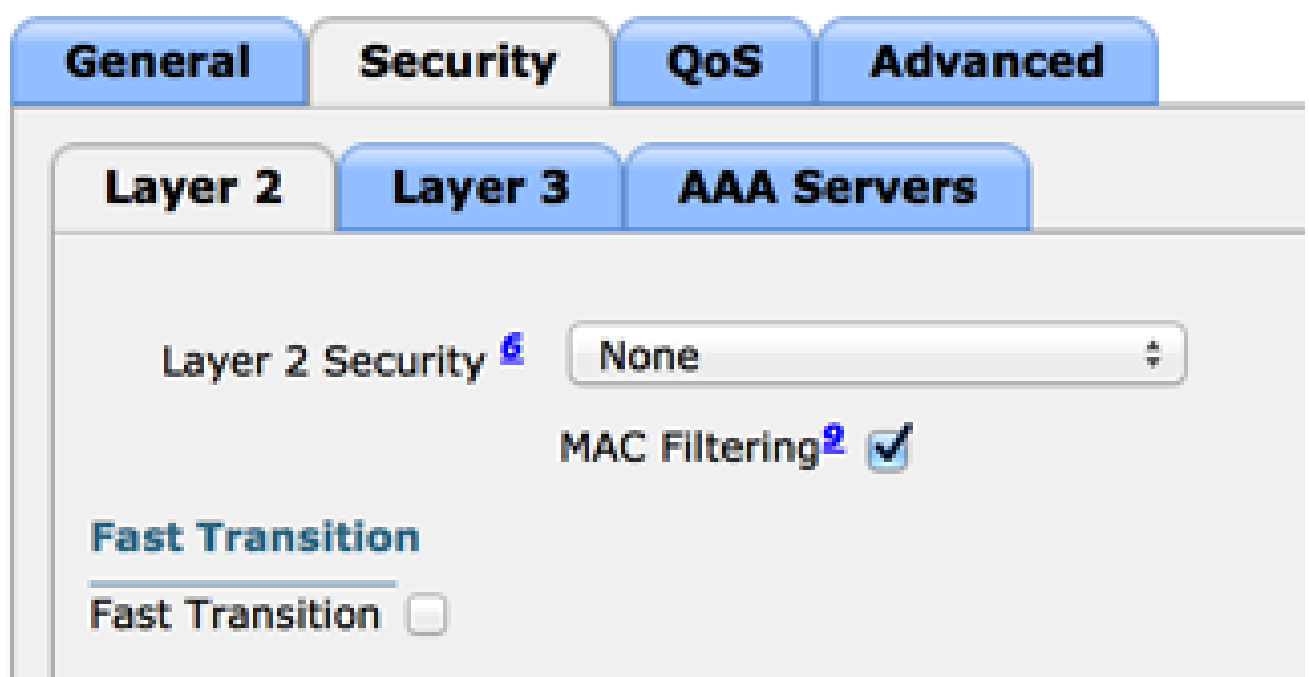
RADIUSサーバにはRFC3576があります

2. 新規 WLAN を作成してください。この例では、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、この設定はあまり効果がないことに注意してください)。



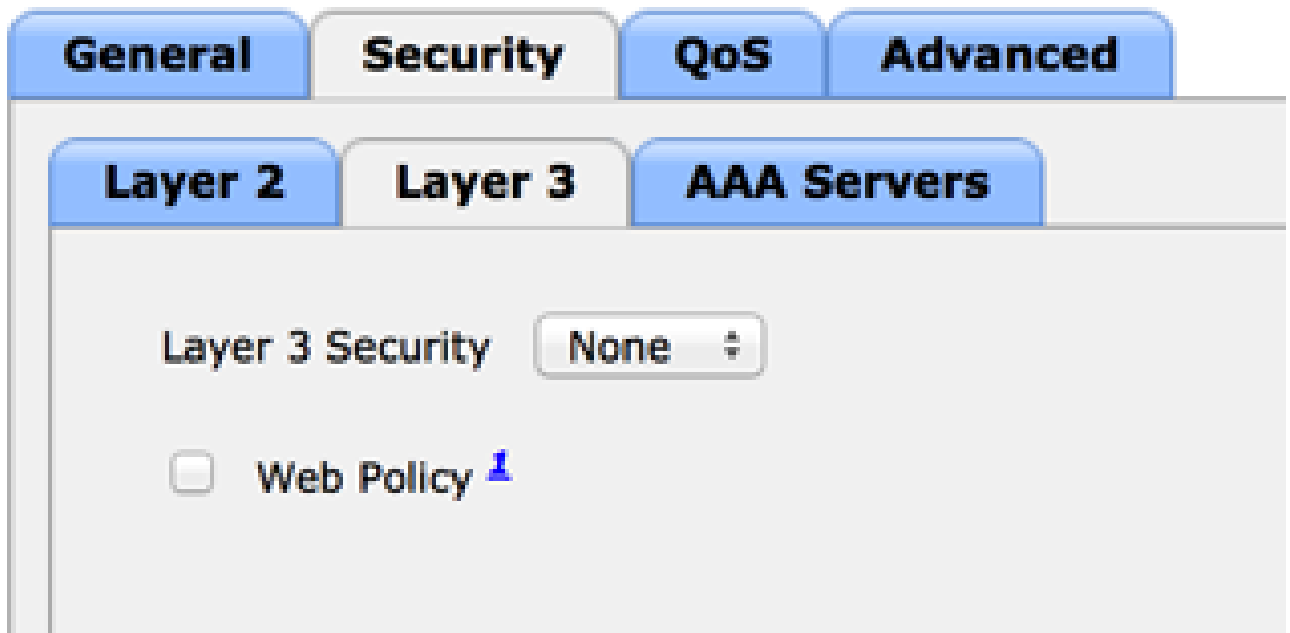
新しいWLANの作成

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。



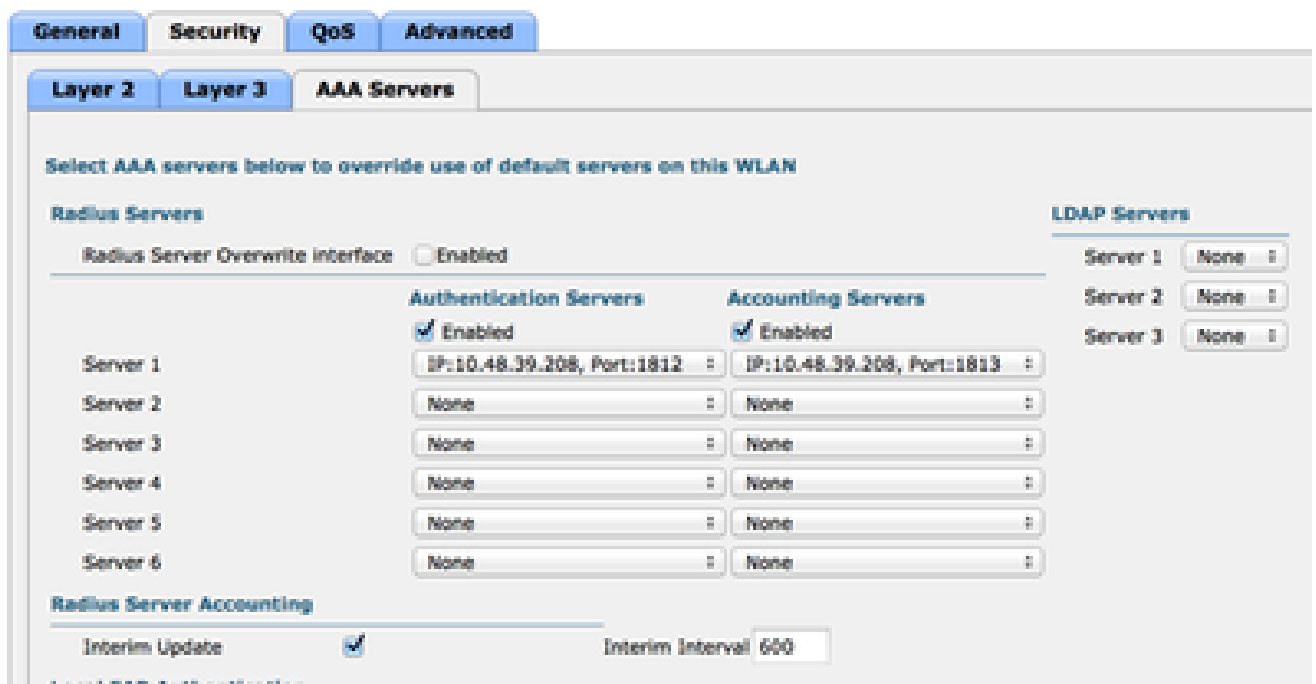
MAC フィルタリングの有効化

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)。



セキュリティが無効になっていることを確認する

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トング用に ISE サーバを選択できます。



ISEサーバの選択

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。

The screenshot shows the 'Advanced' configuration tab with the following settings:

- Allow AAA Override: Enabled
- Coverage Hole Detection: Enabled
- Enable Session Timeout: 1800 (Session Timeout (secs))
- Aironet IE: Enabled
- Diagnostic Channel: Enabled
- Override Interface ACL: IPv4: None, IPv6: None
- P2P Blocking Action: Disabled
- Client Exclusion: Enabled, 60 (Timeout Value (secs))
- Maximum Allowed Clients: 0
- Static IP Tunneling: Enabled
- Wi-Fi Direct Clients Policy: Disabled
- Maximum Allowed Clients Per AP Radio: 200
- Clear HotSpot Configuration: Enabled

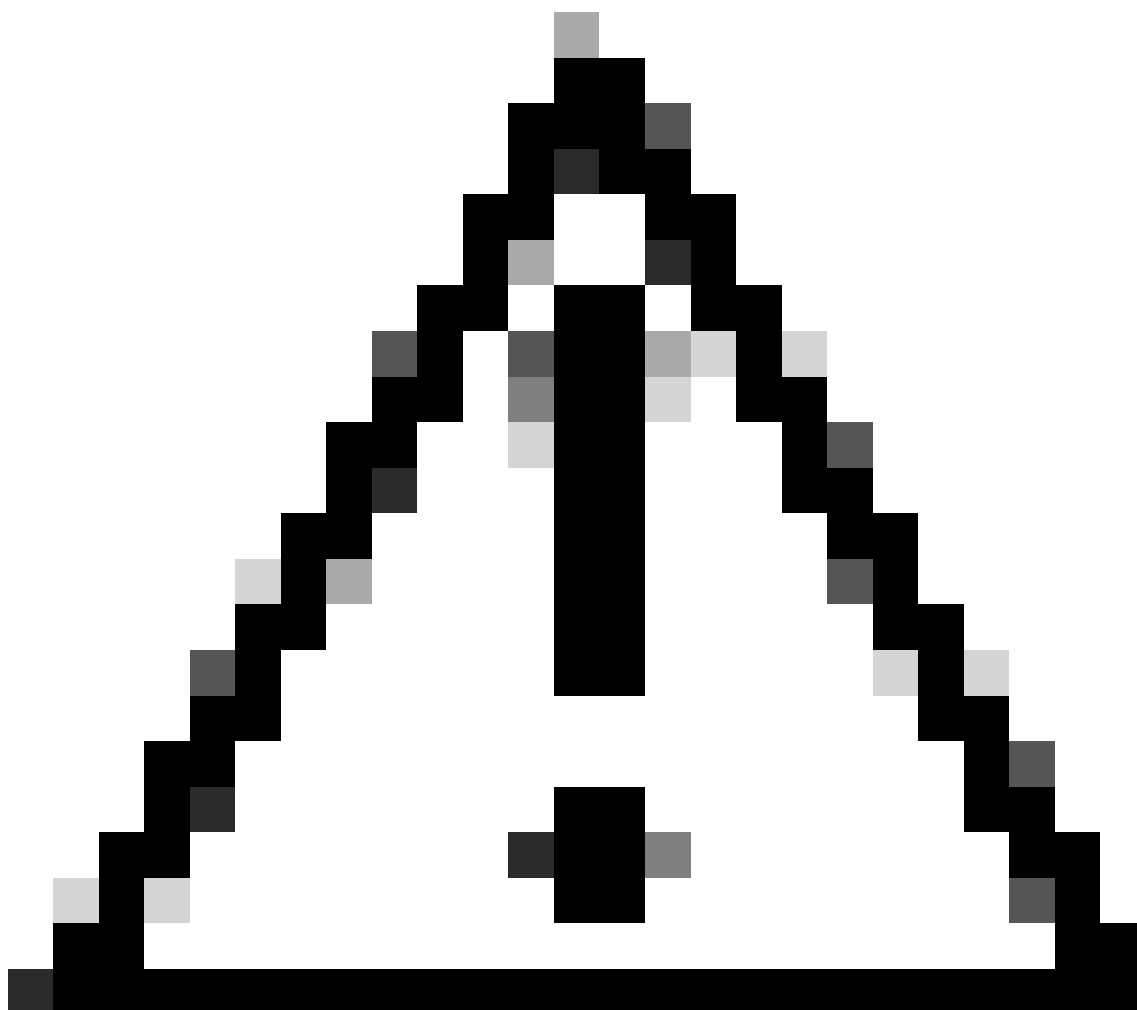
On the right side, the 'NAC' section shows:

- NAC State: Radius NAC

Allow AAA Overrideがチェックされていることを確認します。

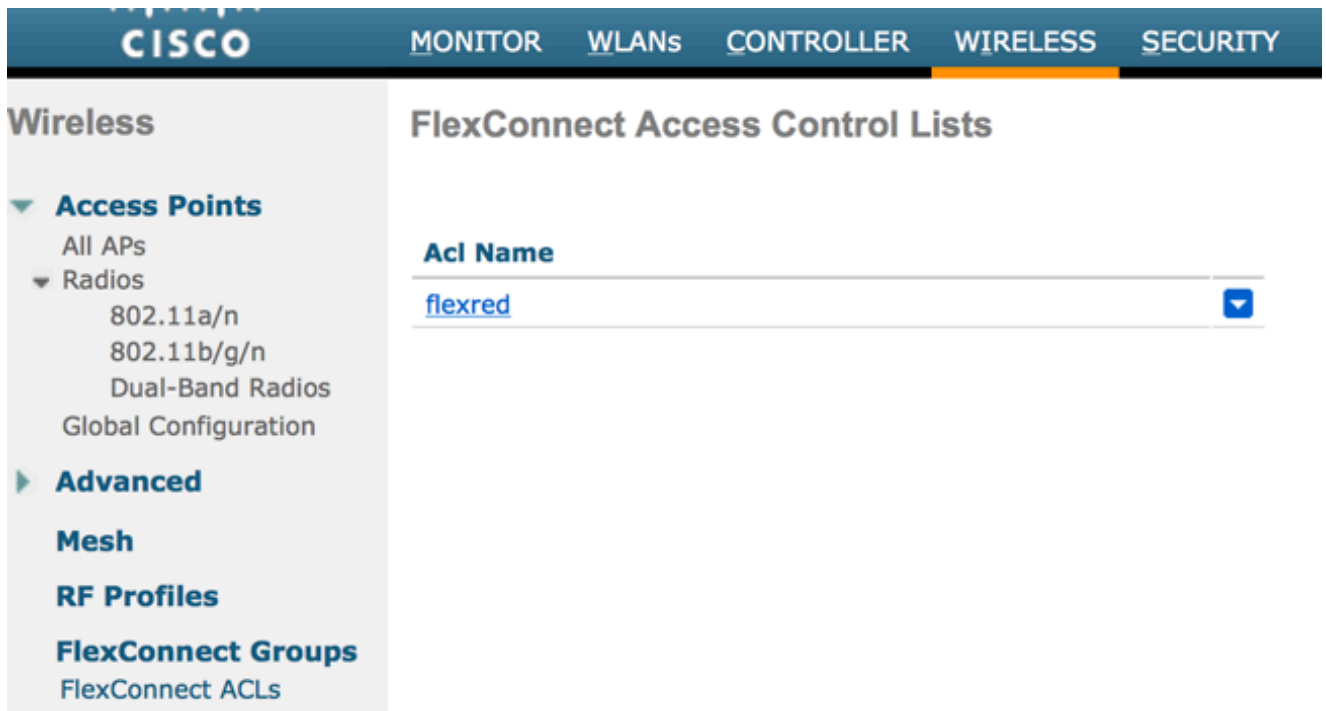
7. リダイレクト ACL を作成します。

このACLは、ISEのAccess-Acceptメッセージで参照され、リダイレクトする必要があるトラフィック (ACLによって拒否される) だけでなく、リダイレクトしない必要があるトラフィック (ACLによって許可される) も定義します。基本的に、DNSとISEとの間のトラフィックを許可する必要があります



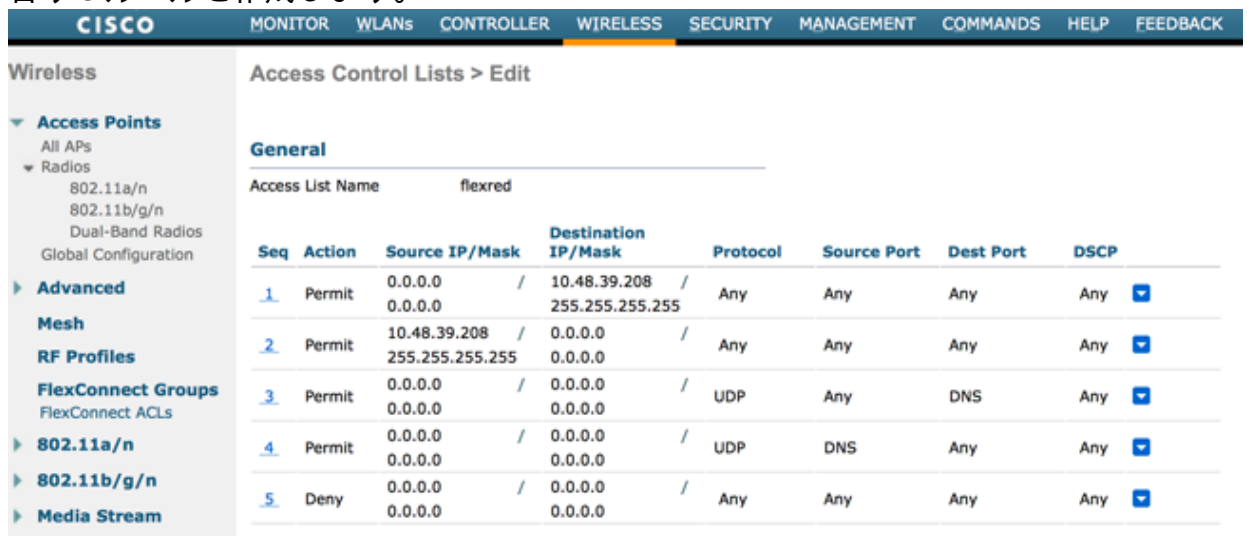
注意: FlexConnect APの問題は、通常のACLとは別にFlexConnect ACLを作成する必要があることです。この問題は、Cisco Bug ID [CSCue68065](#)に記載されており、リリース7.5で修正されています。WLC 7.5以降では、FlexACLのみが必要で、標準ACLは必要ありません。WLC では、ISE によって返されるリダイレクト ACL が標準 ACL であると想定します。ただし、確実に機能させるには、FlexConnect ACLと同じACLを適用する必要があります (シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです)。

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。



Flexredという名前のFlexConnect ACLの作成

- a. 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。



DNSトラフィックの許可

最大限のセキュリティが必要な場合は、ISEへのポート8443だけを許可します（ポスチャする場合は、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）。

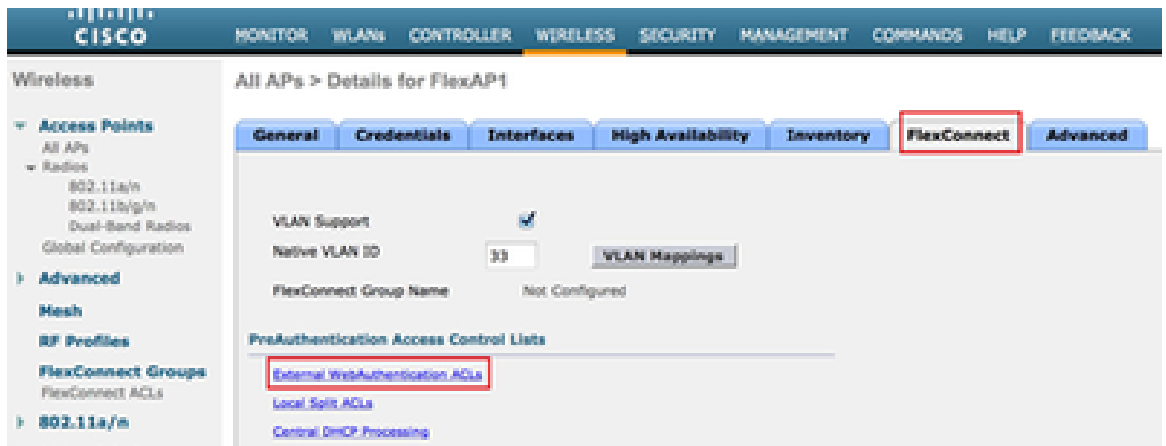
- b. (Cisco Bug [IDCSCue68065](#)により、バージョン7.5より前のコードでのみ)Security > Access Control Listの順に選択し、同じ名前の同じACLを作成します。

The screenshot shows the Cisco configuration interface for Security > Access Control Lists. The left sidebar contains a navigation tree with the following items: AAA (General, RADIUS (Authentication, Accounting, Fallback), TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, Password Policies), Local EAP, Priority Order, Certificate, and Access Control Lists (Access Control Lists, CPU Access Control Lists, FlexConnect ACLs). The 'Access Control Lists' item is selected. The main content area is titled 'Access Control Lists' and features an 'Enable Counters' checkbox which is currently unchecked. Below this is a table with two columns: 'Name' and 'Type'. The table contains one entry with the name 'flexred' and the type 'IPv4'. There is a small blue dropdown arrow icon to the right of the 'flexred' entry.

Name	Type
flexred	IPv4

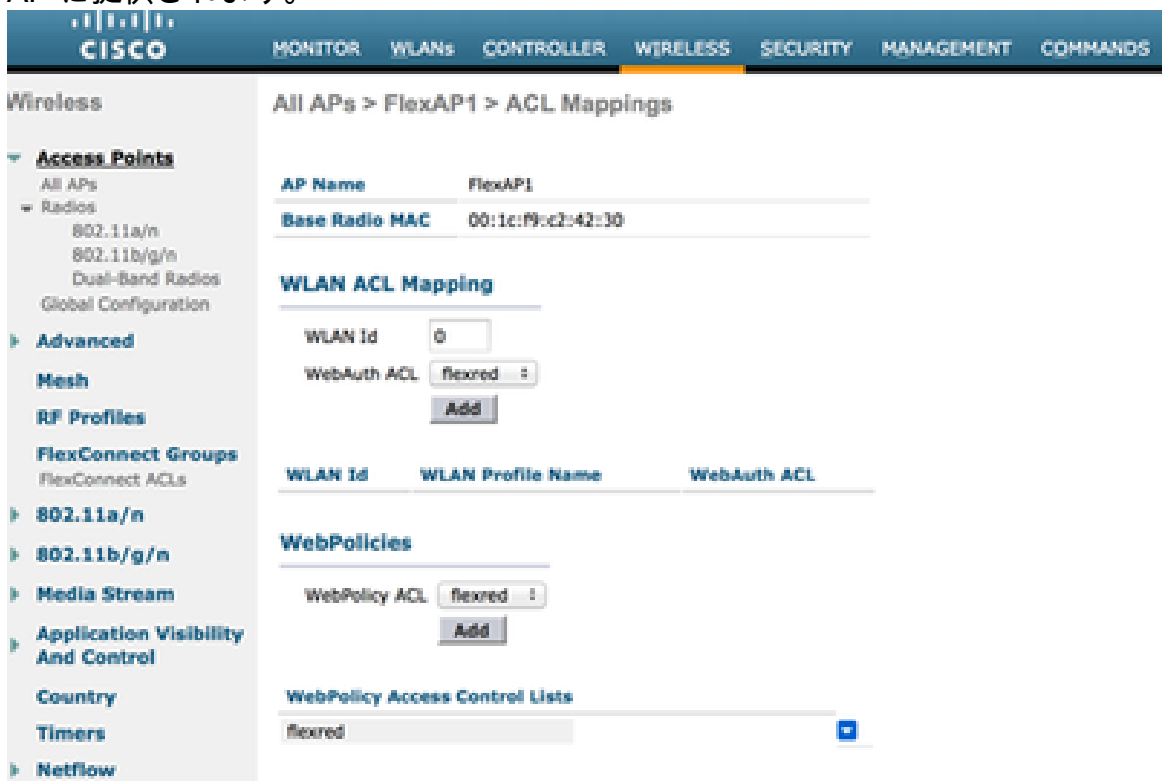
同一のACLの作成

- c. 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。
1. [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。
 2. [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)。



[FlexConnect]タブをクリックします

3. 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。



Webポリシー領域へのACLの追加

WLC の設定はこれで完了しました。

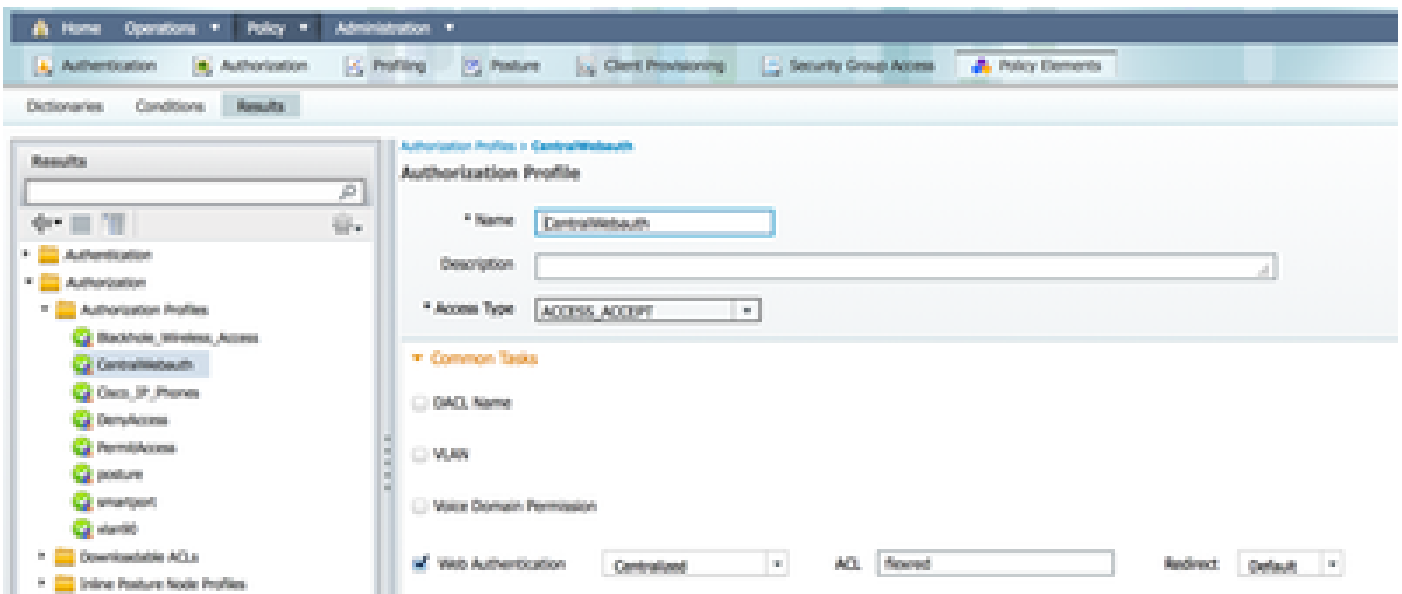
ISE 設定

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 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。



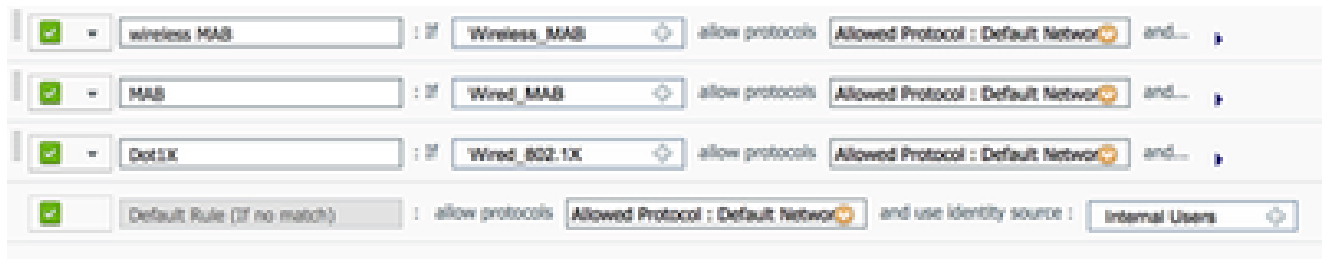
ACLがクライアントから任意の場所へのHTTPトラフィックのリダイレクトをトリガーする

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。

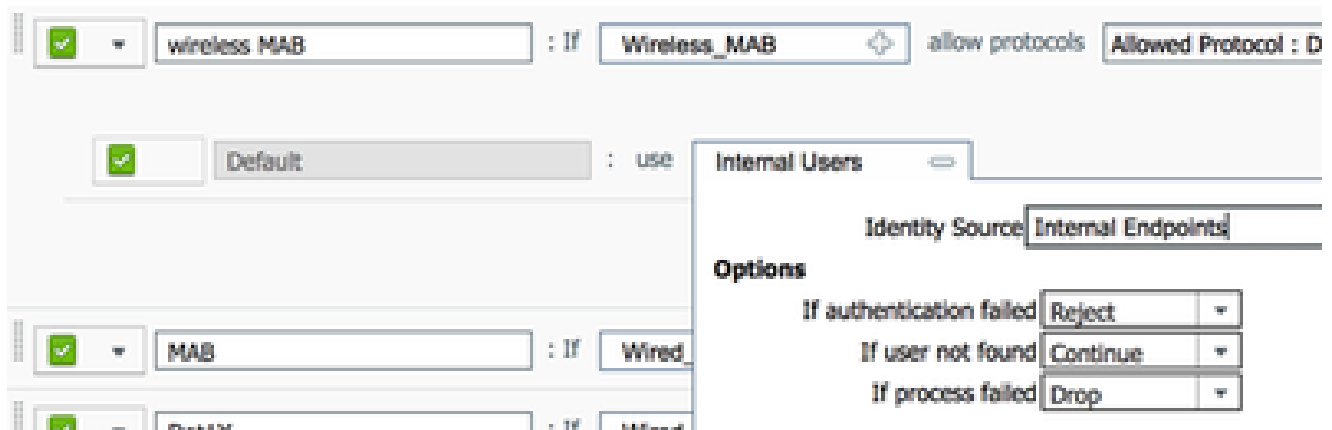
1. [Policy] メニューで [Authentication] をクリックします。

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。



ポリシールールの設定方法

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。






Continueをクリックします

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引き続き認証できるため、この設定を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るため、WebAuthとACLが返

されます。このMAC not knownルールは次の図に示され、このセクションで設定されます。

	2nd AUTH	if	Network Access:UseCase EQUALS Guest Flow	then	vlan34
	IS-a-GUEST	if	IdentityGroup:Name EQUALS Guest	then	PermitAccess
	MAC not known	if	Network Access:AuthenticationStatus EQUALS UnknownUser	then	CentralWebauth

MACが不明

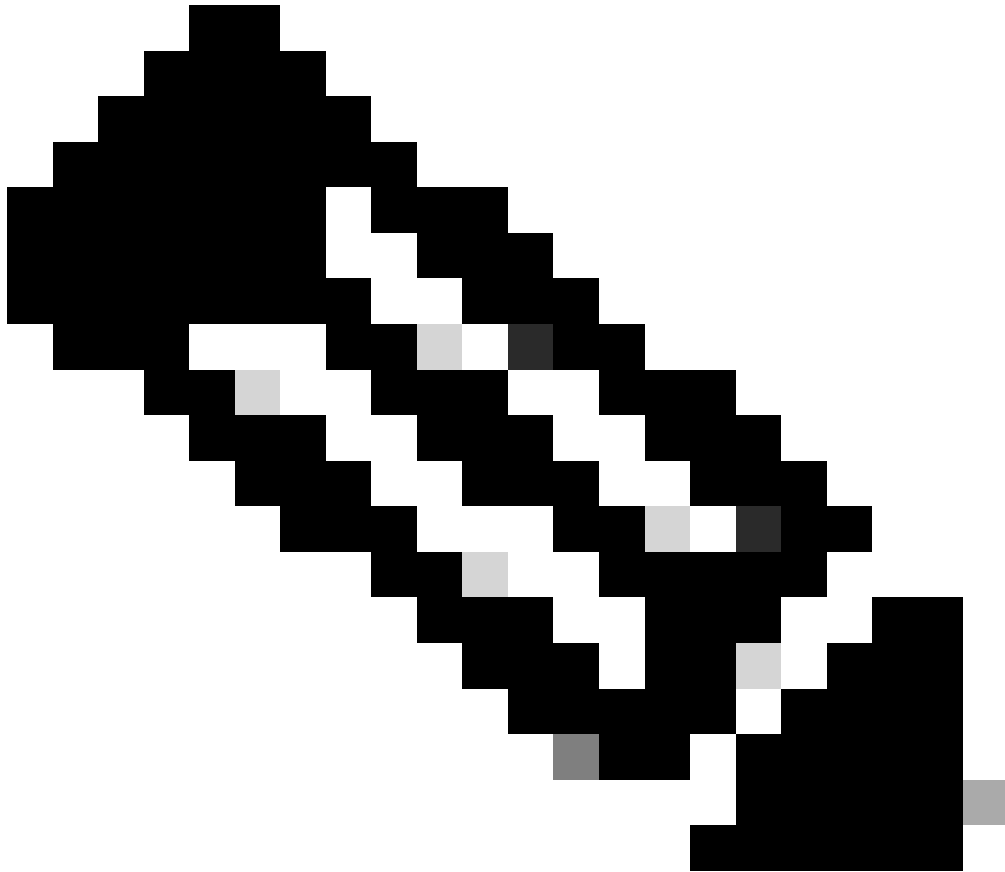
許可ルールを作成するには、次の手順を実行します。

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、ログインページが表示されます。ただし、クレデンシャルを入力すると、ISEで再度認証要求が表示されます。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、UseridentityGroupが Guestis usedと等しく、すべてのゲストがこのグループに属していると仮定しています。

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。

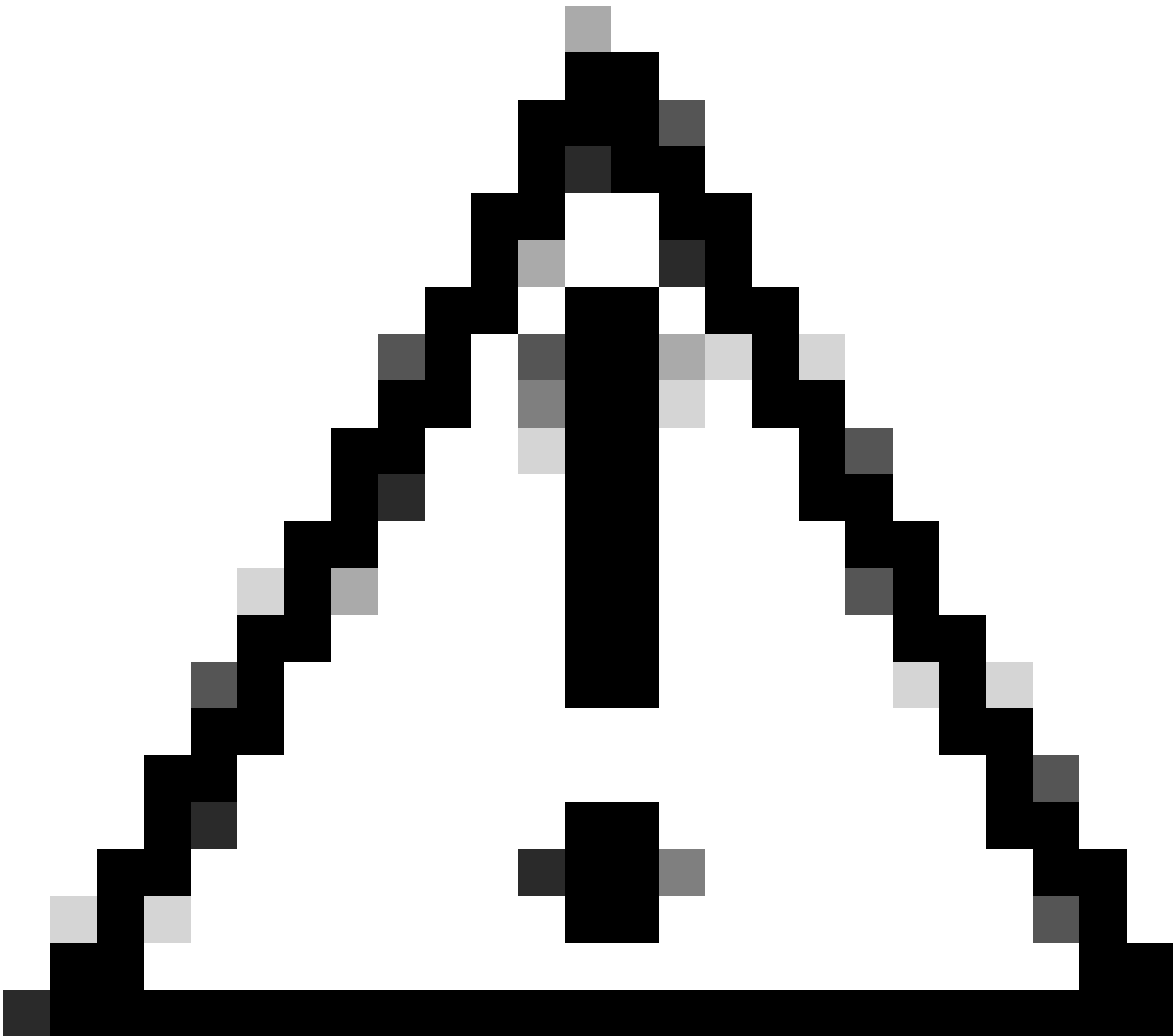


注：この新しいルールは、MAC not knownルールの前に来ることが非常に重要です。

-
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. 認可ページで、プラス(+)
アイコン(横)をクリックして、ルールの結果を選択します。

この例では、事前に設定されたプロファイル(vlan34)が割り当てられます。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。



注意: ISEバージョン1.3では、Web認証のタイプに応じて、ゲストフローの使用例に遭遇することはなくなりました。許可ルールには、唯一の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。

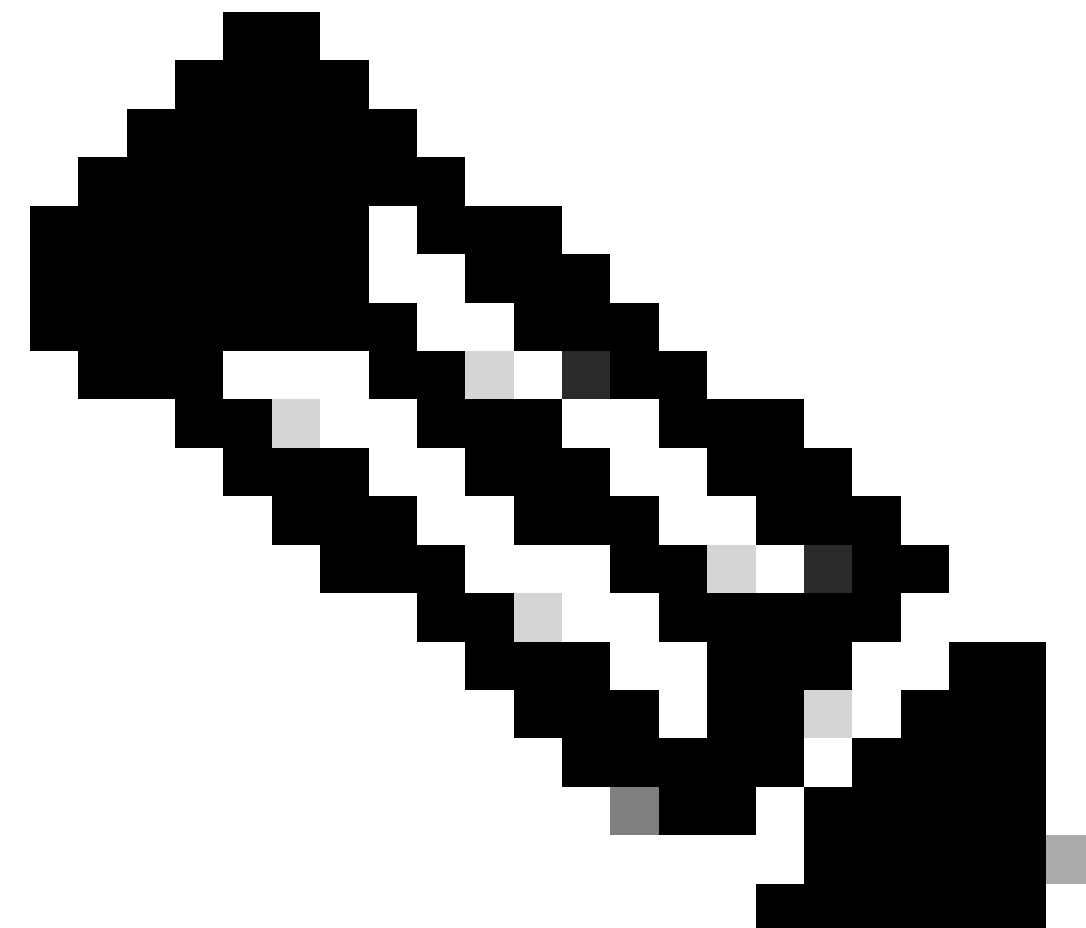
IP 更新の有効化 (オプション)

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。

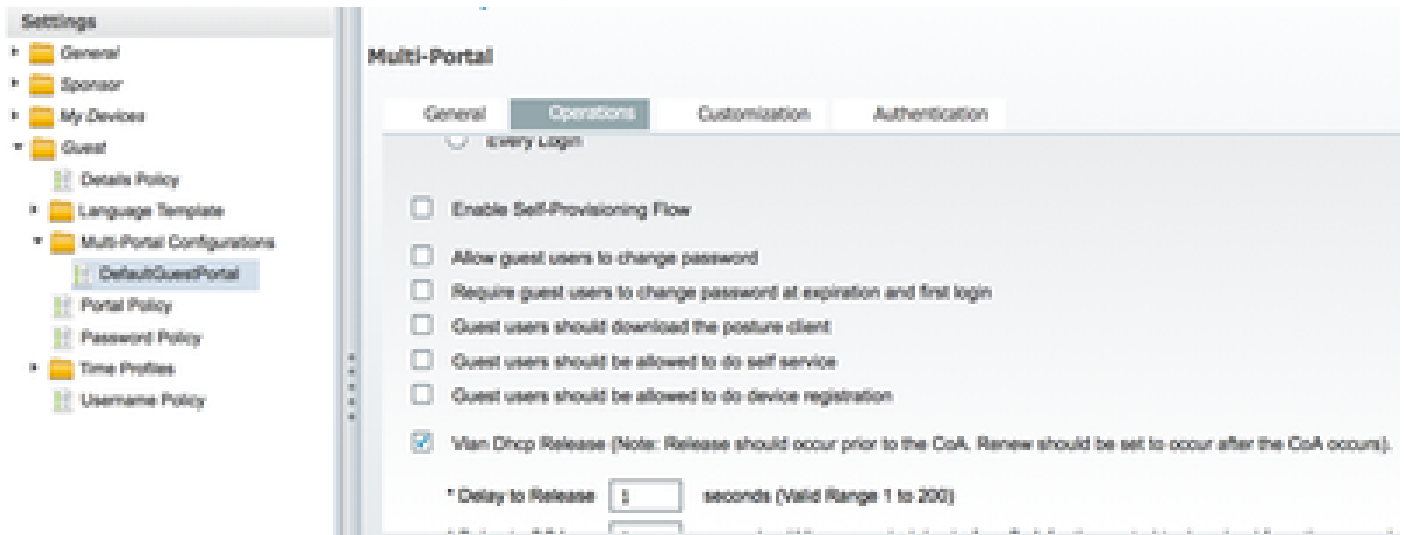
FlexConnect AP では、VLAN が AP 自体に事前に存在している必要があることに注意してください。したがって、VLAN が事前に存在しない場合、AP 自体、または作成する新規 VLAN に ACL をなにも適用しない Flex グループに VLAN-ACL マッピングを作成することができます。これにより、VLAN が実際に作成されます (その VLAN に ACL なしで)。

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をクリックするか、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クライアントでのみ機能します。



Vlan DHCP Releaseチェックボックスをクリックします

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。
- クライアントはDHCP要求を送信し、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その要求がローカルでスイッチされます。
- Central_webauth 状態では、リダイレクト ACL で拒否とマークされたトラフィック (通常 HTTP) は中央にスイッチしたがって、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、クライアントが任意のWebサイトを要求すると、APはCAPWAPでカプセル化してこれをWLCに送信し、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。このリダイレクトは、再度ローカルにスイッチされます (このリダイレクトが Flex のリダイレクト ACL で許可にヒットするため)。
- 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。

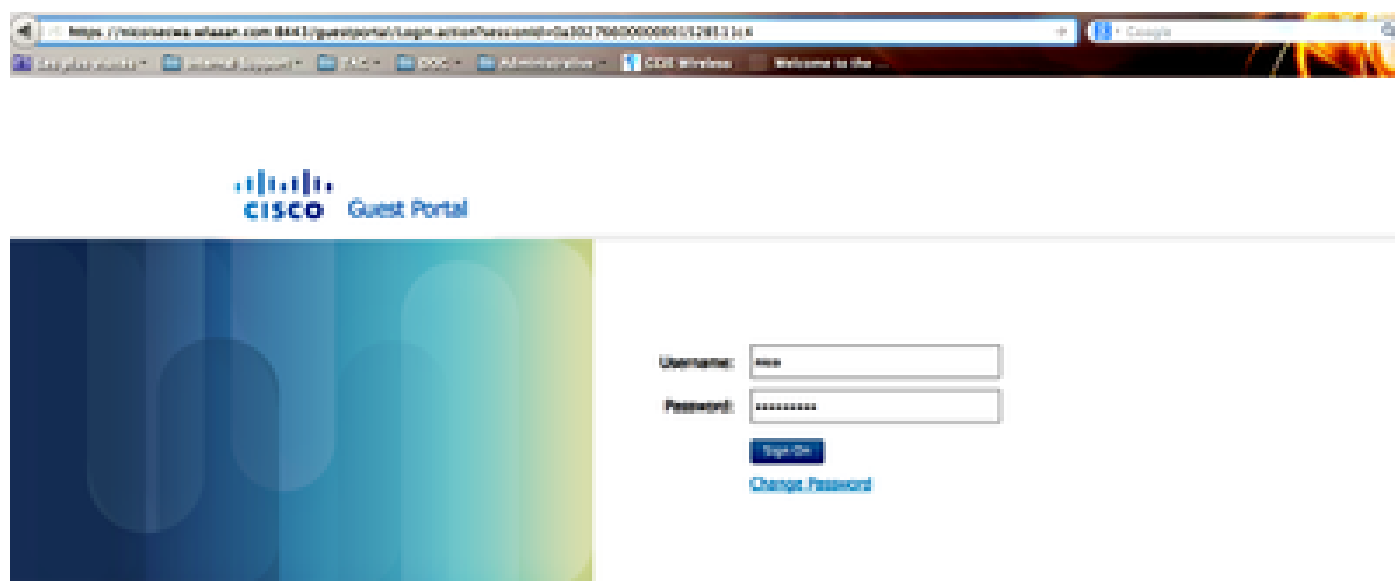
Apr 09, 2011 09:22:17 AM		Nico	06:11:00:11:76:11	nicowk	VlanDH	Guest	NotApplicable
Apr 09, 2011 09:23:17 AM				nicowk			Dynamic Author...
Apr 09, 2011 09:28:30 AM		Nico	06:11:00:11:76:11			Guest	Guest Authentic...
Apr 09, 2011 09:18:47 AM			06:11:00:11:76:11	06:11:00:11:76:11	nicowk	CentralWebauth	Pending Authentication ...

許可が表示される

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。次は、ユーザ名を使用したポータルログインです。その次に、ISE が WLC に CoA を送信し、最後の認証は

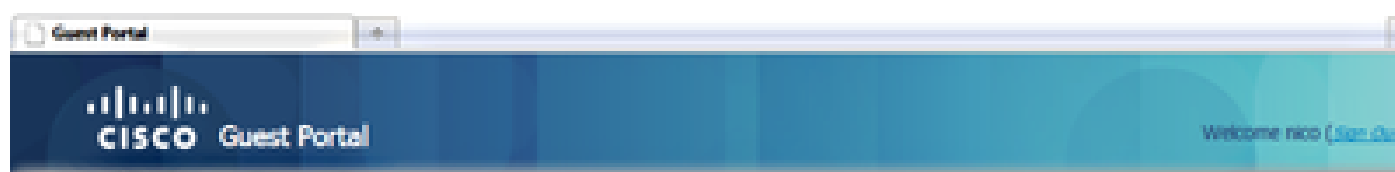
WLC 側のレイヤ 2 の MAC フィルタリング認証ですが、ISE はクライアントとユーザ名を記憶していて、この例で設定した必要な VLAN を適用します。

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。



ISEにリダイレクト

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。



Signed on successfully
You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.



ネットワークアクセスの許可

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。

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

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。