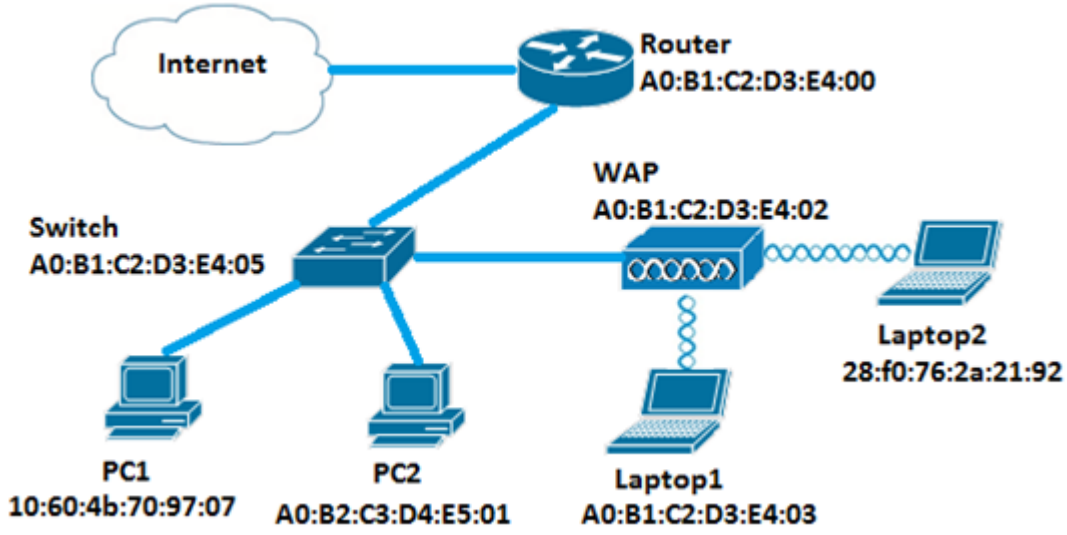
WAP125およびWAP581でのMAC ACLの設定

概要

メディアアクセスコントロール(MAC)アクセスコントロールリスト(ACL)は、レイヤ2 ACLです。各ACLは、ワイヤレスアクセスポイント(WAP)によって受信されるトラフィックに適用される一連のルールです。 このルールは、ネットワークへのアクセスを許可または拒否するために、特定のフィールドの内容を使用するかどうかを指定します。ACLは、送信元または宛先MACアドレス、仮想ローカルエリアネットワーク(VLAN)識別子(ID)、サービスクラス(CoS)などのフレームのフィールドを検査するように設定できます。 フレームがWAPデバイスポートに入ると、フレームが検査され、ACLルールがフレームの内容と照合されます。いずれかのルールがコンテンツに一致する場合、許可または拒否アクションがフレームで実行されます。MAC ACLの設定は、通常、ネットワークリソースへのアクセスを許可して、ネットワーク内のデバイスを選択するために使用されます。

注：作成されたすべてのルールの最後には、暗黙のdenyがあります。



このシナリオでは、PC1を除き、ネットワーク内のすべてのデバイスがWAPの背後にあるLaptop2へのアクセスを許可されます。

目的

この記事では、PC1がWAPの背後にあるLaptop2にアクセスするのを防ぐために、WAP125またはWAP581アクセスポイントでMACベースのACLを設定する方法を説明します。

該当するデバイス

- WAP125
- WAP581

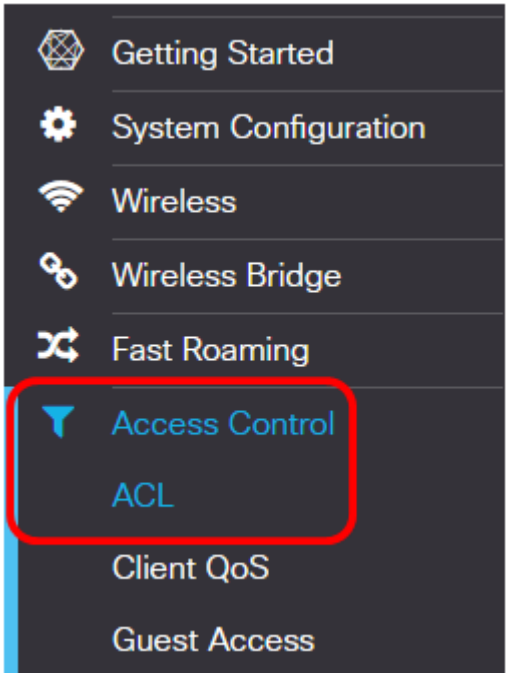
[Software Version]

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

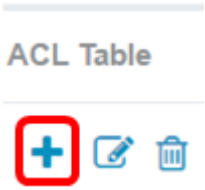
クライアントフィルタリストの設定

注：メニューオプションは、使用しているWAPの正確なモデルによって異なります。次の図は、WAP125から取得したものです。

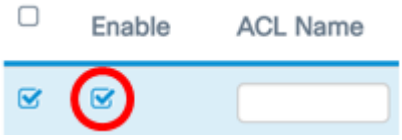
ステップ1:WAPのWebベースのユーティリティにログインし、**[Access Control] > [ACL]を選択します。**



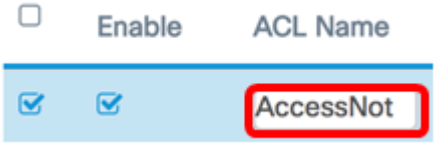
ステップ2：ボタンをクリッ ✚ クします。



ステップ3:ACLがアクティブであることを確認するために、**[Enable]**チェックボックスがオンになっていることを確認します。このオプションはデフォルトでオンになっています。

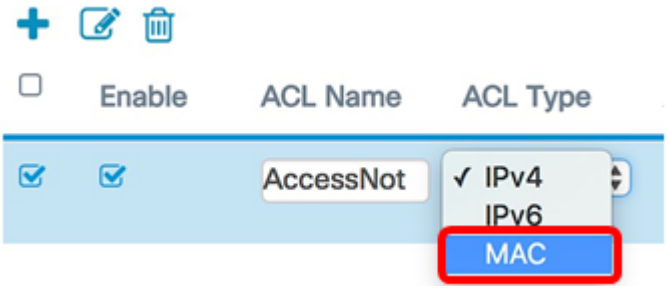


ステップ4:[ACL Name]フィールドにACLの名前を入力し、ACLを識別します。



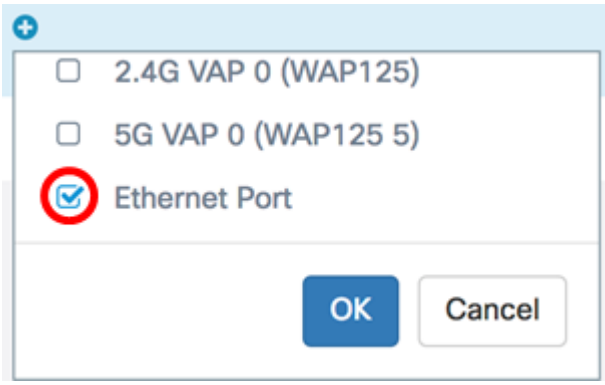
注：この例では、AccessNotを入力します。

ステップ5:[ACL Type] ドロップダウンリストから[MAC]を選択します。



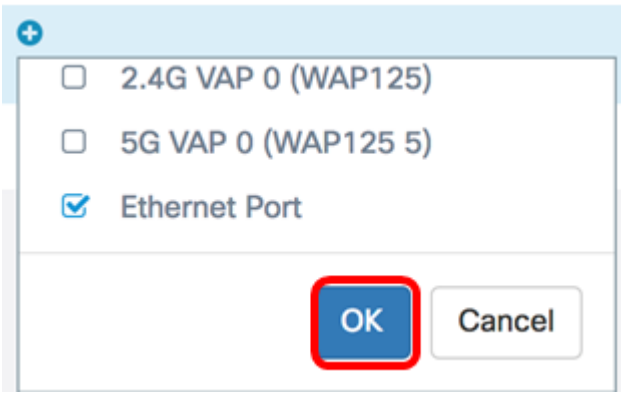
ステップ6：ボタンをクリック し、[Associated Interface]ドロップダウンリストからインターフェイスを選択します。次のオプションがあります。

- 2.4G VAP 0（SSID名）：このオプションは、MAC ACLを2.4 GHz仮想アクセスポイント(VAP)に適用します。 [SSID Name]セクションは、WAPで設定されているSSID名に応じて変更されることがあります。
- 5G VAP0（SSID名）：このオプションは、MAC ACLを5 GHz VAPに適用します。
- [Ethernet Port]：このオプションは、MAC ACLをWAPのイーサネットインターフェイスに適用します。



注：1つのACLに複数のインターフェイスを関連付けることができます。対応するインターフェイスのチェックボックスをオンにして、インターフェイスをACLに関連付けます。インターフェイスとACLの関連付けを解除するには、このチェックボックスをオフにします。この例では、イーサネットポートがACLに関連付けられています。

手順 7：[OK] をクリックします。

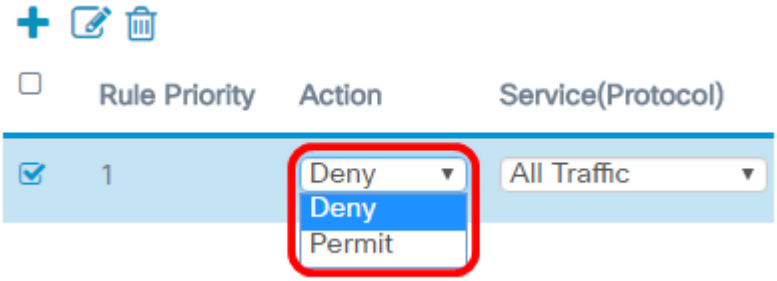


ステップ8:[More...]ボタンをクリックして、ACLのパラメータを設定します。

ステップ9：ボタンをクリックし ✚ て、新しいルールを追加します。

ステップ10:[Action]ドロップダウンリストからアクションを選択します。次のオプションがあります。

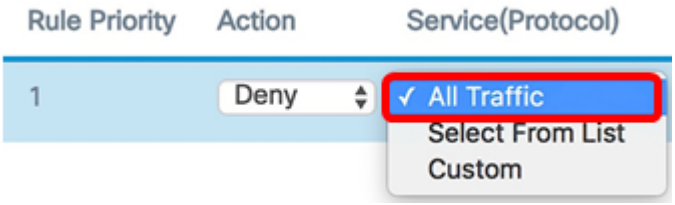
- [Permit]：このオプションは、ACL基準に一致するパケットがネットワークに接続することを許可します。
- [Deny]：このオプションを使用すると、ACL基準に一致するパケットがネットワークに接続できなくなります。



注：この例では、[Deny]が選択されています。

ステップ11:[Service (Protocol)]ドロップダウンリストから、フィルタリングするサービスまたはプロトコルを選択します。次のオプションがあります。

- [All Traffic]：このオプションは、すべてのパケットをACLフィルタに一致するものとして扱います。
- [Select From List]：このオプションを使用すると、ACLのフィルタとしてappletalk、arp、ipv4、ipv6、ipx、netbios、およびpppoeを選択できます。このオプションを選択した場合は、ステップ12に進みます。
- [Custom]：このオプションを使用すると、パケットのフィルタとしてカスタムプロトコルIDを入力できます。値は4桁の16進数です。範囲は0600 ~ FFFFです。



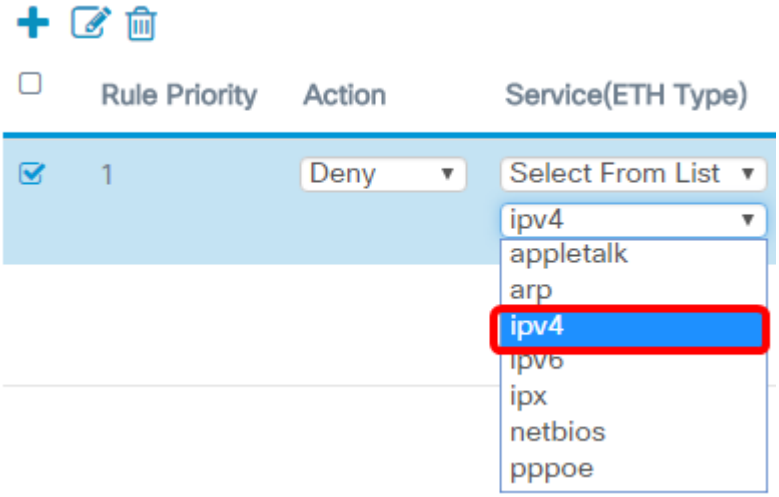
注：この例では、[All Traffic]**が選択**されています。

ステップ12:(オプション)[Select from]リストを選択した場合は、次のいずれかのオプションを選択します。

- appletalk：このオプションは、ACLのステートメントに基づいてappletalkパケットをフ

ィルタリングします。Appletalkは、AppleがMacコンピュータ用に開発したネットワークプロトコルのセットです。これらの機能の1つは、中央のルータやサーバを必要とせずに、ローカルエリアネットワーク(LAN)を接続できる機能です。

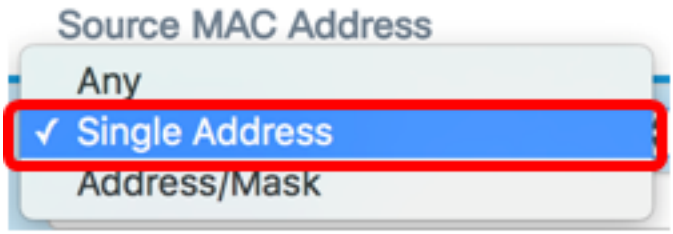
- arp：このオプションは、ACLのステートメントに基づいてアドレス解決プロトコル(ARP)パケットをフィルタリングします。ARPは、MACアドレスがIPアドレスにマッピングされるテーブルを維持します。
- ipv4：このオプションは、ACLのステートメントに基づいてipv4パケットをフィルタリングします。
- ipv6：このオプションは、ACLのステートメントに基づいてipv6パケットをフィルタリングします。IPv6は、ネットワークアドレッシングにおけるIPv6のサクセサです。
- ipx：このオプションは、ACLのステートメントに基づいてInternetwork Packet Exchange(IPX)パケットをフィルタリングします。appletalkと同様に、IPXも独自のネットワークプロトコルです。NovellクライアントとNovellサーバを使用するネットワークを接続します。
- netbios：このオプションは、ACLのステートメントに基づいてNetwork Basic Input and Output System(NetBIOS)パケットをフィルタリングします。NetBIOSを使用すると、別のコンピュータ上のアプリケーションが通信できるサービスを提供することによって、アプリケーションが通信できるようになります。
- pppoe：このオプションは、ACLのステートメントに基づいてPoint-to-Point Protocol over Ethernet(PPPoE)パケットをフィルタリングします。主にデジタル加入者線(DSL)サービスで使用されます。



注：この例では、ipv4が選択されています。

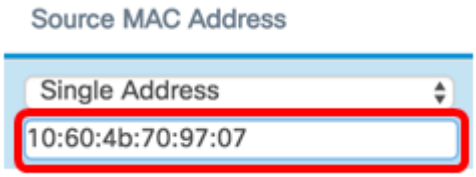
ステップ13:[Source MAC Address]ドロップダウンリストから送信元MACアドレスを定義します。次のオプションがあります。

- Any：このオプションを使用すると、WAPは任意のMACアドレスからのパケットにフィルタを適用できます。
- Single Address：このオプションを使用すると、WAPは指定されたMACアドレスからのパケットにフィルタを適用できます。
- Address/Mask：このオプションを使用すると、WAPはMACアドレスとWAPのマスクにパケットにフィルタを適用できます。



注：この例では、[Single Address]が選択されています。

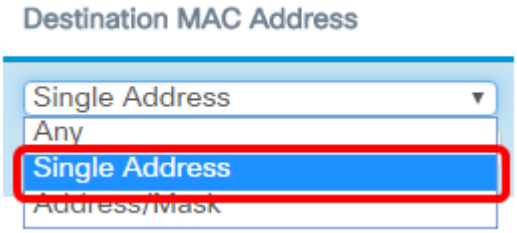
ステップ14:[Source MAC Address]フィールドに送信元MACアドレスを入力してください。



注：この例では、10:60:4b:70:97:07と入力します。これはPC1のMACアドレスです。

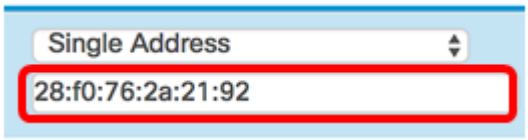
ステップ15:[Destination MAC Address]ドロップダウンリストから宛先MACアドレスを定義します。次のオプションがあります。

- Any：このオプションを使用すると、WAPは任意のMACアドレスからのパケットにフィルタを適用できます。
- Single Address：このオプションを使用すると、WAPは指定されたMACアドレスからのパケットにフィルタを適用できます。
- Address/Mask：このオプションを使用すると、WAPはMACアドレスとWAPのマスクにパケットにフィルタを適用できます。



注：この例では、[Single Address]が選択されています。

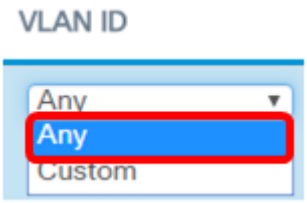
ステップ16:[Destination MAC Address]フィールドに宛先MACアドレス**を入力**します。



注：この例では、28:f0:76:2a:21:92と入力します。これはLaptop2のMACアドレスです。

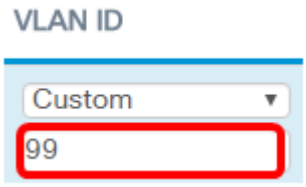
ステップ17：ドロップダウンリストからVLAN IDを選択します。

- [任意(Any)]：このオプションは、ネットワークを介して任意のVLAN IDを許可します。
- [Custom]：このオプションを使用すると、特定のVLAN IDを入力できます。このオプションを選択した場合は、ステップ18に進みます。



注：この例では、[Any]が選択されています。

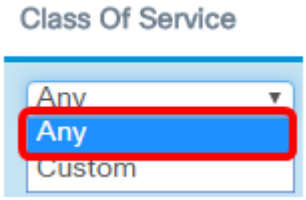
ステップ18:(オプション)[カスタム]を選択した場合は、[VLAN ID]フィールドにVLAN IDを入力します。



注：この例では、99を入力します。

ステップ19:（オプション）ドロップダウンリストからサービスクラスを選択します。次のオプションがあります。

- [任意(Any)]：任意のプライオリティレベルのパケットをネットワークに接続できます。
- [Custom]：このオプションを使用すると、特定のプライオリティレベルでパケットをフィルタリングできます。

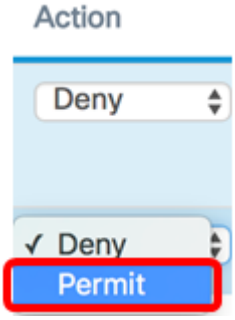


注：この例では、[Any]が選択されています。[カスタム]を選択した場合は、[サービスクラス]フィールドに*[優先度]*を入力します。

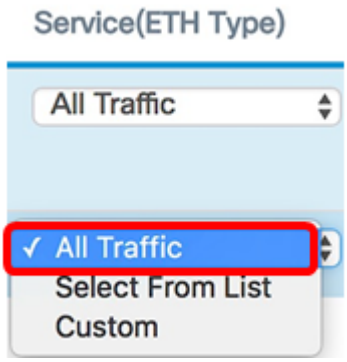
ステップ20：もう一度ボタンをクリック ✚ して、許可ルールを追加します。

注：作成されたすべてのルールの最後には暗黙の拒否があるため、ネットワーク内の他のデバイスからのトラフィックを許可するために、許可ルールをACLに追加することを強く推奨します。

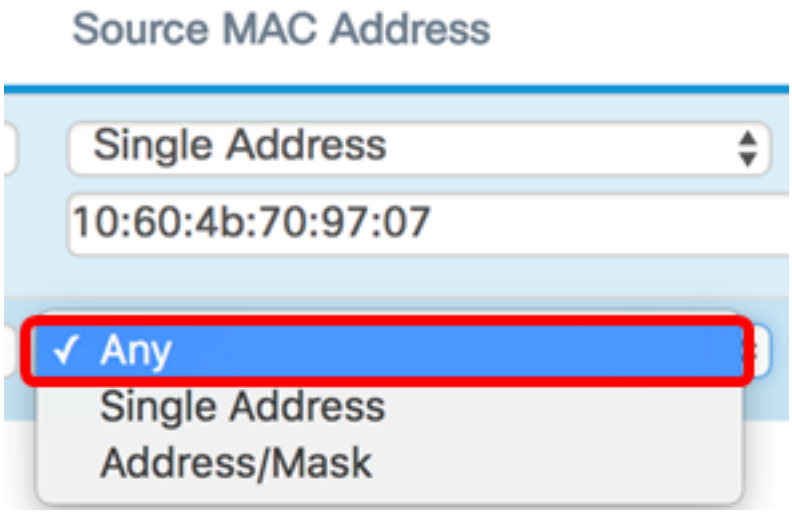
ステップ21:[Action]ドロップダウン矢印をクリックし、[**Permit**]を選択します。



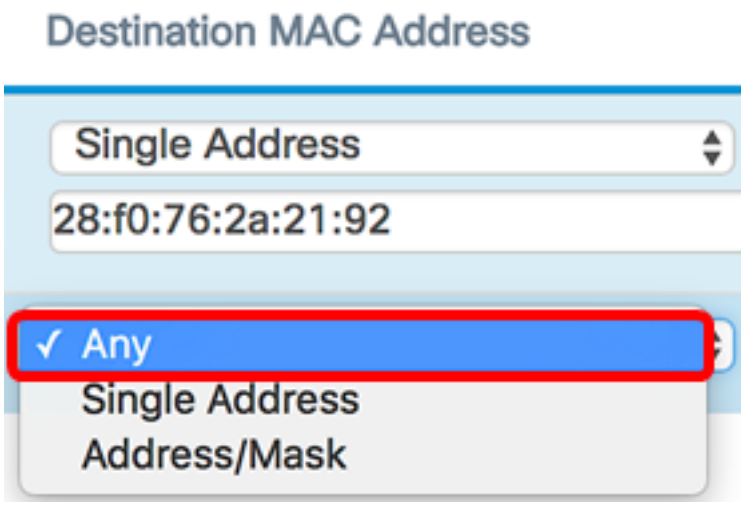
ステップ22:[Service(ETH Type)]ドロップダウン矢印をクリックし、[**All Traffic**]を選択します。



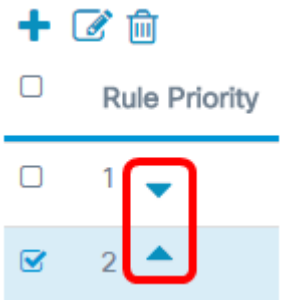
ステップ23:[Source MAC Address]ドロップダウンメニューをクリックし、[Any]を選択します。これにより、ネットワーク内の他のMACアドレスからのトラフィックが許可されます。ただし、最初のルールに示されているPC1のMACアドレスは許可されません。



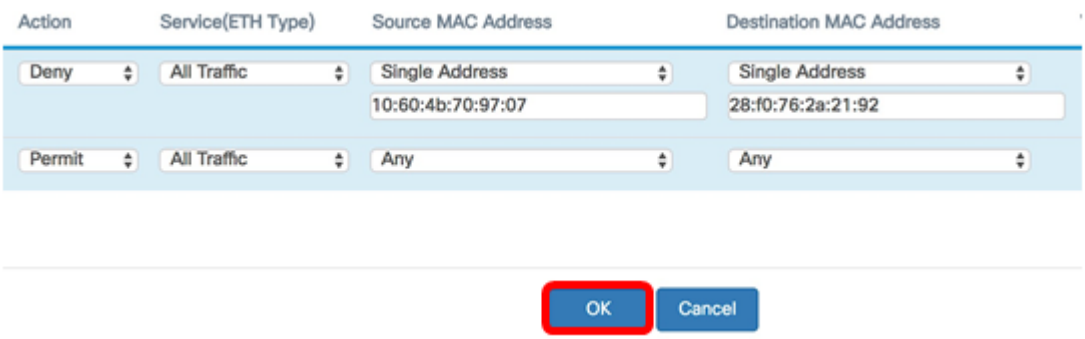
ステップ24:[Destination MAC Address]ドロップダウンメニューをクリックし、[Any]を選択します。これにより、ネットワーク内の任意のMACアドレスへのトラフィックが許可されます。



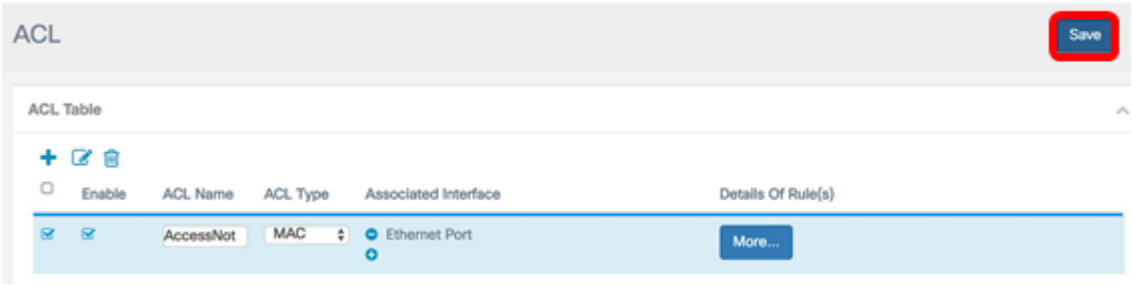
ステップ25.（オプション）ルールが設定されるまで、上下の矢印をクリックしてルールの優先順位を変更します。



手順 26：[OK] をクリックします。



ステップ27:[Save]をクリックします。



これで、WAP125またはWAP581アクセスポイントにMAC ACLが設定されました。

この記事に関連するビデオを表示...

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください]