クライアントの複数認証

クライアントの複数認証について

複数認証機能は、クライアント接続でサポートされるレイヤ2およびレイヤ3セキュリティ タイプの拡張機能です。

（注） 特定の SSID に対して L2 認証と L3 認証の両方を有効にすることができます。

（注） 複数認証機能は、通常のクライアントにのみ適用されます。

クライアントに対する認証の組み合わせのサポートに関する情報

クライアントの複数認証では、WLANプロファイルで設定された特定のクライアントに対する複数の認証の組み合わせがサポートされます。

次の表に、サポートされる認証の組み合わせの概要を示します。

レイヤ 2	レイヤ 3	サポートあり
MAB	CWA	はい
MAB のエラー	LWA	対応
802.1X	CWA	はい

PSK	CWA	はい
iPSK + MAB	CWA	はい
iPSK	LWA	非対応
MAB のエラー + PSK	LWA	非対応 対応
MAB のエラー + PSK	CWA	非対応

16.10.1 以降では、WLAN の 802.1X 設定で、WPA または WPA2 設定を使用した Web 認証設定がサポートされます。

この機能は、次の AP モードもサポートしています。

- Local
- FlexConnect
- ファブリック

クライアントの複数認証の設定

802.1X およびローカル Web 認証用の WLAN の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 表示された WLAN のリストから必要な WLAN を選択します。
ステップ 3 [Security] > [Layer2] タブを選択します。
ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。
ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオンにします。
ステップ 6 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。
ステップ 7 MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストからオプションを選択します。
ステップ 8 [Security] > [Layer3] タブを選択します。
ステップ 9 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。
ステップ 10 [Web Auth Parameter Map] および [Authentication List] ドロップダウンリストから、オプションを選択します。
ステップ 11 [Update & Apply to Device] をクリックします。

802.1X およびローカル Web 認証用の WLAN の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • profile-name：設定されている WLAN のプロファイル名。 • wlan-id：ワイヤレス LAN の ID。範囲は 1 ～ 512 です。 • SSID_Name：最大 32 文字の英数字からなる SSID。 （注） すでにこのコマンドを設定している場合は、wlan profile-name コマンドを入力します。
ステップ 3	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。 この設定は、すべての dot1x セキュリティ WLAN で類似しています。
ステップ 4	**security web-auth** 例： `Device(config-wlan)# security web-auth`	Web 認証を有効にします。
ステップ 5	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list default`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name*	パラメータ マップをマッピングします。

	コマンドまたはアクション	目的
	例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	（注） パラメータマップが WLAN に関連付けられていない場合は、グローバルパラメータマップの設定と見なされます。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

例

```
wlan wlan-test 3 ssid-test
 security dot1x authentication-list default
 security web-auth
 security web-auth authentication-list default
 security web-auth parameter-map WLAN1_MAP
 no shutdown
```

事前共有キー（PSK）およびローカル Web 認証用の WLAN の設定（GUI）

手順

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

ステップ 2 必要な WLAN を選択します。

ステップ 3 [Security] > [Layer2] タブを選択します。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。

ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオフにします。

ステップ 6 [PSK] チェックボックスをオンにします。

ステップ 7 [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。

ステップ 8 [Security] > [Layer3] タブを選択します。

ステップ 9 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。

ステップ 10 [Web Auth Parameter Map] ドロップダウンリストから [Web Auth Parameter Map] を選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 11 [Update & Apply to Device] をクリックします。

事前共有キー（PSK）およびローカル Web 認証用の WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**security wpa psk set-key** *ascii/hex key password* 例： `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	PSK 共有キーを設定します。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	PSK サポートを設定します。
ステップ 6	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。

	コマンドまたはアクション	目的
ステップ 7	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list webauth`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 8	**security web-auth parameter-map** *parameter-map-name* 例： `(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップを設定します。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。

例

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

PSK または iPSK（ID 事前共有キー）および中央 Web 認証用の WLAN の設定（GUI）

手順

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

ステップ 2 必要な WLAN を選択します。

ステップ 3 [Security] > [Layer2] タブを選択します。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストからセキュリティ方式を選択します。

ステップ 5 [Auth Key Mgmt] で、[802.1x] チェックボックスをオフにします。

ステップ 6 [PSK] チェックボックスをオンにします。

ステップ 7 [Pre-Shared Key] を入力し、[PSK Format] ドロップダウンリストから PSK フォーマットを選択し、[PSK Type] ドロップダウンリストから PSK タイプを選択します。

ステップ 8 [MAC Filtering] チェックボックスをオンにして、機能を有効にします。

ステップ 9 MAC フィルタリングを有効にした状態で、[Authorization List] ドロップダウンリストから認可リストを選択します。

ステップ 10 [Security] > [Layer3] タブを選択します。

ステップ 11 [Web Policy] チェックボックスをオンにして、Web 認証ポリシーを有効にします。

ステップ 12 [Web Auth Parameter Map] ドロップダウンリストから [Web Auth Parameter Map] を選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 13 [Update & Apply to Device] をクリックします。

PSK または iPSK（ID 事前共有キー）および中央 Web 認証用の WLAN の設定

WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa psk set-key** *ascii/hex key password* 例：	PSK AKM の共有キーを設定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	
ステップ 5	**mac-filtering** *auth-list-name* 例： `Device(config-wlan)# mac-filtering test-auth-list`	MAC フィルタリング パラメータを設定します。

例

```
wlan wlan-test 3 ssid-test
 no security wpa akm dot1x
 security wpa psk set-key ascii 0 PASSWORD
 mac-filtering test-auth-list
```

WLAN へのポリシー プロファイルの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-iot`	デフォルト ポリシー プロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは ISE サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシー プロファイルに NAC を設定します。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を停止します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。

例

```
wireless profile policy policy-iot
 aaa-override
 nac
 no shutdown
```

コントローラでの 802.1x および中央 Web 認証の設定（CLI）

AAA 認証の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。

外部認証用の AAA サーバーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**radius-server attribute wireless authentication call-station-id ap-name-ssid** 例： `Device(config)# radius-server attribute wireless authentication call-station-id ap-name-ssid`	RADIUS 認証メッセージで送信される発信側ステーション識別子を設定します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server ISE2`	RADIUS サーバーを設定します。
ステップ 4	**address ipv4** *radius-server-ip-address* 例： `Device(config-radius-server)# address ipv4 111.111.111.111`	RADIUS サーバーのアドレスを指定します。
ステップ 5	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 10`	秒単位のタイムアウト値を指定します。範囲は 10 ～ 1000 秒です。
ステップ 6	**retransmit** *number-of-retries* 例： `Device(config-radius-server)# retransmit 10`	サーバーへの再試行回数を指定します。範囲は 0 ～ 100 です。
ステップ 7	**key** *key* 例： `Device(config-radius-server)# key cisco`	デバイスと、RADIUS サーバー上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 *key* には次の値を使用できます。 • 0：暗号化されていないキーを指定します。 • 6：暗号化されたキーを指定します。 • 7：「隠し」キーを指定します。 • Word：暗号化されていない（クリアテキスト）サーバー キー。
ステップ 8	**exit** 例：	コンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# exit`	
ステップ 9	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius ISE2`	RADIUS サーバーグループの ID を作成します。
ステップ 10	**server name** *server-name* 例： `Device(config)# server name ISE2`	サーバー名を設定します。
ステップ 11	**radius-server deadtime** *time-in-minutes* 例： `Device(config)# radius-server deadtime 5`	DEAD とマークされたサーバーがその状態で保持される時間を分単位で定義します。このデッドタイムが経過すると、コントローラはサーバーを UP（ALIVE）としてマークし、登録クライアントに状態の変更を通知します。状態が UP としてマークされた後もサーバーに到達できない場合、および DEAD 条件が満たされている場合、そのサーバーはデッドタイム間隔で再び DEAD としてマークされます。 *time-in-mins*：有効な値の範囲は 1 ～ 1440 分です。デフォルト値はゼロです。デフォルト値に戻すには、**no radius-server deadtime** コマンドを使用します。 **radius-server deadtime** コマンドは、グローバルに設定することも、AAA グループサーバーレベルで設定することもできます。 **show aaa dead-criteria** または **show aaa servers** コマンドを使用して、デッドサーバーの検出を確認できます。デフォルト値がゼロの場合、デッドタイムは設定されません。

認証用の AAA の設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa authentication login** 例： `Device# aaa authentication login ISE_GROUP group ISE2 local`	ログイン時の認証方法を定義します。
ステップ 2	**aaa authentication dot1x** 例： `Device(config)# aaa authentication network ISE_GROUP group ISE2 local`	dot1x での認証方法を定義します。

アカウンティング ID リストの設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* 例： `Device# aaa accounting identity ISE start-stop group ISE2`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。 （注） 名前付きリストの代わりにデフォルトのリストを使用することもできます。

中央 Web 認証用の AAA の設定

始める前に

RADIUS サーバーと AAA サーバー グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa server radius dynamic-author** 例：	コントローラの認可変更（CoA）を設定します。

	コマンドまたはアクション	目的
	`Device# aaa server radius dynamic-author`	
ステップ 2	**client** *client-ip-addr* **server-key** *key* 例： `Device(config-locsvr-da-radius)# client 111.111.111.111 server-key ciscokey`	RADIUS クライアントのサーバーキーを設定します。

Radius サーバーのアクセス制御リストの定義

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip access-list extended redirect** 例： `Device(config)# ip access-list extended redirect`	ISE がリダイレクト ACL（**redirect** という名前）を使用するように設定されているため、HTTP および HTTPS ブラウジングは（他の ACL ごとの）認証なしでは機能しません。
ステップ 3	*sequence-number* **deny icmp any** 例： `Device(config-ext-nacl)# 10 deny icmp any`	シーケンス番号に従って拒否するパケットを指定します。 （注） 拒否シーケンスには、DHCP、DNS、および ISE サーバーが必要です。「Radius サーバーのアクセス制御リストを定義する構成例」を参照してください。この例で、*111.111.111.111* は ISE サーバーの IP アドレスを指します。
ステップ 4	**permit TCP any any eq** *web-address* 例： `Device(config-ext-nacl)# permit TCP any any eq www`	すべての HTTP または HTTPS アクセスを Cisco ISE のログインページにリダイレクトします。

Radius サーバーのアクセス制御リストを定義する構成例

この例では、RADIUS サーバーのアクセス制御リストを定義する方法を示します。

```
Device# configure terminal
Device(config-ext-nacl) # 10 deny icmp any
Device(config-ext-nacl) # 20 deny udp any any eq bootps
Device(config-ext-nacl) # 30 deny udp any any eq bootpc
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # 50 deny tcp any host 111.111.111.111 eq 8443
Device(config-ext-nacl) # 55 deny tcp host 111.111.111.111 eq 8443 any
Device(config-ext-nacl) # 40 deny udp any any eq domain
Device(config-ext-nacl) # end
```

WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** *wlan-name* 例： `Device(config)# wlan wlan30`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**security dot1x authentication-list ISE_GROUP** 例： `Device(config-wlan)# security dot1x authentication-list ISE_GROUP`	WLAN の 802.1X を設定します。
ステップ 4	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

ポリシー プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy wireless-profile1`	ポリシープロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバーまたは Cisco Identify Services Engine（ISE）サーバーから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**accounting-list** *list-name* 例： `Device(config-wireless-policy)# accounting-list ISE`	IEEE 802.1x のアカウンティング リストを設定します。
ステップ 5	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	WLAN の DHCP パラメータを設定します。
ステップ 6	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルでネットワーク アクセス コントロール（NAC）を設定します。NAC は、中央 Web 認証（CWA）をトリガーするために使用されます。
ステップ 7	**vlan 25** 例： `Device(config-wireless-policy)# vlan 25`	ゲスト VLAN プロファイルを設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

ポリシータグへの WLAN とポリシープロファイルのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy xx-xre-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan wlan30 policy wireless-profile1`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

中央 Web 認証と Dot1x 用の ISE の設定（GUI）

ゲストポータルの定義

始める前に

ゲストポータルを定義するか、デフォルトのゲストポータルを使用します。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。
ステップ 2 **[Work Centers]** > **[Guest Access]** > **[Portals & Components]** の順に選択します。
ステップ 3 [Guest Portal] をクリックします。

クライアントの認証プロファイルの定義

始める前に

要件に応じて、ゲストポータルおよびその他の追加パラメータを使用する認証プロファイルを定義できます。認証プロファイルは、クライアントを認証ポータルにリダイレクトします。Cisco ISE の最新バージョンでは、Cisco_Webauth 認証結果がすでに存在しており、これを編集して、コントローラの構成と一致するようにリダイレクト ACL の名前を変更できます。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [許可（Authorization）] > [認証プロファイル（Authorization Profiles）]** を選択します。

ステップ 3 [Add] をクリックして独自のカスタムを作成するか、Cisco_Webauth のデフォルトの結果を編集します。

認証ルールの定義

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[Policy] > [Policy Sets]** の順に選択し、適切なポリシーセットをクリックします。

ステップ 3 [Authentication] ポリシーを展開します。

ステップ 4 [Options] を展開し、適切な [User ID] を選択します。

認証ルールの定義

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 **[Policy] > [Policy Sets] > [Authorization Policy]** の順に選択します。

ステップ 3 特定の SSID で 802.1x の条件に一致するルールを作成します（Radius-Called-Station-ID を使用）。

（注） CWA リダイレクト属性が表示されます。

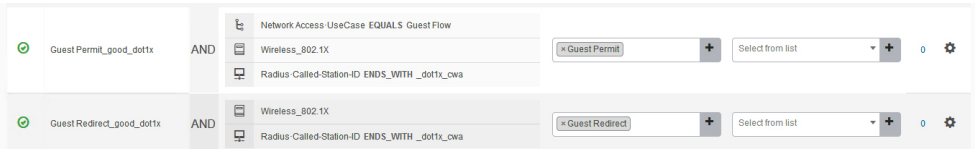
ステップ 4 作成済みの認証プロファイルを選択します。

ステップ 5 [Result/Profile] 列から、作成済みの認証プロファイルを選択します。

ステップ 6 [Save] をクリックします。

（注）　次の図に、機能する構成例を参考として示します。

図 *1:* 機能する構成例



ゲストフロー条件に一致するルールの作成

始める前に

ユーザーがポータルで認証を完了したらゲストフロー条件に一致してネットワークアクセスの詳細に戻る 2 番目のルールを作成する必要があります。

手順

ステップ 1　Cisco Identity Services Engine（ISE）にログインします。

ステップ 2　**[Policy]** > **[Policy Sets]** > **[Authorization Policy]** の順に選択します。

ステップ 3　Network Access-UseCase EQUALS Guest、および特定の SSID で 802.1x の条件に一致するルールを作成します（Radius-Called-Station-ID を使用）。

（注）　アクセス許可が表示されます。

ステップ 4　[Result/Profile] 列から、作成済みの認証プロファイルを選択します。

ステップ 5　デフォルトまたはカスタマイズされたアクセス許可を選択します。

ステップ 6　[Save] をクリックします。

複数の認証設定の確認

レイヤ 2 認証

L2 認証（Dot1x）が完了すると、クライアントは Webauth Pending 状態に移行します。

L2 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
---------------------------------------------------------------------------------------------------
```

```
58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50
```

```
Device# show platform software wireless-client chassis active R0

        ID  MAC Address      WLAN  Client     State
------------------------------------------------------------------------------------------

  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0

    ID     MAC Address   WLAN  Client     State  AOM ID    Status
-------------------------------------------------------------------------------------------------
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
   Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO    LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL               AN - ANCHOR
FR - FOREIGN          MT - MTE
IV - INVALID


EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-----------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
-----------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

レイヤ 3 認証

L3 認証が成功すると、クライアントは Run 状態に移行します。

L3 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0

Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800

Device# show platform software wireless-client chassis active R0

ID          MAC Address     WLAN    Client State
-------------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run

Device# show platform software wireless-client chassis active f0

ID         MAC Address       WLAN    Client State   AOM ID.  Status
-----------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done

Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
RG - REGULAR   BLE - BLE
HL - HALO      LI - LWFL INT

Auth State Abbrevations:
UK - UNKNOWN    IP - LEARN    IP IV - INVALID
L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
UK - UNKNOWN       IN - INIT
LC - LOCAL         AN - ANCHOR
FR - FOREIGN       MT - MTE
IV - INVALID
EoGRE Abbreviations:
N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
-------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary

Vlan   pal_if_hd1        mac            Input Uidb     Output Uidb
------------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```

PSK + WebAuth 設定の確認

```
Device# show wlan summary

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020


Number of WLANs: 1

ID Profile Name SSID Status Security
-----------------------------------------------------------------------------------------------------------------------------

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。