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 （1 ページ）
- クライアントの複数認証の設定 （2 ページ）
- 複数の認証設定の確認 （9 ページ）

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	対応
PSK	CWA	はい

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

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]
```