



秘密共有キー

- [秘密事前共有キーについて \(1 ページ\)](#)
- [WLAN での PSK の設定 \(CLI\) \(2 ページ\)](#)
- [WLAN での PSK の設定 \(GUI\) \(3 ページ\)](#)
- [WLAN へのポリシー プロファイルの適用 \(GUI\) \(4 ページ\)](#)
- [WLAN へのポリシー プロファイルの適用 \(CLI\) \(4 ページ\)](#)
- [秘密 PSK の確認 \(4 ページ\)](#)

秘密事前共有キーについて

Internet of Things (IoT) の出現により、インターネットに接続されるデバイスの数は著しく増加しています。これらのデバイスがすべて 802.1x サブリカントをサポートしているわけではないため、インターネットに接続するための代替メカニズムが必要です。セキュリティメカニズムの1つである WPA-PSK が代替手段として考えられます。現在の設定では、PSK は同じ WLAN に接続するすべてのクライアントで同じです。教育機関などの一部の設置環境では、これによりキーが不正ユーザーに共有され、セキュリティ違反が生じます。このため、大規模な範囲でクライアントごとに一意の PSK をプロビジョニングすることが必要になります。

Identity PSK は、同じ SSID の個人またはユーザー グループのために作成される一意の PSK です。クライアントに複雑な設定は必要ありません。PSK と同じシンプルさで、IoT、BYOD (Bring Your Own Device)、およびゲスト展開に適しています。PSK SSID のデフォルトパスワードは password です。

Identity PSK は 802.1x 未対応のほとんどのデバイスでサポートされるため、より強力な IoT セキュリティを実現します。他に影響を与えずに1つのデバイスまたは個人に対するアクセスを簡単に取り消せます。何千ものキーを簡単に管理でき、AAA サーバーを介して配布することができます。

IPSK ソリューション

クライアントの認証時に、AAA サーバーはクライアントの MAC アドレスを認証し、Cisco-AV ペアリストの一部としてパスフレーズ (設定されている場合) を送信します。組み込みワイヤレスコントローラは RADIUS 応答の一部としてパスフレーズを受信し、さらに処理して PSK を計算します。

クライアントが、対応するアクセスポイントによる SSID ブロードキャストに対して関連付け要求を送信すると、組み込みワイヤレスコントローラは、クライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバーに中継します。

RADIUS サーバーは認証を実行し、クライアントが許可されているかどうか、および WLC への応答として ACCESS-ACCEPT または ACCESS-REJECT のいずれかを送信するかどうかをチェックします。

Identity PSK をサポートするために、認証サーバーは認証応答を送信するだけでなく、この特定のクライアントに AV ペア パスフレーズを提供します。これは、PMK の計算に使用されます。

RADIUS サーバーは、ユーザー名、VLAN、Quality of Service (QoS) など、このクライアントに固有の追加パラメータも応答に含めることがあります。1 人のユーザーが複数のデバイスを所有している場合は、すべてのデバイスで同じパスフレーズを使用できます。



(注) PSK の長さが連邦情報処理標準 (FIPS) の 15 文字未満の場合、コントローラにより WLAN 設定は許可されますが、コンソールに次のエラーメッセージが表示されます。

「AP は接続できますが、対応する WLAN はアクセスポイントにプッシュされません (AP is allowed to join but corresponding WLAN will not be pushed to the access point)」

WLAN での PSK の設定 (CLI)

WLAN で PSK を設定するには、次の手順に従います。

始める前に

- WLAN で事前共有キー (PSK) のセキュリティを設定する必要があります。
- AAA サーバーからのオーバーライドがない場合は、対応する WLAN 上の値が認証用と見なされます。
- 連邦情報処理標準 (FIPS) およびコモンクライトリアモードでは、PSK WLAN に少なくとも 15 文字の ASCII 文字が含まれていることを確認します。含まれていない場合、AP はコントローラに接続しません。

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	wlan wlan-name wlan-id ssid 例 : Device(config)# wlan test-profile 4 abc	WLAN と SSID を設定します。
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 akm psk 例 : Device(config-wlan)# security wpa akm psk	セキュリティ タイプ PSK を設定しま す。
ステップ 5	security wpa akm psk set-key ascii/hex key 例 : Device(config-wlan)# security wpa akm psk set-key ascii 0	PSK 認証キー管理 (AKM) の共有キー を設定します。
ステップ 6	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 7	mac-filtering auth-list-name 例 : Device(config-wlan)# mac-filtering test1	WLAN で MAC フィルタリングを指定し ます。

WLAN での PSK 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 [Wireless Networks] ページで [Security] タブをクリックします。
 - ステップ 3 表示される [Layer 2] ウィンドウで、[WPA Parameters] セクションに移動します。
 - ステップ 4 [Auth Key Mgmt] ドロップダウンから [PSK] を選択します。
 - ステップ 5 [Save & Apply to Device] をクリックします。
-

WLAN へのポリシー プロファイルの適用 (GUI)

手順

-
- ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
 - ステップ 2 [Manage Tags] ページで、[Policy] タブをクリックします。
 - ステップ 3 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。
 - ステップ 4 ポリシー タグの名前と説明を入力します。
 - ステップ 5 [Add] をクリックして、WLAN とポリシーをマッピングします。
 - ステップ 6 適切なポリシープロファイルを使用してマッピングする WLAN プロファイルを選択し、チェック アイコンをクリックします。
 - ステップ 7 [Save & Apply to Device] をクリックします。
-

WLAN へのポリシー プロファイルの適用 (CLI)

WLAN にポリシープロファイルを適用するには、次の手順に従います。

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 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。

秘密 PSK の確認

WLAN とクライアントの設定を確認するには、次の **show** コマンドを使用します。

Device# **show wlan id 2**

```

WLAN Profile Name      : test_ppsk
=====
Identifier              : 2
Network Name (SSID)    : test_ppsk
Status                  : Enabled
Broadcast SSID         : Enabled
Universal AP Admin     : Disabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 0
Number of Active Clients : 0
Exclusionlist Timeout  : 60
CHD per WLAN          : Enabled
Interface              : default
Multicast Interface    : Unconfigured
WMM                    : Allowed
WifiDirect             : Invalid
Channel Scan Defer Priority:
  Priority (default)   : 4
  Priority (default)   : 5
  Priority (default)   : 6
Scan Defer Time (msecs) : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support : Enabled
CCX - Diagnostics Channel Capability : Disabled
Peer-to-Peer Blocking Action : Disabled
Radio Policy           : All
DTIM period for 802.11a radio : 1
DTIM period for 802.11b radio : 1
Local EAP Authentication : Disabled
Mac Filter Authorization list name : test1
Accounting list name   : Disabled
802.1x authentication list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys       : Disabled
  802.1X                : Disabled
  Wi-Fi Protected Access (WPA/WPA2) : Enabled
    WPA (SSN IE)        : Disabled
    WPA2 (RSN IE)       : Enabled
    TKIP Cipher         : Disabled
    AES Cipher          : Enabled
  Auth Key Management
    802.1x              : Disabled
    PSK                 : Enabled
    CCKM                : Disabled
    FT dot1x            : Disabled
    FT PSK              : Disabled
    PMF dot1x          : Disabled
    PMF PSK            : Disabled
  CCKM TSF Tolerance    : 1000
  FT Support            : Disabled
    FT Reassociation Timeout : 20
    FT Over-The-DS mode    : Enabled
  PMF Support           : Disabled
    PMF Association Comeback Timeout : 1
    PMF SA Query Time     : 200
  Web Based Authentication : Disabled
  Conditional Web Redirect : Disabled
  Splash-Page Web Redirect : Disabled
  Webauth On-mac-filter Failure : Disabled

```

```

Webauth Authentication List Name      : Disabled
Webauth Parameter Map                 : Disabled
Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping                         : Disabled
Passive Client                        : Disabled
Non Cisco WGB                         : Disabled
Band Select                           : Disabled
Load Balancing                        : Disabled
Multicast Buffer                       : Disabled
Multicast Buffer Size                  : 0
IP Source Guard                       : Disabled
Assisted-Roaming
  Neighbor List                       : Disabled
  Prediction List                     : Disabled
  Dual Band Support                   : Disabled
IEEE 802.11v parameters
  Directed Multicast Service          : Disabled
  BSS Max Idle                       : Disabled
  Protected Mode                     : Disabled
  Traffic Filtering Service           : Disabled
  BSS Transition                     : Enabled
  Disassociation Imminent            : Disabled
  Optimised Roaming Timer             : 40
  Timer                               : 200
  WNM Sleep Mode                     : Disabled
802.11ac MU-MIMO                      : Disabled

```

Device# **show wireless client mac-address a886.adb2.05f9 detail**

```

Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name :
Input Policy State : None
Input Policy Source : None
Output Policy Name :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0

```

```
Mobility:
  Move Count           : 0
  Mobility Role        : Local
  Mobility Roam Type    : None
  Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)|
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface           : capwap_90000005
  IIF ID              : 0x90000005
  Device Type         : Apple-Device
  Protocol Map        : 0x000001
  Authorized          : TRUE
  Session timeout     : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID    : 0x00000000
  Auth Method Status List
    Method : MAB
      SM State        : TERMINATE
      Authen Status   : Success
  Local Policies:
    Service Template : wlan_svc_default-policy-profile (priority 254)
    Absolute-Timer   : 320
    VLAN             : 58
  Server Policies:
  Resultant Policies:
    VLAN             : 58
    Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
```

```
Number of EAP Request Msg Timeouts :  
Number of EAP Key Msg Timeouts :  
Number of Policy Errors : 0  
Radio Signal Strength Indicator : -32 dBm  
Signal to Noise Ratio : 58 dB  
Fabric status : Disabled
```