



マルチ事前共有キー

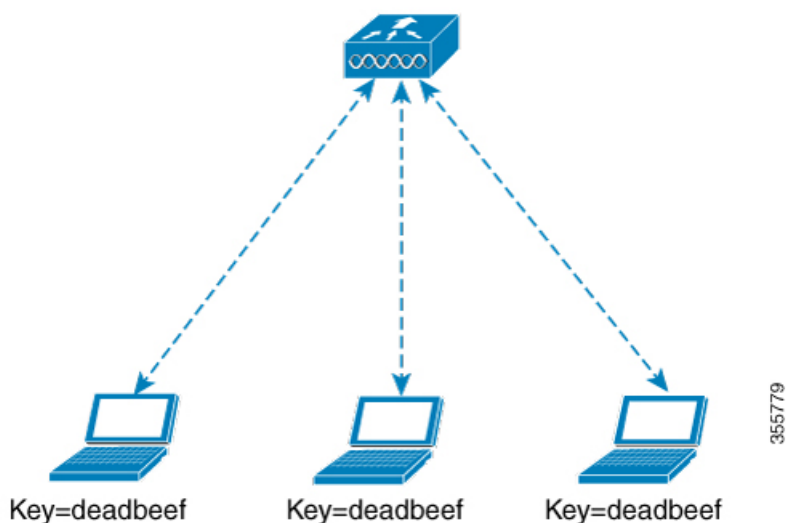
- [マルチ事前共有キーについて \(1 ページ\)](#)
- [マルチ PSK の制約事項 \(2 ページ\)](#)
- [マルチ事前共有キーの設定 \(GUI\) \(2 ページ\)](#)
- [マルチ事前共有キーの設定 \(CLI\) \(5 ページ\)](#)
- [マルチ PSK 設定の確認 \(6 ページ\)](#)

マルチ事前共有キーについて

マルチ PSK 機能は、1 つの SSID で同時に複数の PSK をサポートします。設定された PSK のいずれかを使用してネットワークに接続できます。これは Identity PSK (iPSK) とは異なり、同じ SSID 上の個人またはユーザー グループに対して一意の PSK が作成されます。

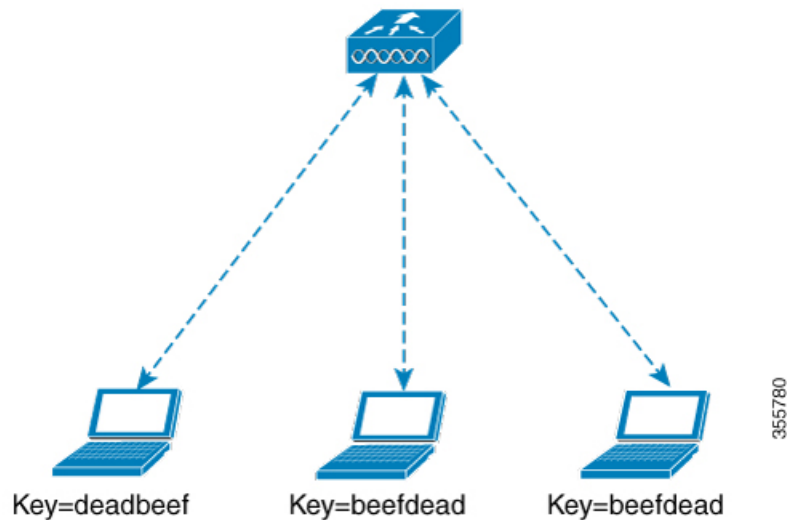
従来の PSK では、次の図に示すように、ネットワークに接続しているすべてのクライアントが同じパスワードを使用します。

図 1: 従来の PSK



ところがマルチ PSK を使用すると、クライアントは次の図に示すように設定済みの事前共有キーのいずれかを使用してネットワークに接続できます。

図 2: マルチ PSK



マルチ PSK では、同じ SSID に 2 つのパスワード（deadbeef と beefdead）が設定されます。このシナリオでは、クライアントはいずれかのパスワードを使用してネットワークに接続できます。

マルチ PSK の制約事項

- 中央認証は、ローカル、フレックス、およびファブリックモードでのみサポートされています。
- 中央認証フレックスモードの場合、スタンドアロン AP は、最もプライオリティの高い PSK（*priority 0* キー）を使用するクライアントの接続を許可します。最もプライオリティの高い PSK を使用しない新しいクライアントは、スタンドアロンモードでは拒否されません。
- マルチ PSK はローカル認証をサポートしません。

マルチ事前共有キーの設定（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 WLAN の名前をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。

ステップ 4 [Layer2] タブで、[Layer2 Security Mode] を次のオプションから選択します。

- [None] : レイヤ 2 セキュリティなし
- [802.1X] : WEP 802.1X データ暗号化タイプ
- [WPA + WPA2] : Wi-Fi Protected Access
- [Static WEP] : 静的 WEP 暗号化パラメータ
- [Static WEP+802.1X] : 静的 WEP と 802.1X の両方のパラメータ。

パラメータ	説明
802.1X	
WEP Key Size	キーサイズを選択します。使用可能な値は、[None]、[40 bits]、および [104 bits] です。
WPA + WPA2	
Protected Management Frame	次のオプションから選択します。 <ul style="list-style-type: none"> • デイセーブル • 任意 • 必須
WPA Policy	WPA ポリシーを有効にするには、このチェックボックスをオンにします。
WPA Encryption	WPA 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。
WPA2 Policy	WPA2 ポリシーを有効にするには、このチェックボックスをオンにします。
WPA2 Encryption	WPA2 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。

パラメータ	説明
Auth Key Mgmt	次のオプションからキー再生成メカニズムを選択します。 <ul style="list-style-type: none"> • 802.1X • [FT + 802.1X] • [PSK] : PSK 形式と事前共有キーを指定する必要があります • Cisco Centralized Key Management : Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。 • 802.1X + Cisco Centralized Key Management : Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。 • FT + 802.1X + Cisco Centralized Key Management : Cisco Centralized Key Management のタイムスタンプの許容値を指定する必要があります。
Static WEP	
Key Size	次のオプションからキーサイズを選択します。 <ul style="list-style-type: none"> • 40 ビット • 104 ビット
Key Index	1 ~ 4 の範囲でキー インデックスを選択します。各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化に設定できる WLAN は 4 つのみです。
Key Format	暗号キーの形式として、ASCII または HEX のいずれかを選択します。
Encryption Key	長さが 13 文字の暗号キーを入力します。
Static WEP + 802.1X	
Key Size	次のオプションからキーサイズを選択します。 <ul style="list-style-type: none"> • 40 ビット • 104 ビット

パラメータ	説明
Key Index	1～4の範囲でキーインデックスを選択します。各WLANに1つの一意なWEPキーインデックスを適用できます。WEPキーインデックスは4つしかないため、静的WEPレイヤ2暗号化に設定できるWLANは4つのみです。
Key Format	暗号キーの形式として、ASCIIまたはHEXのいずれかを選択します。
Encryption Key	長さが13文字の暗号キーを入力します。
WEP Key Size	次のオプションから選択します。 <ul style="list-style-type: none"> • なし • 40ビット • 104ビット

ステップ5 [Save & Apply to Device] をクリックします。

マルチ事前共有キーの設定 (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# <code>configure terminal</code>	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 wlan-id ssid 例： デバイス(config)# <code>wlan mywlan 1 SSID_name</code>	WLAN と SSID を設定します。
ステップ3	no security wpa akm dot1x 例： デバイス(config-wlan)# <code>no security wpa akm dot1x</code>	dot1x に対するセキュリティのAKMをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 4	security wpa akm psk 例： デバイス(config-wlan)# security wpa akm psk	PSK を設定します。
ステップ 5	security wpa wpa2 mpsk 例： デバイス(config-wlan)# security wpa wpa2 mpsk	マルチ PSK を設定します。
ステップ 6	priority priority_value set-key {ascii [0 8] pre-shared-key hex [0 8] pre-shared-key} 例： デバイス(config-mpsk)# priority 0 set-key ascii 0 deadbeef	PSK のプライオリティおよび関連するすべてのパスワードを設定します。 <i>priority_value</i> の範囲は 0 ~ 4 です。 (注) マルチ PSK には priority 0 キーを設定する必要があります。
ステップ 7	no shutdown 例： デバイス(config-mpsk)# no shutdown	WLAN を有効にします。
ステップ 8	exit 例： デバイス(config-wlan)# exit	WLAN コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 9	end 例： デバイス(config)# end	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

マルチ PSK 設定の確認

WLAN とクライアントの設定を確認するには、次のコマンドを使用します。

```
Device# show wlan id 8
WLAN Profile Name      : wlan_8
=====
Identifier              : 8
Network Name (SSID)    : ssid_8
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 : 200
Number of Active Clients : 0
```

```

CHD per WLAN : Enabled
Multicast Interface : Unconfigured
WMM : Allowed
WifiDirect : Invalid
Channel Scan Defer Priority:
  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 : Disabled
Mac Filter Override Authorization list name : Disabled
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys : Disabled
  802.1X : Disabled
  Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled
    WPA (SSN IE) : Disabled
    WPA2 (RSN IE) : Enabled
      MPSK : Enabled
      AES Cipher : Enabled
      CCMP256 Cipher : Disabled
      GCMP128 Cipher : Disabled
      GCMP256 Cipher : Disabled
    WPA3 (WPA3 IE) : Disabled
  Auth Key Management
    802.1x : Disabled
    PSK : Enabled
    CCKM : Disabled
    FT dot1x : Disabled
    FT PSK : Disabled
    FT SAE : Disabled
    PMF dot1x : Disabled
    PMF PSK : Disabled
    SAE : Disabled
    OWE : Disabled
    SUITEB-1X : Disabled
    SUITEB192-1X : Disabled
  CCKM TSF Tolerance : 1000
  FT Support : Adaptive
    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 Authorization List Name : Disabled
  Webauth Parameter Map : Disabled
  Tkip MIC Countermeasure Hold-down Timer : 60
Non Cisco WGB : Disabled
Band Select : Enabled

```

```

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
802.11ax parameters
  OFDMA Downlink              : unknown
  OFDMA Uplink                : unknown
  MU-MIMO Downlink            : unknown
  MU-MIMO Uplink              : unknown
  BSS Color                   : unknown
  Partial BSS Color           : unknown
  BSS Color Code              :

```

WLANの詳細を表示するには、次のコマンドを使用します。

```

Device# show run wlan
wlan wlan_8 8 ssid_8
security wpa psk set-key ascii 0 deadbeef
no security wpa akm dot1x
security wpa akm psk
security wpa wpa2 mpsk
priority 0 set-key ascii 0 deadbeef
priority 1 set-key ascii 0 deaddead
priority 2 set-key ascii 0 d123d123
priority 3 set-key hex 0 0234567890123456789012345678901234567890123456789012345678901234

priority 4 set-key hex 0 1234567890123456789012345678901234567890123456789012345678901234

no shutdown

```