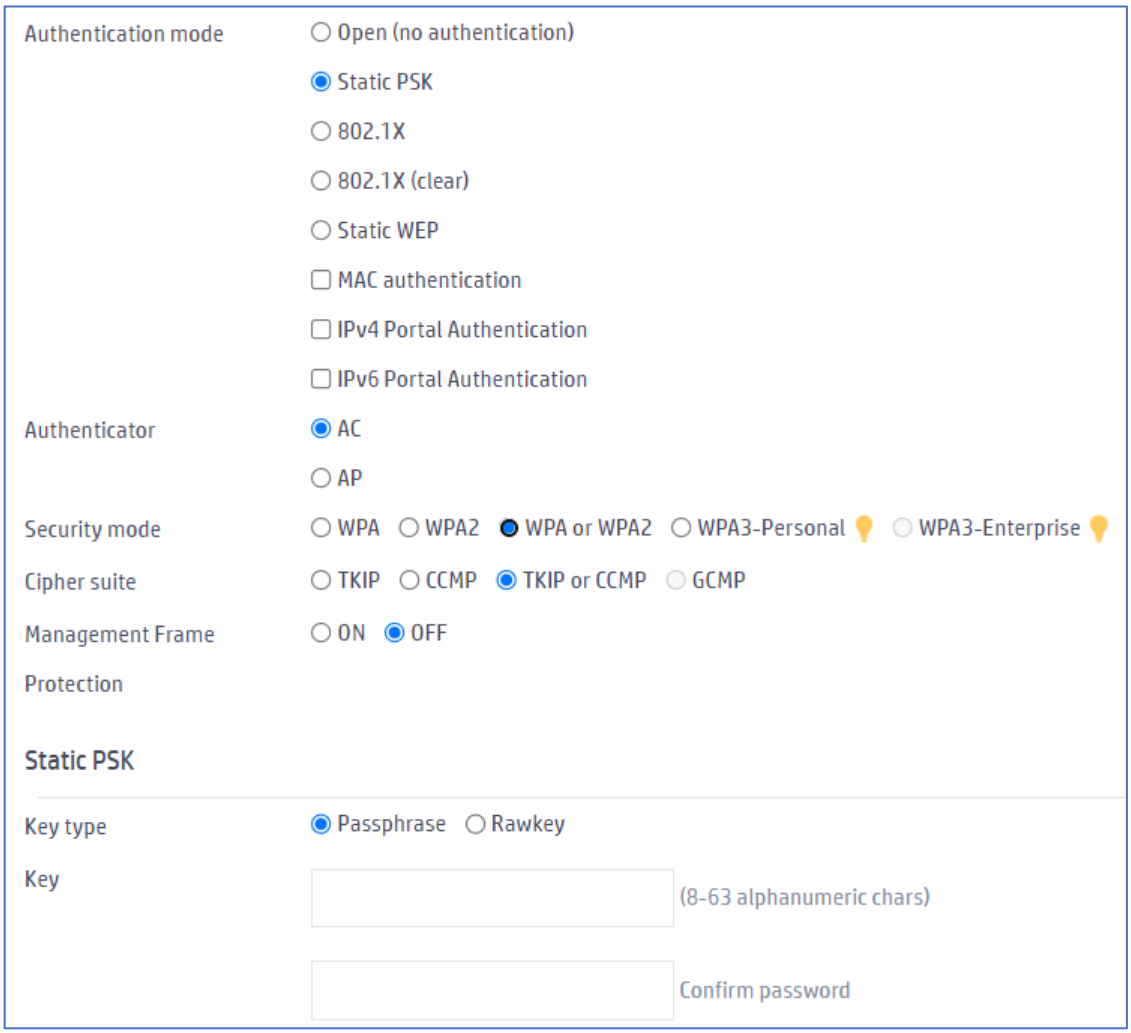
H3C
The Leader in Digital Solutions

H3C 無線コントローラのGUIでのSSID認証設定例

Comware 7 : SSIDの暗号化設定 (GUI)



```
#
################################
# Authentication mode: Static PSK
# Security mode: WPA2
# ( Cipher suite : AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$EZKnZU1oJCQdKFqEojI09QlBlEbGSHuJBuDh/Pw=
 cipher-suite ccmp
 security-ie rsn

################################
# Authentication mode: Static PSK
# Security mode: WPA or WPA2
# ( Cipher suite : TKIP or AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$EZKnZU1oJCQdKFqEojI09QlBlEbGSHuJBuDh/Pw=
 cipher-suite ccmp
 cipher-suite tkip
 security-ie rsn
 security-ie wpa

################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Required
# ( Cipher suite : AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$EZKnZU1oJCQdKFqEojI09QlBlEbGSHuJBuDh/Pw=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory

################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Optional
# ( Cipher suite : AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$EZKnZU1oJCQdKFqEojI09QlBlEbGSHuJBuDh/Pw=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal optional
```

```
################################
# Authentication mode: 802.1X
# Security mode: WPA2
# ( Cipher suite : AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain system

################################
# Authentication mode: 802.1X
# Security mode: WPA or WPA2
# ( Cipher suite : TKIP or AES-CCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode dot1x
 cipher-suite ccmp
 cipher-suite tkip
 security-ie rsn
 security-ie wpa
 client-security authentication-mode dot1x
 dot1x domain system

################################
# Authentication mode: 802.1X
# Security mode: WPA3-Enterprise
# ( Cipher suite : AES-GCMP )
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode dot1x
 cipher-suite gcmp
 security-ie rsn
 wpa3 enterprise
 client-security authentication-mode dot1x
 dot1x domain system
```

```
#################################
# Authentication mode: 802.1X ( clear )
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 client-security authentication-mode dot1x
 dot1x domain system

#################################
# Authentication mode: 802.1X ( clear )
# Handshake
# Re-authentication
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 client-security authentication-mode dot1x
 dot1x handshake enable
 dot1x re-authenticate enable
 dot1x domain system

#################################
# Authentication mode: Static PSK
# MAC Authentication
# Security mode: WPA or WPA2
# ( Cipher suite : TKIP or AES-CCMP )
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$b2tziJ8W+8HK+ahVcXUckiSkOKScFNPhPc4WYS8=
 cipher-suite ccmp
 cipher-suite tkip
 security-ie rsn
 security-ie wpa
 client-security authentication-mode mac
 mac-authentication domain system

#################################
# Authentication mode: Static PSK
# MAC Authentication
# Security mode: WPA
# ( Cipher suite : TKIP or AES-CCMP )
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$b2tziJ8W+8HK+ahVcXUckiSkOKScFNPhPc4WYS8=
 cipher-suite ccmp
 cipher-suite tkip
 security-ie wpa
 client-security authentication-mode mac
 mac-authentication domain system
```

```
#################################
# Authentication mode: Open ( no authentication )
#################################
wlan service-template 5
 ssid H3C_Wifi_x

#################################
# Authentication mode: Open ( no authentication )
# MAC Authentication
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 client-security authentication-mode mac
 mac-authentication domain system

#################################
# Authentication mode: Open
# ( Security mode: WPA2, AES-CCMP )
#################################
Openの設定にはWPA2, AESの設定がないのでCLIで追加設定
 cipher-suite ccmp      ( ccmp = AES-CCMP ),  ( gcmp = AES-GCMP )
 security-ie rsn
```

Comware 9 : SSIDの暗号化設定 (GUI)

Security mode
ベスト プラクティスとして、WPA3 を有効にしてセキュリティ モードを**Personal**に設定した後、Management Frame保護をONにします。

SAE PasswordElement
WPA3-SAEセキュリティモードにおいて、SAEプロセス中にPWEを生成する方法を指定します。特定の方法を指定すると、その方法をサポートしていない端末はワイヤレスネットワークに接続できなくなります。

WPA3 Anti-Downgrade
この機能を有効にすると、WPA3ネットワークに接続したWPA3クライアントは、同じSSIDを持つWPA2ネットワークに接続できなくなります。これにより、端末がセキュリティ性能の低い無線ネットワークに接続するのを防ぎます。

Management Frame
この機能を有効にすると、偽造された認証解除フレームやアソシエーション解除フレームなどの攻撃を防ぐための管理フレーム保護が行われます。

```
################################
# Authentication mode: Enhanced-Open
################################
wlan service-template 5
 ssid H3C_Wifi_x
 enhanced-open enable

################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Required
# SAE PasswordElement: H2E or HnP
# WPA3 Anti-Downgrade :OFF
# ( Cipher suite : AES-CCMP )
# Management Frame: OFF
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$ANlI+fet+KzKd2+mw2UrHfG5PCtPPK58wNxtneE=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory

################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Required
# SAE PasswordElement: H2E
# WPA3 Anti-Downgrade :OFF
# ( Cipher suite : AES-CCMP )
# Management Frame: OFF
################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$ANlI+fet+KzKd2+mw2UrHfG5PCtPPK58wNxtneE=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory
 akm sae pwe h2e
```

```
#################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Required
# SAE PasswordElement: HnP
# WPA3 Anti-Downgrade :OFF
# ( Cipher suite : AES-CCMP )
# Management Frame: OFF
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$ANlI+fet+KzKd2+mw2UrHfG5PCtPPK58wNxtneE=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory
 akm sae pwe hnp

#################################
# Authentication mode: Static PSK
# Security mode: WPA3-Personal
# WPA3-Personal Mode: Required
# SAE PasswordElement: HZE or HnP
# WPA3 Anti-Downgrade :ON
# ( Cipher suite : AES-CCMP )
# Management Frame: OFF
#################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode psk
 preshared-key pass-phrase cipher $c$3$ANlI+fet+KzKd2+mw2UrHfG5PCtPPK58wNxtneE=
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory
 wpa3 transit-wpa2-disable
```

** WiFi 7に適応 **
Authentication mode: **Static PSK**
Security mode: **WPA3-Personal**
WPA3-Personal Mode: **Required**
SAE PasswordElement: H2e
WPA3 Anti-Downgrade :OFF
(Cipher suite : **AES-CCMP)**
Management Frame: ON
##################################
wlan service-template staff-wpa3
 ssid staff-wpa3
 akm mode psk
 preshared-key pass-phrase simple h3cjapan123
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal mandatory
 akm sae pwe h2e
 pmf mandatory

** WiFi 7に適応 **
Authentication mode: **Static PSK**
Security mode: **WPA3-Personal**
WPA3-Personal Mode: **Optional**
SAE PasswordElement: HnP
WPA3 Anti-Downgrade :OFF
(Cipher suite : **AES-CCMP)**
Management Frame: OFF
##################################
wlan service-template user-wpa3
 ssid user-wpa3
 akm mode psk
 preshared-key pass-phrase simple h3cjapan123
 cipher-suite ccmp
 security-ie rsn
 wpa3 personal optional
 akm sae pwe hnp
 pmf optional

##################################
Authentication mode: **802.1x**
Security mode: **WPA3-Enterprise** (設定不可:WPA3−Personal)
(Cipher suite : **AES-GCMP)**
Management Frame: OFF
Dynamic WEP: off
Handshake: OFF
Reauthentication: OFF
Domain name: system
##################################
wlan service-template 5
 ssid H3C_Wifi_x
 akm mode dot1x
 cipher-suite gcmp
 security-ie rsn
 wpa3 enterprise
 wpa3 transit-wpa2-disable
 client-security authentication-mode dot1x
 dot1x domain system

AES-CCMP (**C**ounter Mode with **C**ipher Block Chaining **M**essage Authentication Code **P**rotocol) と AES-GCMP (**G**alois/**C**ounter **M**ode **P**rotocol) は、Wi-Fiネットワークにおける暗号化方式の一部であり、それぞれに特徴と用途があります。以下に両者の主な違いを示します。

1. 暗号化モード

AES-CCMP:
カウンタモード (Counter Mode) を使用して暗号化を行い、CBC-MAC (Cipher Block Chaining Message Authentication Code) を使用してデータの整合性を確認します。
データのセキュリティと整合性をバランスよく提供します。

AES-GCMP:
ガロア/カウンタモード (Galois/Counter Mode) を使用します。
ガロアフィールドを利用した高速なデータ整合性チェックを可能にします。
より新しいプロトコルで、計算効率が高い。

2. セキュリティ

AES-CCMP:
WPA2の標準暗号化方式として広く使用されています。
セキュリティは高いが、特定の攻撃シナリオではGCMPよりも若干遅いことがあります。

AES-GCMP:
WPA3において採用され、WPA2と比較してさらに強化されたセキュリティを提供します。
データの認証と暗号化が統合されているため、効率的かつ安全性が高い。

3. パフォーマンス

AES-CCMP:
暗号化と認証が独立して実行されるため、計算量が多くなりがちです。
パフォーマンスが求められるシナリオではGCMPに劣ることがあります。

AES-GCMP:
認証と暗号化を一体化した設計により、CCMPよりも処理速度が速い。
特に高速ネットワークや大規模な通信量がある環境で有利。

4. 適用シナリオ

AES-CCMP:
既存のWPA2ネットワークでの使用。
互換性を重視する場合に適しています。

AES-GCMP:
新しいWi-Fi規格 (特にWi-Fi 6やWPA3) に対応するアクセスポイントやデバイスに適しています。
高速かつ安全な通信が必要な場合に推奨。

www.h3c.com