

使用預共用金鑰配置WPA/WPA2:IOS 15.2JB及更高版本

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[使用GUI配置](#)

[使用CLI進行配置](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹使用預先共用金鑰(PSK)的無線保護存取(WPA)和WPA2的組態範例。

必要條件

需求

思科建議您瞭解以下主題：

- 熟悉Cisco IOS®軟體的GUI或命令列介面(CLI)
- 熟悉PSK、WPA和WPA2的概念

採用元件

本檔案中的資訊是根據執行Cisco IOS軟體版本15.2JB的Cisco Aironet 1260存取點(AP)。

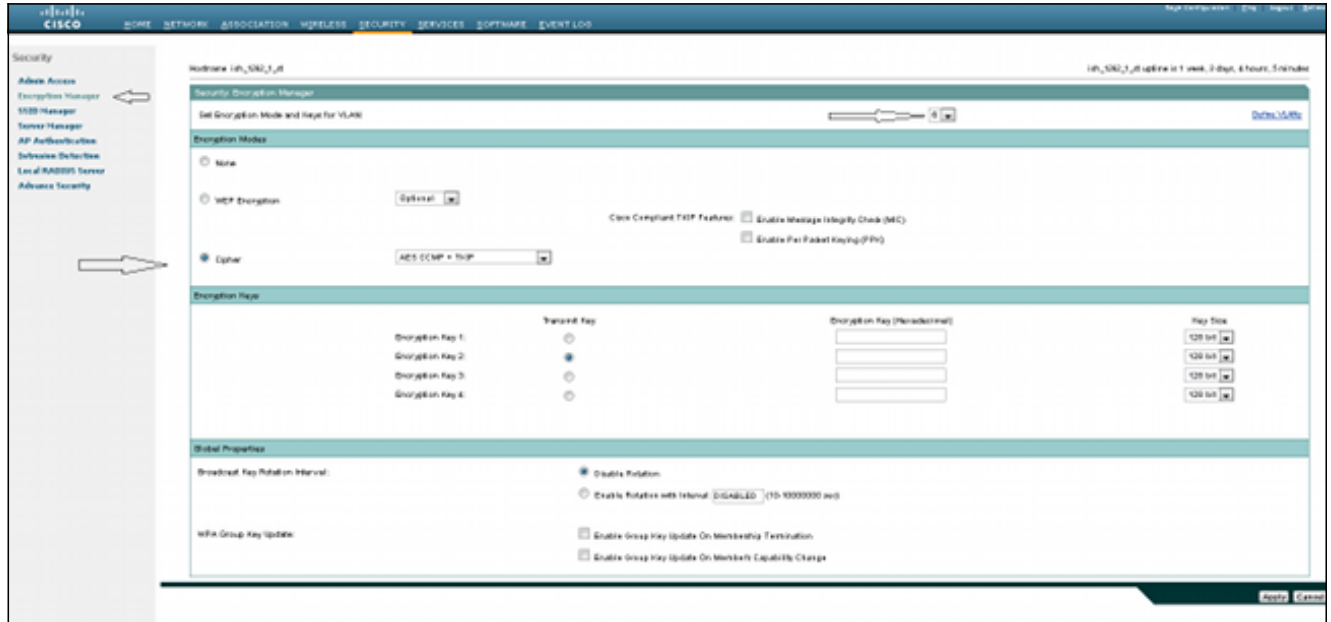
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

使用GUI配置

以下過程介紹如何在Cisco IOS軟體GUI中使用PSK配置WPA和WPA2:

1. 為為服務集識別符號(SSID)定義的VLAN設定加密管理器。導覽至**Security > Encryption Manager**，確保啟用密碼，然後選擇**AES CCMP + TKIP**作為兩個SSID使用的密碼。



2. 使用步驟1中定義的加密引數啟用正確的VLAN。導航到**Security > SSID Manager**，然後從**Current SSID List**中選擇SSID。此步驟對於WPA和WPA2配置都是通用的。



3. 在SSID頁面中，將Key Management設定為**Mandatory**，然後選中**Enable WPA**覆取方塊。從下拉選單中選擇**WPA**以啟用WPA。輸入WPA預共用金鑰。



4. 從下拉選單中選擇**WPA2**以啟用WPA2。



使用CLI進行配置

附註：

使用[命令查詢工具](#)(僅供[已註冊](#)客戶使用)可獲取本節中使用的命令的更多資訊。

[輸出直譯器工具](#)(僅供[已註冊](#)客戶使用)支援某些show命令。使用輸出直譯器工具來檢視show命令輸出的分析。

此配置與CLI中的配置相同：

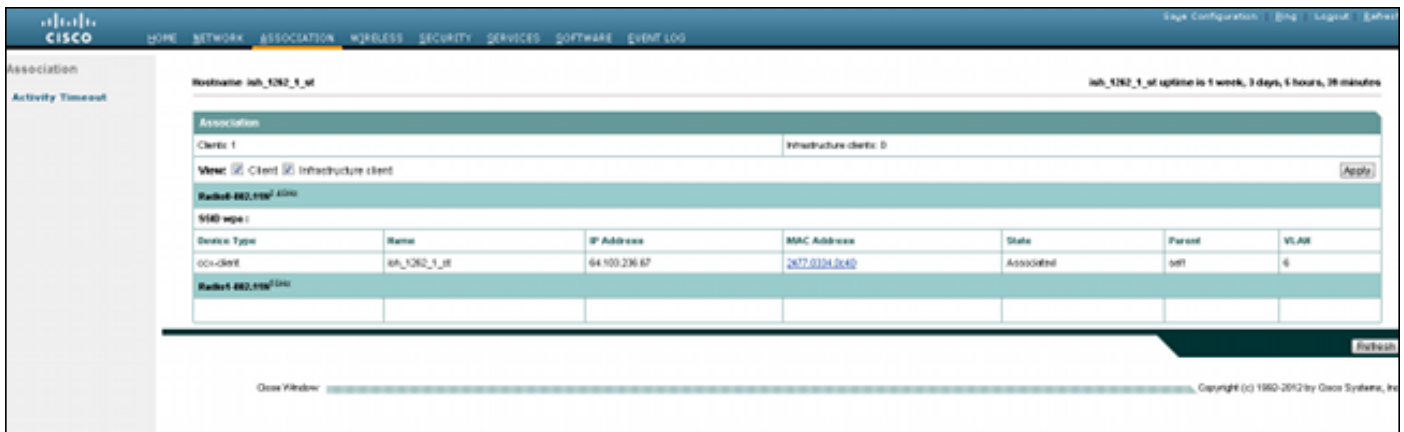
```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ish_1262_1_st
!
!
logging rate-limit console 9
enable secret 5 $1$Iykv$1tUkNYeB6omK41S181TbQ1
!
no aaa new-model
ip cef
ip domain name cisco.com
!
!
!
dot11 syslog
!
dot11 ssid wpa
vlan 6
authentication open
authentication key-management wpa
mbssid guest-mode
wpa-psk ascii 7 060506324F41584B56
!
dot11 ssid wpa2
vlan 7
authentication open
authentication key-management wpa version 2
wpa-psk ascii 7 110A1016141D5A5E57
!
bridge irb
!
!
!
interface Dot11Radio0
```

```
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
ssid wpa2
!
antenna gain 0
mbssid
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.6
encapsulation dot1Q 6
no ip route-cache
bridge-group 6
bridge-group 6 subscriber-loop-control
bridge-group 6 spanning-disabled
bridge-group 6 block-unknown-source
no bridge-group 6 source-learning
no bridge-group 6 unicast-flooding
!
interface Dot11Radio0.7
encapsulation dot1Q 7
no ip route-cache
bridge-group 7
bridge-group 7 subscriber-loop-control
bridge-group 7 spanning-disabled
bridge-group 7 block-unknown-source
no bridge-group 7 source-learning
no bridge-group 7 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 6 mode ciphers aes-ccm tkip
!
encryption vlan 7 mode ciphers aes-ccm tkip
!
ssid wpa
!
ssid wpa2
!
antenna gain 0
no dfs band block
mbssid
channel dfs
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
```

```
!  
interface Dot11Radio1.6  
encapsulation dot1Q 6  
no ip route-cache  
bridge-group 6  
bridge-group 6 subscriber-loop-control  
bridge-group 6 spanning-disabled  
bridge-group 6 block-unknown-source  
no bridge-group 6 source-learning  
no bridge-group 6 unicast-flooding  
!  
interface Dot11Radio1.7  
encapsulation dot1Q 7  
no ip route-cache  
bridge-group 7  
bridge-group 7 subscriber-loop-control  
bridge-group 7 spanning-disabled  
bridge-group 7 block-unknown-source  
no bridge-group 7 source-learning  
no bridge-group 7 unicast-flooding  
!  
interface GigabitEthernet0  
no ip address  
no ip route-cache  
duplex auto  
speed auto  
no keepalive  
bridge-group 1  
bridge-group 1 spanning-disabled  
no bridge-group 1 source-learning  
!  
interface GigabitEthernet0.6  
encapsulation dot1Q 6  
no ip route-cache  
bridge-group 6  
bridge-group 6 spanning-disabled  
no bridge-group 6 source-learning  
!  
interface GigabitEthernet0.7  
encapsulation dot1Q 7  
no ip route-cache  
bridge-group 7  
bridge-group 7 spanning-disabled  
no bridge-group 7 source-learning  
!  
interface BVI1  
ip address 10.105.132.172 255.255.255.128  
no ip route-cache  
!  
ip forward-protocol nd  
ip http server  
ip http secure-server
```

驗證

若要確認組態是否正常運作，請導覽至 **Association**，驗證使用者端是否已連線：



您也可以在CLI中使用此系統日誌消息驗證客戶端關聯：

```
*Mar 11 05:39:11.962: %DOT11-6-ASSOC: Interface Dot11Radio0, Station  
ish_1262_1_st 2477.0334.0c40 Associated KEY_MGMT[WPAv2 PSK]
```

疑難排解

附註：使用 `debug` 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

使用以下debug命令可對連線問題進行疑難排解：

- `debug dot11 aaa manager keys` — 此調試顯示AP和客戶端之間的握手，作為成對臨時金鑰 (PTK)和組臨時金鑰(GTK)協商。
- `debug dot11 aaa authenticator state-machine` — 此調試顯示客戶端在關聯和身份驗證時經歷的各種協商狀態。狀態名稱表示這些狀態。
- `debug dot11 aaa authenticator process` — 此調試可幫助您診斷協商通訊的問題。詳細資訊顯示協商中的每個參與者傳送的内容，並顯示另一個參與者的響應。您還可以將此調試與`debug radius authentication`命令結合使用。
- `debug dot11 station connection failure` — 此調試可幫助您確定客戶端連線是否失敗，並幫助您確定失敗的原因。