Configurazione di WPA/WPA2 con chiave già condivisa: IOS 15.2JB e versioni successive

Sommario

Introduzione

In questo documento viene descritta una configurazione di esempio per WPA (Wireless Protected Access) e WPA2 con una chiave precondivisa (PSK).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Familiarità con la GUI o l'interfaccia della riga di comando (CLI) per il software Cisco IOS®.
- Familiarità con i concetti di PSK, WPA e WPA2

Componenti usati

Per questo documento, è stato usato un Access Point (AP) Cisco Aironet 1260 con software Cisco IOS versione 15.2JB.

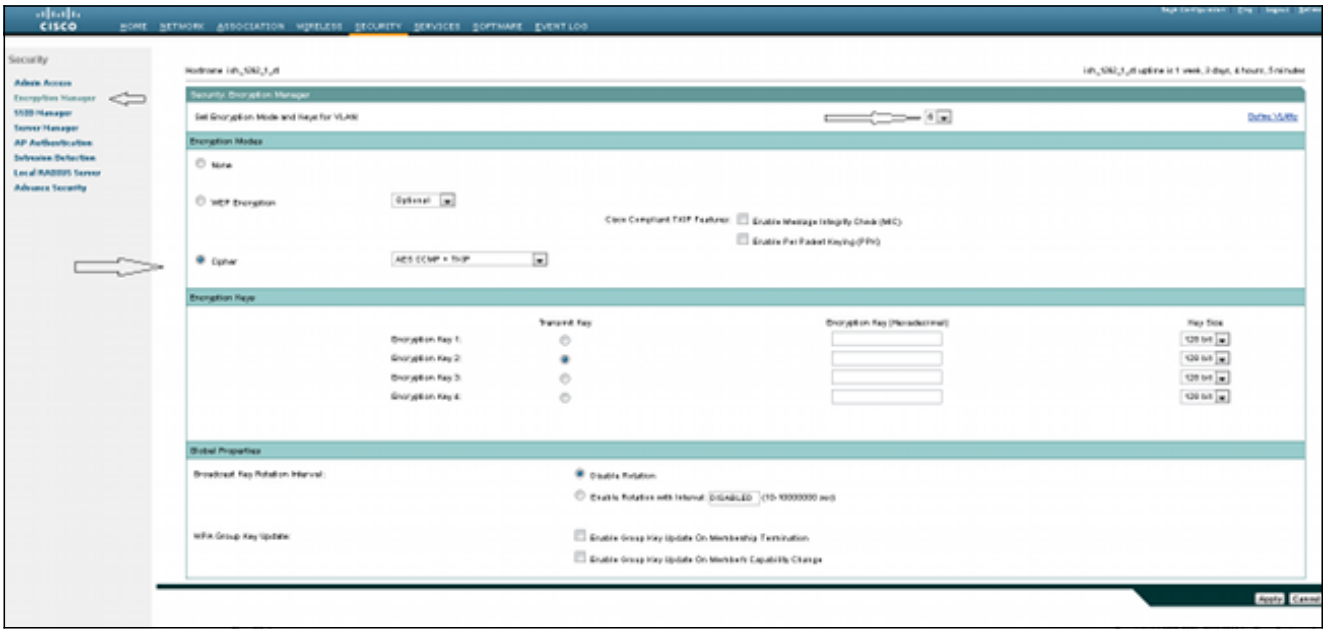
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Configurazione con GUI

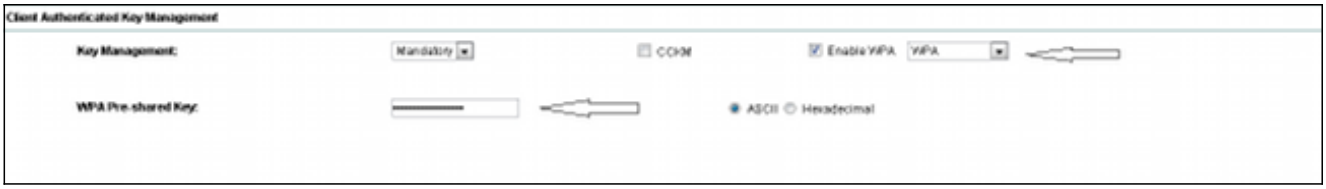
In questa procedura viene descritto come configurare WPA e WPA2 con una chiave già condivisa nell'interfaccia utente del software Cisco IOS:

1. Configurare Gestione crittografia per la VLAN definita per l'SSID (Service Set Identifier). Selezionare **Security > Encryption Manager**, verificare che la crittografia sia abilitata e selezionare **AES CCMP + TKIP** come crittografia da utilizzare per entrambi gli SSID.



2. Abilitare la VLAN corretta con i parametri di crittografia definiti nel passaggio 1. Selezionare **Security > SSID Manager**, quindi selezionare il SSID dall'elenco SSID corrente. Questo passaggio è comune per la configurazione di WPA e WPA2.

3. Nella pagina SSID, impostare Gestione chiavi su **Obbligatorio** e selezionare la casella di controllo **Abilita WPA**. Per abilitare WPA, selezionare **WPA** dall'elenco a discesa. Immettere la chiave già condivisa WPA.



4. Selezionare **WPA2** dall'elenco a discesa per abilitare WPA2.

Configurazione con CLI

Note:

per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Questa è la stessa configurazione eseguita nella CLI:

```
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$1tUkNYeB6omK41S18lTbQ1
!
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, passare a **Associazione** e verificare che il client sia connesso:

Èpossibile anche verificare l'associazione del client nella CLI con questo messaggio syslog:

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

Risoluzione dei problemi

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Utilizzare questi comandi di debug per risolvere i problemi di connettività:

- **debug dot11 aaa manager keys**: questo debug visualizza l'handshake che si verifica tra l'access point e il client durante la negoziazione della chiave temporanea pairwise (PTK) e della chiave temporanea di gruppo (GTK).
- **macchina a stati dell'autenticatore debug dot11 aaa** - Questo debug mostra i vari stati delle negoziazioni attraversate da un client durante l'associazione e l'autenticazione del client. I nomi degli stati indicano questi stati.
- **debug dot11 aaa authentication process** - Questo debug consente di diagnosticare i problemi relativi alle comunicazioni negoziate. Le informazioni dettagliate mostrano ciò che ogni partecipante alla negoziazione invia e mostrano la risposta dell'altro partecipante. È possibile usare questo debug anche con il comando **debug radius authentication**.
- **debug dot11 station connection failure** - Questo debug consente di determinare se i client non riescono a connettersi e di determinare la causa degli errori.