Configuration de WPA/WPA2 avec clé prépartagée : IOS 15.2JB et versions ultérieures

Contenu

Introduction

Ce document décrit un exemple de configuration pour Wireless Protected Access (WPA) et WPA2 avec une clé prépartagée (PSK).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de l'interface utilisateur graphique ou de l'interface de ligne de commande (CLI) du logiciel Cisco IOS®
- Connaissance des concepts de PSK, WPA et WPA2

Components Used

Les informations de ce document sont basées sur le point d'accès Cisco Aironet 1260 qui exécute le logiciel Cisco IOS Version 15.2JB.

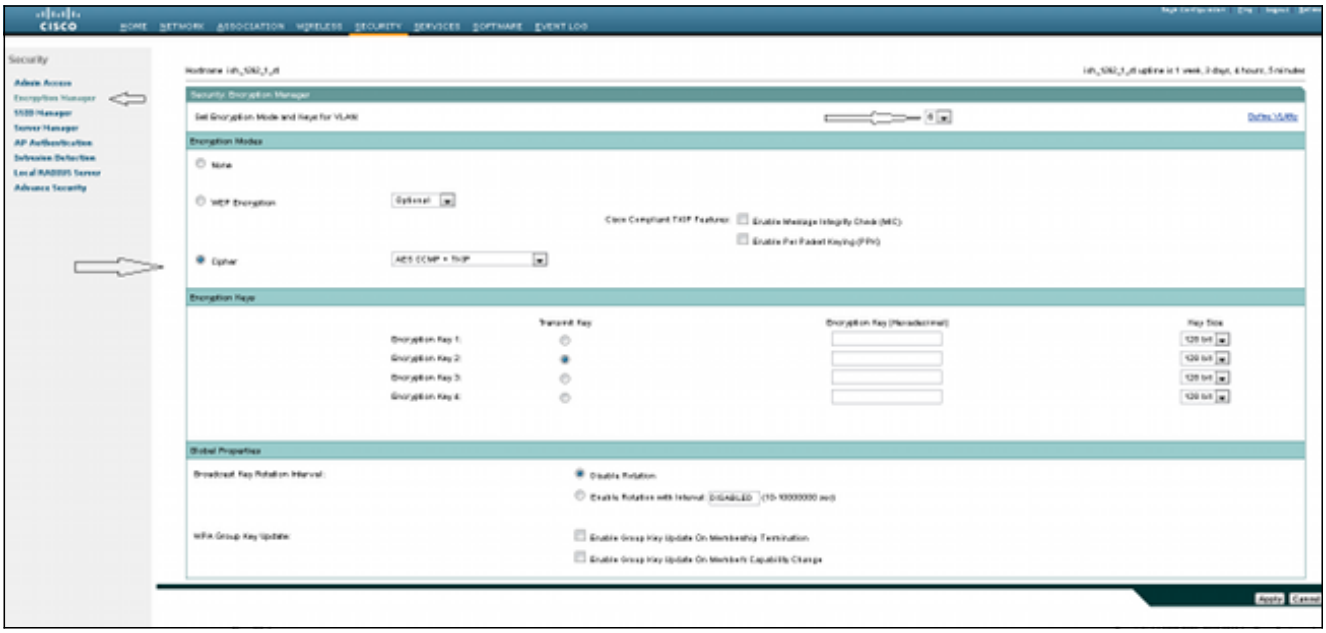
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration

Configuration avec interface utilisateur graphique

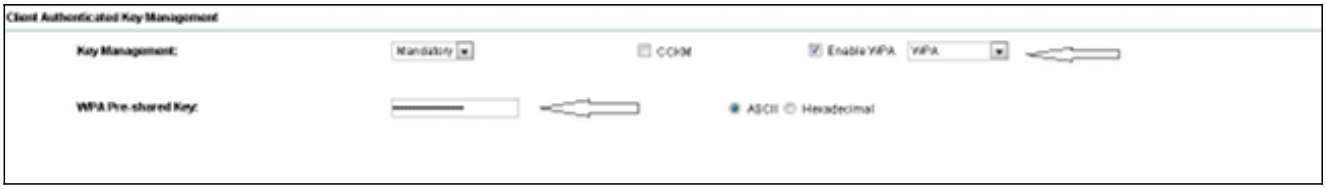
Cette procédure décrit comment configurer WPA et WPA2 avec un PSK dans l'interface utilisateur graphique du logiciel Cisco IOS :

1. Configurez le gestionnaire de cryptage pour le VLAN défini pour le SSID (Service Set Identifier). Accédez à **Security > Encryption Manager**, assurez-vous que Cipher est activé et sélectionnez **AES CCMP + TKIP** comme chiffre à utiliser pour les deux SSID.



2. Activez le VLAN correct avec les paramètres de chiffrement définis à l'étape 1. Accédez à **Security > SSID Manager**, puis sélectionnez le SSID dans la liste des SSID actuels. Cette étape est courante pour la configuration WPA et WPA2.

3. Dans la page SSID, définissez Key Management sur **Mandatory**, et cochez la case **Enable WPA**. Sélectionnez **WPA** dans la liste déroulante afin d'activer WPA. Saisissez la clé pré-partagée WPA.



4. Sélectionnez **WPA2** dans la liste déroulante afin d'activer WPA2.

Configuration avec CLI

> **Remarques :**
>
> Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Il s’agit de la même configuration effectuée dans l’interface de ligne de commande :

```
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
```

Vérification

Afin de confirmer que la configuration fonctionne correctement, accédez à **Association** et vérifiez que le client est connecté :

Vous pouvez également vérifier l'association du client dans l'interface de ligne de commande avec ce message 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]
```

Dépannage

> **Note**: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Utilisez ces commandes debug afin de résoudre les problèmes de connectivité :

- **debug dot11 aaa manager keys** - Ce débogage montre la connexion qui se produit entre le point d'accès et le client en tant que négociation de la clé transitoire par paire (PTK) et de la clé transitoire par groupe (GTK).
- **debug dot11 aaa authenticator state-machine** - Ce débogage montre les différents états de négociations qu'un client passe en tant que client s'associe et s'authentifie. Les noms d'état indiquent ces états.
- **debug dot11 aaa authenticator process** - Ce débogage vous aide à diagnostiquer les problèmes de communications négociées. Les informations détaillées montrent ce que chaque participant à la négociation envoie ainsi que la réponse de l'autre participant. Vous pouvez également employer ce débogage avec la commande **debug radius authentication.**
- **debug dot11 station connection fail** - Ce débogage vous aide à déterminer si les clients échouent à la connexion et vous aide à déterminer la raison des échecs.