Configuration de WPA/WPA2 avec la clé pré-partagée : IOS 15.2JB et plus tard

Contenu

Introduction

Ce document décrit une configuration d'échantillon pour Protected Access Sans fil (WPA) et le WPA2 avec une clé pré-partagée (PSK).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Les informations dans ce document sont basées sur Cisco Aironet 1260 Points d'accès (AP) que la version du logiciel Cisco IOS 15.2JB de passages.

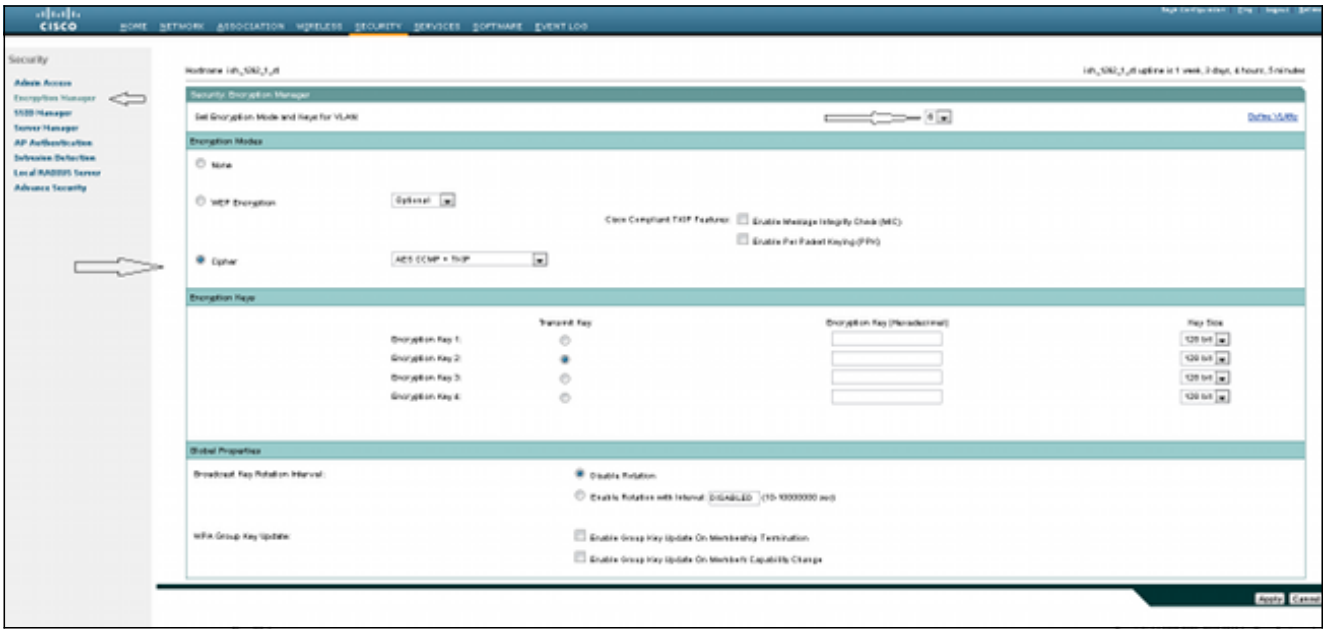
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Configuration avec le GUI

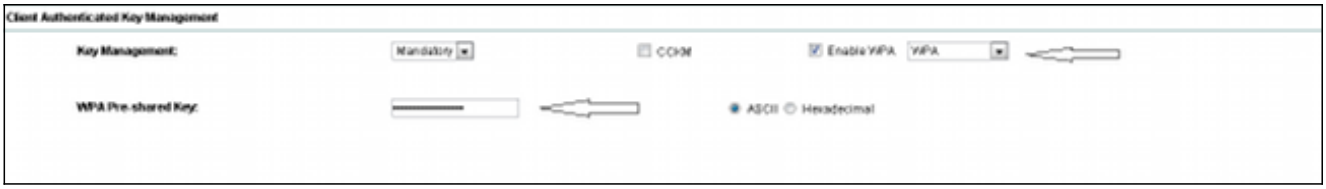
Cette procédure décrit comment configurer le WPA et le WPA2 avec un PSK dans le GUI de logiciel de Cisco IOS :

1. Installez le gestionnaire de cryptage pour le VLAN défini pour l'Identifiant SSID (Service Set Identifier). Naviguez vers le **Security > Encryption Manager**, assurez que le chiffrement est activé, et **AES** choisi **CCMP + TKIP** comme chiffrement à utiliser pour des les deux SSID.



2. Activez le VLAN correct avec les paramètres de chiffrement définis dans l'étape 1. naviguent vers le **Security > SSID Manager**, et sélectionnent le SSID de la liste du courant SSID. Cette étape est commune pour la configuration WPA et WPA2.

3. Dans la page SSID, placez la gestion des clés à **obligatoire**, et vérifiez la case à cocher de l'**enable WPA**. Sélectionnez le **WPA de la** liste déroulante afin d'activer le WPA. Introduisez la clé pré-partagée WPA.



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

Configuration avec le CLI

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

C'est la même configuration faite dans le 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
```

Vérifiez

Afin de confirmer que la configuration fonctionne correctement, naviguez vers l'**association**, et vérifiez que le client est connecté :

Vous pouvez également vérifier l'association de client dans le CLI avec ce message de 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]
```

Dépannez

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

Employez ces commandes de débogage afin de dépanner des problèmes de connectivité :

- **clés de gestionnaire de debug dot11 aaa** - Ceci mettent au point des expositions la prise de contact qui se produit entre AP et le client comme clé par paires passagère (PTK) et la clé passagère de groupe (GTK) négocient.
- **state-machine d'authentificateur de debug dot11 aaa** - Ceci mettent au point des expositions les divers états de négociations qu'un client traverse pendant que le client s'associe et authentifie. Les noms d'état indiquent ces états.
- **processus d'authentificateur de debug dot11 aaa** - Ceci mettent au point des aides que vous diagnostiquez des problèmes avec des transmissions 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**.
- **panne de connexion de station de debug dot11** - Ceci mettent au point des aides que vous déterminez si les clients manquent la connexion et vous aidez à déterminer la raison pour des pannes.