Configuração de WPA/WPA2 com chave pré-compartilhada: IOS 15.2JB e posterior

Contents

Introduction

Este documento descreve um exemplo de configuração para Wireless Protected Access (WPA) e WPA2 com uma chave pré-compartilhada (PSK).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Familiaridade com a GUI ou a interface de linha de comando (CLI) para o software Cisco IOS®
- Familiaridade com os conceitos de PSK, WPA e WPA2

Componentes Utilizados

As informações neste documento são baseadas no Access Point (AP) Cisco Aironet 1260 que executa o Cisco IOS Software Release 15.2JB.

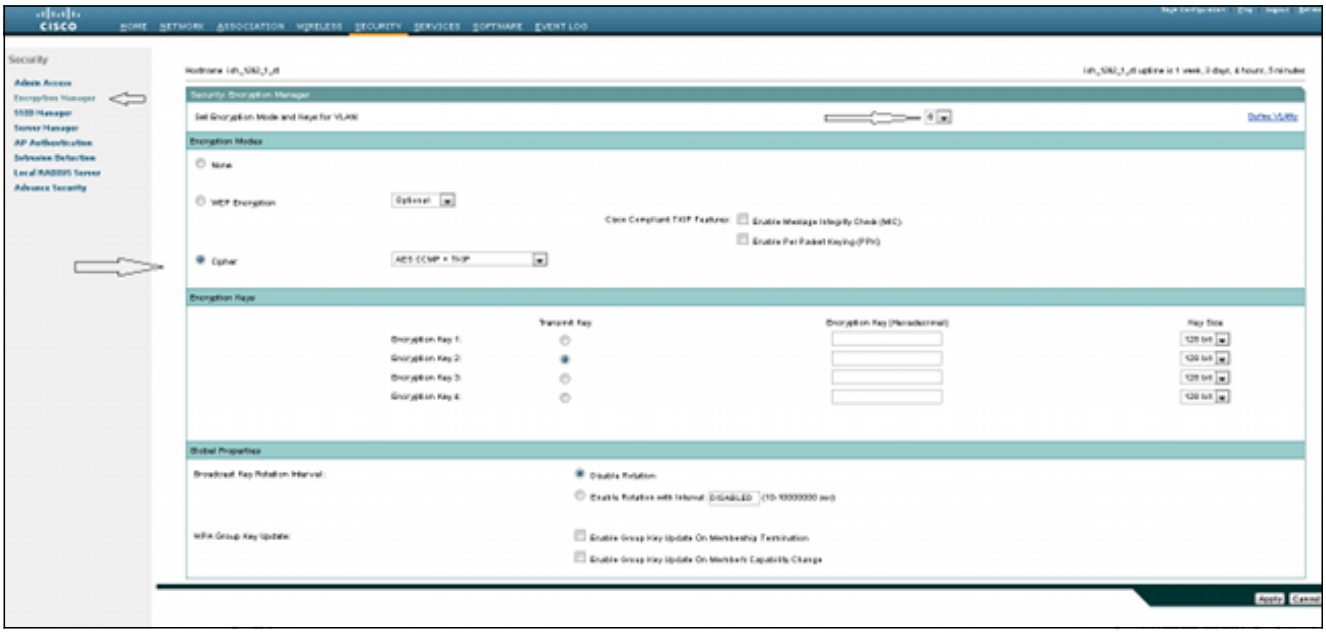
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Configuração com GUI

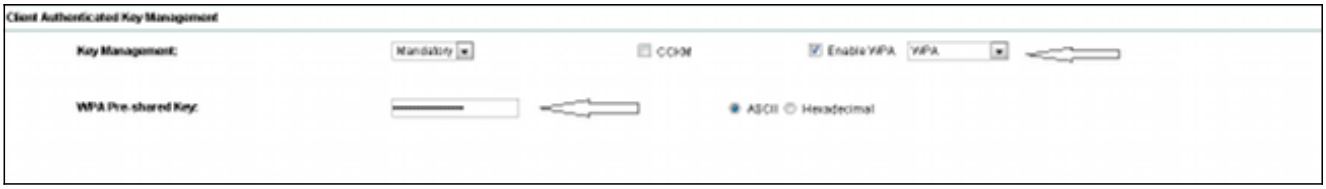
Este procedimento descreve como configurar WPA e WPA2 com uma PSK na GUI do software Cisco IOS:

1. Configure o Encryption Manager para a VLAN definida para o Service Set Identifier (SSID). Navegue até **Security > Encryption Manager**, verifique se Cipher está habilitada e selecione **AES CCMP + TKIP** como a cifra a ser usada para ambos os SSIDs.



2. Ative a VLAN correta com os parâmetros de criptografia definidos na Etapa 1. Navegue até **Security > SSID Manager** e selecione o SSID na Lista de SSID atual. Essa etapa é comum para a configuração de WPA e WPA2.

3. Na página SSID, defina Key Management como **Obrigatory** e marque a caixa de seleção **Enable WPA**. Selecione **WPA** na lista suspensa para habilitar a WPA. Insira a chave pré-compartilhada WPA.



4. Selecione **WPA2** na lista suspensa para habilitar a WPA2.

Configuração com CLI

Notas:

Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Esta é a mesma configuração feita na 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
```

Verificar

Para confirmar se a configuração funciona corretamente, navegue até **Association** e verifique se o cliente está conectado:

Você também pode verificar a associação do cliente na CLI com esta mensagem 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]
```

Troubleshoot

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Use estes comandos debug para solucionar problemas de conectividade:

- **debug dot11 aaa manager keys** - Esta depuração mostra o handshake que ocorre entre o AP e o cliente como a chave transiente (PTK) emparelhada e a chave transiente de grupo (GTK) negociada.
- **debug dot11 aaa authenticator state-machine** - Esta depuração mostra os vários estados de negociações pelos quais um cliente passa enquanto o cliente associa e autentica. Os nomes de estado indicam esses estados.
- **debug dot11 aaa authenticator process** - Esta depuração ajuda a diagnosticar problemas com comunicações negociadas. As informações detalhadas mostram o que cada participante na negociação envia e mostra a resposta do outro participante. Você também pode usar essa depuração em conjunto com o comando **debug radius authentication**.
- **debug dot11 station connection failure** - Essa depuração ajuda a determinar se os clientes estão falhando na conexão e ajuda a determinar o motivo das falhas.