Configuration of WPA/WPA2 with Pre−Shared Key: IOS 15.2JB and Later

Document ID: 116599

Contributed by Ishaan Sanji, Cisco TAC Engineer.
Oct 23, 2013

Contents

Introduction

This document describes a sample configuration for Wireless Protected Access (WPA) and WPA2 with a pre−shared key (PSK).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Familiarity with the GUI or the command−line interface (CLI) for the Cisco IOS® software
- Familiarity with the concepts of PSK, WPA, and WPA2

Components Used

The information in this document is based on Cisco Aironet 1260 Access Point (AP) that runs Cisco IOS Software Release 15.2JB.

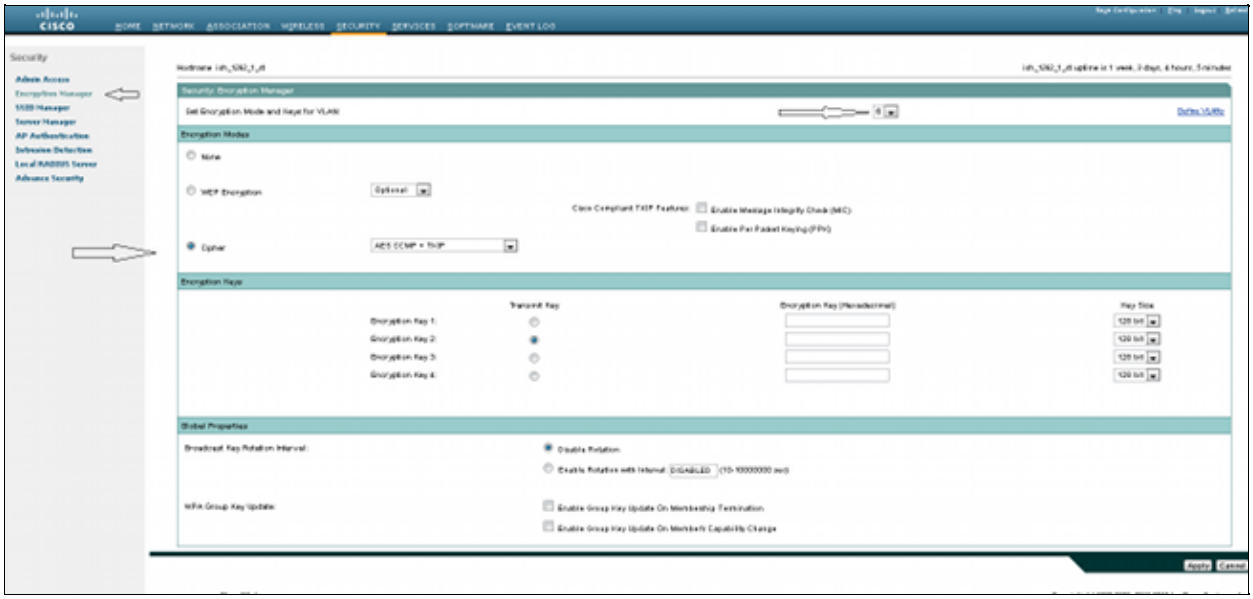
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Configuration with GUI

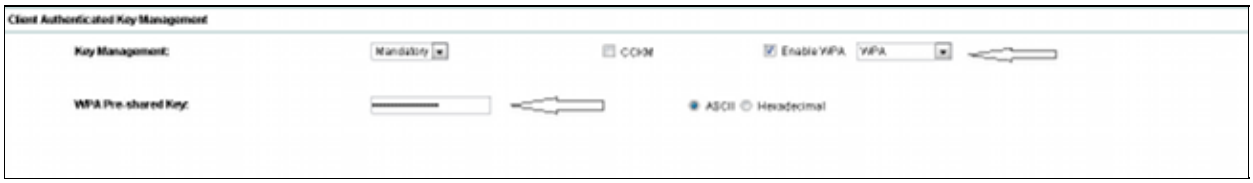
This procedure describes how to configure WPA and WPA2 with a PSK in the Cisco IOS software GUI:

1. Set up the Encryption Manager for the VLAN defined for the Service Set Identifier (SSID). Navigate to ***Security*** > ***Encryption Manager***, ensure Cipher is enabled, and select ***AES CCMP + TKIP*** as the cipher to be used for both SSIDs.



2. Enable the correct VLAN with the encryption parameters defined in Step 1. Navigate to ***Security*** > ***SSID Manager***, and select the SSID from the Current SSID List. This step is common for both WPA and WPA2 configuration.

3. In the SSID page, set Key Management to ***Mandatory***, and check the ***Enable WPA*** checkbox. Select ***WPA*** from the drop−down list in order to enable WPA. Enter the WPA Pre−shared Key.



4. Select ***WPA2*** from the drop−down list in order to enable WPA2.

Configuration with CLI

Notes:

Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

The Output Interpreter Tool (registered customers only) supports certain ***show*** commands. Use the Output Interpreter Tool in order to view an analysis of ***show*** command output.

This is the same configuration done within the CLI:

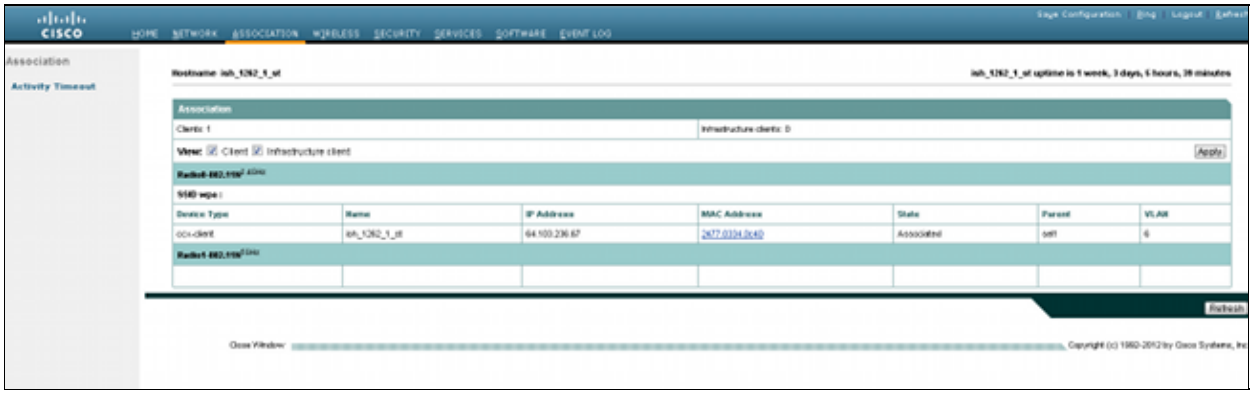
```
sh run
Building configuration...Current configuration : 5284 bytes
!
! Last configuration change at 04:40:45 UTC Thu Mar 11 1993
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ish_1262_1_st
!
!
logging 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
```

Verify

In order to confirm that the configuration works properly, navigate to ***Association***, and verify that the client is connected:



You can also verify the client association in the CLI with this syslog message:

```
*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: Refer to Important Information on Debug Commands before you use ***debug*** commands.

Use these debug commands in order to troubleshoot connectivity issues:

- ***debug dot11 aaa manager keys*** − This debug shows the handshake that occurs between the AP and the client as the pairwise transient key (PTK) and group transient key (GTK) negotiate.
- ***debug dot11 aaa authenticator state−machine*** − This debug shows the various states of negotiations that a client passes through as the client associates and authenticates. The state names indicate these states.
- ***debug dot11 aaa authenticator process*** − This debug helps you diagnose problems with negotiated communications. The detailed information shows what each participant in the negotiation sends and shows the response of the other participant. You can also use this debug in conjunction with the ***debug radius authentication*** command.
- ***debug dot11 station connection failure*** − This debug helps you determine if the clients are failing the connection and helps you determine the reason for failures.

Updated: Oct 23, 2013 Document ID: 116599