CHAPTER 15

Configure DMP Wi-Fi Settings

Revised: April 4, 2012
OL-15762-04

- Concepts, page 15-1
- Procedures, page 15-5
- Reference, page 15-8

Audience

We prepared this material with specific expectations of you.

✓ You have deployed DMP 4400G endpoints at sites with WLANs.

Concepts

- Glossary, page 15-1
- ASCII Passphrases and Hexadecimal Keys for WEP, page 15-3

Glossary

Timesaver

Go to terms that start with... [**numerals** | **A** | **C** | **E** | **P** | **S** | **T** | **W**].

numerals

802.11b A wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g A wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibilitywith 802.11b devices.

A

AAA

Authentication, Authorization, and Accounting.

See also EAP-FAST, EAP-MD5 server, LEAP server, and PEAP server.

access point

A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

C

Return to Top

CCMP

Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's FIPS Publication 197, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

See also WEP keys.

E

Return to Top

EAP

Extensible Authentication Protocol. A protocol that WPA uses to authorize user access to wireless networks. Common implementations include EAP-FAST and EAP-MD5.

EAP-FAST

EAP-FAST is a two-phase implementation of the EAP authentication protocol:

- Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credentials).
- Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password.

See also AAA and EAP.

EAP-MD5 server

Servers that use EAP to provide dynamic, session-specific wireless encryption keys, central user administration, and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords.

See also AAA and EAP.

P

Return to Top

PEAP server

Protected EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also AAA, EAP-MD5 server, and WEP keys.

PSK

Pre-Shared Key.

S *Return to Top*

SSID *Service Set ID*. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish among multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

Caution **The Broadcast SSID setting must be enabled on your wireless access points.** Otherwise, your DMPs are prevented from connecting to your WLAN or obtaining IP addresses.

Caution **When you change SSID settings for your WLAN, your DMPs lose their wireless network connections.** Because they are disconnected, they cannot reconnect automatically. In this case, affected DMPs will appear to associate to your WLAN access point but will not receive any IP address.

T *Return to Top*

TKIP *Temporal Key Integrity Protocol*, also known as key hashing, is used as part of server-based EAP authentication.

W *Return to Top*

WEP *Wired Equivalent Privacy* is a method to encrypt data transmitted on a wireless network.

WEP keys Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.

WPA *Wi-Fi Protected Access*. WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP for data protection and 802.1X for authenticated key management.

ASCII Passphrases and Hexadecimal Keys for WEP

Tip **You can ignore this topic if your Wi-Fi network uses WPA and not WEP.**

Many Wi-Fi access points (wireless routers) accept only a hexadecimal passphrase for WEP-64 and WEP-128. And yet, DMPs accept only an ASCII passphrase for WEP. For this reason, it might be necessary at times to translate your WEP passphrase from ASCII to hexadecimal.

Note **Many third-party converters are available.** We do not offer any Cisco converter for this purpose.

The typical workflow is as follows.

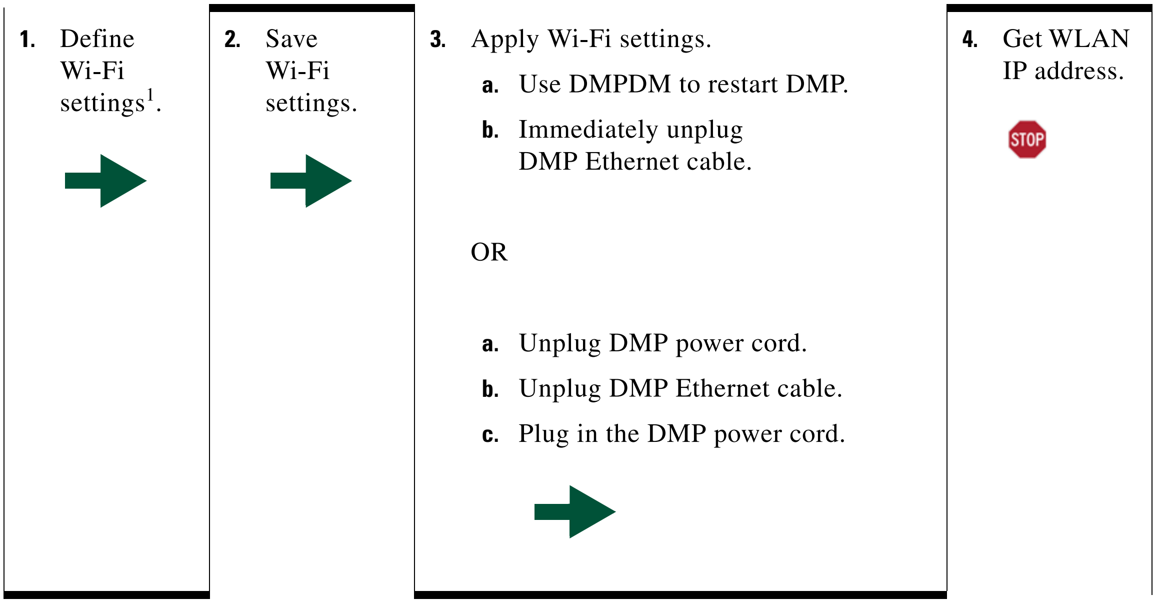
1. Pick an ASCII passphrase. For example, *PassphraseWEP128*.
2. Convert your string of ASCII characters to the hexadecimal key or keys for your network.
   - WEP-64 uses four short hexadecimal keys.
   - WEP-128 uses one long hexadecimal key.
3. Configure your DMP to use the ASCII from which you derived the hexadecimal.
4. Configure your wireless router to use the appropriate hexadecimal key or keys.

Related Topics

- Establish a Wireless Network Connection (802.11), page 15-6

Workflow

It is not necessary, useful, or correct to restart a DMP immediately after you define its Wi-Fi settings. Instead, the typical workflow is as follows.



1. Define Wi-Fi settings[1]. →
2. Save Wi-Fi settings. →
3. Apply Wi-Fi settings.
   a. Use DMPDM to restart DMP.
   b. Immediately unplug DMP Ethernet cable.

   OR

   a. Unplug DMP power cord.
   b. Unplug DMP Ethernet cable.
   c. Plug in the DMP power cord.

   →
4. Get WLAN IP address.

[1] Verify that the Broadcast SSID setting is enabled on your wireless access points. Otherwise, your DMPs are prevented from obtaining IP addresses.

Restrictions

- **Ethernet connections take priority over Wi-Fi connections on DMPs where both are active.**
- The Broadcast SSID setting must be enabled on your wireless access points (also known as *wireless routers* or *WLAN controllers*). Otherwise, your DMPs cannot connect to your WLAN and are prevented from obtaining IP addresses.
- We do not support "open" Wi-Fi networks. They are a security risk.
- We do not support multicast or other streams over Wi-Fi.
- DMP 4305G endpoints and DMP 4310G endpoints do not support Wi-Fi.
- When your wireless DMP will not have access to any DHCP server, you must configure its wireless access point to issue a static IP address. You cannot use DMM or DMPDM for this purpose.

Procedures

- Establish a Wired Network Connection, page 15-5
- Establish a Wireless Network Connection (802.11), page 15-6

Establish a Wired Network Connection

Note **See the printed documentation that shipped with your DMP to understand its reliance on DHCP.**

A DMP must already be reachable before it can receive Wi-Fi settings. Therefore, you must establish a wired connection before you can deploy Wi-Fi settings.

Before You Begin

- Verify that the Broadcast SSID setting is enabled on your wireless access points. Otherwise, your DMPs cannot connect to your WLAN and are prevented from obtaining IP addresses.
- Does a security policy in your network restrict DHCP address assignments to known MAC addresses? If so, locate the **MAC** address printed on a sticker that is affixed to your DMP. Then, share this address with your security policy administrator.

Procedure

Step 1 Plug one end of a standard Ethernet cable into the corresponding socket on your DMP.

Step 2 Plug the other end of this cable into a network hub, network switch, or router that participates in an IP network that uses DHCP for dynamic address allocation.

Step 3 Stop. You have completed this procedure.

What to Do Next

- Go to the "Establish a Wireless Network Connection (802.11)" section on page 15-6.

Related Topics

- DMP Network Interfaces, page 15-8

Establish a Wireless Network Connection (802.11)

You can create and save applications that describe the important attributes of wireless 802.11 networks throughout your organization. After you define and save these settings, you can deploy them to centrally managed DMPs individually or to any of your DMP groups.

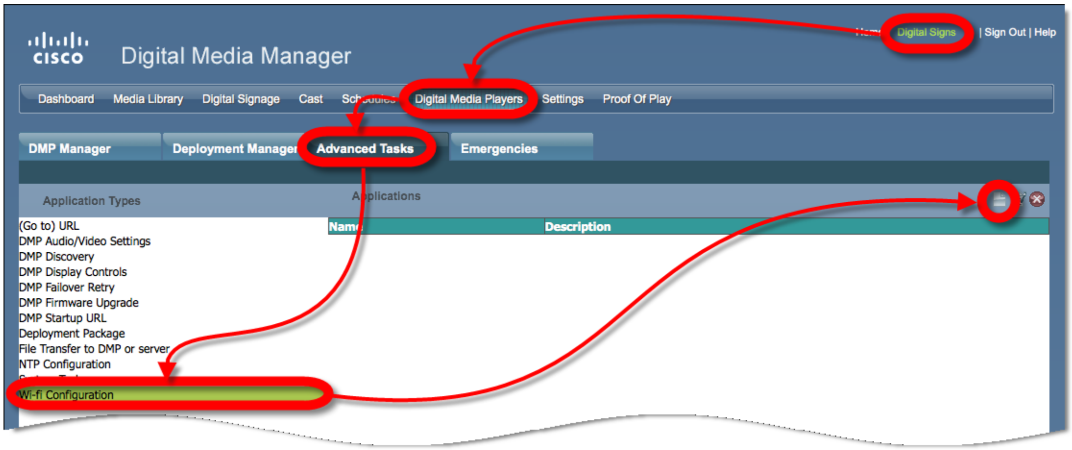
Before You Begin

- Do your DMPs all support wireless connectivity? Some models do not. See their datasheets on Cisco.com.
- Verify that the Broadcast SSID setting is enabled on your wireless access points. Otherwise, your DMPs cannot connect to your WLAN and are prevented from obtaining IP addresses.
- Does a security policy in your network restrict DHCP address assignments to known MAC addresses? If so, locate the **WLAN** address printed on a sticker that is affixed to your DMP. Then, share this address with your security policy administrator.
- Verify that your wireless network is working correctly, is available, and you understand how it authenticates connection requests.
- Complete all steps in the "Establish a Wired Network Connection" section on page 15-5.

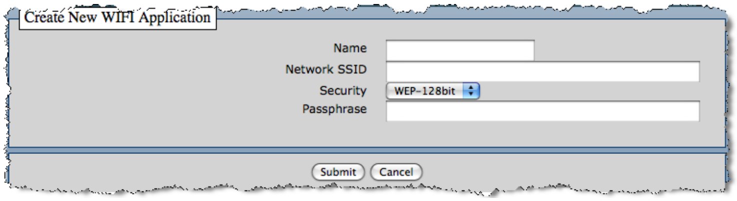
Procedure

Step 1 Choose **Digital Signs** from the global navigation.

Step 2 Choose **Digital Media Players > Advanced Tasks > Wi-fi Configuration > Add New Application**.



The Create New WIFI Application page opens.



Create New WIFI Application

Security WEP-128bit

Step 3 Enter a meaningful name for the Wi-Fi network that this application describes.

For example, you might use a name that specifies the locale, the building, and the security method for this network.

Step 4 Enter in the Network SSID field the SSID for the network that this application describes.

Tip **In the future, if you reconfigure SSID settings in your WLAN, your DMPs will lose their network connections.** If this occurs, simply restart your DMPs to restore normal operation.

Step 5 Choose from the Security list the security method for your network. The options are:

- WEP-64bit
- WEP-128bit
- WPA-PSK
- WPA-EAP
- WPA2-PSK
- WPA2-EAP

The security method that you choose controls, in part, which other fields and options you see.

Step 6 Do the following, as needed.

- Did you choose a WEP-based security method? And do you see the Passphrase field? If so, enter in it the key from which your 64-bit or 128-bit passphrase is cryptographically derived.
- Did you choose a WPA-based or WPA-2-based security method? And do you see the Passphrase field? If so, enter in it the pre-shared key for your network.
- Do you see the Encryption list? If so, choose from it either **TKIP** or **CCMP**.
- Do you see the EAP list? If so, choose from it either **FAST**, **MD5**, or **PEAP (ver.0)**.
- Do you see the Username and Password fields? If so, enter in them respectively a valid username for your wireless network and the password to authenticate that username.

Step 7 Click **Submit** to save this application.

Step 8 Deploy this application to your DMPs, as appropriate.

- *Immediately*—Click the **DMP Manager** tab, choose which DMPs to reconfigure, choose this named application from the "W-Fi Configuration" options in the Actions list, and then click **Go**.
- *In the future*—Click the **Schedules** tab and define deployment parameters for this application.

Step 9 Verify that your DMPs have IP addresses as nodes on the wireless network.

Step 10 After the deployment is successful, **unplug the Ethernet cables** from your DMPs.

Otherwise, their Ethernet connections will take priority over their Wi-Fi connections.

Step 11 After you unplug their Ethernet cables, restart these DMPs.

Step 12 Stop. You have completed this procedure.

Related Topics

- Establish a Wired Network Connection, page 5

Reference

- DMP Network Interfaces, page 15-8
- FAQs and Troubleshooting, page 15-8

DMP Network Interfaces

Table 15-1 Network Interfaces

Category	Subcategory	Chassis Label
Wired[1]	Gigabit Ethernet (10/100/1000)	• RJ45
Wireless (WiFi)	802.11b/g Antenna	• Antenna

[1] Category 5 or better. Maximum length: 328 ft (100 m). For any distance greater than 165 ft (50 m), we recommend that you use Category 5e or Category 6 certified Ethernet cabling. We do not ship any Ethernet cable with any DMP model. You must obtain this cable separately.

FAQs and Troubleshooting

- FAQs, page 15-8

FAQs

Q. What configuration errors might cause the following combination of symptoms to occur simultaneously?

- I cannot ping DMPs on my WLAN.
- I cannot open any instances of DMPDM for DMPs on my WLAN.
- Digital Signs software on my DMM appliance shows that DMPs are rea on my WLAN.
- I can deploy commands and assets from my Digital Signs software to DMPs in my WLAN.

A. It is likely that your DMPs are configured correctly. Please check for errors in the network security settings for your WLAN.

Q. What might prevent my DMPs from connecting to my WLAN or obtaining IP addresses?

A. The Broadcast SSID setting must be enabled on your wireless access points.

Q. Why did my DMPs lose their wireless network connectivity?

A. This can occur after you change SSID settings for your WLAN. Please restart your DMPs to restore their connections.

Q. Can I overcome the SSID broadcast requirement if I wait until my DMP is connected before I turn off the SSID broadcast?

A. No. Your DMP will lose its connection to your WLAN.

Q. What prevents my DMPs from receiving IP addresses even after they have associated to my WLAN access point?

A. This can occur whenever you change SSID settings for your WLAN. Please restart your DMPs to restore their connections.

Q. How can my wireless DMP use a static IP address?

A. Configure your wireless access point to assign the address.

Q. Why might I see references to TKIP after I configure my DMPs to use WPA2-EAP with AES CCMP?

A. This is a known issue. Although the Digital Signs software user interface might state that you use TKIP, your DMP uses WPA2-EAP with AES CCMP successfully, just as you configured it to do.

Q. Why might I see references to DHCP after I configure my DMPs to use static IP addresses on my WLAN?

A. This is a known issue. Although the Digital Signs software user interface might state that you use DHCP, your DMPs continue to use the static IP addresses that you configured.