使用RADIUS伺服器的EAP身份驗證

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[設定](#)
[網路EAP或使用EAP的開放式身份驗證](#)
[定義身份驗證伺服器](#)
[定義客戶端身份驗證方法](#)
[驗證](#)
[疑難排解](#)
[疑難排解程式](#)
[指令疑難排解](#)
[相關資訊](#)

簡介

本檔案將提供基於Cisco IOS®的存取點的組態範例，以針對RADIUS伺服器存取的資料庫，對無線使用者進行可擴充驗證通訊協定(EAP)驗證。

由於接入點在EAP中扮演被動角色（將來自客戶端的無線資料包橋接為目的地為身份驗證伺服器的有線資料包，反之亦然），此配置實際上用於所有EAP方法。這些方法包括（但不限於）LEAP、受保護的EAP(PEAP)-MS-Challenge握手身份驗證協定(CHAP)版本2、PEAP — 通用令牌卡(GTC)、通過安全隧道的EAP-Flexible身份驗證(FAST)、EAP — 傳輸層安全(TLS)和EAP — 隧道TLS(TTLS)。 您必須為每個EAP方法正確配置身份驗證伺服器。

本文說明如何設定存取點(AP)和RADIUS伺服器，即本檔案組態範例中的Cisco Secure ACS。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 您熟悉Cisco IOS GUI或CLI。
- 您熟悉EAP身份驗證背後的概念。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行Cisco IOS的Cisco Aironet AP產品。
- 假設網路中只有一個虛擬LAN(VLAN)。
- 成功整合到使用者資料庫的RADIUS身份驗證伺服器產品。以下是Cisco LEAP和EAP-FAST支援的身份驗證伺服器：思科安全存取控制伺服器(ACS)Cisco Access Registrar(CAR)放克鋼帶半徑互連優點以下是Microsoft PEAP-MS-CHAP版本2和PEAP-GTC支援的身份驗證伺服器：Microsoft Internet身份驗證服務(IAS)Cisco Secure ACS放克鋼帶半徑互連優點Microsoft可以授權的任何其他身份驗證伺服器。**注意：**GTC或一次性密碼需要額外的服務，這些服務需要在客戶端和伺服器端使用額外的軟體，以及硬體或軟體令牌生成器。有關其產品支援EAP-TLS、EAP-TTLS和其他EAP方法的身份驗證伺服器的詳細資訊，請諮詢客戶端請求方的製造商。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

此配置描述如何在基於IOS的AP上配置EAP身份驗證。在本文檔的示例中，LEAP被用作RADIUS伺服器的EAP身份驗證方法。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

與大多數基於密碼的身份驗證演算法一樣，Cisco LEAP容易受到字典攻擊。這不是Cisco LEAP的新攻擊或新漏洞。建立強密碼策略是緩解字典攻擊的最有效方法。這包括使用強密碼和密碼定期過期。請參閱針對Cisco LEAP的字典攻擊，以獲取有關字典攻擊及其預防方法的更多資訊。

本檔案將針對GUI和CLI使用以下設定：

- AP的IP地址為10.0.0.106。
- RADIUS伺服器(ACS)的IP位址是10.0.0.3。

網路EAP或使用EAP的開放式身份驗證

在任何基於EAP/802.1x的身份驗證方法中，您都可以詢問「網路EAP」和「使用EAP的開放式身份驗證」之間的區別。這些專案引用管理和關聯資料包報頭中的Authentication Algorithm欄位中的值。大多數無線客戶端製造商將此欄位設定為值0（開放式身份驗證），然後表示希望在關聯過程中稍後進行EAP身份驗證。Cisco設定值的方式與使用Network EAP標誌開始關聯時不同。

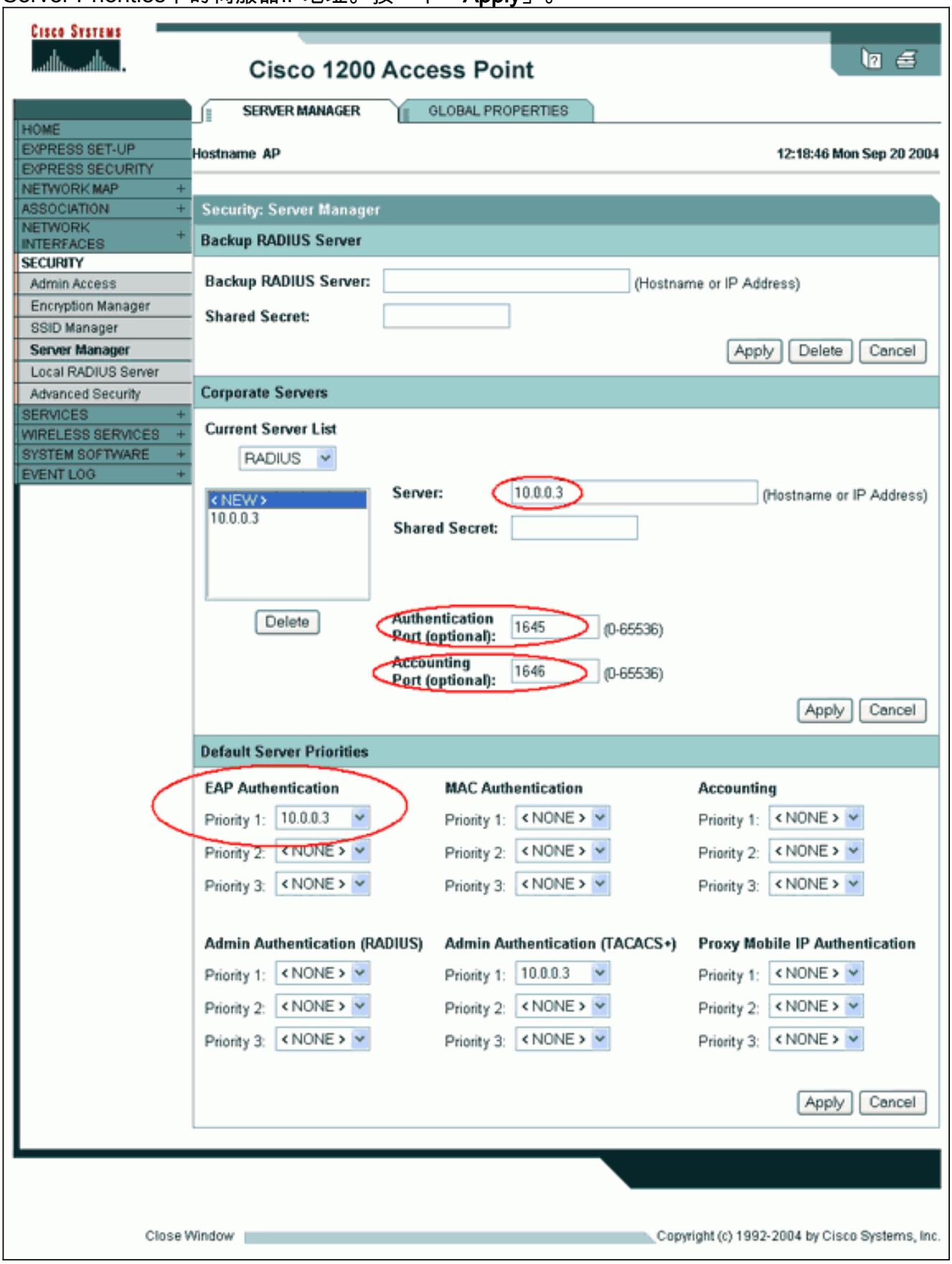
如果您的網路有以下使用者端：

- Cisco clients — 使用Network-EAP。
- 第三方客戶端（包括符合CCX標準的產品） — 使用Open with EAP。
- 思科和第三方客戶端的組合 — 同時選擇Network-EAP和Open with EAP。

定義身份驗證伺服器

EAP配置的第一步是定義身份驗證伺服器並與它建立關係。

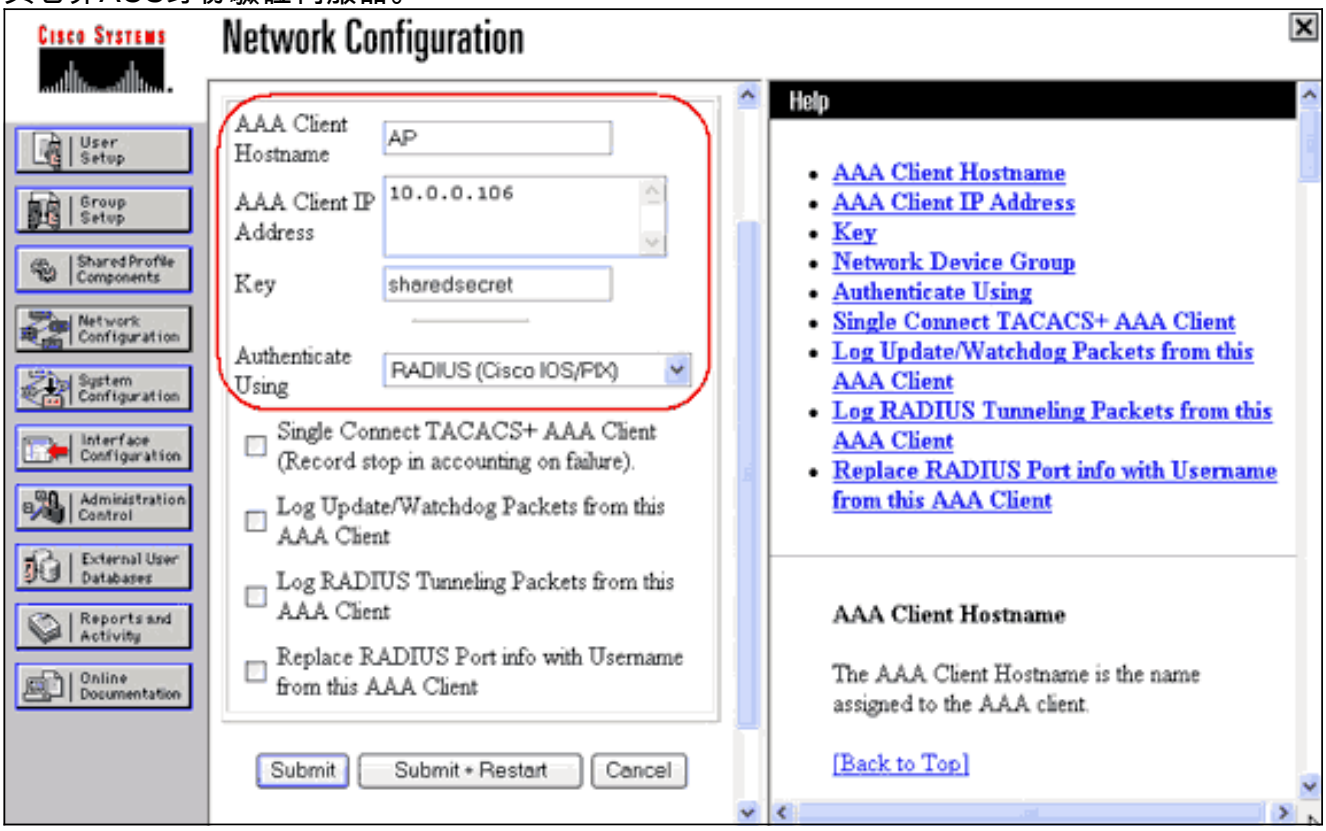
1. 在接入點的「伺服器管理器」(Server Manager)頁籤(**Security > Server Manager**)選單項下)完成以下步驟：在「伺服器」欄位中輸入身份驗證伺服器的IP地址。指定共用金鑰和埠。按一下**Apply**以建立定義並填充下拉式清單。將EAP Authentication type Priority 1欄位設定為Default Server Priorities下的伺服器IP地址。按一下「**Apply**」。



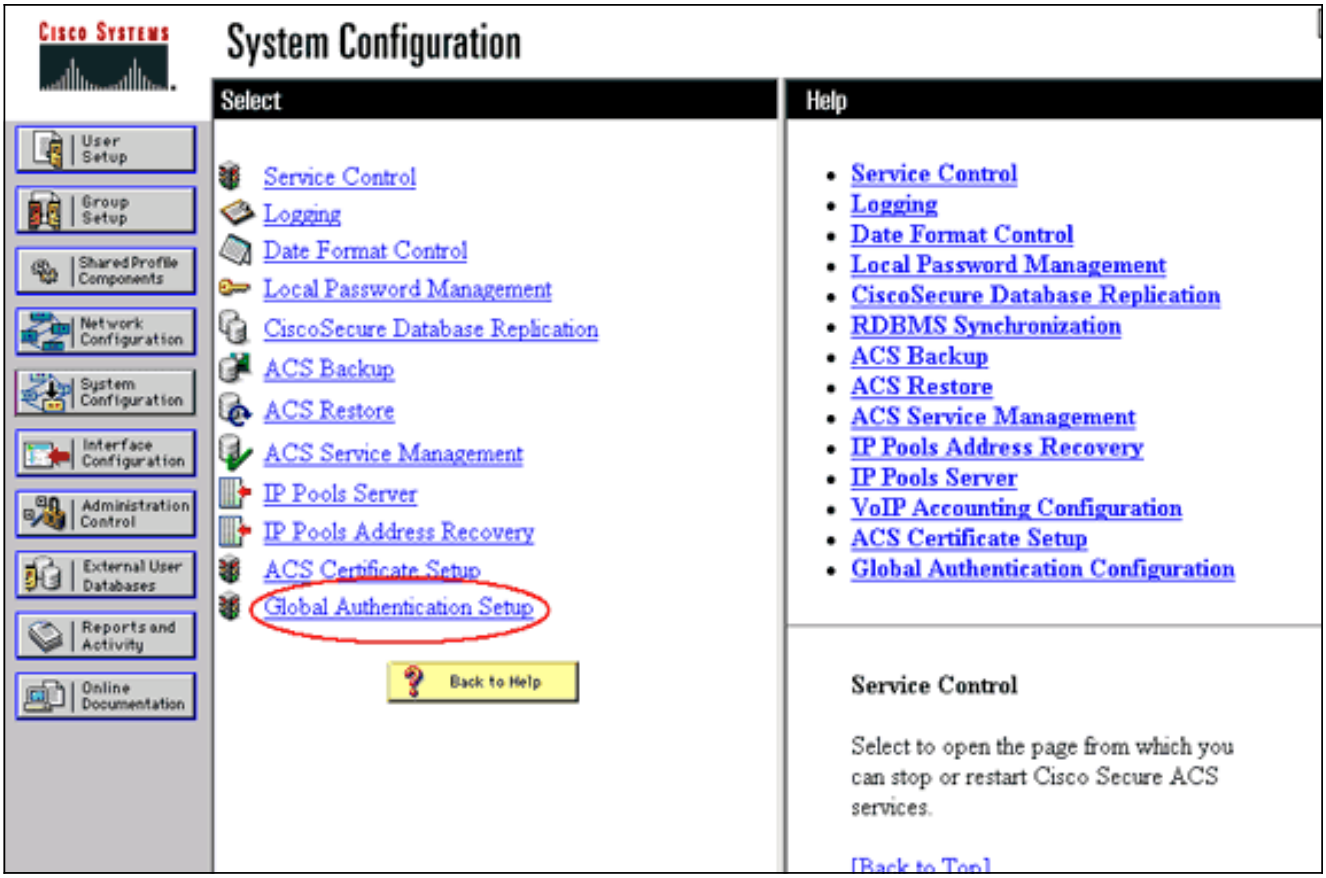
您也可以從CLI發出以下命令：

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#aaa group server radius rad_eap

AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646

AP(config-sg-radius)#exit

AP(config)#aaa new-model

AP(config)#aaa authentication login eap_methods group rad_eap

AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#end

AP#write memory
```

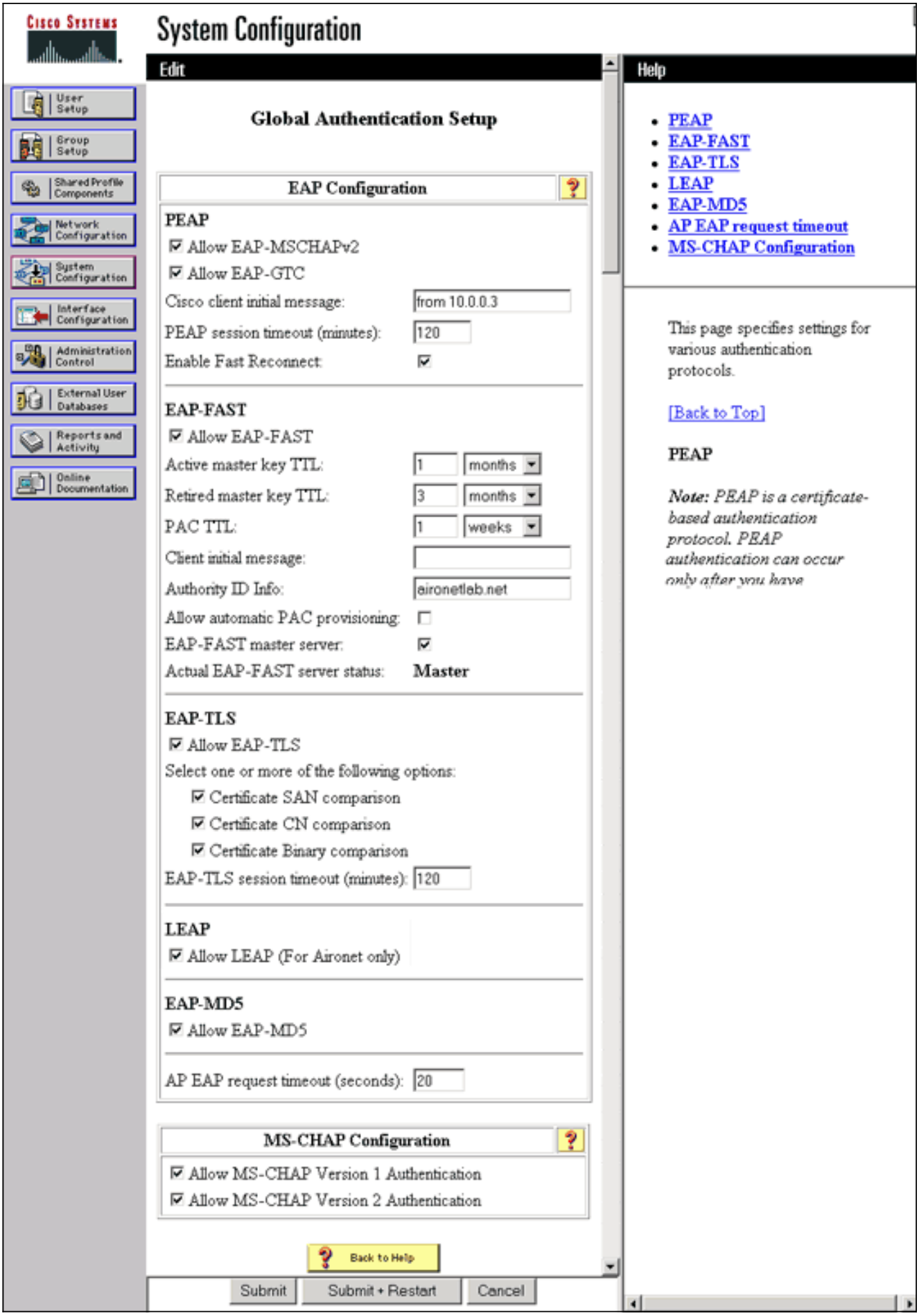
2. 接入點必須在身份驗證伺服器中配置為AAA客戶端。例如，在Cisco Secure ACS中，這發生在Network Configuration頁面上，該頁面定義了接入點的名稱、IP地址、共用金鑰和身份驗證方法（RADIUS Cisco Aironet或RADIUS Cisco IOS/PIX）。請參閱製造商提供的文檔，瞭解其它非ACS身份驗證伺服器。



確保身份驗證伺服器配置為執行所需的EAP身份驗證方法。例如，對於執行LEAP的Cisco Secure ACS，請在System Configuration - Global Authentication Setup頁面上配置LEAP身份驗證。按一下**System Configuration**，然後按一下**Global Authentication Setup**。有關其他非ACS身份驗證伺服器或其他EAP方法，請參閱製造商提供的文檔。



此圖顯示為PEAP、EAP-FAST、EAP-TLS、LEAP和EAP-MD5配置的Cisco Secure ACS。

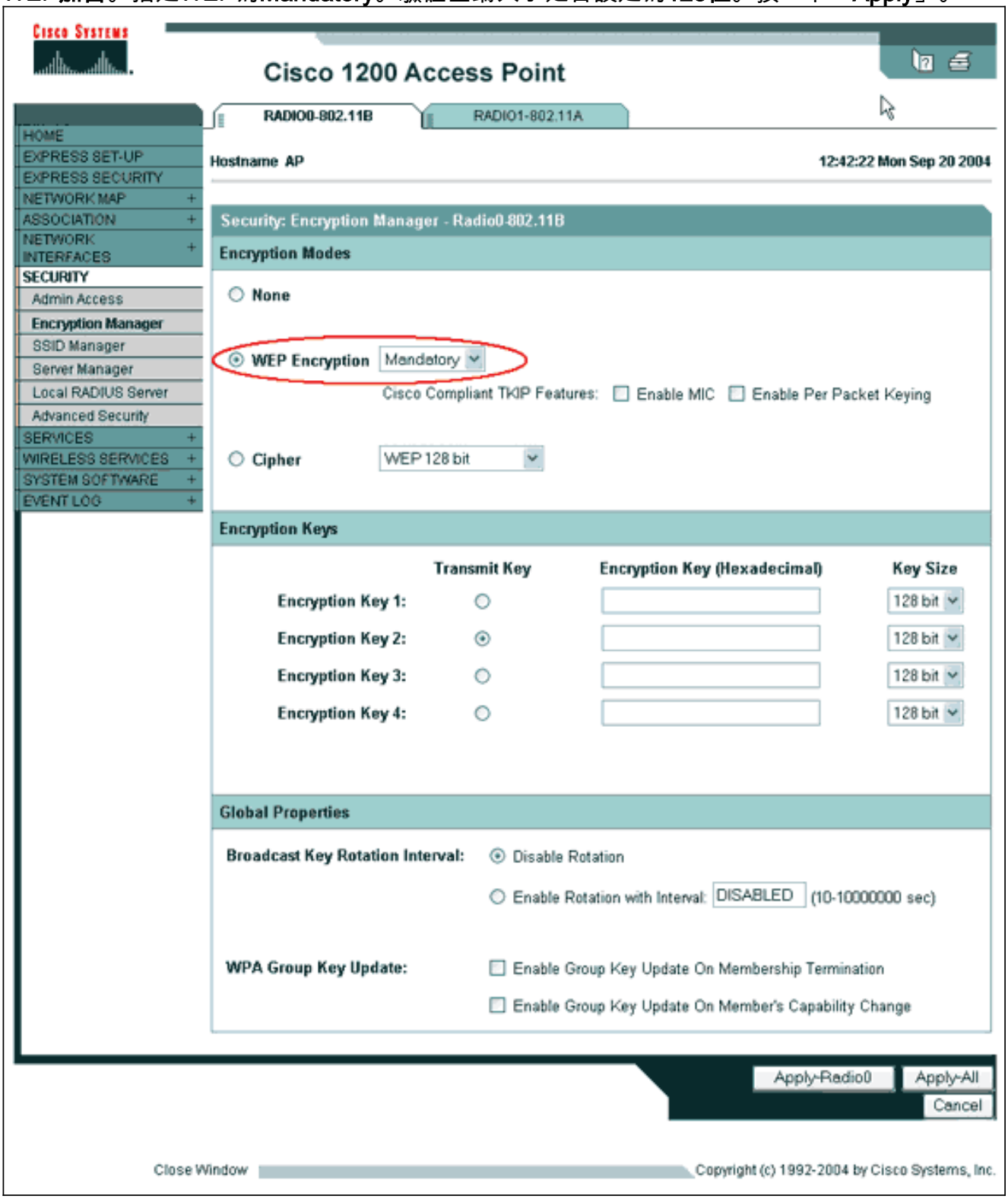


[定義客戶端身份驗證方法](#)

一旦接入點知道要將客戶端身份驗證請求傳送到何處，請將其配置為接受這些方法。

注意：這些說明適用於基於WEP的安裝。對於WPA（使用密碼而不是WEP），請參閱WPA配置概述。

1. 在接入點加密管理器頁籤(在**安全>加密管理器**選單項下)上，完成以下步驟：指定要使用WEP**加密**。指定WEP為**Mandatory**。驗證金鑰大小是否設定為**128位**。按一下「**Apply**」。

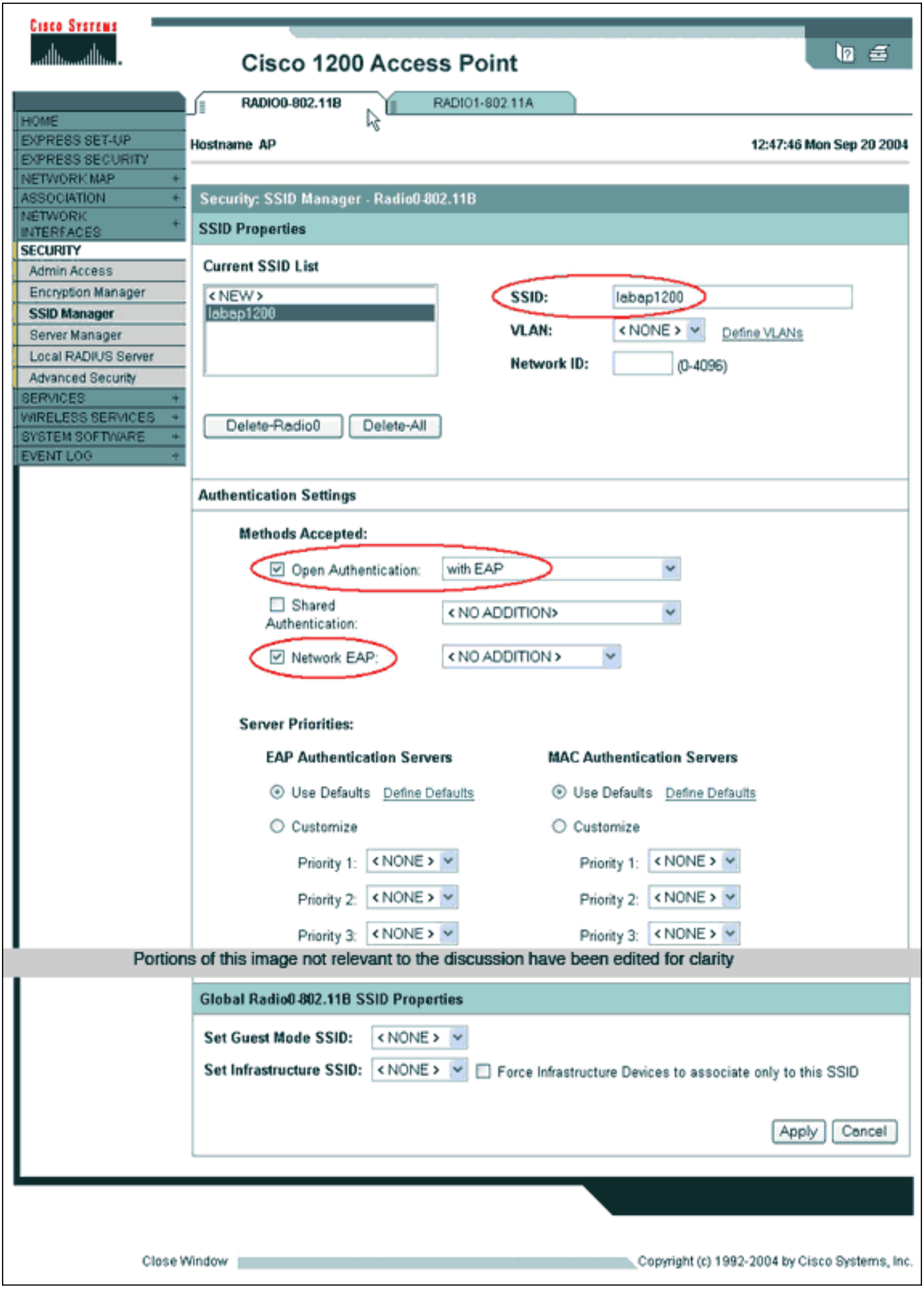


您也可以從CLI發出以下命令：

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0
```

```
AP(config-if)#encryption mode wep mandatory

AP(config-if)#end

AP#write memory
```

2. 在AP SSID Manager頁籤上(在**Security > SSID Manager選單項下)完成**以下步驟：選擇所需的SSID。在「Authentication Methods Accepted」下，選中標籤為**Open**的框，並使用下拉選單選擇**With EAP**。如果您有Cisco客戶端卡，請選中標籤為**Network-EAP**的框。請參閱網路EAP或使用EAP的開放式身份驗證部分中的討論。按一下「**Apply**」。



您也可以從CLI發出以下命令：

```
AP#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

AP(config)#interface dot11radio 0

AP(config-if)#ssid labap1200

AP(config-if-ssid)#authentication open eap eap_methods

AP(config-if-ssid)#authentication network-eap eap_methods

AP(config-if-ssid)#end

AP#write memory
```

通過基本EAP配置確認基本功能後，您可在以後新增其他功能和金鑰管理。在功能基礎之上新增更複雜的功能，以便更輕鬆地進行故障排除。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show radius server-group all** — 顯示AP上所有已配置RADIUS伺服器組的清單。

疑難排解

疑難排解程式

完成以下步驟即可對組態進行疑難排解。

1. 在客戶端實用程式或軟體中，使用相同或相似的引數建立新的配置檔案或連線，以確保客戶端的配置沒有損壞任何內容。
2. 要消除阻止身份驗證成功的RF問題的可能性，請臨時禁用身份驗證，如以下步驟所示：在CLI中使用**no authentication open eap eap_methods**、**no authentication network-eap eap_methods**和**authentication open**命令。在GUI的SSID Manager頁面上，取消選中**Network-EAP**，選中**Open**，然後將下拉選單設回**No Addition**。如果客戶端成功關聯，則RF不會導致關聯問題。
3. 驗證共用金鑰口令在接入點和身份驗證伺服器之間是否同步。否則，您可能會收到以下錯誤訊息：
   `Invalid message authenticator in EAP request`
   在CLI中，檢查`radius-server host x.x.x.x auth-port x acct-port x key <shared_secret>`行。在GUI的「伺服器管理器」(Server Manager)頁面上，在標有「共用金鑰」(Shared Secret)的框中重新輸入相應伺服器的共用金鑰。RADIUS伺服器上接入點的共用金鑰條目必須包含與前面提到的共用金鑰相同的共用金鑰密碼。
4. 從RADIUS伺服器中刪除任何使用者組。有時RADIUS伺服器定義的使用者組和基礎域中的使用者組之間會發生衝突。檢查RADIUS伺服器的日誌中是否有失敗的嘗試，以及這些嘗試失敗的原因。

指令疑難排解

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

調試身份驗證提供了大量有關如何收集和解釋與EAP相關的調試輸出的詳細資訊。

注意：發出**debug**命令之前，**請參閱**有關Debug命令的重要資訊**。**

- **debug dot11 aaa authenticator state-machine** — 顯示客戶端和身份驗證伺服器之間協商的主要劃分（或狀態）。以下是**成功驗證**的輸出：

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CL IENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
------------------Lines Omitted for simplicity------------------
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SE RVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
0040.96ac.dd05
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)
```

  註：在12.2(15)JA之前的Cisco IOS軟體版本中，此**debug**命令的語法為**debug dot11 aaa dot1x state-machine**。
- **debug dot11 aaa authenticator process** — 顯示客戶端和身份驗證伺服器之間協商的單個對話條目。**注意：**在12.2(15)JA之前的Cisco IOS軟體版本中，此debug命令的語法為**debug dot11 aaa dot1x process**。
- **debug radius authentication** — 顯示伺服器和客戶端（兩者均由AP橋接）之間的RADIUS協商。以下是**failed authentication**的輸出：

```
*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
```

```
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
--------------------------Lines Omitted-----------------------------------
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
---------------------------------Lines Omitted----------------------
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed
```

- debug aaa authentication — 顯示客戶端裝置和身份驗證伺服器之間身份驗證的AAA協商。

相關資訊

- 調試身份驗證

- 配置身份驗證型別
- 本地RADIUS伺服器上的LEAP驗證
- 設定RADIUS和TACACS+伺服器
- 配置Cisco Secure ACS for Windows v3.2（使用PEAP-MS-CHAPv2電腦身份驗證）
- 適用於Windows v3.2的Cisco安全ACS，採用EAP-TLS電腦身份驗證
- 在Microsoft IAS上配置PEAP/EAP
- 排除Microsoft IAS作為RADIUS伺服器的故障
- Microsoft 802.1X驗證使用者端
- 技術支援與文件 - Cisco Systems