統一無線網路本地EAP伺服器配置示例

目錄

簡介

本檔案介紹在思科無線LAN控制器(WLC)中設定本機可擴充驗證通訊協定(EAP)伺服器以進行無線使用者驗證。

本地EAP是一種身份驗證方法，它允許使用者和無線客戶端在本地進行身份驗證。本產品專為遠端辦公室所設計，可在後端系統中斷或外部驗證伺服器故障時，維持與無線使用者端的連線。啟用本地EAP時，控制器充當身份驗證伺服器和本地使用者資料庫，從而消除對外部身份驗證伺服器的依賴。本地EAP從本地使用者資料庫或輕量級目錄訪問協定(LDAP)後端資料庫中檢索使用者憑證以驗證使用者。本機EAP支援在控制器與無線使用者端之間的輕量EAP (LEAP)、透過安全通道的EAP-Flexible驗證(EAP-FAST)，以及EAP-傳輸層安全性(EAP-TLS)驗證。

請注意，如果WLC中存在全局外部RADIUS伺服器配置，則本地EAP伺服器不可用。所有驗證要求都會轉送到全域外部RADIUS，直到本機EAP伺服器可用為止。如果WLC失去與外部RADIUS伺服器的連線，則本地EAP伺服器將變為活動狀態。如果沒有全局RADIUS伺服器配置，本地EAP伺服器將立即變為活動狀態。本地EAP伺服器不能用於驗證連線到其他WLC的客戶端。換句話說，一個WLC無法將其的EAP要求轉送到另一個WLC進行驗證。每個WLC都應該有自己的本地EAP伺服器和單獨的資料庫。

注意：使用以下命令可停止WLC向外部RADIUS伺服器傳送請求。

```
config wlan disable
        config wlan radius_server auth disable
        config wlan enable
```

本地EAP伺服器在4.1.171.0軟體版本及更高版本中支援以下協定：

- LEAP
- EAP-FAST（使用者名稱/密碼和憑證）
- EAP-TLS

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解如何設定WLC和輕量存取點(LAP)以執行基本操作
- 輕量存取點協定(LWAPP)和無線安全方法的知識
- 本機EAP驗證的基本知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Windows XP（含CB21AG介面卡和Cisco安全服務使用者端4.05版）
- Cisco 4400無線LAN控制器4.1.171.0
- Windows 2000伺服器上的Microsoft憑證授權單位

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

在思科無線區域網控制器上配置本地EAP

本檔案假設WLC的基本組態已經完成。

本地EAP配置

要配置本地EAP，請完成以下步驟：

1. 新增本機網路使用者：

從GUI中。選擇Security > Local Net Users > New，輸入使用者名稱、密碼、訪客使用者、WLAN ID和說明，然後按一下Apply。

從CLI中，可以使用config netuser add <username> <password> <WLAN id> <description>命令：

注意：由於空間原因，此命令已分成兩行。

```
<#root>

(Cisco Controller) >

config netuser add eapuser2 cisco123 1 Employee user local database
```

2. 指定使用者認證擷取順序。

從GUI中，選擇Security > Local EAP > Authentication Priority。然後選擇LDAP，按一下「<」按鈕，然後按一下Apply。這會先將使用者證明資料放在本機資料庫中。

在CLI上：

```
<#root>

(Cisco Controller) >

config local-auth user-credentials local
```

3. 增加EAP配置檔案：

為了從GUI中執行此操作，請選擇Security > Local EAP > Profiles，然後按一下New。當新窗口出現時，鍵入配置檔名稱並按一下Apply。

您也可以使用CLI命令config local-auth eap-profile add <profile-name>執行此操作。 在我們的示例中，配置檔名稱為EAP-test。

```
<#root>

(Cisco Controller) >

config local-auth eap-profile add EAP-test
```

4. 向EAP配置檔案增加方法。

從GUI中選擇Security > Local EAP > Profiles，然後按一下要為其增加身份驗證方法的配置檔名稱。本示例使用LEAP、EAP-FAST和EAP-TLS。按一下Apply以設定方法。

您還可以使用CLI命令config local-auth eap-profile method add <method-name> <profile-name> 。在我們的示例配置中，我們將三種方法增加到配置檔案EAP-test中。這些方法分別是LEAP、EAP-FAST和EAP-TLS，其方法名稱分別為leap、fast和tls。此輸出顯示CLI配置命令：

```
<#root>

(Cisco Controller) >

config local-auth eap-profile method add leap EAP-test

(Cisco Controller) >

config local-auth eap-profile method add fast EAP-test

(Cisco Controller) >

config local-auth eap-profile method add tls EAP-test
```

5. 配置EAP方法的引數。這隻用於EAP-FAST。要配置的引數包括：

   - Server Key (server-key) -用於加密/解密受保護訪問憑證(PAC)的伺服器金鑰（十六進位制格式）。
   - PAC的生存時間(pac-ttl) -設定PAC的生存時間。
   - Authority ID (authority-id) - 設定授權識別符號。
   - Anonymous Provision (anon-provn) -配置是否允許匿名提供。依預設會啟用此功能。

   對於透過GUI進行的配置，請選擇Security > Local EAP > EAP-FAST Parameters，然後輸入伺服器金鑰、PAC的存活時間、授權ID（以十六進位制表示）和授權ID Information值。

   以下是CLI配置命令，用於為EAP-FAST設定以下引數：

```
<#root>

(Cisco Controller) >

config local-auth method fast server-key 12345678

(Cisco Controller) >

config local-auth method fast authority-id 43697369f1 CiscoA-ID

(Cisco Controller) >

config local-auth method fast pac-ttl 10
```

6. 啟用每個WLAN的本地身份驗證：

   從GUI的頂部選單選擇WLANs，並選擇您要配置本地身份驗證的WLAN。此時將出現一個新窗

口。按一下Security > AAA頁籤。選中Local EAP authentication，然後從下拉選單中選擇正確的EAP Profile Name，如以下示例所示：

您也可以發出CLI config wlan local-auth enable <profile-name> <wlan-id> 配置命令，如下所示：

```
<#root>

(Cisco Controller) >

config wlan local-auth enable EAP-test 1
```

7. 設定第2層安全引數。

在GUI介面中，在WLAN Edit窗口中轉到Security > Layer 2頁籤並從Layer 2 Security下拉選單中選擇WPA+WPA2。在「WPA+WPA2 Parameters」部分下，將「WPA Encryption」設定為TKIP和「WPA2 Encryption AES」。然後按一下Apply。

在CLI中，使用以下命令：

```
<#root>

(Cisco Controller) >

config wlan security wpa enable 1

(Cisco Controller) >

config wlan security wpa wpa1 ciphers tkip enable 1

(Cisco Controller) >

config wlan security wpa wpa2 ciphers aes enable 1
```

8. 驗證設定:

```
<#root>

(Cisco Controller) >

show local-auth config

User credentials database search order:
    Primary .....................................

Local DB
```

```
Timer:
    Active timeout ..............................  Undefined

Configured EAP profiles:


 Name ..................................... EAP-test

      Certificate issuer ........................ cisco
      Peer verification options:
        Check against CA certificates ........... Enabled
        Verify certificate CN identity .......... Disabled
        Check certificate date validity ......... Enabled
      EAP-FAST configuration:
        Local certificate required .............. No
        Client certificate required ............. No


Enabled methods ........................... leap fast tls



Configured on WLANs ....................... 1


EAP Method configuration:
    EAP-FAST:
--More-- or (q)uit
      Server key ................................ <hidden>
      TTL for the PAC ........................... 10
      Anonymous provision allowed ............... Yes
      Authority ID .............................. 43697369f10000000000000000000000
      Authority Information ..................... CiscoA-ID
```

您可以使用show wlan <wlan id> 命令檢視wlan 1的特定引數：

```
<#root>

(Cisco Controller) >

show wlan 1


WLAN Identifier.................................. 1
Profile Name..................................... austinlab
Network Name (SSID).............................. austinlab
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
```

```
CCX - AironetIe Support..........................  Enabled
CCX - Gratuitous ProbeResponse (GPR).............  Disabled
Dot11-Phone Mode (7920)..........................  Disabled
Wired Protocol...................................  None
--More-- or (q)uit
IPv6 Support.....................................  Disabled
Radio Policy.....................................  All

Local EAP Authentication.........................  Enabled (Profile 'EAP-test')

Security


   802.11 Authentication:........................  Open System
   Static WEP Keys...............................  Disabled
   802.1X........................................  Disabled


Wi-Fi Protected Access (WPA/WPA2).............  Enabled
      WPA (SSN IE)............................  Enabled
         TKIP Cipher..........................  Enabled

         AES Cipher...........................  Disabled


   WPA2 (RSN IE)............................  Enabled

         TKIP Cipher..........................  Disabled


  AES Cipher.............................  Enabled

                                                                  Auth Key Management
         802.1x...............................  Enabled
         PSK..................................  Disabled
         CCKM.................................  Disabled
   CKIP ....................................  Disabled
   IP Security..............................  Disabled
   IP Security Passthru.....................  Disabled
   Web Based Authentication.................  Disabled
--More-- or (q)uit
   Web-Passthrough..........................  Disabled
   Conditional Web Redirect.................  Disabled
   Auto Anchor..............................  Disabled
   Cranite Passthru.........................  Disabled
   Fortress Passthru........................  Disabled
   H-REAP Local Switching...................  Disabled
   Infrastructure MFP protection............  Enabled
                                          (Global Infrastructure MFP Disabled)
   Client MFP...............................  Optional
   Tkip MIC Countermeasure Hold-down Timer.....  60

 Mobility Anchor List
 WLAN ID     IP Address       Status
```

還可以配置其他本地身份驗證引數，特別是活動超時計時器。此計時器配置所有RADIUS伺服器發生故障後使用本地EAP的期間。

在GUI中，選擇Security > Local EAP > General並設定時間值。然後按一下Apply。

從CLI發出以下命令：

```
<#root>

(Cisco Controller) >

config local-auth active-timeout ?

<1 to 3600> Enter the timeout period for the Local EAP to remain active,
in seconds.
(Cisco Controller) >

config local-auth active-timeout 60
```

當您發出show local-auth config命令時，可以驗證此計時器的設定值。

```
<#root>

(Cisco Controller) >

show local-auth config

User credentials database search order:
    Primary ..................................... Local DB


Timer:
    Active timeout ............................. 60


Configured EAP profiles:
    Name ........................................ EAP-test
... Skip
```

9. 如果需要生成並載入手動PAC，可以使用GUI或CLI。

在GUI中，從頂部選單中選擇COMMANDS，並從右側的清單中選擇Upload File。從「File Type」下拉選單中選擇PAC(Protected Access Credential)。輸入所有引數並按一下Upload。

在CLI中輸入以下命令：

```
<#root>

(Cisco Controller) >

transfer upload datatype pac


(Cisco Controller) >

transfer upload pac ?


username     Enter the user (identity) of the PAC
```

```
 (Cisco Controller) >
transfer upload pac test1 ?

<validity>     Enter the PAC validity period (days)
(Cisco Controller) >
transfer upload pac test1 60 ?

<password>     Enter a password to protect the PAC
 (Cisco Controller) >
transfer upload pac test1 60 cisco123

(Cisco Controller) >
transfer upload serverip 10.1.1.1

(Cisco Controller) >
transfer upload filename manual.pac

(Cisco Controller) >
transfer upload start

Mode..................................................... TFTP
TFTP Server IP........................................... 10.1.1.1
TFTP Path................................................ /
TFTP Filename............................................ manual.pac
Data Type................................................ PAC
PAC User................................................. test1
PAC Validity............................................. 60 days
PAC Password............................................. cisco123

Are you sure you want to start? (y/N) y
PAC transfer starting.
File transfer operation completed successfully.
```

Microsoft證書頒發機構

若要使用EAP-FAST版本2和EAP-TLS驗證，WLC和所有使用者端裝置都必須具有有效的憑證，而且必須知道憑證授權機構的公用憑證。

安裝

如果Windows 2000 Server尚未安裝證書頒發機構服務，則需要安裝它。

要在Windows 2000 Server上啟用Microsoft證書頒發機構，請完成以下步驟：

1. 從「控制台」中，選擇增加/刪除程式。：
2. 在左側選擇增加/刪除Windows元件。
3. 選中證書服務。

   繼續操作之前，請檢視此警告：
4. 選取您要安裝的憑證授權單位型別。要建立簡單獨立授權，請選擇Stand-alone root CA。
5. 輸入有關憑證授權單位的必要資訊。此資訊會為您的憑證授權單位建立自簽憑證。請記住您使用的CA名稱。

   證書頒發機構將證書儲存在資料庫中。此範例使用Microsoft建議的預設設定：
6. Microsoft Certification Authority服務使用IIS Microsoft Web Server建立和管理客戶端和伺服器證書。它需要重新啟動下列專案的IIS服務：

   Microsoft Windows 2000 Server現在會安裝新服務。您需要有Windows 2000 Server安裝光碟才能安裝新的Windows元件。

   憑證授權單位現在已安裝。

在思科無線LAN控制器中安裝證書

要在Cisco無線區域網控制器的本地EAP伺服器上使用EAP-FAST版本2和EAP-TLS，請執行以下步驟：

1. 在無線LAN控制器上安裝裝置憑證。
2. 將廠商CA憑證下載到無線區域網路控制器。
3. 設定無線區域網路控制器使用EAP-TLS。

請注意，在本文檔中顯示的示例中，訪問控制伺服器(ACS)與Microsoft Active Directory和Microsoft證書頒發機構安裝在同一主機上，但如果ACS伺服器位於其他伺服器上，則配置應該相同。

在無線LAN控制器上安裝裝置憑證

請完成以下步驟：

1. .完成以下步驟，以便產生要匯入到WLC的憑證：

   a. 轉到http://<serverIpAddr>/certsrv。

   b. 選擇請求證書並按一下下一步。

   c. 選擇高級請求並按一下下一步。

d. 選擇Submit a certificate request to this CA using a form，然後按一下Next。

e. 選擇Web server作為證書模板並輸入相關資訊。然後將金鑰標籤為可導出。

f. 您現在會收到需要安裝在您電腦中的憑證。

2. 完成以下步驟，以便從PC檢索證書：

a. 打開Internet Explorer瀏覽器，然後選擇工具> Internet選項> 內容。

b. 按一下證書。

c. 從下拉選單中選擇新安裝的證書。

d. 按一下Export。

e. 按一下Next兩次並選擇Yes export the private key。此格式為PKCS#12（.PFX格式）。

f. 選擇Enable strong protection。

g. 輸入密碼。

h. 將其儲存在檔案<tme2.pfx>中。

3. 將PKCS#12格式的憑證複製到已安裝Openssl的任何電腦上，以便將其轉換為PEM格式。

```
openssl pkcs12 -in tme2.pfx -out tme2.pem

!--- The command to be given, -in


          .


Enter Import Password:

!--- Enter the password given previously, from step 2g.

MAC verified OK
Enter PEM pass phrase:

!--- Enter a phrase.

Verifying - Enter PEM pass phrase:
```

4. 將轉換後的PEM格式的裝置證書下載到WLC上。

```
<#root>

(Cisco Controller) >

transfer download datatype eapdevcert


(Cisco Controller) >

transfer download certpassword password


!--- From step 3.

Setting password to <cisco123>

(Cisco Controller) >

transfer download filename tme2.pem


(Cisco Controller) >

transfer download start


Mode..................................................... TFTP
Data Type................................................ Vendor Dev Cert
TFTP Server IP........................................... 10.1.1.12
TFTP Packet Timeout...................................... 6
TFTP Max Retries......................................... 10
TFTP Path................................................ /
TFTP Filename............................................ tme2.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

5. 重新開機後，請檢查憑證。

```
<#root>

(Cisco Controller) >

show local-auth certificates


Certificates available for Local EAP authentication:

Certificate issuer ..............................  vendor
  CA certificate:
    Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
     Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
      Valid: 2007 Feb 28th, 19:35:21 GMT to 2012 Feb 28th, 19:44:44 GMT
```

```
Device certificate:
  Subject: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme2
   Issuer: C=US, ST=ca, L=san jose, O=cisco, OU=wnbu, CN=tme
    Valid: 2007 Mar 28th, 23:08:39 GMT to 2009 Mar 27th, 23:08:39 GMT
```

將廠商CA憑證下載到無線LAN控制器

請完成以下步驟：

1. 要檢索供應商CA證書，請完成以下步驟：
   a. 轉到http://<serverIpAddr>/certsrv。
   b. 選擇檢索CA證書並按一下下一步。
   c. 選擇CA證書。
   d. 按一下DER encoded。
   e. 按一下Download CA certificate，並將證書另存為rootca.cer。
2. 使用openssl x509 -in rootca.cer -inform DER -out rootca.pem -outform PEM命令，將供應商CA從DER格式轉換為PEM格式。

   輸出檔案是PEM格式的rootca.pem。
3. 下載供應商CA證書：

<#root>

```
(Cisco Controller) >
transfer download datatype eapcacert

(Cisco Controller) >
transfer download filename ?

<filename>     Enter filename up to 16 alphanumeric characters.
(Cisco Controller) >
transfer download filename rootca.pem

(Cisco Controller) >
transfer download start ?

(Cisco Controller) >
transfer download start
```

```
Mode..................................... TFTP
Data Type................................ Vendor CA Cert
TFTP Server IP........................... 10.1.1.12
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /
TFTP Filename............................ rootca.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
  Reboot the switch to use new certificate.
```

設定無線區域網路控制器使用EAP-TLS

請完成以下步驟：

在GUI中，選擇Security > Local EAP > Profiles，選擇配置檔案並檢查以下設定：

- 已啟用本地證書「必需」。
- 啟用了「需要客戶端證書」。
- 憑證簽發者是廠商。
- 已啟用CA證書檢查。

在客戶端裝置上安裝證書頒發機構證書

下載並安裝使用者端的根CA憑證

使用者端必須從憑證授權單位伺服器取得根CA憑證。有幾種方法可用來取得使用者端憑證並將其安裝在Windows XP機器上。要獲取有效證書，Windows XP使用者必須使用其使用者ID登入，並且必須具有網路連線。

使用Windows XP使用者端上的Web瀏覽器，以及網路的有線連線，從私人根憑證授權機構伺服器取得使用者端憑證。此程式是用來從Microsoft憑證授權單位伺服器取得使用者端憑證：

1. 在客戶端上使用Web瀏覽器，並將瀏覽器指向證書頒發機構伺服器。為此，請輸入http://IP-address-of-Root-CA/certsrv。
2. 使用Domain_Name\user_name登入。您必須使用使用XP使用者端之個人的使用者名稱登入。
3. 在「歡迎」窗口上，選擇檢索CA證書並按一下下一步。
4. 選擇Base64編碼和下載CA證書。

5. 在「Certificate Issued」窗口中，按一下Install this certificate，然後按一下Next。

6. 選擇Automatically select the certificate store，然後按一下Next，顯示成功的導入消息。

7. 連線到證書頒發機構以檢索證書頒發機構證書：

8. 按一下Download CA certificate。

9. 要檢查證書頒發機構證書是否已正確安裝，請打開Internet Explorer並選擇工具> Internet選項>內容>證書。

   在受信任的根憑證授權單位中，您應該會看到新安裝的憑證授權單位：

為客戶端裝置生成客戶端證書

使用者端必須從憑證授權單位伺服器取得憑證，WLC才能驗證WLAN EAP-TLS使用者端。有幾種方法可用於獲取客戶端證書並將其安裝到Windows XP電腦上。為了取得有效的憑證，Windows XP使用者必須使用他們的使用者ID登入，而且必須有網路連線（有線連線或停用802.1x保全性的WLAN連線）。

使用Windows XP使用者端上的Web瀏覽器以及網路的有線連線，從私人根憑證授權機構伺服器取得使用者端憑證。此程式是用來從Microsoft憑證授權單位伺服器取得使用者端憑證：

1. 在客戶端上使用Web瀏覽器，並將瀏覽器指向證書頒發機構伺服器。為此，請輸入http://IP-address-of-Root-CA/certsrv。

2. 使用Domain_Name\user_name登入。您必須使用使用XP使用者端之個人的使用者名稱登入。（使用者名稱嵌入客戶端證書中。）

3. 在「歡迎」窗口上，選擇請求證書並按一下下一步。

4. 選擇高級請求並按一下下一步。

5. 選擇Submit a certificate request to this CA using a form，然後按一下Next。

6. 在「高級證書請求」表單上，選擇使用者作為「證書模板」，將「金鑰大小」指定為1024，然後按一下提交。

7. 在「Certificate Issued」窗口中，按一下Install this certificate。這會導致在Windows XP客戶端上成功安裝客戶端證書。

8. 選擇Client Authentication Certificate。

   現在已建立使用者端憑證。

9. 要檢查證書是否已安裝，請轉到Internet Explorer並選擇工具> Internet選項>內容>證書。在「個人」標籤中，您應該會看到憑證。

EAP-TLS與客戶端裝置上的Cisco安全服務客戶端

請完成以下步驟：

1. 預設情況下，WLC會廣播SSID，因此它會顯示在掃描的SSID的「建立網路」清單中。要建立網路配置檔案，您可以按一下清單中的SSID(Enterprise)，然後按一下Create Network。

   如果WLAN基礎設施配置為停用廣播SSID，則必須手動增加SSID。為此，請按一下Access Devices下的Add，然後手動輸入適當的SSID（例如Enterprise）。配置客戶端的活動探測行為。亦即，客戶端主動探查其配置的SSID。在「Add Access Device」窗口中輸入SSID之後，指定Actively search for this access device。

   注意：如果沒有先為設定檔設定EAP驗證設定，則連線埠設定不允許企業模式(802.1X)。

2. 按一下Create Network以啟動Network Profile窗口，該窗口允許您將選擇（或已配置的）SSID與身份驗證機制關聯。指定設定檔的描述性名稱。

   註：在此身份驗證配置檔案下，可以關聯多個WLAN安全型別和/或SSID。

3. 開啟驗證並檢查EAP-TLS方法。然後按一下Configure以配置EAP-TLS屬性。

4. 在「Network Configuration Summary」下，按一下Modify以配置EAP/憑據設定。

5. 指定Turn On Authentication，在Protocol下選擇EAP-TLS，然後選擇Username作為身份。

6. 指定Use Single Sign on Credentials，以使用登入憑據進行網路身份驗證。按一下Configure以設定EAP-TLS引數。

7. 為了具有安全的EAP-TLS配置，您需要檢查RADIUS伺服器證書。為此，請選中驗證伺服器證書。

8. 若要驗證RADIUS伺服器憑證，您必須提供思科安全服務使用者端資訊，以便僅接受正確的憑證。選擇Client > Trusted Servers > Manage Current User Trusted Server。

9. 指定規則名稱並檢查伺服器憑證的名稱。

   EAP-TLS配置已完成。

10. 連線到無線網路設定檔。Cisco Secure Services Client要求使用者登入：

    Cisco Secure Services Client接收伺服器證書並對其進行檢查（配置了規則並安裝了證書頒發機構）。然後會要求使用者使用憑證。

11. 在客戶端驗證之後，在「Manage Networks」頁籤中的「Profile」下選擇SSID，然後按一下Status以查詢有關連線的詳細資訊。

    Connection Details窗口提供有關客戶端裝置、連線狀態和統計資訊以及身份驗證方法的資訊。WiFi詳細資訊標籤提供802.11連線狀態的詳細資訊，包括RSSI、802.11通道和驗證/加密。

調試命令

輸出直譯器工具(僅供註冊客戶使用) (OIT)支援某些show指令。使用OIT檢視對show命令輸出的分

析。

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

可以在WLC上使用以下debug命令來監控身份驗證交換的進度：

- debug aaa events enable
- debug aaa detail enable
- debug dot1x events enable
- debug dot1x states enable
- debug aaa local-auth eap events enable

  或

- debug aaa all enable

相關資訊

- Cisco無線LAN控制器組態設定指南4.1版
- WLAN技術支援
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。