Cisco Aironet無線安全常見問題

目錄

[簡介](#)
[一般常見問題](#)
[故障排除和設計常見問題](#)
[相關資訊](#)

簡介

本文檔提供有關Cisco Aironet無線安全的最常見問題(FAQ)的資訊。

一般常見問題

問：無線安全有什麼需要？

A.在有線網路中，資料會保留在連線終端裝置的電纜中。但是無線網路通過向空中廣播射頻訊號來傳輸和接收資料。由於WLAN使用的廣播性質，駭客或入侵者訪問或破壞資料的威脅更大。為了緩解此問題，所有WLAN都需要新增：

1. 使用者身份驗證，防止對網路資源的未經授權的訪問。
2. 資料隱私保護傳輸資料的完整性和隱私（也稱為加密）。

問： 802.11無線LAN標準定義了哪些不同的身份驗證方法？

A. 802.11標準定義了兩種無線LAN使用者端驗證機制：

1. 開放式身份驗證
2. 共用金鑰驗證

還有另外兩種常用的機制：

1. 基於SSID的身份驗證
2. MAC地址身份驗證

問：什麼是開放式身份驗證？

A.開放式身份驗證基本上是一個空的身份驗證演算法，這意味著沒有對使用者或機器進行驗證。開放式身份驗證允許任何裝置向接入點(AP)發出身份驗證請求。 開放式身份驗證使用明文傳輸允許客戶端與AP關聯。如果未啟用加密，任何知道WLAN SSID的裝置都可以訪問網路。如果在AP上啟用有線等效保密(WEP)，則WEP金鑰將成為一種訪問控制方式。沒有正確WEP金鑰的裝置無法通過AP傳輸資料，即使身份驗證成功。此類裝置也無法解密接入點傳送的資料。

問：客戶端與AP關聯時，開放式身份驗證涉及哪些步驟？

1. 客戶端向AP傳送探測請求。
2. AP傳送回探測響應。
3. 客戶端評估AP響應並選擇最佳AP。
4. 客戶端向AP傳送身份驗證請求。
5. AP確認身份驗證並註冊客戶端。
6. 然後客戶端向AP傳送關聯請求。
7. AP確認關聯並註冊客戶端。

問：開放式身份驗證有哪些優點和缺點？

A.開放式身份驗證的優缺點如下：

優勢：開放式身份驗證是一種基本身份驗證機制，可用於不支援複雜身份驗證演算法的無線裝置。802.11規範中的身份驗證是面向連線的。通過設計身份驗證要求，裝置可以快速訪問網路。在這種情況下，您可以使用開放驗證。

缺點：Open Authentication無法檢查客戶端是否為有效客戶端而不是駭客客戶端。如果您未將WEP加密與開放式身份驗證配合使用，則任何知道WLAN SSID的使用者都可以訪問網路。

問：什麼是共用金鑰身份驗證？

A.共用金鑰身份驗證的工作方式與開放式身份驗證類似，但有一個主要區別。當您使用帶WEP加密金鑰的開放式身份驗證時，WEP金鑰用於加密和解密資料，但在身份驗證步驟中未使用。在共用金鑰身份驗證中，WEP加密用於身份驗證。與開放式身份驗證類似，共用金鑰身份驗證要求客戶端和AP具有相同的WEP金鑰。使用共用金鑰身份驗證的AP向客戶端傳送質詢文本資料包。客戶端使用本地配置的WEP金鑰加密質詢文本並回覆隨後的身份驗證請求。如果AP能夠解密身份驗證請求並檢索原始質詢文本，則AP會以授權客戶端訪問的身份驗證響應進行響應。

問：客戶端與AP關聯時，共用金鑰身份驗證涉及哪些步驟？

1. 客戶端向AP傳送探測請求。
2. AP傳送回探測響應。
3. 客戶端評估AP響應並選擇最佳AP。
4. 客戶端向AP傳送身份驗證請求。
5. AP傳送包含未加密質詢文本的身份驗證響應。
6. 客戶端使用WEP金鑰加密質詢文本，並將文本傳送到AP。
7. AP將未加密的質詢文本與加密的質詢文本進行比較。如果身份驗證可以解密和檢索原始質詢文本，則身份驗證成功。

共用金鑰身份驗證在客戶端關聯過程中使用WEP加密。

問：共用金鑰身份驗證有哪些優點和缺點？

A.在共用金鑰身份驗證中，客戶端和AP交換質詢文本（明文）和加密質詢。因此，此類身份驗證容易受到中間人攻擊。駭客可以偵聽未加密質詢和加密質詢，並從此資訊提取WEP金鑰（共用金鑰）。當駭客知道WEP金鑰時，整個身份驗證機制會受到危害，因此駭客可以訪問WLAN網路。這是共用金鑰身份驗證的主要缺點。

問：什麼是MAC地址身份驗證？

答：雖然802.11標準沒有指定MAC地址身份驗證，但WLAN網路通常使用此身份驗證技術。因此，大多數無線裝置供應商（包括思科）都支援MAC地址身份驗證。

在MAC地址身份驗證中，客戶端根據其MAC地址進行身份驗證。客戶端的MAC地址根據儲存在AP本地或外部身份驗證伺服器上的MAC地址清單進行驗證。MAC身份驗證比802.11提供的開放式和共用金鑰身份驗證更強的安全機制。這種身份驗證形式進一步降低了未經授權裝置訪問網路的可能性。

問：在Cisco IOS軟體版本12.3(8)JA2中，MAC驗證為什麼與Wi-Fi保護存取(WPA)不起作用？

A. MAC身份驗證的唯一安全級別是根據允許的MAC地址清單檢查客戶端的MAC地址。這被認為非常薄弱。在早期的Cisco IOS軟體版本中，您可以設定MAC驗證和WPA以加密資訊。但是，由於WPA本身具有要檢查的MAC地址，思科決定在以後的Cisco IOS軟體版本中不允許此型別的配置，並決定只改進安全功能。

問：是否可以使用SSID驗證無線裝置？

A.服務集識別符號(SSID)是WLAN用作網路名稱的一個唯一、區分大小寫的字母數字值。SSID是一種允許對無線LAN進行邏輯分隔的機制。SSID不提供任何資料隱私功能，SSID也不真正對AP驗證客戶端。SSID值在Beacons、Probe Requests、Probe responses和其他型別的幀中以明文形式廣播。竊聽者可以使用802.11無線LAN資料包分析器（例如Sniffer Pro）輕鬆確定SSID。Cisco建議您不要將SSID用作保護WLAN網路的方法。

問：如果我禁用SSID廣播，是否可在WLAN網路中實現增強的安全性？

A.禁用SSID廣播時，不會在信標消息中傳送SSID。但是，其他幀（如「探測請求」和「探測響應」）仍具有明文形式的SSID。因此，如果您禁用SSID，將無法實現增強的無線安全性。SSID並非設計為安全機制，也並非設計為用於安全機制。此外，如果您禁用SSID廣播，則可能會遇到混合客戶端部署的Wi-Fi互操作性問題。因此，Cisco建議您不要將SSID用作安全模式。

問： 802.11安全存在哪些漏洞？

A. 802.11安全的主要漏洞可總結如下：

- 僅裝置身份驗證較弱：客戶端裝置是經過身份驗證的，而不是經過使用者身份驗證。
- 弱資料加密：有線等效保密(WEP)作為加密資料的一種手段已被證明是無效的。
- 無消息完整性：完整性檢查值(ICV)作為確保報文完整性的一種手段已被證明是無效的。

問： 802.1x身份驗證在WLAN中起到什麼作用？

A.為了解決802.11標準定義的原始身份驗證方法中的缺陷和安全漏洞，802.1X身份驗證框架包含在802.11 MAC層安全增強草案中。IEEE 802.11任務組i(TGi)目前正在開發這些增強功能。802.1X框架為鏈路層提供可擴展的身份驗證，通常只在更高層才可見。

問： 802.1x框架定義的三個實體是什麼？

A.802.1x框架要求這三個邏輯實體驗證WLAN網路上的裝置。

1. **Supplicant** — 請求方駐留在無線LAN客戶端上，也稱為EAP客戶端。
2. **Authenticator** — 身份驗證器駐留在AP上。
3. **Authentication Server** — 身份驗證伺服器位於RADIUS伺服器上。

問：使用802.1x身份驗證框架時，如何進行無線客戶端身份驗證？

A.當無線客戶端（EAP客戶端）變為活動狀態時，無線客戶端將使用開放或共用身份驗證進行身份驗證。802.1x使用開放式身份驗證，並在客戶端成功與AP關聯後啟動。客戶端站可以關聯，但只能在成功802.1x身份驗證後傳遞資料流量。以下是802.1x驗證中的步驟：

1. 為802.1x配置的AP（身份驗證器）從客戶端請求使用者身份。
2. 客戶在規定的時間段內以其身份作出回應。
3. 如果使用者的身份存在於客戶端的資料庫中，伺服器將檢查使用者的身份並開始與客戶端進行身份驗證。
4. 伺服器向AP傳送成功消息。
5. 一旦客戶端通過身份驗證，伺服器將加密金鑰轉發到AP，AP用於加密/解密傳送到客戶端或從客戶端傳送的流量。
6. 在步驟4中，如果使用者的身份在資料庫中不存在，伺服器將丟棄身份驗證並向AP傳送失敗消息。
7. AP將此消息轉發給客戶端，客戶端必須再次使用正確的憑據進行身份驗證。

注意：在整個802.1x身份驗證過程中，AP只將身份驗證消息轉發到客戶端或從客戶端轉發出去。

問：我可以在802.1x身份驗證框架中使用哪些不同的EAP變體？

A.802.1x定義驗證使用者端的程式。802.1x框架中使用的EAP型別定義了802.1x交換中使用的憑證型別和身份驗證方法。802.1x框架可以使用以下EAP變體：

- EAP-TLS — 可擴展身份驗證協定傳輸層安全
- EAP-FAST - EAP通過安全隧道的靈活身份驗證
- EAP-SIM - EAP使用者身份模組
- Cisco LEAP — 輕量級可擴展身份驗證協定
- EAP-PEAP - EAP受保護的可擴展身份驗證協定
- EAP-MD5 - EAP — 消息摘要演算法5
- EAP-OTP - EAP按時密碼
- EAP-TTLS - EAP隧道傳輸層安全

問：如何從可用的不同變型中選擇802.1x EAP方法？

A.您必須考慮的最重要因素是EAP方法是否與現有網路相容。此外，思科建議您選擇支援相互驗證的方法。

問：什麼是本地EAP身份驗證？

A.本地EAP是WLC充當身份驗證伺服器的機制。使用者憑證儲存在WLC本機上以驗證無線使用者端，當伺服器關閉時，無線使用者端會作為遠端辦公室的後端程式。可以從WLC上的本地資料庫或外部LDAP伺服器檢索使用者憑據。LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2和PEAPv1/GTC是本地EAP支援的不同的EAP身份驗證。

問：什麼是Cisco LEAP?

A.輕量可擴展身份驗證協定(LEAP)是思科專有的身份驗證方法。Cisco LEAP是適用於無線LAN(WLAN)的802.1X驗證型別。 Cisco LEAP支援客戶端和RADIUS伺服器之間通過登入密碼作為共用金鑰進行強雙向身份驗證。Cisco LEAP提供動態的每使用者、每會話加密金鑰。LEAP是部署802.1x的最簡單方法，僅需要RADIUS伺服器。有關LEAP的資訊，請參閱Cisco LEAP。

問：EAP-FAST如何工作？

A. EAP-FAST使用對稱金鑰演算法來實現隧道式身份驗證過程。隧道建立依賴於受保護的訪問憑證(PAC),EAP-FAST可以通過身份驗證、授權和記帳(AAA)伺服器（例如Cisco安全訪問控制伺服器[ACS] v.3.2.3）動態地調配和管理EAP-FAST。 通過相互驗證的隧道，EAP-FAST提供針對字典攻擊和中間人漏洞的保護。以下是EAP-FAST的各個階段：

EAP-FAST不僅可降低被動字典攻擊和中間人攻擊帶來的風險，還可根據當前部署的基礎架構啟用安全身份驗證。

- 第1階段：建立相互驗證的通道 — 客戶端和AAA伺服器使用PAC相互驗證並建立安全通道。
- 第2階段：在已建立的隧道中執行客戶端身份驗證 — 客戶端傳送使用者名稱和密碼以進行身份驗證並建立客戶端授權策略。
- 或者，第0階段 — EAP-FAST身份驗證不經常使用此階段來使客戶端能夠使用PAC進行動態調配。此階段在使用者與網路之間安全地生成每使用者訪問憑證。身份驗證的第1階段使用此每使用者憑據，稱為PAC。

有關詳細資訊，請參閱Cisco EAP-FAST。

問：cisco.com上有說明如何在Cisco WLAN網路中配置EAP的文檔嗎？

A.有關如何在WLAN網路中配置EAP身份驗證的資訊，請參閱使用RADIUS伺服器的EAP身份驗證。

有關如何配置PEAP身份驗證的資訊，請參閱受保護的EAP應用程式說明。

有關如何配置LEAP身份驗證的資訊，請參閱使用本地RADIUS伺服器的LEAP身份驗證。

問：無線網路中最常用的加密機制有哪些？

A.以下是無線網路中最常用的加密方案：

- WEP

- TKIP
- AES

AES是一種硬體加密方法，而WEP和TKIP加密是在韌體上處理的。通過韌體升級，WEP裝置可以支援TKIP，因此它們可以互操作。AES是最安全、最快的方法，而WEP是最不安全的方法。

問：什麼是WEP加密？

A. WEP代表有線等效保密。WEP用於加密和解密在WLAN裝置之間傳輸的資料訊號。WEP是一項可選的IEEE 802.11功能，可防止在傳輸過程中洩漏和修改資料包，並為網路的使用提供訪問控制。WEP使WLAN鏈路與有線鏈路一樣安全。正如標準規定的那樣，WEP使用40位或104位金鑰的RC4演算法。RC4是對稱演算法，因為RC4使用相同的金鑰對資料進行加密和解密。啟用WEP後，每個電台「電台」都有一個金鑰。該金鑰用於在通過無線電波傳輸資料之前對資料進行加擾。如果站點收到的資料包未使用適當的金鑰進行加擾，則該站點會丟棄該資料包，並且不會將此類資料包傳送到主機。

有關如何配置WEP的資訊，請參閱配置有線等效保密(WEP)。

問：什麼是廣播金鑰輪替？廣播金鑰輪換的頻率是多少？

A.廣播金鑰輪替允許AP生成儘可能最佳的隨機組金鑰。廣播金鑰輪替定期更新所有能夠進行金鑰管理的客戶端。啟用廣播WEP金鑰輪換時，AP會提供一個動態廣播WEP金鑰，並按您設定的間隔更改金鑰。如果您的無線LAN支援非思科無線客戶端裝置或無法升級到思科客戶端裝置的最新韌體的裝置，廣播金鑰輪替是TKIP的絕佳替代方案。有關如何配置廣播金鑰輪替功能的資訊，請參閱啟用和禁用廣播金鑰輪替。

什麼是TKIP?

A. TKIP代表臨時金鑰完整性協定。引入TKIP以解決WEP加密的缺點。TKIP也稱為WEP金鑰雜湊，最初稱為WEP2。 TKIP是解決WEP金鑰重複使用問題的臨時解決方案。TKIP使用RC4演算法執行加密，與WEP相同。與WEP的主要區別在於TKIP更改每個資料包的時間金鑰。臨時金鑰會更改每個資料包，因為每個資料包的雜湊值會更改。

問：使用TKIP的裝置是否可以與使用WEP加密的裝置互操作？

A. TKIP的一個優勢是，具有現有基於WEP的AP和無線電的WLAN可以通過簡單的韌體補丁升級到TKIP。此外，僅WEP裝置仍可與使用WEP的啟用TKIP的裝置互操作。

問：什麼是消息完整性檢查(MIC)?

A. MIC是解決WEP加密漏洞的又一增強功能。MIC可防止對加密資料包的位翻轉攻擊。在位翻轉攻擊期間，入侵者截獲加密消息，修改該消息，然後重新傳輸修改後的消息。接收方不知道消息已損壞並且不是合法消息。為了解決此問題，MIC功能向無線幀新增一個MIC欄位。MIC欄位提供幀完整性檢查，該檢查不會像ICV一樣易受數學缺陷的影響。MIC還將序列號欄位新增到無線幀中。AP丟棄接收到的亂序幀。

什麼是WPA?WPA 2與WPA有何不同？

A. WPA是Wi-Fi聯盟提供的基於標準的安全解決方案，可解決本地WLAN中的漏洞。WPA為WLAN系統提供增強的資料保護和訪問控制。WPA解決了原始IEEE 802.11安全實施中的所有已知有線等效保密(WEP)漏洞，為企業和小型辦公室、家庭辦公室(SOHO)環境中的WLAN網路帶來了即

時安全解決方案。

WPA2是下一代Wi-Fi安全性。WPA2是已批准的IEEE 802.11i標準的Wi-Fi聯盟互操作性實施。WPA2使用計數器模式及密碼塊鏈結消息驗證代碼協定(CCMP)，實施美國國家標準與技術研究所(NIST)推薦的高級加密標準(AES)加密演算法。AES計數器模式是一種分組密碼，使用128位加密金鑰一次加密128位資料塊。WPA2比WPA具有更高的安全性。WPA2在每個關聯上建立新的會話金鑰。WPA2用於網路中每個客戶端的加密金鑰是唯一的且特定於該客戶端。最後，通過無線方式傳送的每個資料包都使用唯一金鑰進行加密。

WPA1和WPA2都可以使用TKIP或CCMP加密。（某些接入點和某些客戶端確實會限制組合，但可能有四種組合）。 WPA1和WPA2之間的區別在於資訊元素被放入信標、關聯幀和4次握手幀中。這些資訊元素中的資料基本相同，但使用的識別符號不同。金鑰握手的主要區別在於，WPA2在四向握手中包含初始組金鑰，並且跳過第一個組金鑰握手，而WPA需要執行此額外握手來傳遞初始組金鑰。組金鑰的重新加密以相同的方式發生。握手發生在選擇和使用密碼套件（TKIP或AES）傳輸使用者資料包之前。在WPA1或WPA2握手期間，確定要使用的密碼套件。選擇後，密碼套件將用於所有使用者流量。因此，WPA1加AES不是WPA2。WPA1允許（但通常受客戶端限制）TKIP或AES密碼。

什麼是AES?

A. AES代表高級加密標準。AES提供了更強大的加密。AES使用Rijndael演算法，該演算法是具有128、192和256位金鑰支援的分組密碼，比RC4強得多。要支援AES的WLAN裝置，硬體必須支援AES而不是WEP。

問： Microsoft Internet身份驗證服務(IAS)伺服器支援哪些身份驗證方法？

A. IAS支援以下身份驗證協定：

- 密碼驗證通訊協定(PAP)
- Shiva密碼驗證通訊協定(SPAP)
- 詢問交握驗證通訊協定(CHAP)
- Microsoft質詢握手身份驗證協定(MS-CHAP)
- Microsoft質詢握手身份驗證協定版本2(MS-CHAP v2)
- 可擴展身份驗證協定 — 消息摘要5 CHAP(EAP-MD5 CHAP)
- EAP — 傳輸層安全(EAP-TLS)
- 受保護的EAP-MS-CHAP v2(PEAP-MS-CHAP v2)（也稱為PEAPv0/EAP-MSCHAPv2）

安裝Windows 2000 Server Service Pack 4時，Windows 2000 Server中的PEAP-TLS IAS支援PEAP-MS-CHAP v2和PEAP-TLS。有關詳細資訊，請參閱用於IAS的身份驗證方法 。

問：如何在無線環境中實施VPN?

A. VPN是第3層安全機制；無線加密機制在第2層實施。VPN通過802.1x、EAP、WEP、TKIP和AES實施。當第2層機制到位時，VPN會增加實施開銷。在公共熱點和酒店等沒有實施安全的地方，VPN是實施的有效解決方案。

故障排除和設計常見問題

問：在室外無線LAN中部署無線安全有什麼最佳實踐？

A.參閱室外無線安全的最佳做法。本文提供有關部署室外無線LAN的最佳安全實踐的資訊。

問：是否可以將Windows 2000或2003伺服器與Active Directory配合使用來用於RADIUS伺服器來驗證無線客戶端？

A.具有Active Directory的Windows 2000或2003伺服器可以作為RADIUS伺服器工作。有關如何配置此RADIUS伺服器的資訊，您需要聯絡Microsoft，因為Cisco不支援Windows伺服器配置。

問：我的站點即將從開放式無線網路（350和1200系列AP）遷移到PEAP網路。我想讓開放式SSID（為開放驗證配置的SSID）和PEAP SSID（為PEAP驗證配置的SSID）同時在同一個AP上工作。這讓我們有時間將客戶端遷移到PEAP SSID。是否可以在同一個AP上同時託管開放式SSID和PEAP SSID?

A.Cisco AP支援VLAN（僅第2層）。 這實際上是實現你想做事情的唯一途徑。您需要建立兩個VLAN（本徵VLAN和其他VLAN）。 然後，您可以為其中一個提供WEP金鑰，而不為另一個提供WEP金鑰。這樣，您可以為開放式身份驗證配置其中一個VLAN，為對等點身份驗證配置另一個VLAN。如果要瞭解如何配置VLAN，請參閱將VLAN與Cisco Aironet無線裝置一起使用。

請注意，您需要為dot1Q和VLAN間路由、L3交換機或路由器配置交換機。

問：我想設定我的Cisco AP 1200 VxWorks，讓無線使用者向Cisco 3005 VPN集中器進行身份驗證。AP和客戶端需要提供什麼配置才能完成此操作？

A.此方案的AP或客戶端不需要特定配置。您必須在VPN集中器上執行所有配置。

問：我正在部署Cisco 1232 AG AP。我想瞭解我可以使用此AP部署的最安全的方法。我沒有AAA伺服器，我的唯一資源是AP和Windows 2003域。我熟悉如何使用靜態128位WEP金鑰、非廣播SSID和MAC地址限制。使用者大多使用Windows XP工作站和一些PDA。此設定最安全的實施方式是什麼？

A.如果您沒有像Cisco ACS這樣的RADIUS伺服器，則可以將AP配置為用於LEAP、EAP-FAST或MAC身份驗證的本地RADIUS伺服器。

注意：必須考慮的一個非常重要的點是，您是否要將客戶端用於LEAP或EAP-FAST。如果是，您的客戶端必須擁有支援LEAP或EAP-FAST的實用程式。Windows XP實用程式僅支援PEAP或EAP-TLS。

問：PEAP身份驗證失敗，並出現錯誤「EAP-TLS或PEAP身份驗證在SSL握手期間失敗」。 為什麼？

答：此錯誤可能是由於思科錯誤ID CSCee06008**(僅限註冊客戶)所致**。PEAP在ADU 1.2.0.4中失敗。此問題的解決方法是使用最新版本的ADU。

問：是否可以在同一個SSID上進行WPA和本地MAC身份驗證？

答：Cisco AP不支援同一服務集識別符號(SSID)中的本地MAC身份驗證和Wi-Fi保護訪問預共用金鑰(WPA-PSK)。 當您使用WPA-PSK啟用本地MAC身份驗證時，WPA-PSK不起作用。之所以會出現此問題，是因為本地MAC身份驗證從配置中刪除WPA-PSK ASCII密碼行。

問：我們目前為我們的資料VLAN設定了三個使用密碼128位WEP加密的Cisco 1231無線AP。我們不廣播SSID。在我們的環境中沒有單獨的RADIUS伺服器。有人通過掃描工具確定了WEP金鑰，並用該工具監控了幾個星期的無線流量。我們如何防止這種情況並使網路安全？

A.靜態WEP易受此問題的影響，如果駭客捕獲了足夠的資料包並能夠獲取具有相同初始化向量(IV)的兩個或更多的資料包，則可以匯出靜態WEP。

有幾種方法可以防止此問題的發生：

1. 使用動態WEP金鑰。
2. 使用WPA。
3. 如果只有思科介面卡，請啟用Per Packet Key和MIC。

問：如果我有兩個不同的WLAN，兩者都配置為Wi-Fi保護訪問(WPA) — 預共用金鑰(PSK)，則每個WLAN的預共用金鑰是否可以不同？如果不同，是否會影響使用不同的預共用金鑰配置的其他WLAN?

A.WPA-PSK的設定應針對每個WLAN。如果變更一個WPA-PSK，則不應影響已設定的另一個WLAN。

問：在我的環境中，我主要使用英特爾Pro/無線、可擴展身份驗證協定 — 通過安全隧道的靈活身份驗證(EAP-FAST)，以及連結到Windows Active Directory(AD)帳戶的思科安全訪問控制伺服器(ACS)3.3。問題在於當使用者密碼即將到期時，Windows不會提示使用者更改密碼。最終，帳戶將過期。是否有解決方案讓Windows提示使用者更改密碼？

A.Cisco Secure ACS密碼老化功能可讓您強制使用者在以下一種或多種情況下更改密碼：

- 在指定的天數（按日期計齡規則）之後
- 在指定的登入數之後（按使用期限規則）
- 新使用者首次登入時（密碼更改規則）

有關如何為此功能配置Cisco Secure ACS的詳細資訊，請參閱為CiscoSecure使用者資料庫啟用密碼時效。

問：當使用者使用LEAP無線登入時，會獲得用於對映網路驅動器的登入指令碼。但是，如果使用Wi-Fi保護訪問(WPA)或WPA2和PEAP身份驗證，登入指令碼將不會運行。使用者端和存取點都是思科，RADIUS(ACS)也是如此。 為什麼登入指令碼無法在RADIUS(ACS)上運行？

A.要使登入指令碼正常工作，必須進行電腦身份驗證。這樣，無線使用者就可以在使用者登入之前獲得載入指令碼的網路訪問許可權。

有關如何使用PEAP-MS-CHAPv2配置電腦身份驗證的資訊，請參閱使用PEAP-MS-CHAPv2電腦身份驗證配置Cisco Secure ACS for Windows v3.2。

問：在Cisco Aironet Desktop Utility(ADU)版本3.0中，當使用者配置可擴展身份驗證協定傳輸層安全(EAP-TLS)的電腦身份驗證時，ADU不允許使用者建立配置檔案。為

什麼？

A.這是因為思科錯誤ID CSCsg32032(僅限註冊客戶)。 如果客戶端PC安裝了電腦證書並且沒有使用者證書，則可能會發生這種情況。

因應措施是將電腦證書複製到使用者儲存區，建立EAP-TLS配置檔案，然後從使用者儲存區中刪除僅電腦身份驗證配置的證書。

問：有沒有辦法根據客戶端的MAC地址在無線LAN上分配VLAN?

不，這不可能。從RADIUS伺服器分配的VLAN僅適用於802.1x，不適用於MAC身份驗證。如果MAC地址在RADIUS伺服器（在LEAP/PEAP中定義為使用者ID/密碼）進行身份驗證，則可以使用RADIUS推送具有MAC身份驗證的VSA。

相關資訊

- 無線網路安全
- 無線LAN安全白皮書
- 無線區域網安全概述
- 無線LAN網路的EAP-TLS部署指南
- Cisco LEAP
- 設定有線等效保密(WEP)
- 無線產品支援
- 技術支援與文件 - Cisco Systems