

Cisco LEAP

這份問答文件是以 Cisco 的 Cisco LEAP 延伸驗證協定 (Extensible Authentication Protocol) 型態為主

總覽

問. 何為 Cisco® LEAP ?

答. Cisco LEAP 是一項針對無線區域網路 (WLAN) 的 802.1X 驗證型態，可在用戶端與 RADIUS 伺服器之間使用登入密碼做為共享秘密，支援強大的相互驗證功能。它可針對個別使用者/通訊會期，提供動態的加密鑰。

問. Cisco Wireless Security Suite、WPA (Wi-Fi Protected Access) 與 WPA2 (Wi-Fi Protected Access 2) 是否支援 Cisco LEAP ?

答. 是。Cisco Wireless Security Suite 支援不同的 EAP (Extensible Authentication Protocol) 驗證型態，包括 Cisco LEAP 在內。如同其他所有型態的 EAP，Cisco LEAP 也可用於 WPA 與 WPA2 網路。

問. 何為 Cisco Wireless Security Suite ?

答. Cisco Wireless Security Suite 是由 Cisco 針對 Cisco Aironet®無線產品與 Cisco Compatible Extensions 用戶端設備，所提供的企業級、標準化 WLAN 安全方案。Cisco Wireless Security Suite 可與 Cisco Self-Defending Network 整合，也獲得 Cisco SWAN (Structured Wireless-Aware Network) 的全面支援。

Cisco Wireless Security Suite 提供堅實的 WLAN 安全服務，可與有線區域網路的安全功能緊密併用。它提供領先業界的 WLAN 安全服務，滿足行動網路在一致、可靠與安全的需求。這項企業級的解決方案可避免精密的 WLAN 攻擊，並整合一系列的用戶端，兼具可靠度、延展性與集中式安全管理。網路管理人員能以具延展性、零缺失的的安全管理作業來部署企業的 WLAN，不造成 IT 人員的額外負擔。

Cisco Wireless Security Suite 具備 Cisco 許多創新的強化功能，並支援 WPA、WPA2 與 Wi-Fi 認證的用戶端設備，透過強大的動態加密功能，根據個別使用者/通訊會期的相互驗證，以及資料隱私權，來提供存取控管。

問. Cisco LEAP 是否內含於 Cisco Aironet 產品與 Cisco Compatible 用戶端設備 ?

答. 是。Cisco LEAP 內含於 Cisco Aironet 產品與 Cisco Compatible 用戶端設備，且不另計費。

問. Cisco LEAP 是一項標準嗎？

答. Cisco LEAP 可利用標準化 802.1X 框架的優點。雖然目前現有的用戶端作業系統並未提供 EAP 支援，但 Cisco 仍搶先針對 WLAN 提供 EAP 支援。Cisco 在 2000 年 12 月發表 Cisco LEAP，以求儘速改善 WLAN 驗證的整體安全性。

問. Cisco LEAP 可否與 Cisco SWAN 併用？

答. 是。Cisco LEAP 是 Cisco Wireless Security Suite 的功能元件之一，且獲得 Cisco SWAN 的全面支援。

問. 何為 Cisco SWAN？

答. 針對部署 WLAN 的企業，Cisco SWAN 以最低 TCO（total cost of ownership）來提供框架，以整合並擴充有線及無線網路。Cisco SWAN 將「無線感知」納為網路基礎架構的重要元素，為 WLAN 提供與企業有線網路同級的安全性、延展性、可靠度、易於部署及管理功能。Cisco SWAN 協助企業與服務供應商的網路主管，部署、運作、管理與保護散佈在多家企業或部署環境的千百個存取器。欲知 Cisco SWAN 更多資訊，請造訪：
<http://www.cisco.com/go/swan>

功能與效益

問. Cisco LEAP 有哪些安全效益？

答. Cisco LEAP 透過對後端目錄（Windows NT、Windows Active Directory 與 Open Database Connectivity/ODBC）或 Cisco LEAP 快取 RADIUS 伺服器如 Cisco ACS（Access Control Server）與 Cisco Network Registrar®來擴充驗證支援，克服 802.11 無線安全的主要缺失。

問. Cisco LEAP 的企業效益為何？

答. Cisco LEAP 是 Cisco Wireless Security Suite 廣獲部署並經過市場實證的功能元件。它支援多種用戶端轉接型態，包括 ASD（application-specific devices），以及 Cisco 與 Cisco Compatible Extensions 協力夥伴，還有許多用戶端設備與網路介面製造商的設備。Cisco LEAP 提供：

- 可使用 Windows NT/2000 Active Directory 的現有使用者名稱與密碼執行單一登入
- 為 IT 主管提供簡化且平價的部署及管理
- 兼具可靠度與延展性的集中式安全管理
- 高效能且可持續升級的企業級安全性
- 與 TKIP（Temporal Key Integrity Protocol）與 AES（Advanced Encryption Standard）共用，動態保護隱私

部署

問. Cisco LEAP 驗證如何運作？

答. 無線用戶端需先通過 RADIUS 伺服器的驗證，在取得驗證之前，只能傳送 EAP 傳輸。終端使用者登入後，即會進行用戶端與 RADIUS 伺服器的相互驗證。在用戶端與 RADIUS 伺服器相互驗證的過程中，會產生動態加密鑰。RADIUS 伺服器會經由安全通道傳送動態加密鑰給存取器。存取器接收加密鑰之後，即可為通過驗證的用戶端提供一般的網路傳輸。用於驗證的憑證如登入密碼，不會在未加密的情況下經由無線媒介傳送。用戶端登出後，該用戶在存取器的相關入口將恢復未驗證狀態。

問. Cisco LEAP 支援哪些用戶端作業系統？

答. Cisco LEAP 支援許多用戶端作業系統，包括 Microsoft Windows、Mac OS、Linux、DOS 與 Windows CE。

問. Cisco LEAP 支援哪些 RADIUS 伺服器與使用者資料庫？

答. Cisco LEAP 支援下列 RADIUS 伺服器與使用者資料庫：Cisco Secure ACS、Cisco Network Registrar、Funk Odyssey Server、Funk Steel-Belted，以及使用 Interlink Networks 伺服器程式碼的產品（如 LeapPoint 裝置）。

問. Cisco LEAP 支援哪些 Cisco Aironet 設備？

答. Cisco LEAP 支援多種 Cisco Aironet 產品，包括 Cisco Aironet 存取器、群組橋接器、無線橋接器與增益器，以及 Cisco 與 Cisco Compatible 的許多 WLAN 用戶端設備。

問. Cisco 以外的供應商是否也針對無線用戶端提供 Cisco LEAP 驗證？

答. 是。Cisco LEAP 驗證涵蓋 Cisco Compatible Extensions 產品。

問. 我想得知更多關於部署 Cisco LEAP 的資訊？

答. 請閱讀 [Deployment Guide : Configuring the Cisco Wireless Security Suite](#)，以取得更多部署 Cisco LEAP 的資訊。

EAP 型態比較

問. PEAP (Protected EAP)、EAP-FAST (EAP-Flexible Authentication via Secure Tunneling)、Cisco LEAP 與 EAP-TLS (EAP-Transport Layer Security) 之間有何不同？

答. 表 1 是對 PEAP、EAP-FAST、Cisco LEAP 與 EAP-TLS 的綜合比較。

表 1. PEAP、EAP-FAST、Cisco LEAP 與 EAP-TLS 比較表

	PEAP-GTC (Generic Token Card)	PEAP-MSCHAP (Microsoft Challenge Authentication Protocol) v2	EAP-FAST	Cisco LEAP	EAP-TLS
使用者驗證資料庫與伺服器	OTP (One-time password)、LDAP (Lightweight Directory Access Protocol)、Novell NDS、Windows NT Domains、Active Directory	Windows NT Domains、Active Directory	Windows NT Domains、Active Directory、LDAP (有限)	Windows NT Domains、Active Directory	OTP、LDAP、Novell NDS、Windows NT Domains、Active Directory
需經伺服器認證	是	是	否	否	是
需經用戶端認證	否	否	否	否	是
作業系統支援	Windows XP、Windows 2000、Windows CE* 搭配協力廠商工具；其他作業系統**	Windows XP、Windows 2000、Windows CE 搭配協力廠商工具；其他作業系統**	Windows XP、Windows 2000、Windows CE*** 搭配協力廠商工具；其他作業系統**	Windows 98、Windows 2000、Windows NT、Windows Me、Windows XP、Mac OS、Linux、Windows CE、DOS	Windows XP、Windows 2000、Windows CE 搭配協力廠商工具；其他作業系統
ASD 支援	否	否	是	是	否
使用憑證	用戶端：Windows、NDS、LDAP 密碼：OTP 或密碼環 伺服器：數位認證	Windows 密碼	Windows 密碼、LDAP 使用者 ID/密碼 (需以手動提供 Pac 支援)	Windows 密碼****	數位認證
以 Windows 簽入單一登入	否	是	是	是	是
密碼有效期限與更改	否	是	是	否	--
與快速安全漫遊機制共用	否	否	是	是	否
與 WPA 及 WPA2 共用	是	是	是	是	是

* Cisco Compatible 第二版以上的用戶端支援 PEAP/GTC

** Meetinghouse 與 Funk 套件提供更多作業系統支援

*** Cisco Aironet 350 Series WLAN 用戶端設備與 Cisco Aironet 5 GHz 54 Mbps 無線網路用戶端轉接卡 (CB20A) 支援 Windows XP、Windows 2000 與 Windows CE 作業系統的 EAP-FAST

**** 需複雜密碼。詳閱：[Cisco Response to Dictionary Attacks on Cisco LEAP](#)

企業應用

問. Cisco LEAP 是否支援快速安全漫遊？

答. 是。Cisco Aironet Series 存取器和 Cisco 及 Cisco Compatible 用戶端設備皆支援快速安全漫遊。有了快速安全漫遊，經過驗證的用戶端設備即可安全地在不同存取器之間漫遊，免除重新連結的延遲時間。快速安全漫遊支援具延遲敏感性的應用程式，例如：無線 VoIP（Voice over IP）、ERP（Enterprise Resource Planning）或 Citrix 類型的解決方案。

問. Cisco LEAP 是否支援 WAN 連結遠端據點的受損存活功能？

答. 是。Cisco LEAP 支援 IEEE 802.1X 本端驗證服務，也稱之為遠端據點受損存活功能。這項功能是由存取器的 IEEE 802.1X 本端驗證服務所提供。有了 IEEE 802.1X 本端驗證服務，Cisco Aironet 存取器即可在驗證、授權與帳戶伺服器無法運作時，組態成為驗證無線用戶端的本端驗證伺服器。此舉可為未配備 RADIUS 伺服器的遠端或分支辦公室的 WLAN 提供安全的驗證服務，且在 WAN 連結或伺服器故障時，為本端資源的存取，例如：檔案伺服器或印表機，提供備用的驗證服務。

WLAN 安全性

問. 我如何取得更多部署安全 WLAN 的資訊？

答. 請詳閱下列文件以取得更多部署安全 WLAN 的資訊：

- [SAFE: Wireless LAN Security in Depth—Version 2](#)
- [Wireless LAN Security White Paper](#)
- [Cisco Aironet Technical Reference](#)

問. 我如何取得更多關於 WLAN 安全性的資訊？

答. 請詳閱 [Cisco Aironet WLAN Security](#) 手冊，以取得更多 WLAN 安全性的相關資訊。

問. 我如何取得更多針對 Cisco LEAP 的字典式攻擊（Dictionary Attacks）的資訊？

答. 請詳閱 [Cisco Response to Dictionary Attacks on Cisco LEAP](#) 產品佈告，以取得更多針對 Cisco LEAP 的字典式攻擊的資訊。

其他資訊

Cisco Wireless Security Suite 的更多資訊：

<http://www.cisco.com/go/aironet/security>

Cisco Wireless Security Suite手冊：

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html

Cisco Aironet產品的更多資訊：

<http://www.cisco.com/go/aironet>

Cisco Secure ACS的更多資訊：

<http://www.cisco.com/go/acs>

Cisco CNS Access Registrar的更多資訊：

<http://www.cisco.com/en/US/products/sw/netmgts/ps411/index.html>

EAP-FAST的更多資訊：

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

PEAP的更多資訊：

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aec801764fa.shtml

802.11i、WPA與WPA2的更多資訊：

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aec801e3e59.shtml