



Q&A

CISCO LEAP

This document answers questions about Cisco LEAP an Extensible Authentication Protocol type from Cisco Systems®.

OVERVIEW

Q. What is Cisco® LEAP?

A. Cisco LEAP is an 802.1X authentication type for wireless LANs (WLANs) that supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys.

Q. Is Cisco LEAP supported by Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)?

A. Yes. Like all EAP types, Cisco LEAP can be used with WPA and WPA2 networks.

Q. Is Cisco LEAP included with all Cisco wireless products, Cisco Aironet products, and Cisco Compatible client devices?

A. Yes. Cisco LEAP is included, at no additional cost, with all Cisco wireless products, Cisco Aironet products, and Cisco Compatible client devices including Cisco Aironet autonomous and lightweight access points and Cisco wireless LAN controllers.

Q. Is Cisco LEAP a standard?

A. Cisco LEAP takes advantage of the standard 802.1X framework. Cisco was the pioneer in introducing Extensible Authentication Protocol (EAP) support for WLANs at a time when none of the existing client operating systems provided EAP support. Cisco introduced Cisco LEAP in December 2000 as a way to quickly improve the overall security of WLAN authentication.

Q. Is Cisco LEAP supported by the Cisco Unified Wireless Network?

A. Yes. The [Cisco Unified Wireless Network](#) supports a variety of EAP authentication types, including Cisco LEAP.

Q. What is the Cisco Unified Wireless Network?

A. The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the WLAN security, deployment, management, and control issues facing enterprises. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The Cisco Unified Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Unified Wireless Network supports an enterprise-ready, standards-based, wireless security solution that gives network administrators' confidence that their data will remain private and secure when they use Cisco wireless products, Cisco Aironet Series products, Cisco Compatible Extensions products or Wi-Fi Certified WLAN client devices. This enterprise-class wireless security solution supports robust wireless LAN security services that closely parallel the security available in a wired LAN. It fulfills the need for consistent, reliable, and secure mobile networking by delivering industry-leading WLAN security services. It mitigates sophisticated passive and active WLAN attacks, interoperates with a range of client devices and provides reliable, scalable, centralized security management. The Cisco Unified Wireless Network allows network administrators to deploy large-scale enterprise WLANs with scalable problem-free security administration that does not increase the burden on the IT staff.

FEATURES AND BENEFITS

Q. What are the security benefits of Cisco LEAP?

A. Cisco LEAP overcomes the major limitations of 802.11 wireless security through extensible authentication support to other back-end directories (Windows NT, Windows Active Directory, and Open Database Connectivity [ODBC]) or to Cisco LEAP proxy RADIUS servers such as Cisco Secure Access Control Server (ACS) and Cisco Network Registrar®.

Q. What are the enterprise benefits of Cisco LEAP?

A. Cisco LEAP is a widely deployed, market-proven component of the Cisco Unified Wireless Network. It is available with numerous client adapter types, including application-specific devices (ASDs), from Cisco, Cisco Compatible Extensions partners, and numerous client device and network interface card (NIC) manufacturers. Cisco LEAP provides:

- True single login with an existing user name and password using Windows NT/2000 Active Directory
- Simplified, inexpensive deployment and administration for IT managers
- Reliable, scalable, centralized security management
- High-performance, upgradable enterprise-class security
- Dynamic privacy protection when used in conjunction with Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES)

DEPLOYMENT

Q. How does Cisco LEAP authentication work?

A. A wireless client needs to be authenticated by a RADIUS server, and can only transmit EAP traffic until it is authenticated. After end-user login, mutual authentication between the client and the RADIUS server occurs. A dynamic encryption key is derived during this mutual authentication at the client and the RADIUS server. The RADIUS server sends the dynamic encryption key to the access point via a secure channel. After the access point receives the key, regular network traffic forwarding is enabled at the access point for the authenticated client. The credentials used for authentication, such as a login password, are never transmitted over the wireless medium without encryption. Upon client logoff, the client association entry in the access point returns to the nonauthenticated mode.

Q. What client operating systems does Cisco LEAP support?

A. Cisco LEAP supports numerous client operating systems, including Microsoft Windows, Mac OS, Linux, DOS, and Windows CE.

Q. What RADIUS servers and user databases does Cisco LEAP support?

A. Cisco LEAP supports the following RADIUS servers and user databases: Cisco Secure ACS, Cisco Network Registrar, Funk Odyssey Server, Funk Steel-Belted, and products that use the Interlink Networks server code (such as LeapPoint appliances).

Q. What Cisco wireless devices does Cisco LEAP support?

A. Cisco LEAP supports several Cisco wireless products, including Cisco Aironet autonomous and lightweight access points, Cisco wireless LAN controllers, workgroup bridges, wireless bridges, and repeaters, and many Cisco and Cisco Compatible WLAN client devices.

Q. Is Cisco LEAP authentication available on wireless clients from vendors other than Cisco?

A. Yes. Cisco LEAP authentication is available for [Cisco Compatible Extensions](#) products.

Q. Where can I learn more about deploying Cisco LEAP?

A. Please read the [Deployment Guide: Configuring the Cisco Wireless Security Suite](#) to learn more about deploying Cisco LEAP.

EAP TYPE COMPARISONS

Q. What are the differences between [Protected EAP \(PEAP\)](#), [EAP-Flexible Authentication via Secure Tunneling \(EAP-FAST\)](#), Cisco LEAP, and EAP-Transport Layer Security (EAP-TLS)?

A. Table 1 provides a summary comparison of PEAP, EAP-FAST, Cisco LEAP, and EAP-TLS.

Table 1. PEAP, EAP-FAST, Cisco LEAP and EAP-TLS Comparison Chart

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
User Authentication Database and Server	One-time password (OTP), Lightweight Directory Access Protocol (LDAP), Novell NDS, Windows NT Domains, Active Directory	Windows NT Domains, Active Directory	Windows NT Domains, Active Directory, LDAP (limited)	Windows NT Domains, Active Directory	OTP, LDAP, Novell NDS, Windows NT Domains, Active Directory
Requires Server Certificates	Yes	Yes	No	No	Yes
Requires Client Certificates	No	No	No	No	Yes
Operating System Support	<i>Driver:</i> Windows XP, Windows 2000, Windows CE* <i>With third-party utility:</i> Other OS**	<i>Driver:</i> Windows XP, Windows 2000, Windows CE <i>With third-party utility:</i> Other OS**	<i>Driver:</i> Windows XP, Windows 2000, Windows CE*** <i>With third-party utility:</i> Other OS **	<i>Driver:</i> Windows 98, Windows 2000, Windows NT, Windows Me, Windows XP, Mac OS, Linux, Windows CE, DOS	<i>Driver:</i> Windows XP, Windows 2000, Windows CE <i>With third-party utility:</i> Other OS
ASD Support	No	No	Yes	Yes	No
Credentials Used	<i>Client:</i> Windows, NDS, LDAP password; OTP or token <i>Server:</i> Digital certificate	Windows password	Windows password, LDAP user ID/ password (manual provisioning required for Pac provisioning)	Windows password****	Digital certificate
Single Sign-On Using Windows Login	No	Yes	Yes	Yes	Yes
Password Expiration and Change	No	Yes	Yes	No	-

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
Works with Fast Secure Roaming	No	No	Yes	Yes	No
Works with WPA and WPA2	Yes	Yes	Yes	Yes	Yes

* PEAP/GTC is supported on Cisco Compatible Version 2 clients and above.

** Greater operating system coverage is available with Meetinghouse and Funk supplicants.

*** Cisco Aironet 350 Series WLAN client devices and Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapters (CB20A) support EAP-FAST on Windows XP, Windows 2000, and Windows CE operating systems.

**** Requires strong passwords. Read more at: [Cisco Response to Dictionary Attacks on Cisco LEAP](#)

ENTERPRISE APPLICATIONS

Q. Does Cisco LEAP support fast secure roaming?

A. Yes. Fast secure roaming is supported by Cisco Aironet Series access points in conjunction with Cisco and Cisco Compatible client devices. With fast secure roaming, authenticated client devices can roam securely from one access point to another without any perceptible delay during reassociation. Fast secure roaming supports latency-sensitive applications such as wireless voice over IP (VoIP), enterprise resource planning (ERP), or Citrix-based solutions.

Q. Does Cisco LEAP support WAN link remote site survivability?

A. Yes. Cisco LEAP supports IEEE 802.1X Local Authentication Service also called remote site survivability. This feature is enabled via a Cisco Aironet autonomous access point's IEEE 802.1X local authentication service. With IEEE 802.1X local authentication service, Cisco Aironet autonomous access points are configured to act as a local authentication server to authenticate wireless clients when the authentication, authorization, and accounting (AAA) server is not available. This provides secure authentication services for remote or branch-office WLANs without a RADIUS server and provides backup authentication services for access to local resources, such as file servers or printers, during a WAN link or server failure.

WLAN SECURITY

Q. Where can I learn more about deploying secure WLANs?

A. Please read the following documents to learn more about deploying secure WLANs:

- [Wireless LAN Security White Paper](#)
- [Cisco Aironet Technical References](#)

Q. Where can I learn more about WLAN security?

A. Please read the [Cisco Wireless LAN Security](#) brochure to learn more about WLAN security.

Q. Where can I read more about Dictionary Attacks on Cisco LEAP?

A. Please read the [Cisco Response to Dictionary Attacks on Cisco LEAP](#) product bulletin for more information about Dictionary Attacks on Cisco LEAP.

FOR MORE INFORMATION

For more information about Cisco wireless security, visit: <http://www.cisco.com/go/aironet/security>

For more information about the Cisco Unified Wireless Network, visit: <http://www.cisco.com/go/unifiedwireless>

For more information about Cisco Aironet products, visit: <http://www.cisco.com/go/aironet>

For more information about Cisco Secure ACS, visit: <http://www.cisco.com/go/acs>

For more information about Cisco CNS Access Registrar, visit: <http://www.cisco.com/en/US/products/sw/netmgts/ps411/index.html>

For more information about EAP-FAST, visit:

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

For more information about PEAP, visit: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801764fa.shtml

For more information about 802.11i, WPA and WPA2, visit:

http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801e3e59.shtml



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)