

White Paper

PROXIM AND WI-FI PROTECTED ACCESS (WPA)

What is WPA?

As an intermediate WLAN security solution that can be applied to existing WLAN client hardware, the Wi-Fi Alliance has adopted Wi-Fi Protected Access (WPA). Proxim will implement WPA on client and access point products and make this available in the middle of 2003.

WPA is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Wi-Fi Protected Access is derived from, and will be forward compatible with the upcoming IEEE 802.11i standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. The Wi-Fi Alliance plans to begin interoperability certification testing on Wi-Fi Protected Access products starting mid-2003.

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of WEP's known vulnerabilities.

Enterprise-level User Authentication via 802.1X and EAP

WEP (Wired Equivalent Privacy) is an encryption method and is not intended as user authentication mechanism. Wi-Fi Protected Access user authentication is implemented using 802.1X and the Extensible Authentication Protocol (EAP). Together, these technologies provide a framework for strong user authentication. This framework utilizes a central authentication server, which employs mutual authentication so that the wireless user does not accidentally join a rogue network.

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward compatible with the IEEE 802.11i security specification currently under development. Wi-Fi Protected Access is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1X and TKIP. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement.

Which Proxim WLAN products will support WPA?

Clients

To enable WPA on the ORiNOCO clients, a WPA driver as well as a WPA supplicant are required. Proxim will provide WPA drivers for the ORiNOCO clients listed below. Depending on your operating system, supplicants are available from Microsoft, Proxim, or from a third-party company such as Funk or Meetinghouse. See the chart below for details.

		WPA Driver and Supplicant Availability			
Product	Model Numbers	XP	2000	Me	98SE
ORiNOCO 11a/b/g ComboCard, Gold and Silver	8480-xx and 8481-xx	Available now from Proxim website	Available now from Proxim website Provided with Proxim WPA driver	Available Q104 Provided with Proxim WPA driver	Available Q104 Provided with Proxim WPA driver
ORiNOCO 11b/g PC Card, Gold and Silver	8470-xx and 8471-xx	Provided w/ XP (service pack 1)			
ORiNOCO 11a/b/g PCI Card	8482-xx	Also included with Proxim WPA driver			
ORiNOCO 11a/b ComboCard, Gold and Silver	8460-xx and 8461-xx				
ORiNOCO 802.11b PC Card, Gold and Silver	848 441 556 848 441 481 848 441 499 848 441 564 848 499 778 848 499 786	Not available ¹			
ORiNOCO Classic Gold PC Card	8410-xx				
ORiNOCO 11b Client PC Card, Gold and Silver	8420-xx, 8421-xx				

¹ For the strongest security, Proxim recommends migration to IEEE 802.11g client cards as the 802.11b only clients are not upgradeable to AES and IEEE 802.11i due to hardware limitations. Proxim ORiNOCO 802.11g and dual 802.11a/g client cards are upgradeable to AES and 802.11i when ratified.

Access Point

To enable WPA on ORiNOCO Access Points, the radio hardware must meet certain minimum requirements. Unfortunately, the AP-2000 configured with an ORiNOCO 802.11b PC card cannot support WPA. For customers using the AP-2000 with an ORiNOCO 802.11b PC Card, Proxim recommends that an AP-2000 11b/g Upgrade Kit be purchased to replace the ORiNOCO 802.11b PC Card. The AP-2000 11b/g Upgrade Kit allows existing 802.11b clients to be supported while the investment in the original 11b PC Card used in the AP-2000 is also maintained with re-use as a client.

The Access Point configurations that will support WPA are:

Access Point	Proxim Model Number
ORiNOCO AP-2000b/g	8857-xx ¹
ORiNOCO AP-2000 with the AP-2000 11b/g Kit	700 001 103 ² and 8800-xx
ORiNOCO AP-2000 AE with the AP-2000 11b/g Kit	700 001 114 and 8800-xx
ORiNOCO AP-600b/g	8657-xx
ORiNOCO AP-600b with the AP-600 11b/g Upgrade Kit or AP-600 11a/b/g Upgrade Kit	8655-xx with 8658-xx or 8660-xx upgrade, or 8657-xx
ORiNOCO AP-2000 with the AP-2000 11a Upgrade Kit	700 001 103 and 8856-xx
ORiNOCO AP-600a with the AP-600 11a/b/g Upgrade Kit	8656-xx with 8660-xx upgrade

¹Valid for all suffixes

²Order codes for the US power cord versions are reflected in this table

All above configurations require Release 2.3 (or higher) software which is available from the Proxim web site.

WPA Q&A

i What will happen when a WPA client tries to access a non-WPA AP?

A WPA client will not attempt to connect to a non-WPA AP.

When a client that is configured to operate only in WPA mode searches for an AP, it looks for APs with the Wi-Fi Protected Access (WPA) information element (IE) in its Beacon or Probe Responses. When it receives Beacons or Probe Responses without the WPA IE, the client knows that the corresponding AP does not support WPA and will not attempt to associate with this AP.

i What happens when a non-WPA client tries to connect to a WPA protected network and/or access point?

A WPA access point will deny connection attempts from a non-WPA client.

When a non-WPA client attempts to associate with an AP operating in WPA only mode, the client's Association Request frame will not include a WPA IE. The AP operating in WPA only mode recognizes that this client is a non-WPA client because of the lack of the WPA IE and denies the Association Request.

A Mixed mode (supporting WPA and non-WPA clients) would offer network security that is no better than that obtained with a non-WPA network, and thus this mode of operation is discouraged. The AP-2000 and AP-600 do not support this mode of operation on a single radio. However, in the two slot AP-2000, one card can be configured for WPA only mode and the other card can be configured for WEP or No Encryption to provide simultaneous support for WPA and non-WPA clients.

i How difficult is it for the average user to upgrade their ORiNOCO PC Card (or USB) to WPA?

Upgrading the ORiNOCO PC Card (or USB) to WPA is as simple as installing a new driver and loading a new software program. Both a WPA driver and a WPA supplicant for the card must be installed. The work required to install the WPA driver is similar to that associated with updating the driver for a video card or any other PC device. The procedure for this is to first obtain the WPA driver from the Proxim web site, uninstall the current Proxim ORiNOCO driver using the Windows driver maintenance tools, and then install the WPA driver.

A WPA capable supplicant must also be installed. However, in addition to being WPA capable, the supplicant must support the EAP Authentication Methods used by the networks that will be accessed. Typical EAP Methods include EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, and EAP-AKA. Your network administrator can tell you which EAP method is used by each network. Installing a supplicant is similar to installing other Windows programs. For Windows XP and later operating systems, Microsoft plans to provide WPA supplicants that support EAP-PEAP. For Windows XP, it is available as part of a Service Pack. For earlier Windows operating systems, the user will have to obtain a WPA capable supplicant from either Funk or Meetinghouse and install it.

i Can ALL ORiNOCO PC cards be upgraded?

All ORiNOCO PC cards can be upgraded to support WPA except the ORiNOCO 802.11a CardBus Card, (8454-xx), the ORiNOCO 802.11a PCI Card, (8151-xx), the ORiNOCO Classic PC Card (8410-xx) and the ORiNOCO Gold and Silver 802.11b PC Cards (8420-xx, 8421-xx, 848 441 556, 848 441 481, 848 441 499, 848 441 564, 848 499 778, 848 499 786). RangeLAN-DS and Harmony client cards cannot be upgraded. A list of all ORiNOCO clients that can be upgraded follows:

Product	Proxim Model Numbers
ORiNOCO 11a/b/g ComboCard, Gold and Silver	8480-xx ¹ and 8481-xx
ORiNOCO 11b/g PC Card, Gold and Silver	8470-xx and 8471-xx
ORiNOCO 11a/b/g PCI Card	8482-xx
ORiNOCO 11a/b ComboCard, Gold and Silver	8460-xx and 8461-xx

¹Valid for all suffixes

(i) My laptop contains an embedded 802.11b radio. How do I upgrade it to support WPA?

Contact your laptop manufacturer for instructions on how to upgrade the embedded radio and driver to enable WPA.

(i) Which ORiNOCO Access Points can be upgraded to support WPA?

ORiNOCO AP-2000 and AP-600 Access Points can be upgraded to support WPA. Other ORiNOCO Access Points and Gateways cannot be upgraded. A list of all ORiNOCO Access Points that can be upgraded follows:

Access Point	Proxim Model Number
ORiNOCO AP-2000b/g	8857-xx ¹
ORiNOCO AP-2000 with the AP-2000 11b/g Kit	700 001 103 ² and 8800-xx
ORiNOCO AP-2000 AE with the AP-2000 11b/g Kit	700 001 114 and 8800-xx
ORiNOCO AP-600b/g	8657-xx
ORiNOCO AP-600b with the AP-600 11b/g and the 11a/b/g Upgrade Kit	8655-xx with 8658-xx upgrade, or 8657-xx
ORiNOCO AP-2000 with the AP-2000 11a Kit	700 001 103 and 8856-xx
ORiNOCO AP-600a with the AP-600 11a/b/g Upgrade Kit	8656-xx with 8660-xx upgrade, or 8659-xx

¹Valid for all suffixes

²Order codes for the US power cord versions are reflected in this table

i How do I upgrade my ORiNOCO access point network to WPA?

Four steps are required to upgrade an ORiNOCO AP-2000 or AP-600 access point network to support WPA. The four steps are:

1. **Select an EAP Method.** Proxim recommends using EAP-PEAP. It is username/password based, and a supplicant supporting it is provided in Windows XP Service Pack 1 and in future Microsoft Operating Systems.
2. **Obtain and install a WPA capable RADIUS server that supports the selected EAP Method.** Several companies including Funk Software and Microsoft provide RADIUS servers that support multiple EAP types. Both Funk Software and Microsoft's Windows Server 2003 Operating System with included RADIUS server support EAP-PEAP. Configure the usernames and passwords in the RADIUS server. Also configure the RADIUS Shared Secret.
3. **Obtain and install an ORiNOCO WPA enabled radio for the AP-2000 or AP-600.** See the table above to check whether your AP configuration needs a new WPA enabled radio. The newest APs ship with a WPA enabled radio included.
4. **Obtain and install the WPA software for the AP-2000 or AP-600.** Release 2.3 or later supports WPA for the AP-2000 and AP-600 and can be downloaded from the Proxim web site. Configure the IP Address and the Shared Secret for the RADIUS server in the AP-2000 or AP-600 access point.

i Can I easily switch back and forth between WPA and non-WPA operation when moving between different locations?

Yes, you can switch easily between WPA and non-WPA operation using ORiNOCO clients. Both ORiNOCO client utility software and Windows XP include the ability to set up multiple profiles allowing the user to switch settings easily as they move between locations. As an example, the office profile could include WPA for authentication and TKIP for encryption, while for a hot spot at the airport, the profile could include *Open* for authentication and *None* for encryption.