

SUMMIT WI-FI RADIOS AND JUNIPER NETWORKS ODYSSEY ACCESS CLIENT FIPS EDITION

Bringing WPA2-Based FIPS 140-2 to Windows CE and Windows Mobile

Challenge

For mobile computers and other business-critical mobile devices that run Windows CE or Windows Mobile, many federal government installations need a Wi-Fi solution that supports WPA2-based FIPS 140-2 security.

Solution

Thanks to an interface between Summit Wi-Fi radios and Juniper Networks Odyssey Access Client FIPS Edition, mobile devices that run Windows CE or Windows Mobile can support WPA2-based FIPS 140-2 security.

Benefits

By running Juniper Networks OAC FE with Summit Wi-Fi radios, your Wi-Fi devices:

- Use security that is compliant with WPA2 and FIPS 140-2
- Use EAP authentication to gain Wi-Fi network access
- Encrypt all transmitted data using a FIPS-certified cryptographic module

Mobile users at many federal government installations want to use wireless LAN, or Wi-Fi, technology to maintain network connections even while they move about a facility. Every Wi-Fi network connection must be secure, and the ideal security solution is one that is compliant with both the Wi-Fi industry standard of Wi-Fi Protected Access 2 (WPA2) and the Federal Information Processing Standard of FIPS 140-2. Until recently, however, the only client devices that supported a WPA2-based FIPS 140-2 security solution were those that ran the Windows XP operating system.

The Challenge

To protect data that is transmitted over the air, Wi-Fi devices use encryption to scramble the data. WPA2 requires the use of an encryption algorithm called AES-CCMP. That same algorithm is sufficient for FIPS 140-2. Most of today's Wi-Fi client devices provide hardware support for AES-CCMP, but FIPS 140-2 requires that AES-CCMP be implemented in software.

The Juniper Networks® Odyssey Access Client FIPS Edition, includes a FIPS-certified cryptographic module that implements AES-CCMP in software. By supporting WPA2 authentication methods as well as the WPA2 encryption algorithm, Juniper Networks OAC FIPS Edition enables a Wi-Fi client device to be fully compliant with both WPA2 and FIPS 140-2.

Because OAC FIPS Edition runs on many of today's popular laptop models, those laptops can be used with a Wi-Fi network that requires WPA2-based FIPS 140-2 security. Most laptops run Windows XP, but other popular mobile devices, such as mobile computers, run Windows CE or Windows Mobile. Now, thanks to a partnership between Juniper Networks and Summit Data Communications, many Windows CE and Windows Mobile devices support WPA2-based FIPS 140-2 security.

The Juniper Networks and Summit Data Communications Solution

Summit provides Wi-Fi radio modules and cards. Thanks to an interface to Juniper Networks OAC FIPS Edition, Summit radios support WPA2-based FIPS 140-2 security on Windows CE and Windows Mobile, the most popular operating systems for mobile computers and other business-critical mobile devices.



Features and Benefits

By running the Juniper Networks OAC FIPS Edition on client devices that use Summit Wi-Fi radios, an organization can implement a wireless LAN security solution that:

- Is compliant with WPA2 and FIPS 140-2
- Uses WPA2 authentication methods, such as Extensible Authentication Protocol (EAP) types, to ensure that only authorized devices gain access to the wireless LAN
- Ensures that all data is encrypted using an algorithm that is compliant with WPA2 and FIPS 140-2
- Is available on devices that run Windows XP, Windows CE, or Windows Mobile

Solution Components

To implement the solution, you need:

- Any wireless LAN infrastructure that supports WPA2
- Client devices that use Wi-Fi radios from Summit Data Communications and run OAC FIPS Edition with V2.01 or above of Summit software

Summary: The Industry's Only WPA2-Based FIPS 140-2 Solution

Only Juniper Networks and Summit Data Communications enable client devices that run Windows CE or Windows Mobile to participate in a wireless LAN that requires WPA2-based FIPS 140-2 security. Without the joint solution from Juniper Networks and Summit, an installation that requires FIPS 140-2 with devices that run Windows CE or Windows Mobile must abandon WPA2, the Wi-Fi industry standard for security.

Next Steps

To learn more about the solution that Juniper Networks and Summit provide, contact your Juniper Networks representative for more information.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.