Juniper Networks **Odyssey**® **Access Client**

As more users access network resources, the need to provide robust authentication, and to use that information to facilitate access control, has become a mission-critical issue in today's enterprise. This is particularly true in the case of wireless LAN (WLAN) deployments, where security concerns include both authentication and encryption.

The IEEE 802.1X security standard offers an effective framework for authentication and Layer 2 access control to a protected wired or wireless network, as well as a means to add additional security to WLAN deployments.

One Client for Complete 802.1X Protection of Wired and Wireless Networks

Juniper Network's Odyssey Access Client is enterprise-class 802.1X access client software with full support for advanced WLAN security protocols that you require for wireless access to your LAN. Together with an 802.1X-compatible RADIUS server such as Juniper Networks' Odyssey Access Server or Steel-Belted Radius®, OAC secures the authentication and connection of WLAN users, ensuring that only authorized users can connect, that login credentials will not be compromised, and that data privacy will be maintained over the wireless link. OAC is also an ideal client for enterprises that are deploying identity-based (wired 802.1X) networking. OAC fully supports wired 802.1X connections, and saves time and effort by permitting one-time deployment of wireless and wired 802.1X access. The use of a single interface for both functions also simplifies user experience and reduces costs associated with user training.

Value Proposition

Enterprise-Level Security

- Best-in-class wireless LAN security
- Multi-platform, multi-vendor compatibility
- Provides authentication and access control for wired and wireless deployments
- Supports a wide variety of Extensible Authentication Protocol (EAP) types
- Unique features enable enforcement of network security policies
- Specialized FIPS Edition is 140-2 Level 1 validated

Low Total Cost of Ownership

- Auto configuration tools and client update capabilities simplify deployment
- Intuitive operation and usability features ease end user experience for lower support, training, and helpdesk costs
- Sophisticated network logon capabilities

Enterprise-Level Security

Juniper Networks OAC runs on a wide variety of Windows desktop and handheld platforms, and supports all popular WLAN security (EAP) authentication types, for complete security that is easy to deploy.

Features	Benefits
Enterprise-class wireless security	· Work securely across a wireless link · Protect enterprise data and credentials from attack · Gain control over how wireless users access the network
Compatible with popular wired and wireless platforms, including: · Windows XP · 2000 · 98 · Me · Windows Mobile 2003 for Pocket PC · Pocket PC 2002	Ensures security across a wide variety of different platforms, with no changes needed to client software
Supports a wide variety of EAP types, including: · EAP-TTLS · EAP-PEAP · EAP-TLS · EAP-FAST and LEAP, EAP-SIM, and EAP-MD5 Supports advanced encryption protocols, including Wi-Fi Protected Access (WPA) and WPA2	Enables all the benefits of EAP, including: · Credential security, using Transport Layer Security (TLS) for cryptography · Data privacy · The strongest over-the-air encryption of wireless data across all platforms
Market leading policy enforcement features including: · Client lockdown - prohibits a user from editing some or all of his WLAN or wired 802.1X connection settings. · Interface with standards-based endpoint integrity checks before access is allowed	Ensures compliance with enterprise security policies
Specialized FIPS-compliant edition, with features like: · Unique Juniper Odyssey Security Component cryptographic module that has been FIPS 140-2 Level 1 Validated (see FIPS 140-2 Certificate #569) · Conforms to FIPS guidelines, using EAP-TLS authentication 802.11i (WPA2) key derivation, and AES-CCMP data encryption · Support for the xSec protocol, with 3DES encryption · Support for FIPS mode enforcement using client lockdown features	Enables government agencies to deploy secure, scalable WLAN access

Low Total Cost of Ownership

OAC is easily deployed and maintained across all your client devices, enabling you to rapidly deploy secure WLAN and wired 802.1X access to all your users – saving time on both on the initial deployment and on any subsequent configuration updates you need to distribute.

Features	Benefits
Simplified configuration and distribution features, including · Auto configuration tools · Client update capabilities	Initial configuration and subsequent changes to network and security settings, as well as changes to network security policies are easily handled
Ease the end user experience with: · No user interaction required · Autoscan lists for most platforms, allow the end user to associate with any listed network – can automatically connect to the network with the highest priority/ strongest signal · End users can move seamlessly between different networks · Automatic association to the correct network, even if location and security requirements change · Move seamlessly between networks, for example, home, office, hotspot	Dramatic savings in training, helpdesk and support costs
Support for advanced network logon capabilities, including · GINA module · Machine connections · Simplified connection from new wireless-only devices · Automatic login scripts ease use by a single device by multiple users, as well as enable easy background access by network managers · Supports Windows login client and Novell Client for Windows	Significantly improve network connection and administration processes
Works with wired or wireless networks · Compatible with any 802.1X-compatible RADIUS server · Supports multiple adapter cards simultaneously	· Simplifies deployment of client software · Simplifies deployment in existing network infrastructure

Technical Specifications

OAC is available in different editions, tailored to meet the needs of organizations deploying 802.1X-based network access.

Features	Function	Suitable for
OAC	Secure, easily deployed 802.1X supplicant	OAC is suitable for enterprise networks
OAC/FIPS Edition	Extends functionality of OAC to include a cryptographic module that has been FIPS 140-2 Level 1 Validated	OAC FE is suitable for government organizations who wish to deploy WLAN access based on the open 802.1X and 802.11i security standards

OAC System Requirements

- OAC runs on Windows XP, 2000, 98, Me, Windows Mobile 2003, and Pocket PC 2002
- OAC FE runs on Windows XP, 2000

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
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

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501