ODYSSEY ACCESS CLIENT FIPS EDITION

Service Overview

The need today is greater than ever to ensure that systems are securely configured. Government agencies and secure enterprises must provide reliable, secure, and timely network access to employees and contractors while protecting sensitive information and resources. Many government agencies and ministries are also required to procure only IT offerings certified compliant with rigorous, government-set standards while at the same time under mandate to cut costs, driving them in many cases to use commercial off-the-shelf (COTS) products.

Juniper Networks is uniquely positioned to deliver on these needs with proven commercially available security solutions that provide the most flexible, secure network access available among federal government certified solutions.

One Client for Complete, Government-Approved Wired and Wireless Network Protection

Juniper Networks® Odyssey Access Client (OAC) is an enterprise-class 802.1X access client software that delivers comprehensive support for the advanced protocols required for secure network access. Together with an 802.1X-compatible RADIUS server such as Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers, OAC secures the authentication and connection of network users, ensuring only authorized users are able to connect, that user login credentials are not compromised, and that data privacy is maintained.

FIPS-Compliance with the Power of Odyssey Access Client

Juniper provides a version of OAC that meets the most stringent IT and communications requirements set forth by the U.S. federal government, while maintaining OAC's unparalleled feature set. Juniper Networks Odyssey Access Client FIPS Edition (OAC FIPS Edition) incorporates a FIPS 140-2 Level 1 certified cryptographic module and offers the advanced management features required by government and secure enterprise organizations with multiple facilities and deployments.

Value Proposition

Enterprise-Level, Government-Certified Security

- Best-in-class, FIPS 140-2 Level 1 validated cryptography (Validated by the National Institute of Standards and Technology (NIST) and the Canada Communications Security Establishment (CSE))
- Powerful, government-approved cryptography in a COTS product
- Supports the latest security protocols and standards
- Ensures credentials and data stay secure over a wireless link

Low Total Cost of Ownership (TCO)

- Decreases operational costs and increases return on investment by simplifying user and administrative controls
- Delivers auto-configuration tools and processes that ease deployment, distribution, and provisioning
- Lowers training and support costs through consistent user interface, intuitive operation, and powerful diagnostic tools
- A single interface for authentication and access control in wired and wireless deployments
- Multi-platform, multi-vendor compatibility

Enhanced Control

- Enables pre-defined or automated preferred and priority connection capabilities
- Offers support for sophisticated network logon schemes
- Client lockdown permits enforcement of security policies

Certified Support for Government Protocols

Juniper Networks Odyssey Access Client FIPS Edition incorporates the Odyssey Security Component, a cryptographic module that is Federal Information Processing Standard (FIPS) 140-2 Level 1 validated by both the NIST and the CSE, Canada's national cryptologic agency. OAC FIPS Edition was developed specifically to conform to government Information Assurance (IA) requirements.

OAC FIPS Edition is compatible with U.S. Department of Defense (DoD) Common Access Card (CAC) standards and certificates.

Also, OAC FIPS Edition has recently been evaluated and certified for conformance to the Common Criteria (ISO/IEC 15408), the international security standard. The claims being validated include the U.S. Government Protection Profile for Wireless LAN Clients for Basic Robustness Environments. OAC FIPS Edition has been awarded an assurance level of EAL 3 Augmented ALC_FLR.2. Please contact Juniper Networks for the version number of the evaluated client.

OAC FIPS Edition provides 802.11i and TLS-based 802.1X methods that use FIPS-certified cryptography. Please note that using the 802.11i protocol in FIPS mode requires a modified driver for the wireless adapter. Please contact your Juniper Networks sales representative for the latest list of available drivers.

OAC FIPS Edition also supports the xSec protocol, a slight variation on 802.11i that can run in FIPS mode on any existing wireless adapter driver. As with 802.11i, all cryptographic operations in xSec are performed using the Odyssey Security Component cryptographic module. xSec also uses longer Advanced Encryption Standard (AES) keys than 802.11i and encrypts Layer 2 header information that is not encrypted in 802.11i.

Table 1: Support for U.S. Government Standards

FEATURES	BENEFITS
FIPS-certified cryptography • Uses Juniper Networks Odyssey Security Component cryptographic module FIPS 140-2 Level 1, Certificate #569 • Conforms to NIST and DoD guidelines for the use of 802.11i and TLS-based EAP methods • Supports the xSec protocol, with 256-bit AES and Layer 2 header encryption	Enables government agencies to deploy secure, scalable wireless or wired network access
Recently completed evaluation and certification for conformance to the Common Criteria (ISO/IEC 15408) (Please contact Juniper Networks for the evaluation status and the version number of the evaluated client)	Adheres to government and international standards when deploying robust, safe wireless and/or wired network access
Ensures FIPS mode enforcement • Client lockdown features prohibit users from editing some or all 802.1X connection settings • Can be installed as a background task without user interaction • With Client Stealth Mode, can be made transparent to users (if desired) by hiding icons and splash screen	Ensures and maintains compliance with agency security policies

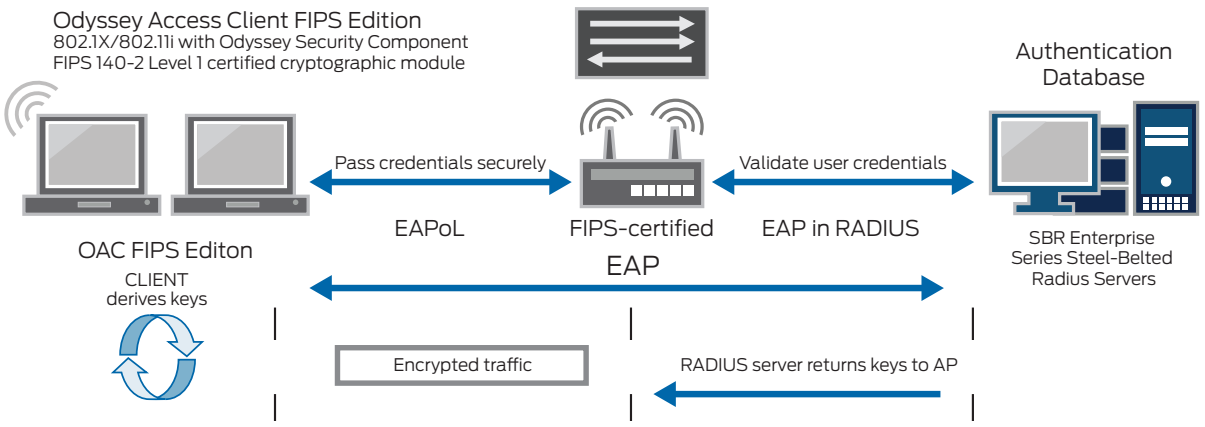

Figure 1: OAC FIPS Edition protects network credentials and transmitted data from breach with government certified encryption, delivering secure network access.

Industry Tested, Government-Certified

Odyssey Access Client FIPS Edition's combination of standards-based, enterprise-driven features and strict, federally-regulated and certified cryptography delivers a government-approved wireless and wired 802.1X/802.11i client with strong security.

Easily implemented and maintained across client devices, OAC FIPS Edition enables the rapid deployment of secure, FIPS-certified 802.1X network access to users – saving time at initial installation and in the distribution of updates.

Table 2: Features and Benefits of OAC FIPS Edition

FEATURES	BENEFITS
Enterprise-class security	· Controls how users access the network · Works securely across wired or wireless connections · Protects government and secure enterprise credentials and data from attack, hack, or theft
Supports heterogeneous hardware environments, including laptops, desktops, and other wired and wireless devices	Enjoy the same level of support with consistent user interfaces, terminology, and operation independent of device and network environment
Simple, quick configuration and distribution · Auto-configuration tools · Client deployment and update capabilities with automated distribution via common enterprise deployment tools · Command line export to script, preserving network configurations across installs and uninstalls · Silent installation	Initial configuration, subsequent changes to network and security settings, and changes to network security policies are easily made and deployed, without the need to touch each device
Enhanced user experience · Automatic association to the correct network even if location and security requirements change · Auto-scan lists allow the user to associate with any listed network; can automatically connect to the network with the highest priority · Users can move seamlessly between different networks · No user interaction required	Dramatic savings in training, administrative, maintenance, and support costs
Emphasizes network security and client usability · Automatically disables wireless interface when a wired connection is available, if configured · Define specific networks to which the user may connect, pre-empting other networks or auto-scan lists selected · Enables the configuration of priority networks with which to be associated when in range · Can be configured to prompt the user for a user name and password, which is very useful for shared devices	Increased security controls assure network security and administrator peace-of-mind
Support for advanced network logon schemes · Supports Windows GINA and Novell Client for Windows · GINA module – Allows the use of logon scripts, making it easy to use a single device for multiple users – Also enables network administrators to access resources on a device to perform maintenance · Machine connections – Allows startup scripts to be run – Facilitates off hours system maintenance, such as Systems Management Server (SMS) pushes	Significantly enhances network connection and administration processes
Works with wired or wireless networks, and is compatible with RADIUS servers that support 802.1X	Simplifies deployment of client software in a new or existing network infrastructure, enabling deployment of a single 802.1X client to work in wired, wireless, and mixed networks

OAC FIPS Edition and Unified Access Control

The latest versions of OAC FIPS Edition are also compatible and interoperate with Juniper's dynamic, comprehensive, standards-based network access control (NAC) solution, Unified Access Control (UAC). The OAC FIPS Edition can interface to and interact with UAC, serving as the UAC Agent, including with FIPS mode enabled. The Odyssey Security Component, the cryptographic module that is FIPS validated, operates with UAC to provide a FIPS-certified cryptologic module for network access control.

OAC FIPS Edition also provides xSec support for the UAC Agent's Microsoft Windows Vista edition, delivering robust, government-approved encryption, via the Advanced Encryption Standard (AES) for in-transit data when operating over Microsoft Windows Vista and with 802.11 adapters and drivers.

System Requirements

Odyssey Access Client FIPS Edition supports the:

- Microsoft Windows 2000, Windows Vista, and Windows XP operating systems.
- Microsoft Windows Mobile 6, Windows Mobile 5, Windows Mobile 2003 (Second Edition) for Pocket PC, Windows 2003 for Pocket PC, and Windows CE 5.0 software.

For more information on platforms supported by OAC, please contact your Juniper Networks sales representative or authorized reseller.

Juniper supplies modified drivers for Windows 2000 and Windows XP. For a current list of drivers supported for all operating systems please contact your Juniper Networks sales representative or authorized reseller.

Note: OAC FIPS Edition requires a modified driver to enable the wireless adapter to run 802.11i in FIPS mode.

Note: No special adapter or driver requirements are needed to run xSec in FIPS mode.

For more information and a 30-day FREE trial of Odyssey Access Client FIPS Edition, please go to: **www.juniper.net/us/en/products-services/software/ipc/odyssey-access-client/odyssey-clients-fips/**.

Juniper Networks Service and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains and faster rollouts of new business models and ventures. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services/.**

Ordering Information

To purchase Juniper Networks Odyssey Access Client (OAC), please contact your Juniper Networks sales representative at 1-866-298-6428 or your Juniper Networks authorized reseller.

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.

1000185-002-EN Feb 2010

Printed on recycled paper