

Juniper Networks Odyssey® Access Client FIPS Edition

Datasheet

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 provides comprehensive support for the advanced protocols required for secure network access. Together with an 802.1X-compatible RADIUS server such as Juniper Networks' Steel-Belted Radius®, 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 offers a version of OAC that meets stringent IT and communications requirements as set forth by the federal government, while maintaining OAC's unparalleled feature set. Odyssey® Access Client FIPS Edition (FE) implements FIPS 140-2 Level 1 certified cryptography and offers the advanced management features required by government organizations with multiple facilities and deployments.

Value Proposition

Enterprise-Level, Government-Certified Security

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



FIPS Certified

The need today is greater than ever to ensure that government systems are securely configured. Government agencies must provide reliable, secure, and timely network access to employees and contractors while protecting sensitive information and resources. They are also required to only procure IT offerings certified compliant with rigorous, government set standards while 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.



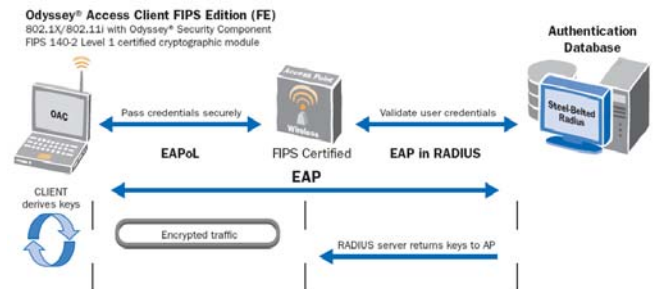
Juniper Networks Odyssey® Access Client FIPS Edition

Certified Support for Government Protocols

Juniper's Odyssey® Access Client (OAC) FE 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 FE is compatible with U.S. Department of Defense (DoD) Common Access Card (CAC) standards and certificates. Also, Odyssey Access Client FE has recently been accepted into evaluation for conformance to the Common Criteria (ISO/IEC 15408), the international security standard. The claims being validated include the US Government Protection Profile for Wireless LAN Clients. Please contact Juniper Networks for the evaluation status and the version number of the evaluated client.

OAC FE 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.



OAC FE 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.

LTI DataComm
23020 Eaglewood Ct. #100
Sterling, VA 20166
www.ltidata.com
800-677-5050

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Copyright LTI DataComm, 2009. All rights reserved.

Features	Benefits
Enterprise-class security	<ul style="list-style-type: none"> Controls how users access the network Works securely across either wireless link or wired connection Protects government data and credentials from attack
FIPS-certified cryptography <ul style="list-style-type: none"> 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 accepted into evaluation for conformance to the Common Criteria (ISO/IEC 15408)	Enables adherence to government and international standards when deploying robust, safe wireless and/or wired network access.
Ensures FIPS mode enforcement	<ul style="list-style-type: none"> Ensures and maintains compliance with agency security policies 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
Support for multiple and mixed 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