

Juniper Networks Odyssey® Access Client FIPS Edition

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.

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 large government organizations with multiple facilities and deployments.

Value Proposition

Enterprise-Level, Government-Certified Security

- Best-in-class, FIPS 140-2 Level 1 validated (by NIST and 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

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 National Institute for Standards and Technology (NIST) and the Canada Communications Security Establishment (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.

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. Please contact your Juniper sales representative for the latest list of available drivers.

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.

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"> • Uses Juniper 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
Ensures FIPS mode enforcement <ul style="list-style-type: none"> • 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
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

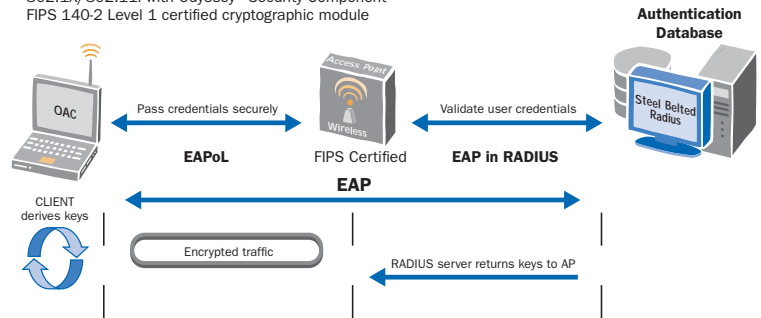
Industry Tested, Government-Certified

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

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

Features	Benefits
<ul style="list-style-type: none"> Simple and 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 	<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Dramatic savings in training, administrative, maintenance, and support costs
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Increased security controls assure network security and administrator peace-of-mind
<ul style="list-style-type: none"> Support for advanced network logon schemes • Supports Windows GINA and Novell Client for Windows • GINA module <ul style="list-style-type: none"> – 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 <ul style="list-style-type: none"> – Allows startup scripts to be run 	<ul style="list-style-type: none"> Significant improvement in network connection and administration processes
<ul style="list-style-type: none"> Works with wired or wireless networks, and is compatible with RADIUS servers that support 802.1X 	<ul style="list-style-type: none"> Simplifies deployment of client software in a new or existing network infrastructure

Odyssey® Access Client FIPS Edition (FE)
802.1X/802.11i with Odyssey® Security Component
FIPS 140-2 Level 1 certified cryptographic module



System Requirements

Odyssey® Access Client FIPS Edition supports Windows 2000 and Windows XP.

OAC FE requires a modified driver to enable the wireless adapter to run 802.11i in FIPS mode. Juniper Networks is in the process of verifying compatibility with a number of wireless adapters. Please contact Juniper Networks for the latest list of verified wireless adapters.

Please note that there are no special adapter or driver requirements needed to run xSec in FIPS mode.

For More Information and a 30-day FREE trial of Odyssey® Access Client, please go to: <http://www.juniper.net/products/aaa/odyssey/>



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, 25/F
ICBC 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
Building 1
Aviator Park
Station Road
Aldrestone
Surrey, KT15 2PG, U.K.
Phone: 44(0)1372-385500
Fax: 44(0)1372-385501

Copyright 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.