ODYSSEY ACCESS CLIENT

Product Overview

As the demand to enable users to work from anywhere, at anytime increases, so does the need for secure network accessibility and robust authentication. Mobility drives the need to harness user and device data to control network access and to ensure secure, appropriate network connectivity. Juniper Networks Odyssey Access Client 802.1X access clients/supplicants ensure the privacy and integrity of user credentials and network data through their robust authentication and data security. OAC is quickly deployed and can be managed enterprise-wide for the lowest TCO. OAC seamlessly integrates with Juniper's standards-based network access control (NAC) solution, Unified Access Control to supply dynamic, comprehensive access control. OAC delivers total control over secure, safe, and appropriate enterprise network connectivity, regardless of access method, allowing the consistent enforcement of organizational security policies for all users.

Product Description

Juniper Networks® Odyssey Access Client is a family of standards-based, enterprise-class 802.1X clients or supplicants built explicitly for use by enterprises and government agencies. OAC delivers comprehensive support for the advanced protocols required for secure network access. It provides robust security for both wired and wireless networks, fully ensuring the safety and integrity of user credentials and transmitted data. OAC secures user authentication and network connectivity, ensuring that users connect to the appropriate network in the appropriate manner, that login credentials are not compromised, and that user and device credentials and transmitted data remain secure and private.

Deploying and managing OAC enterprise-wide is quick and easy, lowering total cost of ownership (TCO). One OAC client can be deployed and used for both wired and wireless 802.1X access, enabling unified enforcement of corporate security policies, and saving administration and provisioning time, effort, and cost. Through its common user interface for both wired and wireless access, OAC delivers a simplified user experience that reduces training and support costs, allowing organizations to standardize on a single network access client across their business, regardless of network connection.

OAC also provides localized versions, with translated user interface and documentation. OAC secures authentication and connectivity for all users, regardless of network connection type, and delivers port-based security and enforcement of network access policies.

Industry Tested, Government-Certified

A specialized edition of OAC is also available that incorporates the Odyssey Security Component, a cryptographic module that has been Federal Information Processing Standards (FIPS) 140-2 Level 1 validated by the National Institute of Standards and Technology (NIST) and the Canada Communications Security Establishment (CSE). Juniper Networks Odyssey Access Client FIPS Edition provides the advanced management features of OAC demanded by large, worldwide public and private sector organizations with multiple facilities and deployments. Odyssey Access Client FIPS Edition conforms to NIST and U.S. Department of Defense (DoD) guidelines for the use of 802.11i and TLS-based EAP methods. OAC FIPS Edition has 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 is also compatible with the U.S. DoD's Common Access Card (CAC) standard. OAC FIPS Edition supports the xSec protocol, which uses 256-bit Advanced Encryption Standard (AES) and Layer 2 header encryption. All client-side cryptographic xSec operations are performed using the Odyssey Security Component cryptographic module.

Architecture and Key Components

When Odyssey Access Client is combined with Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers—the de facto standard in AAA/RADIUS servers—they deliver a complete, seamless, standards-based network security solution that is IEEE 802.1X compatible. OAC and the SBR Enterprise Series combine to ensure that only authorized users access the network; that user connections are configured correctly; and that transmitted credentials and data remain secure. Together, OAC and the SBR Enterprise Series deliver powerful network access policy management, robust user authentication, and durable network security with unparalleled network control, usability, and speedy deployment in standards-based, 802.1X-compliant environments.

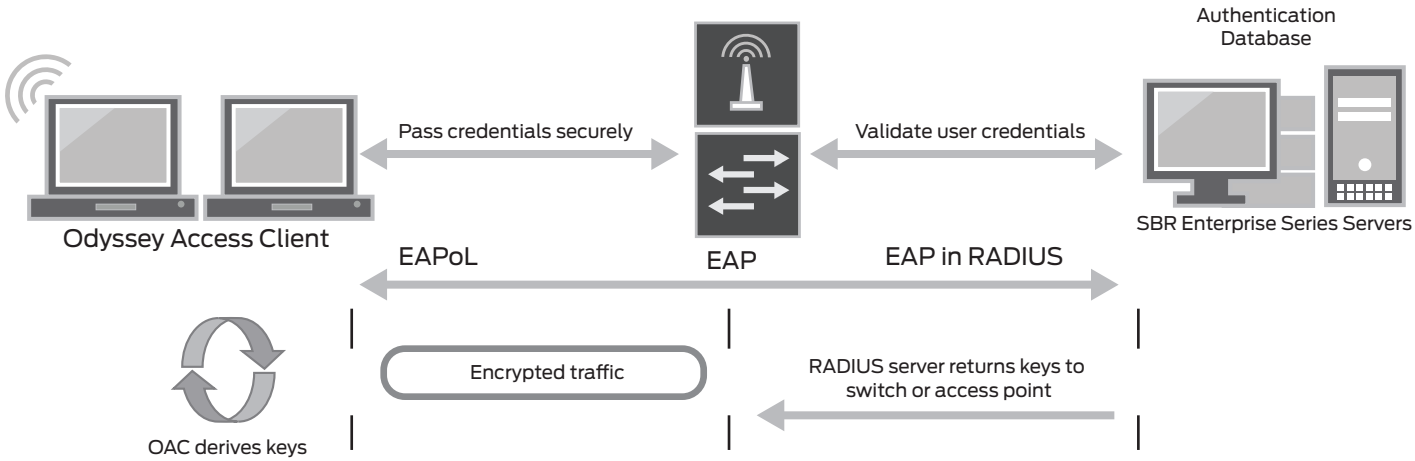

Figure 1: Odyssey Access Client in an 802.1X network environment

OAC and Unified Access Control

OAC is also compatible and seamlessly integrates with Juniper Networks Unified Access Control, Juniper's standards-based, comprehensive network access control (NAC) solution that dynamically combines user identity, device security state, and location information to define session-specific access policy by user. (Please note that only the latest versions of OAC for Microsoft® Windows® are compatible and integrate with UAC.)

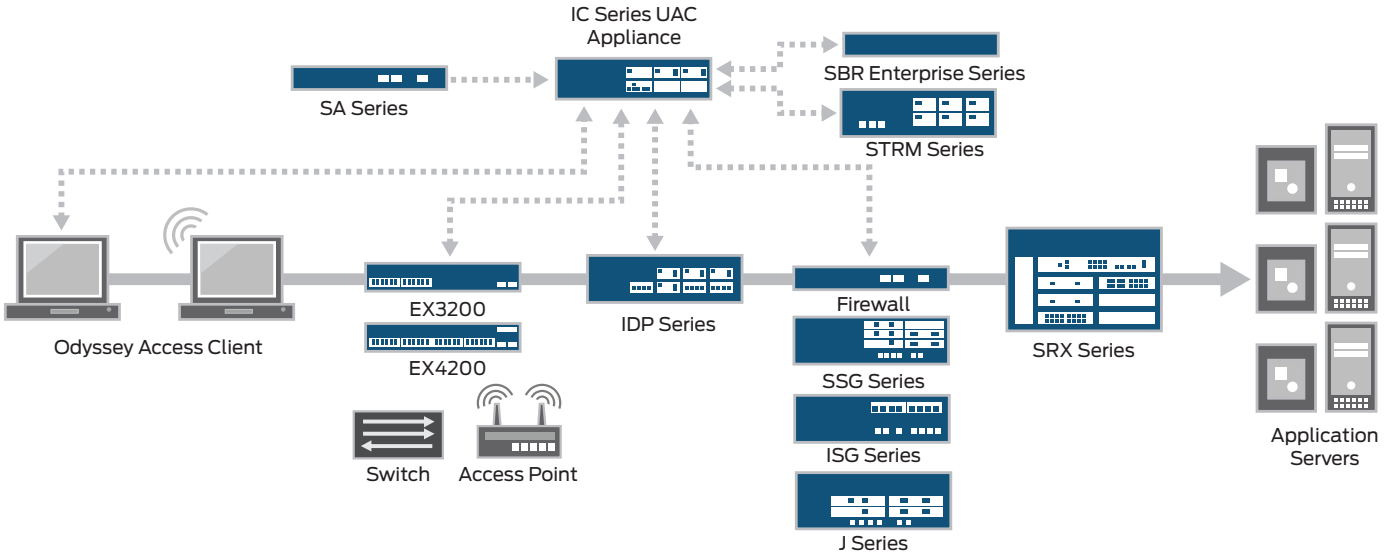

Figure 2: Odyssey Access Client can serve as the agent for UAC, working with existing and new network components to deliver comprehensive network and application access control

Features and Benefits

Enterprise-Level Security

Juniper Networks Odyssey Access Client family of products includes editions which run on a wide variety of Windows, Windows Mobile, Mac OS, and Linux platforms.

Table 1: Enterprise-Level Security

FEATURE	FEATURE DESCRIPTION	BENEFITS
Popular wired and wireless cross-platform compatibility	Editions of OAC are available that are compatible with the following operating systems: • Microsoft® Windows® XP, Windows 7 (32- and 64-bit), and Windows Vista® (32- and 64-bit) operating systems • Windows Mobile® Professional, Windows Mobile, Windows CE, and Windows Mobile 2003 for Pocket PC • Red Hat® Enterprise Linux® (RHEL) • Apple® Mac OS® operating system software Please note that supported features will vary between different OAC editions for specific platforms. For details on supported features by platform, please consult the specific OAC edition's documentation, which may be found at **www.juniper.net/customers/support/**.	Ensures network access and security across a variety of different platforms without necessitating any changes to the access client software.
Supports most Extensible Authentication Protocol (EAP) types	OAC supports most EAP types, including: • EAP-TTLS[1] • EAP-PEAP[1] • EAP-TLS[1] • EAP-FAST and LEAP • EAP-SIM[2] • EAP-AKA[2] • EAP-POTP[2] • EAP-MD5[3] OAC also supports advanced encryption protocols, including Wi-Fi Protected Access (WPA) and WPA2.	• Supports most EAP types in order to support the authentication protocol or protocols that best address your network security needs. Seamlessly enables all of the benefits of EAP, including: • Credential security using Transport Layer Security (TLS) for cryptography • Data privacy • The industry's strongest available encryption of data communicated wired or wirelessly across all platforms.
Client security and policy enforcement features	• Client lockdown, which prohibits a user from editing or modifying any administrator-defined WLAN or wired 802.1X connection or setting. • Additional entries for home networks or hotspots can be defined, but only with the appropriate organizational permissions. • Restricts users who are not credentialed administrators from disabling or exiting—essentially turning off—OAC via the OAC system tray icon by hiding the right-click "Exit" menu entry; or the OAC adapter selection checkbox in the Wi-Fi window of the Odyssey Access Client Manager.	• Ensures that the client remains in complete, constant compliance with your organization's access and security policies. • Makes sure that a user cannot accidentally or purposefully disable or exit OAC.
Integrates with Juniper Networks UAC network access control (NAC) solution[4]	• Compatible and integrates seamlessly with UAC, Juniper's comprehensive NAC solution. • Includes an enhanced user interface with additional elements that become active only upon connection and interoperation with UAC, creating a complete network and application access control solution. • Administrators can use Odyssey Client Administrator to generate a configuration file and upload it to IC Series Unified Access Control Appliances at the heart of UAC for delivery with the client package (MSI).	Enables a complete access control solution that is adaptable and scalable, combining user identity, device security state, and network location to create dynamic, session-specific access control policy for each user and each session—leveraging the network you have in place today.

[1]Not supported in OAC for Macintosh
[2]Not supported in OAC for Linux and OAC for Macintosh
[3]Supported in OAC for Windows ONLY
[4]Supported in OAC for Windows v5.0 or higher, and OAC for Macintosh v5.2 or higher

Lower TCO

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

Table 2: Lower TCO

FEATURE	FEATURE DESCRIPTION	BENEFITS
Single client for wired and wireless networks	• A single OAC client works for both wireless and wired network access. • Works with any 802.1X-compatible RADIUS server. • Supports multiple adapter cards simultaneously.	A single client for use in wired, wireless, and mixed networks simplifies deployment of client software for a new or existing network infrastructure.
Localized versions[5]	OAC's user interface, online help, installer, and documentation has been localized to support the following languages: • Chinese (Simplified) • Chinese (Traditional) • French • German • Japanese • Korean • Spanish	• Localized versions enable organizations with users for whom English is not their native language to use OAC effectively. • Enables the deployment of secure wired and wireless connectivity and control across worldwide organizations and enterprises.
Quick, simple deployment and distribution features	• Embeds enterprise settings, certificates, and permissions into a custom installation package for initial deployment. • Automates client distribution via integration with common enterprise deployment tools, including Systems Management Server (SMS). • Command line export to script preserves network configurations across installs and uninstalls. • XML-based scripting language automates distribution of settings. • Single, unified installer provides a simple, integrated way to install any OAC edition. • Can be installed as a background task with no user interaction required through silent installation option. • Can implement a hidden registry setting that is checked when any upgrade occurs, enabling machine account networks, profiles, and auto-scan lists to be merged during an upgrade to preserve existing configurations.	Eliminates the need to touch every endpoint device on initial configuration, subsequent changes to network and security settings, or changes to network security policies—delivering substantial time and cost savings.
Simple and user-friendly	• Straightforward user interface includes at-a-glance connection information and status. • Provides uncomplicated yet comprehensive user controls. • Auto-scan lists for most platforms allow the user to associate with any network listed. • Self-administrating, requiring no user interaction. • If desired, client stealth mode can hide icons and splash screen from users. • Enables users to move seamlessly between different networks (home, office, hotspot, other).	Makes it easy for users to connect to the network and be productive securely, while delivering dramatic savings in training, helpdesk, and support costs.
Consistent user and administrative experience	• One client supports wired and wireless 802.1X deployments simultaneously. • Common user interface look-and-feel, terminology, and feature sets across all of OAC's supported OS platform versions. • User experience can be customized, if desired. • A common tool is used to administer and provision clients across all supported OS platforms and editions.	Simple, consistent user and administrator experience, decreases training and support costs.
Trouble-free maintenance and support	• Offers enhanced troubleshooting capabilities, including comprehensive debug logs. • Includes a scan airwaves tool for enhanced network planning and troubleshooting. • Log to File gathers information useful to technical support staff and network administrators; logging levels are controllable via the user interface. • Trace and debug logs are accessible and configurable from the Odyssey Access Client Manager.	• Simplifies network diagnostics and troubleshooting, reducing problem diagnosis time to decrease support costs and increase productivity. • Access, configure, search, and save trace and debug logs, saving support and troubleshooting time.

[5]Available in OAC for Windows ONLY

FEATURE	FEATURE DESCRIPTION	BENEFITS
Complete, secure network access	• Exercise complete control over secure, safe, and appropriate network connectivity. • User interface permissions provide uniform enforcement of security policies. • Preferred networks feature allows administrators to configure networks for users in priority order, associating with a higher priority network when users are in range. • Preemptive networks feature allows administrative configuration of priority networks to which users can be associated when they are in range. • Wireless suppression restricts a user's wireless connectivity when their endpoint device is connected to a wired network. • No default connection restricts user connectivity to an available network as a default state. • Prevent users from deselecting OAC as the default wireless access client for a chosen wireless adapter. • Increase compatibility with third-party wireless applications by enabling the application to temporarily disable OAC when the application needs to operate or transmit. • Restrict the length of time that a temporary or "scanned" wireless network may remain configured in OAC; or enable OAC to "forget" the network ever existed.	• Ensures across-the-board enforcement of an organization's security and access policies, and ensures that users are connected to the appropriate network in the appropriate manner, restricting their connectivity in select situations to specific offering(s). • Increases compatibility with third-party wireless applications, enhancing usability and saving administrative or helpdesk calls and time. • Delivers additional protection, to assure that users and devices cannot inadvertently or intentionally connect to networks that should not be trusted.
Supports advanced network logon capabilities	• Supports Microsoft Windows Graphical Identification and Authentication (GINA) and Novell® NetWare® login. • Delivers machine authentication support. • Provides single sign-on (SSO) support for Microsoft Windows and Novell environments. • Login names can be automatically provisioned. • Supplies automatic login scripts. • Simplifies connection from "wireless only" devices. • Prompts user for user name.	• Significantly improves and simplifies network connectivity while ensuring network security, and improves administration processes. • Prompt for user name and automatic login scripts ensure the secure use and connection of a single device employed by multiple users as well as enabling easy background access by network managers.
Supports government certified standards	• 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 of Standards and Technology (NIST) and the Canada Communications Security Establishment (CSE), Canada's national cryptologic agency. • Evaluated and certified for conformance to the Common Criteria (ISO/IEC 15408), the international security standard, and has been awarded an assurance level of EAL 3 Augmented ALC_FLR.2; claims being validated include the U.S. Government Protection Profile for Wireless LAN Clients for Basic Robustness Environments. *(Please contact Juniper Networks for the version number of the evaluated client.)* • Supports xSec for more robust, government-approved encryption, using AES for in-transit data when operating over Microsoft Windows Vista and with 802.11 adapters and drivers. • Compatible with U.S. Department of Defense (DoD) Common Access Card (CAC) standards and certificates. • Conforms to NIST and DoD guidelines for the use of 802.11i and TLS-based EAP methods.	Provides government certified and validated security and encryption that stringently protects transmitted credentials and data from breach or theft.

Product Options—Specific Editions for Specific Requirements

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

Table 3: OAC Editions and Audiences

EDITION	DESCRIPTION	AUDIENCE
Odyssey Access Client	Secure, easily deployed, market-leading 802.1X enterprise-built supplicant.	OAC is suitable for all organizations and enterprise networks.
Odyssey Access Client FIPS Edition	• An 802.1X client (supplicant) that meets stringent government IT and communications requirements, OAC FIPS Edition incorporates the Odyssey Security Component, a cryptographic module that is FIPS 140-2 Level 1, Certificate #569 validated by NIST and the CSE, Canada's national cryptologic agency. • OAC FIPS Edition has been evaluated and certified for conformance to the Common Criteria (ISO/IEC15408), 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. (Note: Please contact Juniper Networks for the version number of the evaluated client.) • OAC FIPS Edition is also compatible with the DoD's CAC standards and certificates.	OAC FIPS Edition has been built for public (government) and private sector organizations that: • Want or must deploy secure, scalable wired or WLAN access based on the open 802.1X and 802.11i security standards • Must meet stringent encryption requirements stipulated by the U.S. government.

OAC is also available in specific editions developed to leverage the particular features and capabilities of different operating systems and software, such as Microsoft Windows, Windows Mobile, Linux, and Apple Mac OS. However, each of these OAC operating system/software specific editions may have differing features and functionality, and may be at different release points and versions than other OAC operating system/software specific editions.

For details on supported features by operating system software and platform for OAC, please consult the specific OAC edition's documentation, which may be found at **www.juniper.net/customers/support/**.

Specifications

Odyssey Access Client System Requirements

Editions of Odyssey Access Client are available to support:

- Microsoft® Windows® (Odyssey Access Client for Windows®)
- Microsoft Windows Mobile, Windows CE, and Windows 2003 for Pocket PC (Odyssey Access Client for Windows Mobile/CE)
- Linux (Odyssey Access Client for Linux)
- Apple Mac OS (Odyssey Access Client for Macintosh®)

For more information on specific platforms and versions supported by OAC, please consult your Juniper Networks representative or authorized reseller.

Odyssey Access Client FIPS Edition System Requirements

Odyssey Access Client FIPS Edition supports the:

- Microsoft Windows operating systems
- Microsoft Windows Mobile, Windows CE, and Windows 2003 for Pocket PC software

Juniper supplies modified drivers for Windows XP for the Odyssey Access Client FIPS Edition. For a current list of drivers supported by Odyssey Access Client FIPS Edition for all operating systems please contact your Juniper Networks sales representative or authorized reseller.

For more detailed information on OAC FIPS Edition, please consult the Odyssey Access Client FIPS Edition datasheet, at **www.juniper.net/us/en/local/pdf/datasheets/1000185-en.pdf**.

For more information on platforms and versions supported by OAC FIPS Edition, please contact your Juniper Networks representative or authorized reseller.

Juniper Networks Services 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

MODEL NUMBER	DESCRIPTION
Odyssey Access Client	
OAC-ADD-1CLT	OAC – 1 Client (License Key only)
OAC-ADD-5CLT	OAC – 5 Clients (License Key only)
OAC-ADD-10CLT	OAC – 10 Clients (License Key only)
OAC-ADD-25CLT	OAC – 25 Clients (License Key only)
OAC-ADD-50CLT	OAC – 50 Clients (License Key only)
OAC-ADD-100CLT	OAC – 100 Clients (License Key only)
OAC-ADD-125CLT	OAC – 125 Clients (License Key only)
OAC-ADD-150CLT	OAC – 150 Clients (License Key only)
OAC-ADD-175CLT	OAC – 175 Clients (License Key only)
OAC-ADD-200CLT	OAC – 200 Clients (License Key only)
OAC-ADD-250CLT	OAC – 250 Clients (License Key only)
OAC-ADD-300CLT	OAC – 300 Clients (License Key only)
OAC-ADD-400CLT	OAC – 400 Clients (License Key only)
OAC-ADD-500CLT	OAC – 500 Clients (License Key only)
OAC-ADD-1000CLT	OAC – 1,000 Clients (License Key only)
OAC-ADD-1500CLT	OAC – 1,500 Clients (License Key only)
OAC-ADD-2000CLT	OAC – 2,000 Clients (License Key only)
OAC-ADD-2500CLT	OAC – 2,500 Clients (License Key only)
OAC-ADD-3000CLT	OAC – 3,000 Clients (License Key only)
OAC-ADD-4000CLT	OAC – 4,000 Clients (License Key only)
OAC-ADD-5000CLT	OAC – 5,000 Clients (License Key only)
Odyssey Access Client—Japanese Edition	
OAC-ADD-1CLT-JP	OAC Japanese Edition – 1 Client (License Key only)
OAC-ADD-5000CLT-JP	OAC Japanese Edition – 5,000 Clients (License Key only)
Odyssey Access Client FIPS Edition	
OAC-ADD-F1CLT	OAC FIPS Edition – 1 Client (License Key only)
OAC-ADD-F5000CLT	OAC FIPS Edition – 5,000 Clients (License Key only)
Odyssey Access Client FIPS Edition—Broadcom Edition	
OAC-ADD-FWF50CLT	OAC FIPS Broadcom Wi-Fi Edition – 50 Clients (License Key only)
OAC-ADD-FWF100000CLT	OAC FIPS Broadcom Wi-Fi Edition – 100,000 Clients (License Key only)

Note: The above table is only a subset of all part numbers available for this product.

For more information on (and a 30-day free trial of) OAC, the market-leading, standards-based, enterprise-built access control client, please contact your Juniper Networks sales representative, Juniper authorized partner, or visit **www.juniper.net/us/en/products-services/software/ipc/odyssey-access-client/**.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. 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.

1000154-004-EN Apr 2011

Printed on recycled paper