



Juniper Networks Unified Access Control (UAC) Solution

Infranet Controller, UAC Agent and Enforcement Points

Your network and applications are no longer separate from your business; access to them must be secure, but pervasive. You need an access control solution that is flexible and continues to evolve to address issues vital to your business' success and security.

Juniper Networks Unified Access Control (UAC) solution reduces threat exposure, delivers comprehensive control, visibility, and monitoring, and decreases access control deployment costs and complexity. It extends access control to network traffic, implementing policy enforcement deeper into your network's core and outward to its edge, mitigating risks and protecting sensitive corporate assets.

Product Description

Today's enterprises need an access control solution that ties together the user's identity, device security state, and network location, and can uniformly enforce policy across the growing number of diverse users and devices, most of which are not managed by the enterprise, that demand access to the network and applications. This solution not only must deliver security pre and post authentication, granular network access control, and quarantine/remediate non-compliant users and devices, but also support unmanageable devices connecting to the network, post admission control, and application access control, visibility and monitoring. The solution must also address the full range of access control use cases, including network protection, guest user access, and control, visibility and monitoring while leveraging existing network investments and deployments. Finally, this comprehensive access control solution must be based on open, industry standards so the enterprise can avoid single vendor "lock-in," and should reduce the complexity and cost associated with access control deployment and management, enabling phased deployments of the solution.

The Juniper Networks Unified Access Control (UAC) solution combines user identity and device security state information with network location to create a unique access control policy for each user. The solution can be enabled at Layer 2 using 802.1X, or at Layer 3 using an overlay deployment. UAC can also be provisioned in mixed mode, using 802.1X for network admission control and Layer 3 for resource access control.

With UAC, enterprises are not constrained by:

- Switching infrastructure – UAC interoperates with any vendor's 802.1X enabled switch or access point.
- Interoperability issues – not only is UAC vendor-agnostic for 802.1X, but Juniper strongly supports open standards from the Trusted Computing Group's Trusted Network Connect (TNC), guaranteeing interoperability with a host of other security offerings.
- Use cases – UAC addresses common access control use cases, including guest user access, network protection, and application control, visibility, and monitoring.
- Lack of network/application visibility – UAC leverages the capabilities of Juniper's Intrusion Detection and Prevention (IDP) platforms to deliver broad application traffic visibility, enabling the enterprise to isolate threats to the user or device level, and to then employ an applicable policy action against the offending user or device. Also, UAC ties user identity and role information to network and application access and use, addressing the demands of regulatory compliance.
- Device types or OS – UAC works across most Microsoft® Windows®, Apple® Mac OS®, Linux, and Solaris platforms.
- Deployment issues – With UAC, the enterprise can make use of its existing 802.1X infrastructure, Juniper firewalls, or both for policy enforcement. Plus deployments can employ both enforcement methods for the most granular access control, without having to re-deploy anything. UAC also enables enterprises to phase their access control deployments. And, UAC dynamically addresses support for unmanageable endpoint devices, enabling enterprises to leverage their existing policy and profile stores or asset discovery or profiling solutions for role and resource-based access control.

The components of the UAC solution include:

- The Infranet Controller, which functions as the centralized security policy engine as well as the interface with existing enterprise AAA infrastructures. The Infranet Controller also features integrated RADIUS capabilities from Juniper's Steel-Belted Radius®, enabling support for an 802.1X transaction when an endpoint enters the network.
- The UAC Agent, which is a dynamically downloadable agent that can be preconfigured, provisioned in real time by the Infranet Controller, or deployed by other means. The UAC Agent is also available as a cross platform, dynamically downloaded lightweight agent. UAC also provides an agent-less mode for circumstances where downloads of software are not practical, like guest networking scenarios. The UAC Agent collects user credentials and assesses the endpoint's security state. It includes integrated 802.1X functionality from Juniper's Odyssey® Access Client (OAC) 802.1X client/supplicant, Layer 3 - 7 functionality, Host Checker functionality which scans endpoints for a variety of security applications and states and custom checks of various elements, and a stateful personal firewall, all contained in a single deployment.
- UAC enforcement points, which include any Juniper Networks firewall/VPN appliances, as well as any vendor's 802.1X-enabled wired or wireless switching infrastructure.

Infranet Controller

The heart of Juniper's Unified Access Control solution is the Infranet Controller, a hardened, centralized policy management server that can push the UAC Agent to the endpoint (or gather information in agent-less mode) to get user authentication, endpoint security state and device location data. The Infranet Controller combines this information to create dynamic policies which are then propagated throughout the network to enforcement points which include vendor-agnostic 802.1X-enabled switches and access points, any Juniper firewall/VPN platform, or both for even greater granularity. The Infranet Controller leverages Juniper's market-leading Secure Access SSL VPN policy control engine to seamlessly integrate with an enterprise's existing AAA/identity and access management infrastructure, and can empower the use of group memberships in authorization directories. These assessments can be repeated at administrator defined times during the session to ensure dynamic policy management and enforcement and also provide granular, policy specific remediation capabilities for non-compliant users or devices.

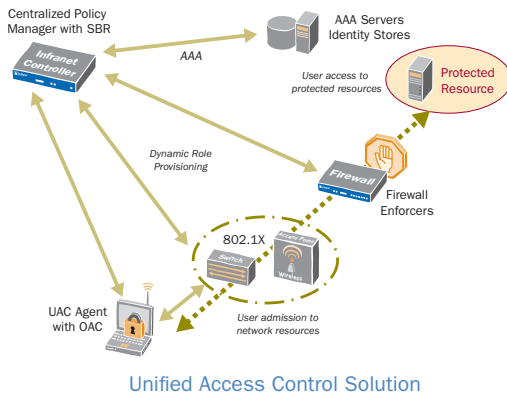
The Infranet Controller is available in two different form factors: Infranet Controller 4000 (IC 4000) and Infranet Controller 6000 (IC 6000). The IC 4000 is designed for the needs of small to medium enterprises or remote/branch offices. It will scale to handle thousands of concurrent endpoints, and can be deployed in cluster pairs for high availability. The IC 6000 is designed for large enterprises with the capability to scale to handle tens of thousands of concurrent endpoints. It has a number of high availability features, including a hot swappable power supply that can be field upgraded, as well as a field-upgradeable hard disk. The IC 6000 can be deployed in multi unit clusters to increase performance and provide additional scalability.

UAC Agent

The UAC Agent is a dynamically downloadable agent that can be preconfigured, provisioned in real-time by the Infranet Controller, installed using Juniper's Installer Service, or deployed by other methods. The UAC Agent is also available as a cross platform, dynamically downloaded lightweight agent. UAC also offers an agent-less mode, for circumstances where downloads of software are not feasible. The UAC Agent collects user and/or device credentials and assesses the endpoint's security state. It delivers integrated 802.1X functionality from Juniper's OAC 802.1X client/supplicant, and Layer 3-7 functionality, including an integrated personal firewall for dynamic client-side enforcement of policies. The UAC Agent also includes specific functionality for Windows devices such as IPSec VPN (which enables encryption from the endpoint to the firewall) and Single SignOn to Active Directory. The UAC Agent's integrated Host Checker functionality, familiar from thousands of Juniper Secure Access SSL VPN deployments, enables an administrator to scan endpoints for a variety of security applications/states, including but not limited to antivirus, malware and personal firewalls. It also enables custom checks of elements such as registry and port status and can perform an MD5 checksum to verify application validity. Deployment is simplified via pre-defined Host Checker policies as well as automatic monitoring of antivirus signature files for the latest definition files for posture assessment. UAC Agent extends its robust support for the most popular enterprise computing platforms with a new Layer 2/Layer 3 UAC Agent for the Microsoft® Windows Vista™ platform. The UAC Agent can also be delivered based on role, linking agent-less or agent-based access dynamically to user or device identity.

Enforcement Points

UAC enforcement points encompass any 802.1X compatible switches and wireless access points and/or any Juniper Networks firewall/VPN platforms as Layer 3 - 7 overlay enforcement points, including the Secure Services Gateway (SSG) appliances and Integrated Security Gateways (ISG) with IDP modules. Support for vendor agnostic 802.1X switches and/or wireless access points enables enterprises to quickly realize the benefits of access control without requiring a hardware overhaul. The wide variety of Juniper firewalls that can be used as enforcement points gives the enterprise both best-in-class firewall functionality and unprecedented access control deployment flexibility. Some Juniper firewalls support threat management capabilities including Juniper's IDP functionality, as well as network-based antivirus, anti-spam and URL filtering capabilities. All of these capabilities can be dynamically leveraged as part of the UAC solution, with UAC not only enforcing access control policies but also applying security policies such as deep packet inspection, antivirus and URL filtering on a per user/session basis. This enables an enterprise to unify the application of access and security policies for comprehensive network access and threat control. Enforcement points can also be set up in transparent mode, which requires no rework of routing/policies or changes to the network infrastructure; and, enforcement points can be set up in audit mode to visualize compliance without enforcement.



Features and Benefits

Key features and benefits of Juniper's UAC solution can be grouped into three high-level value propositions:

- Advanced Network Protection
- Control, Visibility, and Monitoring
- Simple, Flexible Access Control

Advanced Network Protection

Feature	Feature Description	Benefit
Binds endpoint assessment, user/device identity, and network location with real-time, dynamic network security policy enforcement	Combines user identity, device security state and location information to create dynamic session-specific access policy by user that is distributed across the network to enforcement points	Ensures uniform network protection and enforcement of session-specific access policy by user via any new or existing vendor-agnostic, 802.1X-enabled switches, access points or other devices, any Juniper firewall/VPN platform, or both, saving time and delivering network investment protection
Single centralized policy engine	Manages and administers access control before session login and throughout the session	<ul style="list-style-type: none"> • Two hardened form factor policy servers from which to choose, the Infranet Controller 4000 (IC 4000) or Infranet Controller 6000 (IC 6000), allowing enterprises to select the best fit for their needs • Pre-authentication assessment, authentication, role mapping and resource controls all in one location • Easy setup and administration of network resource policy rules • No forklift upgrade of existing infrastructure required to deploy the solution • Dynamic propagation of policy enforcement to endpoints and enforcement points, whether 802.1X-based, Layer 3 overlay-based, or both • Policy can change dynamically as the endpoint or network environment changes
Robust, dynamic UAC Agent	<ul style="list-style-type: none"> • A single, dynamically downloadable agent for wired and wireless deployments that can be preconfigured, provisioned in real time by the Infranet Controller, or deployed by other means • UAC Agent delivers support for the most popular enterprise computing platforms, including a new Layer 2/Layer 3 UAC Agent for the Microsoft® Windows Vista™ platform • A cross platform, dynamically downloaded lightweight UAC Agent is also available for Microsoft Windows®, Apple® Mac OS®, Linux, and Solaris platforms • Includes TNC compliance for seamless interoperability with other TNC compliant security solutions; integrated Host Checker functionality which scans endpoints for a wide variety of best-in-class endpoint security applications and states including antivirus, malware and personal firewalls, enables custom checks of elements (such as registry and port status), and can do an MD5 checksum to verify application validity; a stateful personal firewall that also functions as a client-side policy enforcer and optional secure transport (authenticated and encrypted) using IPSec for session integrity and privacy, and that ensures privacy for communications on the LAN; MS Windows Single SignOn support 	Protects the enterprise network (and other endpoints) from unhealthy, non-compliant, and/or malicious endpoints and allows the enterprise to maintain access control and network security and health even if the enterprise does not own or manage the endpoints.
Agent-less deployment	Agent-less deployment with cross platform support	Enables enterprises to secure Mac OS, Linux, and Solaris platforms in situations where client downloads are not possible or feasible by binding endpoint assessment and user identification and continue the enforcement of network security policies

Feature	Feature Description	Benefit
Coordinated Threat Control	Leverages the robust features and capabilities of Juniper's standalone and integrated Intrusion Detection and Prevention (IDP) platforms to deliver broad Layer 2-7 visibility into application traffic, providing the ability to isolate a threat down to the user or device level and via the standalone Juniper IDP to then employ a specific, configurable policy action against the offending user or device	Delivers strong interoperability with market-leading Juniper IDP products; quickly addresses and mitigates network threats, minimizing network and user downtime
Dynamically addresses unmanageable endpoints	Enables enterprises to employ Media Access Control (MAC) address authentication via RADIUS, in combination with MAC address white listing and black listing, or leveraging existing policy and profile stores (via Lightweight Directory Access Protocol (LDAP) interfaces) or asset discovery or profiling solutions for role and resource-based access control of unmanageable devices, such as networked printers, cash registers, bar code scanners, Voice over Internet Protocol (VoIP) handsets, etc.	Enhances network and application protection, makes it simpler and faster for enterprises to deploy access control across their network regardless of device manageability, and saves time and cost by allowing enterprises to employ existing policy and profile stores or asset discovery/profiling solutions, for role- and resource-based access control of unmanageable devices
Extended automatic remediation	Delivers a self-administering platform that intelligently quarantines non-compliant users and devices, and extends auto-remediation capabilities, enabling users to automatically address and remediate devices that do not meet policy prior to allowing them on to the network; devices are dynamically mapped to an access role upon remediation	Can remediate many non-compliant devices automatically without user intervention or other assistance, minimizing downtime and support calls, saving time and expense, and increasing user and support staff productivity
Integrated, pre-defined patch assessment checks	Patch assessment checks of employee and guest user devices via an OEM integration of Shavlik Technologies' Shavlik NetChk® Protect predefined patch assessment technologies, including endpoint inspection for targeted operating system or application hot fixes, enabling easy policy definition that directly links to the presence or absence of specific hot fixes for defined operating systems and/or applications with the ability to perform pre-defined patch management checks according to vulnerability severity level, enforcing or denying access to certain roles	Enables more enhanced, granular endpoint device health and security state assessments
Dynamic role mapping	Leverages a range of attributes for security requirements that users need to meet before a user login page is presented	Security requirements can be enforced pre-authentication as well as post-authentication throughout the session

Control, Visibility, and Monitoring

Feature	Feature Description	Benefit
Identity-enabled profiler	Ties user identity and role information to network and application usage, enabling enterprises to more effectively track and audit network and application access, which in turn helps address regulatory compliance	Allows enterprises to know who is accessing their network and applications, and when they are being accessed, directly addressing regulatory compliance and auditing
Role-based application of security policies	Delivers enterprises the ability to create and apply role-based threat management policies, like network IDP, network antivirus, network spyware, and/or network URL filtering, enabling them to leverage UAC for both dynamic access control and dynamic threat control	Delivers the ability to populate user/role information in network infrastructure products for network/application access
Granular auditing and logging	Fine-grained auditing and logging capabilities in a clear, easy to understand format	Ensures detailed logging by roles that users belong to, resources that they are trying to access, and the state of compliance of the endpoint and user to the security policies of the network

Simple, Flexible Access Control

Feature	Feature Description	Benefit
Open, standards based solution	Leverages industry-standards, such as 802.1X, RADIUS, IPSec, and others; and innovative open standards, such as those from the Trusted Network Connect (TNC), to deliver a standards-based access control solution	Delivers vendor-agnostic access control and seamless support for heterogeneous networking environments, enabling enterprises to deploy access control quickly, simply, and flexibly, without requiring forklift upgrades, saving time and cost
Based on Juniper's industry-proven, best-in-class security and access control products	Leverages Juniper's Secure Access SSL VPN policy engine, and RADIUS capabilities from Juniper's Steel-Belted Radius (SBR), and 802.1X capabilities from Juniper's Odyssey Access Client (OAC) to complete 802.1X transactions	Builds on market-leading security and access control products that have been field-tested in thousands of deployments around the world ensuring dependability and interoperability with existing, heterogeneous network infrastructures, delivering investment protection, and time and cost savings
Leverages existing 802.1X-enabled switches and/or access points	Leverages existing 802.1X-enabled switches and/or access points	Makes it simple for an enterprise to secure a wireless network or 802.1X-based switching infrastructure without being locked into a single vendor's switching solution

Feature	Feature Description	Benefit
Supports the Trusted Computing Group's Trusted Network Connect (TNC) open standards	Strong support for the Trusted Computing Group's Trusted Network Connect (TNC) open standards	Enables the enterprise to choose endpoint security solutions that work for them without worrying about interoperability, ensuring maximum choice, which leads to faster return on investment
Enables phased approach to access control deployments	UAC's innovative design enables enterprises to start controlling access virtually anywhere on their network - for example, enterprises may start controlling access with wireless LAN users and expand outward or upward using a phased approach for access control deployments; also, UAC's audit mode enables enterprises to track user and device policy compliance without enforcing policies	Saves access control deployment time and cost; audit mode enables users to become familiar with policies and necessary compliance, and enables enterprises to phase in policy compliance enforcement
Dynamic authentication policy leverages existing investment in AAA	Support for 802.1X, RADIUS, LDAP, AD, RSA ACE, NIS, Certificate servers (digital certs/PKI), Local login/password, Netegrity SiteMinder (Computer Associates), RSA Cleartrust, and Oblix (Oracle); and also supports RADIUS Proxy	Leverages the enterprise's existing investment in directories, PKI, and strong authentication, enabling administrators to establish a dynamic authentication policy for each user session; RADIUS Proxy support enables support for deployments where certain authentications have to be supported by a backend RADIUS server
Role-based Agent download	Agent downloads can be based on role, and dynamically delivered in the appropriate manner (agent-based or agent-less)	Enables enterprises to tie agent-less or agent-based access dynamically to user and/or device identity instead of forcing an upfront selection
Extended authentication protocol support	Offers support for additional Extensible Authentication Protocol (EAP) types	Enables enterprises to leverage more network software and devices; network access can be controlled at the Access Layer for a diverse array of deployment scenarios

Product Options

The IC 4000 and IC 6000 have several hardware and software options that can be added to the products.

Option	Option Description	Applicable Products
Coordinated Threat Control	The ability to leverage additional access control and security capabilities via UAC communicating with Juniper IDP products for coordinated threat control based on Juniper IDP intelligence	IC 4000, IC 6000
Redundant hot swappable hard disk	Redundant hot swappable hard disk	IC 6000
Redundant hot swappable power supply	Redundant hot swappable power supply	IC 6000

Specifications

	IC 4000	IC 6000
Dimensions and Power		
Dimensions (W x H x D)	16.7 x 1.7 x 15 in (42.4 x 4.4 x 38.1 cm)	16.7 x 3.5 x 16.2 in (42.4 x 8.9 x 41.2 cm)
Weight	13.6 lbs (6.17 kg) typical (unboxed)	28.5 lbs (12.94 kg) typical (unboxed)
A/C Power Supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 260 Watts	100-240 VAC, 50-60 Hz, 5A Max, 500 Watts
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	65% minimum, at full load	65% minimum, at full load
MTBF	82 khrs	71 khrs
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel
Fans	3 40mm ball bearing fans, 1 40mm ball bearing fan in power supply	2 externally accessible, hot swappable ball-bearing fans

Panel Display

Front Panel Power Button	Yes	Yes
Power LED, HD Activity, Temp	Yes	Yes
PS Fail	No	Yes
HDD Activity and RAID Status LEDs	No	Yes

Ports

Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)
Console	One 9-pin serial console port

Environment

Operating Temp	50° to 95°F (10° to 35°C)
Storage Temp	-40° to 158°F (-40° to 70°C)
Relative Humidity (operating)	8% to 90% noncondensing
Relative Humidity (storage)	5% to 95% noncondensing
Altitude (operating)	-50 to 10,000 ft (3,000m)
Altitude (storage)	-50 to 35,000 ft (10,600m)

Certifications

Safety Certifications	EN60950-1:2001+A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001
Emissions Certifications	FCC Class A, VCCI Class A, CE class A
Warranty	90 days; Can be extended with support contract

Ordering Information

Infranet Controller 4000

Base System	
IC4000	Infranet Controller 4000 Base System

Endpoint Licenses

IC4000-ADD-100E	Add 100 simultaneous users to IC4000
IC4000-ADD-250E	Add 250 simultaneous users to IC4000
IC4000-ADD-500E	Add 500 simultaneous users to IC4000
IC4000-ADD-1000E	Add 1000 simultaneous users to IC4000
IC4000-ADD-2000E	Add 2000 simultaneous users to IC4000
IC4000-ADD-3000E	Add 3000 simultaneous users to IC4000

Feature Licenses

IC4000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC4000
--------------------	---

Clustering Licenses

IC4000-CL	Add Clustering on IC4000
-----------	--------------------------

Coordinated Threat Control Licenses

IC4000-ADD-TCTRL	Add Coordinated Threat Control with IC 4000 and Juniper IDP
------------------	---

Infranet Controller 6000

Base System	
IC6000	Infranet Controller 6000 Base System

Endpoint Licenses

IC6000-ADD-250E	Add 250 simultaneous users to IC6000
IC6000-ADD-500E	Add 500 simultaneous users to IC6000
IC6000-ADD-1000E	Add 1000 simultaneous users to IC6000
IC6000-ADD-2000E	Add 2000 simultaneous users to IC6000
IC6000-ADD-3000E	Add 3000 simultaneous users to IC6000
IC6000-ADD-5000E	Add 5000 simultaneous users to IC6000
IC6000-ADD-10000E	Add 10000 simultaneous users to IC6000
IC6000-ADD-15000E	Add 15000 simultaneous users to IC6000
IC6000-ADD-20000E	Add 20000 simultaneous users to IC6000
IC6000-ADD-25000E	Add 25000 simultaneous users to IC6000

Feature Licenses

IC6000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC6000
--------------------	---

Clustering Licenses

IC6000-CL	Add Clustering on IC6000
-----------	--------------------------

Coordinated Threat Control Licenses

IC6000-ADD-TCTRL	Add Coordinated Threat Control with IC 6000 and Juniper IDP
------------------	---

Accessories

IC6000-HD	Field Upgradeable Secondary Hard Disk for IC6000
IC6000-FAN	Field Upgradeable Fan for IC6000
IC6000-PS	Field Upgradeable Secondary Power Supply for IC6000
SA-ACC-RCKMT-KIT-1U	Secure Access and Infranet Controller Rack Mount Kit - 1U
SA-ACC-RCKMT-KIT-2U	Secure Access and Infranet Controller Rack Mount Kit - 2U
SA-ACC-PWR-AC-UK	Secure Access and Infranet Controller AC Power Cord UK
SA-ACC-PWR-AC-EUR	Secure Access and Infranet Controller AC Power Cord EUR
SA-ACC-PWR-AC-JPN	Secure Access and Infranet Controller AC Power Cord JPN

About Juniper

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 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

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

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.
26/F, City Plaza 1
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright 2007 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.

100137-004 Oct 2007

To purchase Juniper Networks solutions, please contact your Juniper Networks sales representative at 1-866-298-6428 or authorized reseller.