



# UNIFIED ACCESS CONTROL

## IC Series Unified Access Control Appliances, UAC Agent and Enforcement Points

### Product Overview

Network access control is not meant to keep users and devices off of an organization's network, but to ensure they are authorized to access the network and its resources, and meet security posture. Organizations need a flexible solution that protects their network investments today and in the future, supports phased deployments and grows to cover an entire enterprise. Juniper Networks is the only vendor who can deliver comprehensive, standards-based enterprise-wide access control. Unified Access Control is a uniquely extensible, open solution that delivers granular access control to the entire, distributed enterprise, from remote users and branch offices to the data center while reducing cost and complexity. UAC addresses network challenges such as insider threats, guest access, and outsourcing and off-shoring, as well as regulatory compliance, while delivering scalable, adaptive access control—protecting networks, their mission-critical applications, and sensitive data.

### Product Description

Juniper Networks® Unified Access Control (UAC) delivers comprehensive, adaptive network and application access control for even the most diverse, complex environments, reducing cost and maximizing efficiencies. UAC offers best-in-class performance and scalability with centralized policy management, simplifying deployment, administration, and management. UAC combines user identity, device security state, and network location information to create a unique, dynamic access control policy—per user and per session. UAC incorporates different levels of session-specific policy, including authentication and authorization, roles, and resource policies to create extremely granular access control that is easy to deploy, maintain, and dynamically modify.

Juniper Networks UAC can be enabled at Layer 2 using 802.1X, at Layer 3 using an overlay deployment, or in mixed mode using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control. UAC fully integrates with any vendor's 802.1X-enabled access points or switches, including Juniper Networks EX Series Ethernet Switches which, when combined with UAC, deliver additional, rich policy enforcement capabilities. You can leverage your existing 802.1X infrastructure; any Juniper Networks firewall platform, including the SRX Series Services Gateways; or both for policy enforcement and granular access control without the need to redeploy anything. UAC also supports the Juniper Networks J Series Services Routers as Layer 3 enforcement points.

UAC also introduces a new era of granularity and control as the first access control solution to support Layer 2 – Layer 7 policy enforcement, with unparalleled visibility into application traffic at Layer 7 by leveraging the standalone Juniper Networks IDP Series Intrusion Detection and Prevention Appliances as UAC enforcement points.

Juniper Networks UAC is easily deployed, and allows you and your users to ease into access control policy enforcement by enabling you to phase your access control deployment and allowing it to be run in audit mode. UAC also adds industry-leading, dynamic, pre-authentication antispysware and antimalware protection for Microsoft® Windows® endpoint devices attempting network access. UAC expands its already extensive cross-platform capabilities to include support for the Apple® Mac OS® operating system software.

Juniper Networks is a strong supporter of open standards, including those of the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group, which ensure interoperability with a host of network and security offerings. Through its support for the TNC standard Statement of Health (SOH) protocol, UAC interoperates with the Microsoft Windows SOH and embedded Microsoft Network Access Protection (NAP) Agents, enabling you to use your existing Microsoft Windows Vista® and/or Windows XP SP3 clients with Juniper Networks UAC. UAC also supports the TNC's open standard Interface for Metadata Access Point (IF-MAP), enabling integration with third-party network and security devices—including nearly any device that collects information about the happenings on, or the status of, a network. UAC can leverage this data when formulating access control decisions, taking necessary and appropriate access actions.

UAC leverages other network components to ensure secure network and application access control, address specific use cases, and centralize network policy management. It integrates with the standalone Juniper Networks IDP Series to deliver broad application traffic visibility, mitigating insider threats by isolating threats to the user or device level and employing an applicable policy action against an offending user or device. UAC ties user identity and role information to network and application access, addressing regulatory compliance and audit demands. The implementation and enforcement of consistent remote and local access control policy across a distributed enterprise is assured when UAC is deployed with Juniper Networks Network and Security Manager (NSM) and the market-leading Juniper Networks SA Series SSL VPN Appliances. UAC enables the federation of user sessions data between the SA Series and UAC, seamlessly provisioning SSL VPN user sessions into UAC upon login, or alternatively UAC user sessions into SSL VPN. Similarly, federation allows users authenticated to one Juniper Networks IC Series Unified Access Control Appliance to also access resources protected by another IC Series UAC Appliance on the network without reauthentication, enabling "follow-me" policies.

Juniper Networks UAC is composed of the following:

### IC Series UAC Appliance

At the heart of UAC are the IC Series UAC Appliances—hardened, centralized policy management servers that can push the UAC Agent to the endpoint to obtain user authentication, endpoint security state, and device location data. (The IC Series also gathers this same information through UAC's agent-less mode.) The IC Series use this data to create dynamic policies that are propagated to network enforcement points across the distributed network. UAC enforcement points include vendor-agnostic 802.1X-enabled access points and switches, like the Juniper Networks EX3200 Ethernet Switch and Juniper Networks EX4200 Ethernet Switch, any Juniper Networks firewall/VPN platform, J Series Services Routers, or standalone IDP Series appliances. The IC Series UAC Appliances manage and administer access control prior to session login and throughout the session. No forklift upgrade of existing infrastructure is required to deploy UAC. The IC Series leverage Juniper's market-leading SA Series appliances' policy control engine and their ability to seamlessly integrate with existing AAA/identity and access management

infrastructure. They also feature integrated RADIUS capabilities and enhanced services from Juniper Networks SBR Enterprise Series Steel-Belted Radius Servers, which support an 802.1X transaction when an endpoint attempts network connection. The IC Series UAC Appliances centralize pre-authentication assessment, authentication, role mapping, and resource controls in one location.

You can implement access control quickly and simply within your heterogeneous network by deploying a single IC Series UAC Appliance with your existing vendor-agnostic 802.1X switches or access points, or Juniper Networks firewalls or J Series routers. The IC Series are available in several different form factors, including the IC4000, IC4500, IC6000, IC6500 and IC6500 FIPS. The IC4000 and IC4500 address the access control needs of medium to large organizations or remote and branch offices. These devices scale to handle thousands of simultaneous endpoints and may be deployed in cluster pairs for high availability (HA). The IC6000 and IC6500 are designed for use in large organizations and government agencies, offering the capacity to handle tens of thousands of simultaneous endpoints. The IC6500 FIPS meets the needs of the most demanding and complex government agencies and secure enterprise environments—offering the same functionality available on the IC6500 appliance, and adding a dedicated FIPS 140-2 Level 3 certified hardware security module to handle all cryptographic operations. These devices offer a number of redundant and HA features, including a hot swappable power supply and field-upgradeable hard disk (IC6000); and dual, hot swappable mirrored SATA hard drives, dual, hot swappable fans, and, as an option, dual, hot swappable power supplies (IC6500 and IC6500 FIPS). The IC6000, IC6500, and IC6500 FIPS may be deployed in multi-unit clusters to increase performance and provide additional scalability, able to handle multiple tens of thousands of simultaneous endpoints. Also, with UAC's adoption of the TNC's IF-MAP open, standard specification, the IC4500, IC6000, IC6500, and IC6500 FIPS can serve as mixed IC Series appliances and Metadata Access Point (MAP) servers, or as standalone MAP servers, extending UAC's integration with third-party network and security devices, collecting data from those devices about the user and device or the status of the network, and leveraging that information when formulating policies and appropriate access actions.

### UAC Agent

The UAC Agent is a dynamically downloadable agent that can be preconfigured through the Odyssey Client Administrator, provisioned in real time by the IC Series, installed using Juniper's Installer Service, delivered via Systems Management Server (SMS), or deployed by other distribution mechanism or means. The same UAC Agent can be used in wired, wireless, or combined deployments. The UAC Agent is also available as a cross-platform, dynamically downloadable lightweight agent. UAC also offers an agent-less mode for circumstances where the download of software is not feasible. The UAC Agent can be delivered based on role, linking agent-based or agent-less access dynamically to user or device identity. The UAC Agent collects user and device credentials and assesses the endpoint's security state. It delivers integrated 802.1X functionality from Juniper Networks

Odyssey Access Client (OAC)—an 802.1X client/supplicant—as well as Layer 3-7 functionality, including an integrated personal firewall for dynamic client-side policy enforcement. It also includes specific functionality for Microsoft Windows devices such as IPsec VPN as an optional secure transport using IPsec to enable encryption from the endpoint to the firewall for session integrity and privacy, and single sign-on (SSO) to Microsoft Active Directory. The UAC Agent's integrated Host Checker functionality, which is used in thousands of SA Series SSL VPN deployments, enables you to define policy that scans endpoints attempting to connect to your network for a variety of security applications and states—including antivirus, antimalware, 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. UAC also includes industry-tested, dynamic antispyware and antimalware protection for Microsoft Windows endpoint devices that attempt network access, scanning device memory, pre-authentication, for spyware and malware, while providing a real time file-system write and execution shield. The UAC Agent's Host Checker can also assess an endpoint during machine authentication, mapping the device to a different role and placing it into remediation based on assessment results. Deployment is simplified through predefined Host Checker policies and the automatic monitoring of antivirus and antispyware signatures and patches for the latest definition files for posture assessment. Supporting the most popular enterprise computing platforms, the UAC Agent extends its cross-platform support to include Apple Mac OS operating system software, delivering wired and wireless Layer 2 and Layer 3 authentication and endpoint integrity to Apple Macintosh® users.

### UAC Enforcement Points

UAC enforcement points include any 802.1X compatible switch, including the EX3200 and EX4200, and 802.1X-enabled wireless access points; any Juniper Networks firewall/VPN platform;

J Series Services Routers; and standalone IDP Series appliances providing role-based, application-level policy enforcement. Juniper Networks firewall products, including the Juniper Networks SRX Series Services Gateways, Juniper Networks

SSG Series Secure Services Gateways, and Juniper Networks ISG Series Integrated Security Gateways, act as Layer 3-7 overlay enforcement points for UAC, as do J Series Services Routers. For organizations desiring Layer 2 port-based enforcement, support for vendor-agnostic 802.1X switches and/or wireless access points enables them to quickly realize the benefits of access control without requiring a hardware overhaul. The EX3200 and EX4200 provide standards-based 802.1X port-level access control and Layer 2-4 policy enforcement based on user identity, location, and/or device. When used in conjunction with UAC, the EX3200 and EX4200 can also apply quality of service (QoS) policies or mirror user traffic to a central location for logging, monitoring, or threat detection with intrusion prevention systems like Juniper's market-leading IDP Series products. And, with Juniper's standalone IDP Series appliances serving as role-based application-level policy enforcement points, UAC is able to deliver full Layer 2 – Layer 7 policy enforcement. UAC is the first NAC solution that enables you to address application and data access control to the application layer within your network. Many Juniper Networks firewalls also support unified threat management (UTM) capabilities including IDP functionality, network-based antivirus, antispam, anti adware, antiphishing, and Web filtering capabilities. These capabilities can be dynamically leveraged as part of UAC to enforce and unify access control and security policies on a per user and per session basis, delivering comprehensive network access and threat control. UAC enforcement points may also be implemented in transparent mode, which requires no rework of routing and policies or changes to the network infrastructure. They may also be set up in audit mode to determine compliance without enforcement, enabling you and your users to ease into access control.

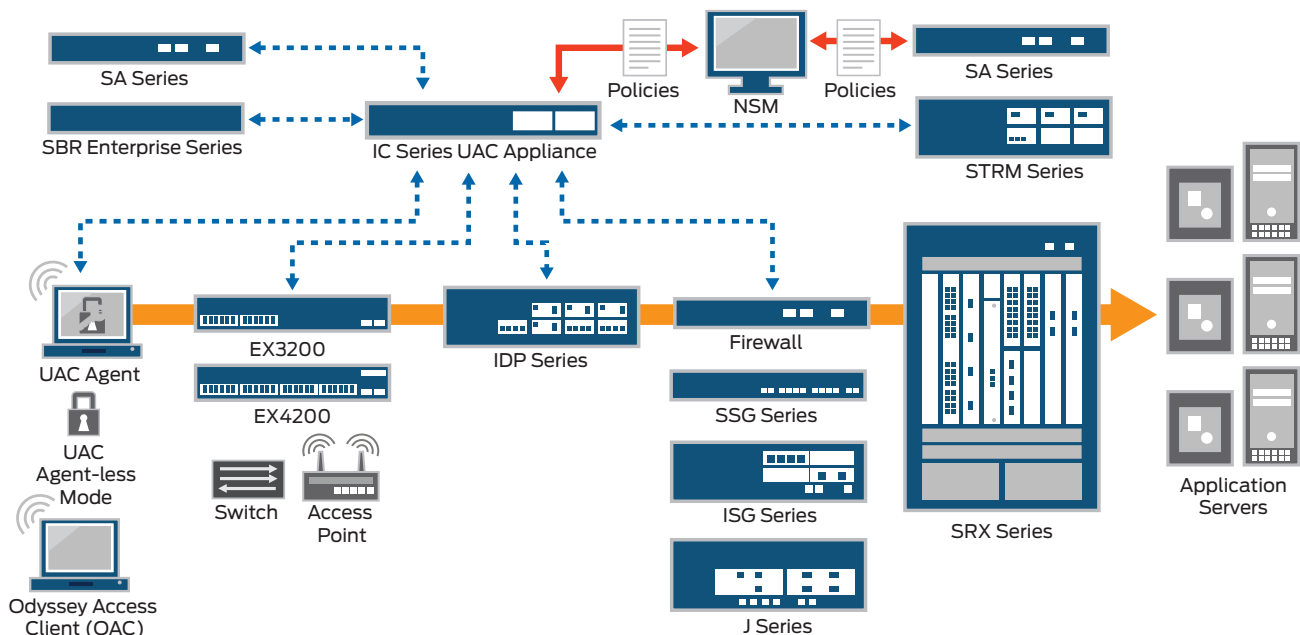


Figure 1: Unified Access Control (UAC) works with existing and new network components to deliver comprehensive network and application access control

## Features and Benefits

Table 1: Advanced Network and Application Protection

FEATURES	FEATURE DESCRIPTION	BENEFITS
Self-administering platform	<ul style="list-style-type: none"> <li>Delivers a platform that intelligently quarantines non-compliant users and devices and extends automatic remediation capabilities</li> <li>Enables the automatic quarantine and remediation of devices that do not meet policy prior to allowing them onto the network and during their network session</li> <li>Maps devices dynamically to an access role upon remediation</li> </ul>	<ul style="list-style-type: none"> <li>Provides automatic remediation for many non-compliant devices without user intervention or other assistance</li> <li>Minimizes downtime and help desk calls, increasing user and support staff productivity</li> <li>Saves time and cost</li> </ul>
Agent-less deployment	Agent-less deployment with cross-platform support	<ul style="list-style-type: none"> <li>Ensures the enforcement of network security policies across all platforms and environments</li> <li>Secures Windows, Mac OS, and Linux platforms in situations where client downloads are not feasible, such as guest access</li> </ul>
Dynamic antispymware /antimalware protection	<ul style="list-style-type: none"> <li>Delivers industry-leading, dynamic antispymware protection from market-leader Webroot which, before authentication, scans the memory of an endpoint device for spyware</li> <li>Also delivers a real time file-system write and execution shield</li> <li>Ties directly into UAC's existing granular policy management framework to allow administrators to quarantine or restrict network access from infected devices</li> <li>Includes automatic remediation for noncompliant devices</li> <li>Spyware signatures automatically downloaded and updated</li> <li>Works with all Windows-based UAC Agents, including Microsoft Windows Vista, as well as in UAC's agent-less mode</li> <li>Antispymware download capability is also available in SA Series SSL VPN Appliances</li> </ul>	<ul style="list-style-type: none"> <li>Ensures unmanaged and managed Windows devices are not running spyware or malware before authentication</li> <li>Quarantine or restrict device access through UAC's existing granular policy management framework</li> </ul>
Predefined patch assessment checks	<ul style="list-style-type: none"> <li>Patch assessment checks of devices are accomplished through OEM integration of Shavlik Technologies' Shavlik NetChk® Protect predefined patch assessment technologies, including endpoint inspection for targeted operating system or application hot fixes</li> <li>Directly link to the presence or absence of specific hot fixes for defined operating systems and applications, and perform role-based, predefined patch management checks according to vulnerability severity level</li> <li>Installed Systems Management Server (SMS) can be leveraged to automatically check for patch updates, quarantining, remediating, and providing authorized network access once a device has been remediated</li> </ul>	<ul style="list-style-type: none"> <li>Enables more enhanced, granular endpoint device health and security state assessments</li> <li>Minimizes user interaction through automatic remediation and management of patches for endpoint devices, reducing help desk calls</li> </ul>
Role-based, application-level enforcement	<ul style="list-style-type: none"> <li>Leverages standalone IDP Series appliances as enforcement points</li> <li>Enables application-specific policy rules to be enforced via any level of policy granularity</li> <li>Policies can also be defined to control time of day and bandwidth restrictions per application or per role</li> </ul>	<ul style="list-style-type: none"> <li>First access control solution to support full Layer 2 - Layer 7 enforcement</li> <li>Enables access control and security policies to be applied to the application-level, granularly protecting your network, applications, and data</li> <li>Ensures that users adhere to application usage policies, controlling access to applications such as instant messaging, peer-to-peer, and other corporate applications</li> </ul>
Coordinated Threat Control	<ul style="list-style-type: none"> <li>Leverages robust features and capabilities of Juniper's standalone IDP Series to deliver broad Layer 2 - Layer 7 visibility into application traffic</li> <li>Isolates a threat down to the user or device level—in conjunction with the IDP Series—and employs a specific, configurable policy action against the offending user or device</li> </ul>	<ul style="list-style-type: none"> <li>Addresses and mitigates network insider threats quickly</li> <li>Minimizes network and user downtime</li> </ul>

Table 2: Identity-Enabled Network and Application Control, Visibility, and Monitoring

FEATURES	FEATURE DESCRIPTION	BENEFITS
Federation – UAC – SA Series and IC Series – IC Series	<ul style="list-style-type: none"> <li>• Federation of user sessions between SA Series SSL VPN Appliances and UAC enables seamless provisioning of SSL VPN user sessions into UAC upon login, or alternatively UAC user sessions into SSL VPN at login</li> <li>• Users authenticated to one IC Series appliance may, if authorized, access resources protected by another IC Series UAC Appliance, enabling “follow-me” policies</li> <li>• UAC leverages the Trusted Computing Group’s (TCG) Trusted Network Connect (TNC) standard protocol Interface for Metadata Access Point (IF-MAP) to enable federation</li> </ul>	Provides users—whether remote or local— with seamless access to corporate resources protected by uniform access control policies through a single login, offering a consistent user access experience
Identity-enabled profiler	Correlates user identity and role information to network and application usage	<ul style="list-style-type: none"> <li>• Know who is accessing your network and applications, when the network and applications are being accessed, what is being accessed, and where the user and device have been on your network</li> <li>• Provides valuable, effective tracking and auditing of network and application access</li> <li>• Addresses regulatory compliance and auditing</li> </ul>
Role-based security policy application	Create and apply role-based threat management policies, such as network IDP, network antivirus, network antispayware, and/or network URL filtering	Delivers both dynamic access control <u>and</u> dynamic threat control

Table 3: Standards-Based, Interoperable Access Control

FEATURES	FEATURE DESCRIPTION	BENEFITS
Built on industry standards and proven, best-in-class products	<ul style="list-style-type: none"> <li>• Leverages industry-standards like 802.1X, RADIUS, IPsec, and innovative open standards—such as TNC—to deliver a standards-based access control solution</li> <li>• Leverages the SA Series policy engine and AAA capabilities, RADIUS capabilities from SBR Enterprise Series servers, and 802.1X capabilities from OAC</li> <li>• Leverages existing 802.1X-enabled switches and access points</li> </ul>	<ul style="list-style-type: none"> <li>• Provides standards-based, vendor-agnostic access control and seamless support for existing, heterogeneous network environments</li> <li>• Facilitates quick, simple, and flexible access control deployments without requiring forklift upgrades</li> <li>• Delivers investment protection, and time and cost savings</li> <li>• Alleviates single vendor lock-in</li> </ul>
TNC open standards support	Adopts and provides strong support for the TCG’s TNC open standards for network access control and network security	<ul style="list-style-type: none"> <li>• Enables choice by empowering organizations to select endpoint and network security solutions that meet their needs without concern for interoperability</li> <li>• Enables ease-of-deployment, leading to faster ROI</li> </ul>
IF-MAP support	<ul style="list-style-type: none"> <li>• Adopts and utilizes the TNC’s open standard IF-MAP</li> <li>• Enables integration with third-party network and security devices, including devices that collect and through IF-MAP, share information on the state and status of a network, user and their device</li> <li>• Allows devices to report back to the IC Series serving as MAP (Metadata Access Point) servers, enabling the collected data to be used in formulating policies and appropriate access actions</li> <li>• Enables IC Series to serve as standalone MAP servers, or as mixed IC Series appliances and MAP servers (separate IF-MAP licenses available)</li> <li>• Supports a MAP server running on standalone IC Series or in active/passive cluster pairs</li> </ul>	<ul style="list-style-type: none"> <li>• Integrates existing, third-party network and security devices into the access control platform</li> <li>• Enhances visibility into the state of and actions on or by a network, user and device—and collects and incorporates that data into the access control policy decision process</li> </ul>

Table 3: Standards-Based, Interoperable Access Control (continued)

FEATURES	FEATURE DESCRIPTION	BENEFITS
Windows Statement of Health (SOH) and embedded NAP agent support	<ul style="list-style-type: none"> <li>Allows organizations— through the TNC SOH standard—to leverage their pre-installed Microsoft Windows Vista and XP SP3 clients with UAC for access control</li> <li>Allows the use of the Windows Security Center (WSC) SOH in access control decisions</li> <li>Can pass the SOH to a Microsoft NPS server for external enforcement and validation of the SOH and transmit the information back to the IC Series for use in access control decisions</li> </ul>	<ul style="list-style-type: none"> <li>Streamlines client deployment</li> <li>Simplifies access control rollout and implementation</li> </ul>
Identity-enabled firewalling in the data center	<ul style="list-style-type: none"> <li>Combines UAC's widely adopted, identity-aware capabilities with the robust networking and security services of the SRX Series</li> <li>Allows SRX Series platforms to be employed as UAC enforcement points</li> <li>Available on all SRX Series Services Gateways running Juniper Networks Junos® 9.4 operating system</li> </ul>	Drastically increases scale for data center environments, enabling organizations to leverage enforcement in the world's most demanding and high-performance data centers
EX Series Ethernet Switch interoperability	<ul style="list-style-type: none"> <li>EX3200 and EX4200 interoperate with and serve as enforcement points within UAC—using standards-based 802.1X port-level access control and Layer 2-4 policy enforcement</li> <li>EX Series are enabled to enforce user-based QoS policies, or mirror user traffic to a central location for logging, monitoring, or threat detection</li> </ul>	Delivers a complete, standards-based, best-in-class network access control solution, allowing organizations to enjoy value-added features and economies of scale for support and service

Table 4: Simple, Flexible Deployment

FEATURES	FEATURE DESCRIPTION	BENEFITS
Easy, extended guest access support	<ul style="list-style-type: none"> <li>One-time use accounts can be provided</li> <li>Guest user accounts may also be provisioned with a predefined timeout period</li> <li>Administrators control the maximum time duration allowed</li> </ul>	Enhances and simplifies an organization's ability to provide guest user access to their networks
Centralized policy management	<ul style="list-style-type: none"> <li>Centralized policy management is delivered when UAC is deployed with Network and Security Manager (NSM) and SA Series</li> <li>Common configuration templates that are created can be shared between SA Series (remote access control) and UAC (LAN access control) deployments using NSM</li> <li>NSM also provides a single management server that can configure key components of a UAC deployment</li> </ul>	<ul style="list-style-type: none"> <li>Saves administrative time and cost, and offers a consistent user and administrative experience by delivering common remote and local access control policy implementation and enforcement across a distributed enterprise</li> <li>Makes possible and simplifies enterprise-wide deployment of uniform network access control</li> </ul>
Phased access control deployment	<ul style="list-style-type: none"> <li>Innovative design allows organizations to start controlling access virtually anywhere on their network</li> <li>Audit mode enables organizations to track user and device policy compliance without enforcing policies</li> </ul>	<ul style="list-style-type: none"> <li>Saves access control deployment time and cost</li> <li>Allows users and administrators to become familiar with policies and necessary compliance, and enables organizations to phase in policy compliance enforcement</li> </ul>
Dynamic authentication policy	<ul style="list-style-type: none"> <li>Leverages an organization's existing investments in directories, PKI, and strong authentication</li> <li>Supports 802.1X, RADIUS, LDAP, Microsoft Active Directory, RSA ACE/Server, Network Information Service (NIS), certificate servers (digital certificates/PKI), local login/password, Netegrity SiteMinder (Computer Associates), RSA ClearTrust, Oblix (Oracle), and RADIUS Proxy</li> </ul>	<ul style="list-style-type: none"> <li>Saves time and expense by leveraging and interfacing with existing AAA infrastructures</li> <li>Establishes a dynamic authentication policy for each user session</li> <li>Enables support—through RADIUS Proxy—for deployments where certain authentications are supported by a backend RADIUS server</li> </ul>

Table 4: Simple, Flexible Deployment (continued)

FEATURES	FEATURE DESCRIPTION	BENEFITS
Dynamically addresses unmanageable endpoint devices	Employs media access control (MAC) address authentication via RADIUS, in combination with MAC address whitelisting and blacklisting; or, leverages existing policy and profile stores (through 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, VoIP handsets, etc.	<ul style="list-style-type: none"> <li>Enhances network and application protection</li> <li>Makes it simpler and faster for organizations to deploy access control across their entire network regardless of device manageability</li> <li>Saves time and cost by allowing organizations to employ existing policy and profile stores, or asset discovery/profiling solutions for role- and resource-based access control of unmanageable devices</li> </ul>
UAC Agent localization	<ul style="list-style-type: none"> <li>Provides fully localized UI, online help, installer, and documentation for the UAC Agent, supporting the following languages:                             <ul style="list-style-type: none"> <li>Chinese (Simplified)</li> <li>Chinese (Traditional)</li> <li>French</li> <li>German</li> <li>Japanese</li> <li>Korean</li> <li>Spanish</li> </ul> </li> </ul>	Enables organizations with users for whom English is not their native language to effectively deploy and employ UAC across their distributed enterprise
Granular auditing and logging	<ul style="list-style-type: none"> <li>Provides fine-grained auditing and logging capabilities, including access to the IC Series RADIUS diagnostic log files—delivered in a clear, easy-to-understand format</li> <li>Captures 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</li> </ul>	<ul style="list-style-type: none"> <li>Simplifies the diagnosis and repair of network issues that arise</li> <li>Addresses industry and government regulatory compliance and audits</li> </ul>
Enhanced RADIUS services	<ul style="list-style-type: none"> <li>Checklist Attribute Processing enables authentication requests to be processed based on information in the RADIUS packet before a connection is authenticated</li> <li>Also allows mapping to realms based on RADIUS request attributes</li> </ul>	Increases accuracy and speed of authentication.



## Product Options

The IC4000, IC4500, IC6000, IC6500, and IC6500 FIPS have several hardware and software options available:

Table 5: Product Options

OPTIONS	OPTION DESCRIPTION	APPLICABLE PRODUCTS
Microsoft SOH licenses	The licensing of the System Health Agent (SHA)/System Health Verifiers (SHV) and SOH protocols from Microsoft are addressed, which are key components that enable UAC to support the Microsoft Windows SOH and embedded NAP Agent through the TNC SOH open and standardized protocol, IF-TNCCS-SOH.	IC4000, IC4500, IC6000, IC6500, IC6500 FIPS
UAC Disaster Recovery licenses	UAC's Disaster Recovery licenses address disaster situations without requiring a permanent purchase of user licenses by a customer for those types of contingencies. Also, periodic testing of disaster recovery deployment is enabled while still providing usage when needed. Disaster Recovery licenses are also available for clusters.	IC4000, IC4500, IC6000, IC6500, IC6500 FIPS
Coordinated Threat Control	This is the ability to leverage additional access control and security capabilities through UAC's communications with IDP Series appliances for Coordinated Threat Control based on IDP Series intelligence.	IC4000, IC4500, IC6000, IC6500, IC6500 FIPS
UAC MAP Server licenses	Leveraging the TNC's IF-MAP specification, IC Series (or IC Series appliance cluster) may operate solely as a MAP server with no additional simultaneous endpoint licenses or OAC-ADD-UAC licenses. In this mode, the IC Series (or clustered IC Series appliances) as MAP servers must have a MAP Server license installed. Mixed IC Series and MAP server mode is defined as any IC Series appliance that simultaneously acts as both an IC Series appliance and as a MAP server, where either a simultaneous endpoint license or an OAC-ADD-UAC license has been installed. In this case, the MAP Server license is not required on that IC Series appliance (or IC Series appliance cluster).	IC4500, IC6000, IC6500, IC6500 FIPS
Enhanced Endpoint Security (EES) subscription licenses	In UAC, the Enhanced Endpoint Security system now offers antispymware/antimalware functionality to ensure that unmanaged and managed Microsoft Windows endpoint devices are not running spyware or other malware. Spyware contaminated devices may be quarantined or have restricted end user access based on policy enforcement. Enhanced Endpoint Security's capabilities scan an endpoint's memory for spyware and provide a real time file-system write and execution shield. A base UAC license includes a free Enhanced Endpoint Security user license for two (2) simultaneous users, allowing users to "try before they buy." Subscription licenses for additional Enhanced Endpoint Security users are available.	IC4500, IC6500, IC6500 FIPS
Hot swappable hard disk drives	Redundant, hot swappable hard disk (IC6000); Dual, mirrored hot swappable SATA hard drives (IC6500, IC6500 FIPS)	IC6000, IC6500, IC6500 FIPS
Hot swappable power supplies	Redundant, hot swappable power supply (IC6000); Optional dual, hot swappable power supplies (IC6500, IC6500 FIPS); IC6500 FIPS – Second power supply optional, DC power supplies available	IC6000, IC6500, IC6500 FIPS
Dual, hot swappable fans	Dual, hot swappable fans	IC6000, IC6500, IC6500 FIPS
Four-port 10/100/1000 copper interface card (Standard)	Four-port 10/100/1000 copper interface card (standard)	IC6500 FIPS

## Specifications

	IC4000	IC6000
<b>Dimensions and Power</b>		
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 lb (6.17 kg) typical (unboxed)	28.5 lb (12.94 kg) typical (unboxed)
A/C power supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 260 W	100-240 VAC, 50-60 Hz, 5 A Max, 500 W
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 40 mm ball bearing fans, 1 40 mm ball bearing fan in power supply	2 externally accessible, hot swappable ball-bearing fans
<b>Panel Display</b>		
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
<b>Ports</b>		
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half duplex (auto-negotiation)	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)
Console	One 9-pin serial console port	One 9-pin serial console port
<b>Environment</b>		
Operating temp	50° to 95°F (10° to 35°C)	50° to 95°F (10° to 35°C)
Storage temp	-40° to 158°F (-40° to 70°C)	-40° to 158°F (-40° to 70°C)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 90% noncondensing	5% to 90% noncondensing
Altitude (operating)	-50 to 10,000 ft (3,000 m)	-50 to 10,000 ft (3,000 m)
Altitude (storage)	-50 to 35,000 ft (10,600 m)	-50 to 35,000 ft (10,600 m)
<b>Certifications</b>		
Safety Certifications	EN60950-1:2001+A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	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	FCC Class A, VCCI Class A, CE class A
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract
	IC4500	IC6500 / IC6500 FIPS
<b>Dimensions and Power</b>		
Dimensions (W x H x D)	17.26 x 1.75 x 14.5 in (43.8 x 4.4 x 36.8 cm)	17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
Weight	15.6 lb (7.1 kg) typical (unboxed)	26.4 lb (12 kg) typical (unboxed) (IC6500) 26.9 lb (12.2 kg) typical (unboxed) (IC6500 FIPS)
Rack mountable	Yes, 1U	Yes, 2U, 19 in
A/C power supply	100-240 VAC, 60-50 Hz, 2.5 A Max, 300 W	100-240 VAC, 60-50 Hz, 2.5 A Max, 400 W
System battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	80% minimum, at full load	80% minimum, at full load
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048 in) cold-rolled steel
Fans	Three 40 mm ball-bearing fans, One 40 mm ball-bearing fan in power supply	Two 80 mm hot swap, One 40 mm ball-bearing fan in power supply

## Specifications (continued)

	IC4500	IC6500 / IC6500 FIPS
<b>Panel Display</b>		
Power LED, HD activity, HW alert	Yes	Yes
PS fail	No	Yes
HDD activity and RAID status LEDs	No	Yes
<b>Ports</b>		
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half duplex (auto-negotiation)	Four RJ-45 Ethernet – full or half-duplex (auto-negotiation) (IC6500) Four-port 10/100/1000 copper interface card (IC6500 FIPS)
Management	N/A	One RJ-45 Ethernet - 10/100/1000 full or half duplex (auto-negotiation)
Fast Ethernet	IEEE 802.3u compliant	IEEE 802.3u compliant
Gigabit Ethernet	IEEE 802.3z or IEEE 802.3ab compliant	IEEE 802.3z or IEEE 802.3ab compliant
Console	One RJ-45 serial console port	One RJ-45 serial console port
<b>Environment</b>		
Operating temp	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)
Storage temp	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8% to 90% noncondensing	8% to 90% noncondensing
Relative humidity (storage)	5% to 95% noncondensing	5% to 95% noncondensing
Altitude (operating)	10,000 ft (3,048 m) maximum	10,000 ft (3,048 m) maximum
Altitude (storage)	40,000 ft (12,192 m) maximum	40,000 ft (12,192 m) maximum
<b>Certifications</b>		
Safety certifications	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001	EN60950-1:2001+ A11, UL60950-1:2003, CAN/CSA C22.2 No. 60950-1-03, IEC 60950-1:2001
Emissions certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A
Warranty	90 days; Can be extended with support contract	90 days; Can be extended with support contract

## UAC Agent and UAC Agent-less Mode – Specifications

- The persistent Layer 2 UAC Agent (802.IX client/supplicant) supports Microsoft Windows Vista (32- and 64-bit), Windows XP, and Windows 2000 operating systems; and Apple Mac OS operating system software.
- The persistent Layer 3 UAC Agent supports Microsoft Windows Vista (32- and 64-bit), Windows XP, and Windows 2000 operating systems; Apple Mac OS operating system software; and Linux operating platforms.
- The UAC agent-less mode secures devices running Microsoft Windows, Apple Mac OS, and Linux operating systems and platforms, interoperating with supported browsers including Microsoft Internet Explorer®, Mozilla Firefox®, and Apple Safari®.

For specific, supported operating system software, operating platform, and browser versions please refer to the latest version of the Unified Access Control Supported Platforms document, which may be found at [www.juniper.net/techpubs/software/uac/](http://www.juniper.net/techpubs/software/uac/).

## 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/](http://www.juniper.net/us/en/products-services/).

## Ordering Information

MODEL NUMBER	DESCRIPTION
<b>IC4000</b>	
<b>Base System</b>	
IC4000	IC4000 base system
<b>Endpoint Licenses</b>	
IC4000-ADD-100E	Add 100 simultaneous endpoints to IC4000
IC4000-ADD-250E	Add 250 simultaneous endpoints to IC4000
IC4000-ADD-500E	Add 500 simultaneous endpoints to IC4000
IC4000-ADD-1000E	Add 1,000 simultaneous endpoints to IC4000
IC4000-ADD-2000E	Add 2,000 simultaneous endpoints to IC4000
IC4000-ADD-3000E	Add 3,000 simultaneous endpoints to IC4000
<b>Feature Licenses</b>	
IC4000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC4000
<b>Cluster Licenses</b>	
IC4000-CL	Add clustering on IC4000
<b>Coordinated Threat Control Licenses</b>	
IC4000-ADD-TCTRL	Add Coordinated Threat Control with IC4000 and Juniper Networks IDP Series
<b>Disaster Recovery Licenses</b>	
IC4000-DR	Disaster recovery license for IC4000
IC4000-DR-CL	Disaster recovery license for IC4000 cluster
<b>Microsoft SOH License</b>	
IC4000-SOH	Microsoft SOH license for IC4000
<b>IC4500</b>	
<b>Base System</b>	
IC4500	IC4500 base system
<b>Endpoint Licenses</b>	
IC4500-ADD-25E	Add 25 simultaneous endpoints to IC4500
IC4500-ADD-50E	Add 50 simultaneous endpoints to IC4500
IC4500-ADD-100E	Add 100 simultaneous endpoints to IC4500
IC4500-ADD-250E	Add 250 simultaneous endpoints to IC4500
IC4500-ADD-500E	Add 500 simultaneous endpoints to IC4500
IC4500-ADD-1000E	Add 1,000 simultaneous endpoints to IC4500
IC4500-ADD-2000E	Add 2,000 simultaneous endpoints to IC4500
IC4500-ADD-3000E	Add 3,000 simultaneous endpoints to IC4500
IC4500-ADD-5000E	Add 5,000 simultaneous endpoints to IC4500
<b>Feature Licenses</b>	
IC4500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC4500
<b>Cluster Licenses</b>	
IC4500-CL-250E	Enables clustering for up to 250 simultaneous endpoints on IC4500
IC4500-CL	Add clustering on IC4500
<b>Coordinated Threat Control Licenses</b>	
IC4500-ADD-TCTRL	Add Coordinated Threat Control with IC4500 and Juniper Networks IDP Series
<b>Disaster Recovery Licenses</b>	
IC4500-DR	Disaster recovery license for IC4500
IC4500-DR-CL	Disaster recovery license for IC4500 cluster

MODEL NUMBER	DESCRIPTION
<b>Microsoft SOH License</b>	
IC4500-SOH	Microsoft SOH license for IC4500
<b>IC6000</b>	
<b>Base System</b>	
IC6000	IC6000 base system
<b>Endpoint Licenses</b>	
IC6000-ADD-250E	Add 250 simultaneous endpoints to IC6000
IC6000-ADD-500E	Add 500 simultaneous endpoints to IC6000
IC6000-ADD-1000E	Add 1,000 simultaneous endpoints to IC6000
IC6000-ADD-2000E	Add 2,000 simultaneous endpoints to IC6000
IC6000-ADD-3000E	Add 3,000 simultaneous endpoints to IC6000
IC6000-ADD-5000E	Add 5,000 simultaneous endpoints to IC6000
IC6000-ADD-10000E	Add 10,000 simultaneous endpoints to IC6000
IC6000-ADD-15000E	Add 15,000 simultaneous endpoints to IC6000
IC6000-ADD-20000E	Add 20,000 simultaneous endpoints to IC6000
IC6000-ADD-25000E	Add 25,000 simultaneous endpoints to IC6000
<b>Feature Licenses</b>	
IC6000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC6000
<b>Cluster Licenses</b>	
IC6000-CL	Add clustering on IC6000
<b>Coordinated Threat Control Licenses</b>	
IC6000-ADD-TCTRL	Add Coordinated Threat Control with IC6000 and Juniper Networks IDP Series
<b>Disaster Recovery Licenses</b>	
IC6000-DR	Disaster recovery license for IC6000
IC6000-DR-CL	Disaster recovery license for IC6000 cluster
<b>Microsoft SOH License</b>	
IC6000-SOH	Microsoft SOH license for IC6000
<b>IC6500</b>	
<b>Base System</b>	
IC6500	IC6500 base system
<b>Endpoint Licenses</b>	
IC6500-ADD-100E	Add 100 simultaneous endpoints to IC6500
IC6500-ADD-250E	Add 250 simultaneous endpoints to IC6500
IC6500-ADD-500E	Add 500 simultaneous endpoints to IC6500
IC6500-ADD-1000E	Add 1,000 simultaneous endpoints to IC6500
IC6500-ADD-2000E	Add 2,000 simultaneous endpoints to IC6500
IC6500-ADD-3000E	Add 3,000 simultaneous endpoints to IC6500
IC6500-ADD-5000E	Add 5,000 simultaneous endpoints to IC6500
IC6500-ADD-10000E	Add 10,000 simultaneous endpoints to IC6500
IC6500-ADD-15000E	Add 15,000 simultaneous endpoints to IC6500
IC6500-ADD-20000E	Add 20,000 simultaneous endpoints to IC6500
IC6500-ADD-25000E	Add 25,000 simultaneous endpoints to IC6500
IC6500-ADD-30000E	Add 30,000 simultaneous endpoints to IC6500
<b>Feature Licenses</b>	
IC6500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC6500
<b>Cluster Licenses</b>	
IC6500-CL-500E	Enables clustering for up to 500 simultaneous endpoints on IC6500
IC6500-CL	Add Clustering on IC6500

## Ordering Information (continued)

MODEL NUMBER	DESCRIPTION
<b>Coordinated Threat Control Licenses</b>	
IC6500-ADD-TCTRL	Add Coordinated Threat Control with IC6500 and Juniper Networks IDP Series

<b>Disaster Recovery Licenses</b>	
IC6500-DR	Disaster recovery license for IC6500
IC6500-DR-CL	Disaster recovery license for IC6500 Cluster

<b>Microsoft SOH License</b>	
IC6500-SOH	Microsoft SOH license for IC6500

<b>IF-MAP License</b>	
IC6500-IFMAP	IF-MAP license for IC6500 /IC6500 FIPS
IC6500-CL-IFMAP	IF-MAP license for IC6500 /IC6500 FIPS cluster

<b>IC6500 FIPS Base System</b>	
IC6500FIPS	IC6500 FIPS base system

<b>Endpoint Licenses</b>	
Please refer to IC6500 endpoint licenses ordering information on previous page.	

<b>Feature Licenses</b>	
Please refer to IC6500 feature licenses ordering information.	

<b>Cluster Licenses</b>	
Please refer to IC6500 cluster licenses ordering information.	

<b>Coordinated Threat Control Licenses</b>	
Please refer to IC6500 Coordinated Threat Control licenses ordering information.	

<b>Disaster Recovery Licenses</b>	
Please refer to IC6500 disaster recovery licenses ordering information.	

<b>Microsoft SOH License</b>	
Please refer to IC6500 Microsoft SOH license ordering information.	

<b>Enhanced Endpoint Security (EES) Subscription Licenses</b>	
ACCESS-EES-10U-1YR	10 Concurrent Users, 1 Year
ACCESS-EES-25U-1YR	25 Concurrent Users, 1 Year
ACCESS-EES-50U-1YR	50 Concurrent Users, 1 Year
ACCESS-EES-100U-1YR	100 Concurrent Users, 1 Year
ACCESS-EES-250U-1YR	250 Concurrent Users, 1 Year
ACCESS-EES-500U-1YR	500 Concurrent Users, 1 Year
ACCESS-EES-1000U-1YR	1000 Concurrent Users, 1 Year
ACCESS-EES-2500U-1YR	2500 Concurrent Users, 1 Year
ACCESS-EES-5000U-1YR	5000 Concurrent Users, 1 Year
ACCESS-EES-7500U-1YR	7500 Concurrent Users, 1 Year

MODEL NUMBER	DESCRIPTION
ACCESS-EES-10U-2YR	10 Concurrent Users, 2 Years
ACCESS-EES-25U-2YR	25 Concurrent Users, 2 Years
ACCESS-EES-50U-2YR	50 Concurrent Users, 2 Years
ACCESS-EES-100U-2YR	100 Concurrent Users, 2 Years
ACCESS-EES-250U-2YR	250 Concurrent Users, 2 Years
ACCESS-EES-500U-2YR	500 Concurrent Users, 2 Years
ACCESS-EES-1000U-2YR	1000 Concurrent Users, 2 Years
ACCESS-EES-2500U-2YR	2500 Concurrent Users, 2 Years
ACCESS-EES-5000U-2YR	5000 Concurrent Users, 2 Years
ACCESS-EES-7500U-2YR	7500 Concurrent Users, 2 Years
ACCESS-EES-10U-3YR	10 Concurrent Users, 3 Years
ACCESS-EES-25U-3YR	25 Concurrent Users, 3 Years
ACCESS-EES-50U-3YR	50 Concurrent Users, 3 Years
ACCESS-EES-100U-3YR	100 Concurrent Users, 3 Years
ACCESS-EES-250U-3YR	250 Concurrent Users, 3 Years
ACCESS-EES-500U-3YR	500 Concurrent Users, 3 Years
ACCESS-EES-1000U-3YR	1000 Concurrent Users, 3 Years
ACCESS-EES-2500U-3YR	2500 Concurrent Users, 3 Years
ACCESS-EES-5000U-3YR	5000 Concurrent Users, 3 Years
ACCESS-EES-7500U-3YR	7500 Concurrent Users, 3 Years

<b>Accessories</b>	
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
IC6500-PS	Field upgradeable secondary power supply for IC6500 /IC6500 FIPS
SA-ACC-RCKMT-KIT-1U	SA Series and IC Series rack mount kit - 1U
SA-ACC-RCKMT-KIT-2U	SA Series and IC Series rack mount kit - 2U
SA-ACC-PWR-AC-UK	SA Series and IC Series AC power cord UK
SA-ACC-PWR-AC-EUR	SA Series and IC Series AC power cord EUR
SA-ACC-PWR-AC-JPN	SA Series and IC Series AC power cord JPN

## 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](http://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](http://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.

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