



Juniper Networks Unified Access Control (UAC)

Infranet Controller, UAC Agent and Enforcement Points

Product Description

Juniper Networks UAC delivers comprehensive, adaptable network and application access control for even the most diverse and complex environments, allowing organizations to reduce cost and maximize efficiencies. It offers best-in-class performance and scalability with centralized policy management to ease deployment, administration and management. Juniper Networks UAC combines user identity, device security state and network location information to create a unique, dynamic access control policy, per user and per session. Juniper Networks 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, or at Layer 3 using an overlay deployment. It can be provisioned in mixed mode using 802.1X for network admission control and a Layer 3 overlay deployment for resource access control. Juniper Networks UAC fully integrates with 802.1X-enabled access points or switches from any vendor, including Juniper Networks EX-series Ethernet switches, to deliver rich policy enforcement capabilities. You can leverage your existing 802.1X infrastructure, Juniper Networks firewalls, or both for policy enforcement and granular access control without the need to re-deploy anything. Juniper Networks UAC enables you to phase your access control deployments and can be run in audit mode, allowing you and your users to ease into access control enforcement. Juniper Networks UAC also dynamically addresses support for unmanageable endpoint devices, enabling you to leverage your existing policy and profile stores, asset discovery or asset profiling solutions for role and resource-based access control.

Not only is the standards-based Juniper Networks UAC vendor-agnostic for 802.1X deployments, but Juniper Networks is a strong supporter of the open standards and specifications from the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Work Group, which ensures interoperability with a host of network and security offerings. Through its support for the TNC standard Statement of Health (SOH) protocol, Juniper Networks 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.

Juniper Networks UAC also leverages other network components to ensure secure network and application access control, address specific use cases, and centralize policy management across the network. It integrates the capabilities of the standalone Juniper Networks Intrusion Detection and Prevention (IDP) platforms to deliver broad application traffic visibility. This mitigates insider threats by enabling you to isolate threats to the user or device level and to employ an applicable policy action against an offending user or device. Juniper Networks UAC ties user identity and role information to network and application access, addressing the demands of regulatory compliance and audits. And, the implementation and enforcement of consistent remote and local access control policy across the distributed network is assured when Juniper Networks UAC is deployed with Juniper Networks Network and Security Manager (NSM) and its market-leading Juniper Networks Secure Access SSL VPN appliances.

Organizations need an access control solution that is flexible and continues to evolve to address the issues vital to a business' security and success. Juniper Networks Unified Access Control (UAC) reduces threat exposure, delivers comprehensive access control, visibility, and monitoring, and centralizes policy management. It is a uniquely flexible, open, standards-based solution that reduces the cost and complexity of delivering granular network access control from the branch to the corporate data center. It also helps you address access control pain points like insider threats, guest user access, and off-shoring/outsourcing. Juniper Networks UAC delivers scalable, adaptable access control that reduces security, regulatory compliance, and business continuity risk, while protecting networks, mission-critical applications, and sensitive data.

Juniper Networks UAC is comprised of:

Infranet Controller

At the heart of Juniper Networks UAC is the Infranet Controller—a hardened, centralized policy management server that can push the UAC Agent to the endpoint to obtain user authentication, endpoint security state, and device location data. (The Infranet Controller can gather this same information through UAC's agent-less mode.) The Infranet Controller uses this information 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 EX 3200 and EX 4200 series switches and any Juniper Networks firewall/VPN platform. The Infranet Controller manages and administers access control prior to session login and throughout the session. No forklift upgrade of existing infrastructure is required to deploy the Infranet Controller. It leverages Juniper's market-leading Secure Access SSL VPN policy control engine to seamlessly integrate with your existing AAA/identity and access management infrastructure. The Infranet Controller also features integrated RADIUS capabilities from Juniper Networks Steel-Belted Radius® (SBR), which enables support for an 802.1X transaction when an endpoint enters the network. It centralizes 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 Infranet Controller appliance with your existing, vendor-agnostic 802.1X switches or access points or Juniper Networks firewall platforms. The Infranet Controller is available in several different form factors: the Infranet Controller 4000 (IC 4000), the Infranet Controller 4500 (IC 4500), the Infranet Controller 6000 (IC 6000), and the Infranet Controller 6500 (IC 6500). The IC 4000 and IC 4500 are designed to address the needs of medium to large organizations or remote/branch offices. These devices scale to handle thousands of simultaneous endpoints and can be deployed in cluster pairs for high availability (HA). The IC 6000 and IC 6500 are designed for use in large organizations and government agencies, offering the capacity to handle tens of thousands of simultaneous endpoints. These devices offer a number of redundant and HA features. The IC 6000 offers a hot-swappable power supply and field-upgradeable hard disk. The IC 6500 offers a dual, hot-swappable mirrored SATA hard drive, dual, hot-swappable fans and, as an option, dual, hot-swappable power supplies. The IC 6000 and IC 6500 can be deployed in multi-unit clusters to increase performance and provide additional scalability, with the ability to handle multiple tens of thousands of simultaneous endpoints.

UAC Agent

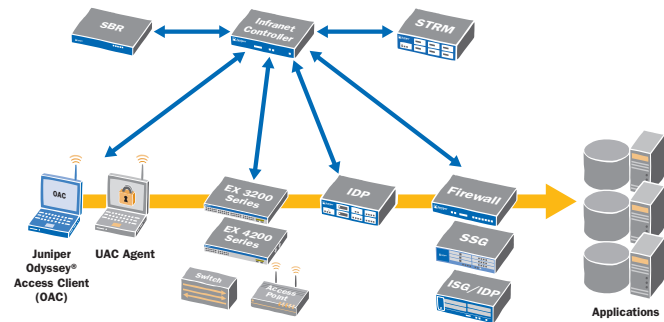
The UAC Agent is a dynamically downloadable agent that can be preconfigured through the Odyssey® Client Administrator (OCA), provisioned in real-time by the Infranet Controller, installed using Juniper's Installer Service, or deployed by other means. The same UAC Agent can be used in wired, wireless, 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 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) 802.1X client/supplicant and 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 Secure Access 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, anti-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. The UAC Agent's Host Checker can assess an endpoint during machine authentication, enabling the device to be mapped to a different role and placed into remediation based on the assessment results. Deployment is simplified through pre-defined Host Checker policies and the automatic monitoring of antivirus signatures and patches for the latest definition files for posture assessment. The UAC Agent supports the most popular enterprise computing platforms. And, the UAC Agent can be delivered based on role, linking agent-based or agent-less access dynamically to user or device identity.

UAC Enforcement Points

UAC enforcement points include any 802.1X compatible switch, including Juniper Networks EX 3200 and EX 4200 series switches, 802.1X-enabled wireless access points, and/or any Juniper Networks firewall/VPN platform. Juniper Networks firewall products, including the Secure Services Gateway (SSG) appliances and Integrated Security Gateways (ISG) with IDP modules, act as Layer 3 - 7 overlay enforcement points. 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. Juniper Networks EX 3200 and EX 4200 series switches 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 Juniper Networks UAC, Juniper Networks EX 3200 and EX 4200 series switches 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 the market-leading Juniper Networks IDP products. Juniper Networks firewalls and switches deliver best-in-class firewall functionality and unprecedented access control deployment flexibility. Some Juniper Networks firewalls also support Unified Threat Management (UTM) capabilities including Juniper Networks IDP functionality, network-based antivirus, anti-spam, anti-adware, anti-phishing, and Web filtering capabilities. These capabilities

can be dynamically leveraged as part of a Juniper Networks UAC solution to enforce and unify access control and security policies on a per user and per session basis to deliver comprehensive network access and threat control. UAC enforcement points can also be implemented in transparent mode which requires no rework of routing and policies or changes to the network infrastructure; they can be also set up in audit mode to determine compliance without enforcement.



Juniper Networks Unified Access Control (UAC) works with network components to deliver comprehensive network and application access control

Features and Benefits

Advanced Network and Application Protection

Feature	Feature Description	Benefit
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, including vendor-agnostic 802.1X-enabled switches, including the Juniper Networks EX 3200 and EX 4200 series switches, access points, and any Juniper firewall/VPN platform.	<ul style="list-style-type: none"> Ensures uniform network protection and enforcement of session-specific access policy by user. Saves deployment cost and time, and delivers network investment protection.
Agent-less Deployment	Agent-less deployment with cross platform support.	<ul style="list-style-type: none"> Ensures the enforcement of network security policies across all platforms and environments. Secures Mac OS, Linux, and Solaris platforms in situations where client downloads are not feasible, such as guest user access.
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 and post-authentication throughout the session.
Coordinated Threat Control	<ul style="list-style-type: none"> Leverages the robust features and capabilities of Juniper's standalone IDP platforms to deliver broad Layer 2-7 visibility into application traffic. In conjunction with the Juniper Networks IDP platforms, the ability to isolate a threat down to the user or device level and employ a specific, configurable policy action against the offending user or device. 	<ul style="list-style-type: none"> Delivers strong interoperability with market-leading Juniper Networks IDP products. Quickly addresses and mitigates network "insider threats." Minimizes network and user downtime.
Dynamically Addresses Unmanageable Endpoint Devices	Employs media access control (MAC) address authentication via RADIUS, in combination with MAC address white listing and black listing; or, leverages existing policy and profile stores (through 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, VoIP handsets, and so on.	<ul style="list-style-type: none"> Enhances network and application protection. Makes it simpler and faster for organizations to deploy access control across their entire network regardless of device manageability. 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.
Self-Administering Platform	<ul style="list-style-type: none"> Delivers a platform that intelligently quarantines non-compliant users and devices and extends automatic remediation capabilities. Enables customers to automatically quarantine and remediate devices that do not meet policy prior to allowing them on to the network and during their network session. Devices are dynamically mapped to an access role upon remediation. 	<ul style="list-style-type: none"> Automatic remediation for many non-compliant devices, without requiring user intervention or other assistance. Minimizes downtime and help desk calls, increasing user and support staff productivity. Saves time and cost.
Pre-defined Patch Assessment Checks	<ul style="list-style-type: none"> Patch assessment checks of devices through OEM integration of Shavlik Technologies' Shavlik NetChk® Protect predefined patch assessment technologies, including endpoint inspection for targeted operating system or application hot fixes. Simple policy definition by directly linking 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 that enforces or denies access to certain roles. 	Enables more enhanced, granular endpoint device health and security state assessments.

Network and Application Control, Visibility, and Monitoring

Feature	Feature Description	Benefit
Identity-Enabled Profiler	Correlates user identity and role information to network and application usage.	<ul style="list-style-type: none"> Know who is accessing your network and applications, when they are being accessed, and what they are accessing. More effective tracking and auditing of network and application access. Directly addresses regulatory compliance and auditing.
Role-based Security Policy Application	The ability to create and apply role-based threat management policies, such as network IDP, network antivirus, network spyware, and/or network URL filtering.	<ul style="list-style-type: none"> Delivers both dynamic access control and dynamic threat control.
Granular Auditing and Logging	Fine-grained auditing and logging capabilities, including access to the Infranet Controller's RADIUS diagnostic log files, delivered in a clear, easy to understand format.	<ul style="list-style-type: none"> 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 RADIUS logs also enhance the diagnosis and repair of network issues that arise.

Adaptable, Scalable Access Control

Feature	Feature Description	Benefit
TNC Open Standards Support	Strong support for the TCG's TNC open standards for network access control and network security.	<ul style="list-style-type: none"> Enables choice by empowering organizations to select endpoint and network security solutions that meet their needs without worrying about interoperability. Enables ease-of-deployment, leading to faster return on investment (ROI).
Interoperability with Juniper Networks EX-series Ethernet Switches	<ul style="list-style-type: none"> Juniper Networks EX 3200 and EX 4200 series Ethernet switches interoperate with and serve as enforcement points within Juniper Networks UAC, using standards-based 802.1X port level access control and Layer 2 - 4 policy enforcement. Enables EX-series switches to enforce user-based QoS policies, or mirror user traffic to a central location for logging, monitoring, or threat detection. 	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.
Built on Industry-Proven, Best-in-Class Products	Leverages Juniper Networks Secure Access SSL VPN policy engine, RADIUS capabilities from Juniper Networks SBR, and 802.1X capabilities from Juniper Networks OAC.	<ul style="list-style-type: none"> Ensures dependability, and interoperability with existing, heterogeneous network infrastructures. Delivers investment protection, and time and cost savings.

Simple, Flexible Deployment

Feature	Feature Description	Benefit
Centralized Policy Management	<ul style="list-style-type: none"> Delivers centralized policy management when deployed with Juniper Networks Network and Security Manager (NSM) and Secure Access SSL VPN appliances. Create common configuration templates that can be shared between Secure Access SSL VPN (remote access control) and UAC (LAN access control) deployments using Juniper Networks NSM. Juniper Networks NSM also delivers a single management server that can configure many key components within a Juniper Networks UAC deployment. 	<ul style="list-style-type: none"> Delivers consistent remote and local access control policy implementation and enforcement across a distributed network. Makes possible and simplifies enterprise-wide deployment of uniform network access control.
Open, Standards-based Solution	<ul style="list-style-type: none"> Leverages industry-standards like 802.1X, RADIUS, IPSec, and innovative open standards, such as TNC to deliver a standards-based access control solution. Leverages existing 802.1X-enabled switches and access points. 	<ul style="list-style-type: none"> Delivers standards-based, vendor-agnostic access control and seamless support for heterogeneous networking environments. Facilitates quick, simple, and flexible access control deployments without requiring forklift upgrades, saving time and cost. No single vendor lock-in.
Phased Access Control Deployment	<ul style="list-style-type: none"> Innovative design allows organizations to start controlling access virtually anywhere on their network. Audit mode enables organizations to track user and device policy compliance without enforcing policies. 	<ul style="list-style-type: none"> Saves access control deployment time and cost. Enables users to become familiar with policies and necessary compliance and allows organizations to phase in policy compliance enforcement.
Windows Statement of Health (SOH) and Embedded NAP Agent Support	<ul style="list-style-type: none"> Through the TNC SOH standard, allows organizations to leverage their pre-installed Microsoft Windows Vista and XP (SP3) clients with UAC for access control. Allows the use of the Windows Security Center (WSC) SOH in access control decisions. Can pass the SOH to a Microsoft NPS server for external enforcement and validation of the SOH and transmit the information back to the Infranet Controller for use in access control decisions. 	<ul style="list-style-type: none"> Streamlines client deployment. Simplifies access control rollout and deployment.

Simple, Flexible Deployment (continued)

Feature	Feature Description	Benefit
Dynamic Authentication Policy (Leveraging Existing AAA Investments)	<ul style="list-style-type: none"> Leverages an organization's existing investment in directories, PKI, and strong authentication. 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. 	<ul style="list-style-type: none"> Establishes a dynamic authentication policy for each user session. RADIUS Proxy enables support for deployments where certain authentications are supported by a backend RADIUS server.
Automatic Realm Decisions Based on Authentication Protocols	Infranet Controller can be configured to make a realm selection based on the authentication protocol in the request.	Improves and eases the administrative experience by offering a simple way to solve a complex challenge without requiring complicated authentication schemes or configuration issues.
Role-based UAC Agent Download	Agent downloads can be based on role and dynamically delivered in the appropriate manner (agent-based or agent-less).	Enables agent-less or agent-based access to be dynamically linked to a user and/or device identity, instead of forcing an upfront selection.

Product Options

The IC 4000, IC 4500, IC 6000 and IC 6500 have several hardware and software options that can be added to the products.

Table 1. Product Options

Option	Option Description	Applicable Products
Microsoft SOH Licenses	Addresses the licensing of the System Health Agent (SHA)/System Health Verifiers (SHV) and SOH protocols from Microsoft, which are key components that enable Juniper Networks UAC to support the Microsoft Windows SOH and embedded NAP Agent through the TNC SOH open and standardized protocol, IF-TNCCS-SOH.	IC 4000, IC 4500, IC 6000, IC 6500
Infranet Controller 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 enables periodic testing of disaster recovery deployment while still providing usage when needed. Also available for clusters.	IC 4000, IC 4500, IC 6000, IC 6500
Coordinated Threat Control	The ability to leverage additional access control and security capabilities through UAC's communications with Juniper Networks IDP platforms for coordinated threat control based on Juniper Networks IDP intelligence.	IC 4000, IC 4500, IC 6000, IC 6500
Hot swappable hard disk drives	Redundant hot swappable hard disk (IC 6000); dual, mirrored hot swappable SATA hard drives (IC 6500).	IC 6000, IC 6500
Hot swappable power supplies	Redundant hot swappable power supply (IC 6000); optional dual, hot swappable power supplies (IC 6500).	IC 6000, IC 6500
Dual, hot swappable fans	Dual, hot swappable fans.	IC 6500

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 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 Watts	100-240 VAC, 50-60 Hz, 5 A 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 40 mm ball bearing fans, 1 40 mm 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 (3,000 m)	
Altitude (storage)	-50 to 35,000 ft (10,600 m)	
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	
	IC 4500	IC 6500
Dimensions and Power		
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)
Rack Mountable	Yes, 1U	Yes, 2U, 19 inch
A/C Power Supply	100-240 VAC, 50-60 Hz, 2.5 A Max, 300 Watts	100-240 VAC, 50-60 Hz, 2.5 A Max, 400 Watts
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
Panel Display		
Power LED, HD Activity, HW Alert	Yes	Yes
HD Activity and Fail LED on Drive Tray	No	Yes

Specifications (continued)

	IC 4500	IC 6500
Ports		
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)	Four RJ-45 Ethernet – full or half-duplex (auto-negotiation) SFP module optional
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	
Console	One RJ-45 serial console port	
Environment		
Operating Temp	41° to 104° F (5° to 40° 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)	10,000 ft (3,048 m) maximum	
Altitude (storage)	40,000 ft (12,192 m) maximum	
Certifications		
Safety Certifications	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	
Warranty	90 days; Can be extended with support contract	

Ordering Information

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

Model Number	Description
Infranet Controller 4000 Base System	
IC4000	Infranet Controller 4000 (IC 4000) Base System
Endpoint Licenses	
IC4000-ADD-100E	Add 100 simultaneous endpoints to IC 4000
IC4000-ADD-250E	Add 250 simultaneous endpoints to IC 4000
IC4000-ADD-500E	Add 500 simultaneous endpoints to IC 4000
IC4000-ADD-1000E	Add 1,000 simultaneous endpoints to IC 4000
IC4000-ADD-2000E	Add 2,000 simultaneous endpoints to IC 4000
IC4000-ADD-3000E	Add 3,000 simultaneous endpoints to IC 4000
Feature Licenses	
IC4000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC 4000
Clustering Licenses	
IC4000-CL	Add Clustering on IC 4000
Coordinated Threat Control Licenses	
IC4000-ADD-TCTRL	Add Coordinated Threat Control with IC 4000 and Juniper Networks IDP
Disaster Recovery Licenses	
IC4000-DR	Disaster Recovery License for IC 4000
IC4000-DR-CL	Disaster Recover License for IC 4000 Cluster
Microsoft SOH License	
IC4000-SOH	Microsoft SOH License for IC 4000
Infranet Controller 4500 Base System	
IC4500	Infranet Controller 4500 (IC 4500) Base System

Model Number	Description
Endpoint Licenses	
IC4500-ADD-25E	Add 25 simultaneous endpoints to IC 4500
IC4500-ADD-50E	Add 50 simultaneous endpoints to IC 4500
IC4500-ADD-100E	Add 100 simultaneous endpoints to IC 4500
IC4500-ADD-250E	Add 250 simultaneous endpoints to IC 4500
IC4500-ADD-500E	Add 500 simultaneous endpoints to IC 4500
IC4500-ADD-1000E	Add 1,000 simultaneous endpoints to IC 4500
IC4500-ADD-2000E	Add 2,000 simultaneous endpoints to IC 4500
IC4500-ADD-3000E	Add 3,000 simultaneous endpoints to IC 4500
IC4500-ADD-5000E	Add 5,000 simultaneous endpoints to IC 4500
Feature Licenses	
IC4500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC 4500
Clustering Licenses	
IC4500-CL-250E	Enables Clustering for up to 250 simultaneous endpoints on IC 4500
IC4500-CL	Add Clustering on IC 4500
Coordinated Threat Control Licenses	
IC4500-ADD-TCTRL	Add Coordinated Threat Control with IC 4500 and Juniper Networks IDP
Disaster Recovery Licenses	
IC4500-DR	Disaster Recovery License for IC 4500
IC4500-DR-CL	Disaster Recover License for IC 4500 Cluster
Microsoft SOH License	
IC4500-SOH	Microsoft SOH License for IC 4500

Ordering Information (continued)

Model Number	Description
Infranet Controller 6000 Base System	
IC6000	Infranet Controller 6000 (IC 6000) Base System
Endpoint Licenses	
IC6000-ADD-250E	Add 250 simultaneous endpoints to IC 6000
IC6000-ADD-500E	Add 500 simultaneous endpoints to IC 6000
IC6000-ADD-1000E	Add 1000 simultaneous endpoints to IC 6000
IC6000-ADD-2000E	Add 2000 simultaneous endpoints to IC 6000
IC6000-ADD-3000E	Add 3000 simultaneous endpoints to IC 6000
IC6000-ADD-5000E	Add 5000 simultaneous endpoints to IC 6000
IC6000-ADD-10000E	Add 10000 simultaneous endpoints to IC 6000
IC6000-ADD-15000E	Add 15000 simultaneous endpoints to IC 6000
IC6000-ADD-20000E	Add 20000 simultaneous endpoints to IC 6000
IC6000-ADD-25000E	Add 25000 simultaneous endpoints to IC 6000
Feature Licenses	
IC6000-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC 6000
Clustering Licenses	
IC6000-CL	Add Clustering on IC 6000
Coordinated Threat Control Licenses	
IC6000-ADD-TCTRL	Add Coordinated Threat Control with IC 6000 and Juniper Networks IDP
Disaster Recovery Licenses	
IC6000-DR	Disaster Recovery License for IC 6000
IC6000-DR-CL	Disaster Recover License for IC 6000 Cluster
Microsoft SOH License	
IC6000-SOH	Microsoft SOH License for IC 6000
Infranet Controller 6500 Base System	
IC6500	Infranet Controller 6500 (IC 6500) Base System
Endpoint Licenses	
IC6500-ADD-100E	Add 100 simultaneous endpoints to IC 6500
IC6500-ADD-250E	Add 250 simultaneous endpoints to IC 6500
IC6500-ADD-500E	Add 500 simultaneous endpoints to IC 6500
IC6500-ADD-1000E	Add 1,000 simultaneous endpoints to IC 6500
IC6500-ADD-2000E	Add 2,000 simultaneous endpoints to IC 6500
IC6500-ADD-3000E	Add 3,000 simultaneous endpoints to IC 6500
IC6500-ADD-5000E	Add 5,000 simultaneous endpoints to IC 6500
IC6500-ADD-10000E	Add 10,000 simultaneous endpoints to IC 6500
IC6500-ADD-15000E	Add 15,000 simultaneous endpoints to IC 6500

Model Number	Description
Endpoint Licenses (continued)	
IC6500-ADD-20000E	Add 20,000 simultaneous endpoints to IC 6500
IC6500-ADD-25000E	Add 25,000 simultaneous endpoints to IC 6500
IC6500-ADD-30000E	Add 30,000 simultaneous endpoints to IC 6500
Feature Licenses	
IC6500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC 6500
Clustering Licenses	
IC6500-CL-500E	Enables Clustering for up to 500 simultaneous endpoints on IC 6500
IC6500-CL	Add Clustering on IC 6500
Coordinated Threat Control Licenses	
IC6500-ADD-TCTRL	Add Coordinated Threat Control with IC 6500 and Juniper Networks IDP
Disaster Recovery Licenses	
IC6500-DR	Disaster Recovery License for IC 6500
IC6500-DR-CL	Disaster Recover License for IC 6500 Cluster
Microsoft SOH License	
IC6500-SOH	Microsoft SOH License for IC 6500
Accessories	
IC6000-HD	Field Upgradeable Secondary Hard Disk for IC 6000
IC6000-FAN	Field Upgradeable Fan for IC 6000
IC6000-PS	Field Upgradeable Secondary Power Supply for IC 6000
IC6500-PS	Field Upgradeable Secondary Power Supply for IC 6500
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 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.



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
Aldershot
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
111.1 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright ©2008 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. JUNOSe is a trademark 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.

100137-007 Aug 2008

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