IC6500 FIPS UNIFIED ACCESS CONTROL APPLIANCE

Product Overview

Daily, government agencies and secure enterprises around the world perform a tenuous balancing act: They must ensure the security of their networks, critical resources, and sensitive—sometimes top secret—information, while delivering timely and pervasive network and data access for employees, contractors, and other authorized users. Many of these organizations are required to deploy network security and access control offerings certified compliant with rigorous, government-approved standards, but are bound by budget cuts. Uniquely positioned to address these needs, Juniper Networks delivers a standards-based access control appliance with a government-certified security module. It's the heart of a comprehensive, flexible, and dependable commercially available network access control (NAC) solution, Unified Access Control that leverages the network you have in place today.

Product Description

A market leader and pioneer in standards-based network access control (NAC), Juniper Networks delivers comprehensive, adaptable network and application access control with Juniper Networks® Unified Access Control (UAC). By combining user identity, device security state, and network location information, UAC empowers organizations to create and enforce unique, dynamic access control policy—per user and per session. UAC offers best-in-class performance, scalability, and centralized policy management to ease deployment, administration, and management.

At the heart of UAC are the Juniper Networks IC Series Unified Access Control Appliances—hardened policy management servers that centralize pre-authentication assessment, authentication, role-mapping, and resource controls in one location. Access control can be deployed and implemented quickly and simply within any existing heterogeneous network using a single IC Series UAC Appliance with existing vendor-agnostic 802.1X access points or switches—including the Juniper Networks EX Series Ethernet Switches, as well as any Juniper Networks firewall platform, J Series Services Routers, or standalone IDP Series Intrusion Detection and Prevention Appliances. No forklift upgrade or rip-and-replace of your existing infrastructure is required.

IC Series appliances are available in several different form factors, including the Juniper Networks IC6500 FIPS Unified Access Control Appliance. The IC6500 FIPS UAC Appliance is built to meet the needs of the most demanding and complex government agencies and secure enterprise environments. It delivers the same functionality available on the Juniper Networks IC6500 UAC Appliance, which includes scaling to support up to tens of thousands of simultaneous endpoint devices. The IC6500 FIPS, though, adds a dedicated FIPS 140-2 Level 3 certified hardware security module to handle all cryptographic operations. The IC6500 FIPS also includes tamper evident labels that deter physical security breaches and provide a visual indication of device integrity. It can be deployed standalone or in three-unit clusters to increase performance and provide additional scalability. The IC6500 FIPS appliance, like the IC6500, also offers a number of redundant, field-upgradable high-availability (HA) features—including dual, hot-swappable, mirrored SATA hard drives; dual, hot-swappable fans; and optional hot-swappable power supplies.

Architecture and Key Components

Juniper Networks UAC is composed of the following:

IC Series Unified Access Control Appliances

The Juniper Networks IC Series Unified Access Control Appliances, such as the IC6500 FIPS, are the hardened, centralized policy management servers at the heart of Juniper Networks UAC. They can push the UAC Agent to the user's endpoint to obtain user authentication, endpoint security state, and device location data. (This same information can be gathered through UAC's agent-less mode, useful in situations where the download of software is not feasible, such as guest access). The IC6500 FIPS appliance uses this information to create dynamic policies that are propagated to UAC enforcement points across the distributed network. Network and application access control is managed by the IC6500 FIPS appliance before session login and throughout the user's network session.

The IC6500 FIPS appliance enables easy setup and administration of network resource policy rules. It also enables dynamic policy changes as the endpoint state or network environment changes. With UAC's adoption of the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) IF-MAP open, standard specification, the IC6500 FIPS can serve as a mixed IC Series appliance and Metadata Access Point (MAP) server, or as a standalone MAP server. When integrated with IF-MAP compliant third-party devices, the IC6500 FIPS can collect data from those devices about the user and device, or the status of the network and leverage that information when formulating policies and appropriate access actions.

UAC Agent and UAC Agent-less Mode

Dynamically downloadable, the UAC Agent collects user and device credentials and assesses the endpoint's security state, reporting this information back to the IC6500 FIPS appliance. It can be provisioned using a variety of automated and offline delivery mechanisms to meet any organizations software distribution needs. A single UAC Agent can be used in wired, wireless, or combined deployments. The UAC Agent provides both Layer 2 (via 802.1X) and Layer 3+ (via firewall enforcement and dynamic IPsec) secure, identity-aware network access. It also includes an integrated, stateful personal firewall that delivers endpoint access control capabilities. The UAC Agent also provides additional functionality for Microsoft Windows devices—such as IPsec VPN as an optional secure transport and single sign-on (SSO) to Microsoft Active Directory. 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 for Apple Macintosh users.

UAC agent-less mode is designed for situations where software downloads are not feasible, such as in guest access. UAC agent-less mode provides the same functionality as the UAC Agent—collecting user and device credentials, assessing endpoint security state, and reporting gathered data to the IC6500 FIPS appliance.

The UAC Agent and UAC's agent-less mode integrate Host Checker functionality, ensuring the enforcement of consistent network security and access policies across all platforms and environments. Host Checker allows you to define network access policy, scans endpoints for various security applications—including antivirus, antimalware, and personal firewalls—and ensures selected applications are installed, running, and up-to-date before granting network access. It also enables custom checks of elements and checks of third-party applications, files, processes, ports, registry keys, and custom DLLs, denying or granting network and application access based on results. With integrated Host Checker, UAC protects your network and endpoint devices from unhealthy, non-compliant, and malicious devices, while allowing you to maintain consistent access control and network security. UAC also checks for specific, defined operating system and application patches. UAC includes industry-tested, dynamic antispyware and antimalware protection for Microsoft Windows endpoint devices, scanning a device's memory registry and load points, pre-authentication, for spyware and keyloggers, and providing automatic remediation, if necessary.

UAC Enforcement Points

UAC enforcement points enforce dynamic, identity-based network access and security policies defined in and distributed by, the IC6500 FIPS appliance. UAC supports enforcement points to meet every networking need, including:

- Any vendor-agnostic 802.1X-compatible switch, including Juniper Networks EX Series switches, and any vendor-agnostic 802.1X-enabled wireless access point for Layer 2 port-based enforcement.
- Any Juniper Networks firewall platform, including the SRX Series Services Gateways as Layer 3+ overlay enforcement points. The Juniper Networks J Series Services Routers also serve as Layer 3 UAC enforcers, delivering Source IP enforcement.
- Juniper Networks IDP Series appliances serving as role-based, application-level policy enforcement points delivering unparalleled visibility into application traffic at Layer 7.

UAC ushers in a new era of granularity and control as the first access control solution to support Layer 2 – Layer 7 policy enforcement.

UAC supports the unified threat management (UTM) capabilities featured in many Juniper Networks firewall platforms—including IPS functionality, network-based antivirus, antispam, antiadware, antiphishing, and Web filtering—dynamically leveraging and applying these capabilities on a per role basis. UAC enforcement points can be implemented in transparent mode, requiring no rework of routing or policies, or changes to network infrastructure. UAC enforcement points can also be deployed in audit mode to determine policy compliance without enforcement, enabling organizations and their users to ease into access control.

Features and Benefits

Worldwide Government-Certified Security

The IC6500 FIPS UAC Appliance is a proven, commercial off-the-shelf (COTS) access control appliance that provides security via a dedicated FIPS 140-2 Level 3 certified hardware security module (HSM), compliant with robust U.S. government security standards also recognized by other nations around the world.

Table 1: Government-Certified Security

Feature	Feature Description	Benefit
FIPS 140-2 Level 3 certified hardware security module (HSM)	• Handles all cryptographic processing as well as key and certificate management. • Complies with the latest best security practices and mandates of the U.S. government. • Recognized by CESG, the U.K. government's National Technical Authority for Information Assurance (IA), as meeting security criteria for use in data traffic categorized as "Private."	• Relieves the appliance CPU of the rigors of cryptographic processing, increasing overall appliance performance while simultaneously delivering a powerful layer of security. • Enables government agencies worldwide to deploy comprehensive, secure, scalable network access control.
Tamper-evident labels	Provides a visual alert to and assurance of the appliance's integrity.	Helps to deter and alleviate physical security breaches.

Identity-Aware Security

UAC delivers identity-aware, granular network and application access control and security, ensuring that only the "right" people can access the network, vital applications, and sensitive data.

Table 2: Identity-Aware Security

Feature	Feature Description	Benefit
Identity-Enabled Profiler	Correlates user identity and role information to network and application usage.	• More effectively track and audit network and application access. • Know who is accessing your network and applications, when they are accessing them, and what they are accessing. • Directly addresses regulatory compliance and auditing.
Coordinated Threat Control	Leverages the robust features and capabilities of the IDP Series Intrusion Detection and Prevention Appliances to deliver broad Layer 2–7 visibility into application traffic, providing the ability to isolate a network threat to the user or device level and then—via UAC and the IC6500 FIPS—employ a specific, configurable policy action against the offending user or device.	• Addresses and mitigates network insider threats quickly. • Minimizes network and user downtime.
Role-based, application-level enforcement	• Leverages deep packet, application-level threat intelligence of standalone IDP Series appliances as enforcement points. • Enables application-specific policy rules to be enforced based on a user's role. • Policies can also be defined to control time of day and bandwidth restrictions per application or per role.	• First access control solution to support full Layer 2 - 7 enforcement. • Enables access control and security policies to be applied to the application-level granularly, protecting your network, applications, and data • Ensures that users adhere to application usage policies.
Identity-enabled firewalling	• The identity-aware capabilities of UAC are combined with the robust networking and security services of SRX Series Services Gateways, employed as UAC enforcement points. • Available on all SRX Series Services Gateways running Junos OS 9.4 software.	Drastically increases scale for data center environments, allowing government agencies and organizations to leverage enforcement in the world's most demanding and high-performance data centers.
EX Series Ethernet Switch interoperability	• The EX3200 Series and EX4200 Series Ethernet switches interoperate with and serve as enforcement points for UAC using standards-based 802.1X port-level access control and Layer 2-4 policy enforcement. • When deployed with UAC, EX Series switches can 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 NAC solution. • Allows government agencies and organizations to enjoy value-added features and economies of scale for support and service.

Open and Standards-Based

Open, standards-based UAC significantly reduces the time to configure and propagate policies across the enterprise, lowering TCO by saving administrative time and cost, ensuring comprehensive, uniform security and access control, and enabling quicker, simpler deployments.

Table 3: Open and Standards-Based

Feature	Feature Description	Benefit
Dynamic authentication policy	· Leverages existing investments in directories, PKI, and strong authentication, establishing a dynamic authentication policy for each user session. · 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.	Saves time and expense by leveraging and interfacing with existing AAA infrastructures.
Industry standards and best-in-class products foundation	· Leverages industry standards such as 802.1X, RADIUS, IPsec, and innovative open standards—such as the TCG's TNC specifications for network access control and security. · Leverages the SA Series policy engine and AAA capabilities, RADIUS capabilities from SBR Enterprise Series servers, and 802.1X capabilities from OAC.	· Delivers standards-based, vendor-agnostic access control and seamless support for existing, heterogeneous networking environments. · Facilitates quick, simple, and flexible access control deployments. No forklift upgrades. · Delivers investment protection, network future-proofing, and time and cost savings. · Alleviates single vendor lock-in, enabling choice.

Enterprise-Wide Access Control

When deployed with Juniper Networks SA Series SSL VPN Appliances, the IC6500 FIPS — and UAC — delivers enterprise-wide access control, saving time and cost by allowing user session data and policies to be shared for local and remote access.

Table 4: Enterprise-Wide Access Control

Feature	Feature Description	Benefit
Federation – IC Series – SA Series and IC Series – IC Series	· Federation of user sessions between SA Series and IC Series appliances, including the IC6500 FIPS, enables seamless provisioning of SSL VPN user sessions into UAC upon login, or alternatively UAC user sessions into SSL VPN at login. · Allows authorized and authenticated users to access resources protected by another IC Series appliance without re-authentication, enabling "follow-me" policies. · Leverages the TNC standard protocol Interface for Metadata Access Point (IF-MAP) to enable federation.	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.
Centralized policy management	· Available when IC6500 FIPS is deployed with Juniper Networks Network and Security Manager (NSM) and SA Series appliances. · Allows common configuration templates to be created and shared between SA Series appliances and IC6500 FIPS appliances via NSM. · NSM also delivers a single management server that can administer and manage key components of a UAC deployment, including the IC6500 FIPS.	· Saves administration time and cost, and offers a consistent user and administrative experience. · Enables the simple enterprise-wide deployment of uniform access control.
IF-MAP support	· Adopts and utilizes the TNC's open standard IF-MAP. · Enables integration with third-party network and security devices, including devices that collect information about the status of a network. · Allows devices to report back to the IC6500 FIPS UAC Appliance serving as a MAP (Metadata Access Point) server, enabling the collected data to be used in formulating policies and appropriate access actions. · Empowers IC6500 FIPS appliances to serve as standalone MAP servers with separate IF-MAP licenses available; or as mixed IC Series UAC Appliances and MAP servers. · Supports a MAP server running on a standalone IC6500 FIPS appliance or in active/passive cluster pairs.	· Leverages and integrates existing, third-party network and security devices as part of the access control platform; and uses the data gathered by these devices to facilitate the access control decision process. · Enhances visibility into the state of and actions on a network.

Proven Endpoint Control

UAC delivers a cross-platform solution that intelligently quarantines and automatically remediates endpoint devices that do not meet policy prior to network access and during their network session, protecting your network, resources, and users.

Table 5: Proven Endpoint Control

Feature	Feature Description	Benefit
Dynamic, preauthentication antispyware/ antimalware protection	• Provides industry-leading, dynamic spyware protection that, before authentication, scans the memory, registry, and load points of endpoint devices for spyware and keyloggers. • Includes automatic remediation for noncompliant devices.Spyware signatures automatically downloaded and updated. • Works with all Windows-based UAC Agents, including Microsoft Windows Vista, as well as in UAC's agent-less mode.	• Ensures unmanaged and managed Windows devices are not running spyware or malware before authentication. • Quarantine or restrict device access through UAC's existing granular policy management framework.
Pre-defined patch assessment checks	• Device patch assessment checks available through OEM integration of Shavlik Technologies' Shavlik NetChk Protect predefined patch assessment technologies, including endpoint inspection for targeted operating system or application hot fixes. • Policies are directly linked to the presence or absence of specific hot fixes for defined operating systems and applications, performing pre-defined patch management checks according to vulnerability severity level to enforce or deny access to certain roles. • Installed Systems Management Server (SMS) is leveraged to automatically check for patch updates, quarantining, remediating, and providing authorized network access once remediated.	• Provides enhanced, granular endpoint device health and security state assessments. • Minimizes user interaction, thereby reducing the possibility of help desk calls.
Windows Statement of Health (SOH) and embedded Network Access Protection (NAP) Agent support	Through the TNC's SOH standard, organizations can leverage pre-installed Microsoft Windows Vista and XP (Service Pack 3) clients with UAC for access control.	• Streamlines client deployment. • Simplifies access control rollout and implementation.

Simple, Flexible Management and Deployment

While network access control can be complex to deploy, UAC simplifies access control management and deployment through its adaptive flexibility, delivering faster ROI.

Table 6: Simple, Flexible Management and Deployment

Feature	Feature Description	Benefit
Phased access control	• 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.	• Saves access control deployment time and cost. • Enables users and administrators to become familiar with policies and necessary compliance and allows organizations to phase in policy compliance enforcement.
Enhanced guest access support	• Dynamically identifies guest users, assigns them roles, and grants them appropriate, differentiated network access. • Enables the creation of one-time use guest accounts on the IC6500 FIPS. • Allows guest accounts to be provisioned with a pre-defined timeout period. • Gives administrators control over all guest access settings, including the maximum time duration a guest is allowed to access the network.	Allows an organization or agency to provide secure, differentiated guest access to its network and resources.

UAC Agent localization	• Provides fully localized UI, online help, installer, and documentation for the UAC Agent, supporting the following languages:
	  - Chinese (Simplified)
	  - Chinese (Traditional)
	  - French
	  - German
	  - Japanese
	  - Korean
	  - Spanish
		Enables organizations with users for whom English is not their native language to effectively deploy and employ UAC across their distributed enterprise.

Table 6: Simple, Flexible Management and Deployment (continued)

Feature	Feature Description	Benefit
Granular auditing and logging	• Offers fine-grained auditing and logging capabilities, delivered in a clear, easy-to-understand format. • Captures detailed logs by roles that users belong to, resources that they try to access, and the state of compliance of the endpoint and user to the security policies of the network.	• Enhances the diagnosis and repair of network issues that arise. • Addresses industry and government regulatory compliance and audits.
Enhanced RADIUS services	• Checklist Attribute Processing enables authentication requests to be processed based on information in the RADIUS packet before a connection is authenticated. • Also allows mapping to realms based on RADIUS request attributes.	• Increases the accuracy and speed of authentication.

Product Options

The IC6500 FIPS has several hardware and software options available:

Table 7: IC6500 FIPS Product Options

Product Option	Option Description
Microsoft SOH licenses	Addresses the licensing of the System Health Agent (SHA)/System Health Verifiers (SHV) and SOH protocols from Microsoft—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.
IC Series UAC Appliances Disaster Recovery licenses	Disaster Recovery licenses address disaster situations without requiring a permanent purchase of user licenses. The licenses enable periodic testing of disaster recovery deployment while still providing usage when needed. Also available for clusters.
Coordinated Threat Control	Leverages additional access control and security capabilities through communications with Juniper Networks IDP Series appliances for coordinated threat control.
UAC MAP Server licenses	Leveraging the TNC's IF-MAP specification, the IC6500 FIPS appliance may operate solely as a MAP server with no additional simultaneous endpoint licenses or OAC-ADD-UAC licenses. In this mode, the IC6500 FIPS appliance (or clustered IC6500 FIPS appliances) as a standalone MAP server must have an IF-MAP license installed. Mixed IC Series appliance and MAP server mode is defined as any IC6500 FIPS 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 IF-MAP license is not required on that IC6500 FIPS appliance (or IC6500 FIPS appliance cluster).
Enhanced Endpoint Security (EES) subscription licenses	UAC offers antispyware/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. EES scans an endpoint's memory, registry and load points for spyware. A base UAC license includes a free EES user license for two (2) simultaneous users, allowing users to "try before they buy." Subscription licenses for additional EES users are available.
Hot-swappable hard disk drives	Dual, mirrored hot-swappable SATA hard drives.
Hot-swappable power supplies	Optional dual, hot-swappable power supplies. (Second power supply optional; DC power supplies available).
Dual, hot-swappable fans	Dual, hot-swappable fans.

IC6500 FIPS

Specifications

Dimensions and Power

- Dimensions (W x H x D): 17.26 x 3.5 x 17.72 in (43.8 x 8.8 x 45 cm)
- Weight: 26.9 lb (12.2 kg) typical (unboxed)
- Rack Mountable: Yes, 2U, 19 in
- AC Power Supply: 100-240 VAC, 60-50 Hz, 2.5 A Max (6 – 2 A), 400 Watts
- System Battery: CR2032 3V lithium coin cell
- Efficiency: 80% minimum, at full load
- Material: 18 gauge (.048 in) cold-rolled steel
- Fans: Two 80 mm hot swap, One 40 mm ball-bearing fan in power supply

Panel Display

- Power LED, HD Activity, HW Alert: Yes
- PS Fail: Yes (audible alarm, blink on HW alert LED, power LED)
- HDD Activity and RAID Status LEDs: Yes

Ports

- Traffic: Four-port 10/100/1000 copper interface card; four ports in total
- Fast Ethernet: IEEE 802.3u compliant
- Gigabit Ethernet: IEEE 802.3z or IEEE 802.3ab compliant
- Console: One RJ-45 serial console port

Environment

- Operating Temp: 41º to 104º F (5º to 40º C)
- Storage Temp: -40º to 158º F (-40º to 70º 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

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
IC6500 FIPS Base System	
IC6500 FIPS	IC6500 FIPS Base System
Endpoint Licenses	
IC6500 -ADD-100E	Add 100 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-250E	Add 250 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-500E	Add 500 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-1000E	Add 1,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-2000E	Add 2,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-3000E	Add 3,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-5000E	Add 5,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-10000E	Add 10,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-15000E	Add 15,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-20000E	Add 20,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-25000E	Add 25,000 simultaneous endpoints to IC6500/IC6500 FIPS
IC6500-ADD-30000E	Add 30,000 simultaneous endpoints to IC6500/IC6500 FIPS
Feature Licenses	
IC6500-OAC-ADD-UAC	Add UAC support to Odyssey Access Clients on IC6500/IC6500 FIPS
Clustering Licenses	
IC6500-CL-500E	Enables clustering for up to 500 simultaneous endpoints on IC6500/IC6500 FIPS
IC6500-CL	Add clustering on IC6500/IC6500 FIPS
Coordinated Threat Control Licenses	
IC6500-ADD-TCTRL	Add Coordinated Threat Control with IC6500/IC6500 FIPS and Juniper Networks IDP Series
Disaster Recovery Licenses	
IC6500-DR	Disaster Recovery license for IC6500/IC6500 FIPS
IC6500-DR-CL	Disaster Recovery license for IC6500/IC6500 FIPS cluster

Model Number	Description
Microsoft SOH License	
IC6500-SOH	Microsoft SOH license for IC6500/IC6500 FIPS
IF-MAP Licenses	
IC6500-IFMAP	IF-MAP license for IC6500/IC6500 FIPS
IC6500-IFMAP-CL	IF-MAP license for IC6500/IC6500 FIPS cluster

Enhanced Endpoint Security (EES) Subscription Licenses

Please refer to the Unified Access Control datasheet — at **www.juniper. net/us/en/local/pdf/datasheets/1000137-en.pdf** - for a complete list of Enhanced Endpoint Security (EES) Subscription Licenses.

Accessories

UNIV-80G-HDD	Field upgradeable secondary 80G hard disk for IC6500 and IC6500 FIPS
UNIV-MR2U-FAN	Field upgradeable fan for IC6500 and IC6500 FIPS
UNIV-PS-400W-AC	400W AC power supply for IC6500 and IC6500 FIPS
UNIV-PS-710W-DC	710W DC power supply for IC6500 and IC6500 FIPS
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 is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

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

1000266-005-EN   Dec 2011   ♻ Printed on recycled paper