



Unified Access Control Solution v2.0: Infranet Controller, UAC Agent and UAC Enforcement Points

Your network must provide access to more diverse users than ever – guests, contractors and mobile employees – some of which have their own devices. Users could download something, become unknowingly infected, and bring those infected devices directly into your network. Or they could just be accessing the Internet from within your LAN without proper security, opening your network to a host of threats. And at the same time that you enable access, you must also control it in a very granular way to protect the company and meet compliance. The Juniper Networks Unified Access Control v2.0 solution helps solve this problem with Layer 3-7 overlay functionality as well as integrated features from both the Odyssey Access Client (OAC) 802.1X supplicant and Steel-Belted Radius (SBR). The result is a uniquely flexible solution that combines user identity, device security state information, and network location to create a session-specific access control policy for each user.

Product Description

Enterprises need a solution that ties together all aspects of the user's identity, device, and network, and can uniformly enforce policy throughout the diverse groups, many of which they do not control. The solution must provide security pre and post authentication, quarantine/remediate non-compliant users, and provide granular network access control. The solution must provide access control for the full range of use cases, including guest users, partners/contractors, and mobile employees, while leveraging existing investments in security and switching infrastructure. Finally, a complete access control solution must be based on open standards, so the enterprise can avoid a single vendor "lock-in."

The Juniper Networks Unified Access Control v2.0 (UAC v2.0) solution combines user identity and device security state information with network location, to create a unique access control policy for each user. The solution can be enabled at Layer 2, using 802.1X, or at Layer 3 using an overlay deployment. UAC v2.0 can also be provisioned in mixed mode, using 802.1X for network admission control and Layer 3 for resource access control.

With UAC v2.0, enterprises are not constrained by:

- Switching infrastructure – UAC interoperates with any vendor's 802.1X enabled switch or access point
- Interoperability issues – not only is UAC vendor-agnostic on 802.1X, but Juniper strongly supports open standards from the Trusted Computing Group's TNC, guaranteeing interoperability with a host of other security vendors
- Use Cases – UAC has a solution for all of the most common use cases, including guest users, contractors, and employees, each of whom need different types of access
- Device types or OS – UAC works with Windows, Mac, Linux and Solaris platforms
- Deployment issues – With UAC, the enterprise can make use of its existing 802.1X infrastructure, Juniper firewalls, or both. Plus deployments can be changed to include both methods for the most granular access control, without having to re-deploy anything.

The products in the UAC v2.0 solution include:

- The Infranet Controller, which functions as the centralized security policy engine as well as the interface with the existing enterprise AAA infrastructure. The Controller also features integrated 802.1X functionality from SBR.
- The UAC Agent, which can be dynamically pushed by the Controller; the Agent includes the means to access the network at Layer 2 via OAC capabilities and Layer 3, as well as Host Checker and Host Enforcer, and a stateful personal firewall, all contained in a single deployment. Access can also be provisioned in agentless mode, in circumstances where downloads of any software are not practical, such as in guest deployments.
- UAC enforcement points, which include the Juniper Networks firewall/VPN appliances, as well as any vendor's 802.1X-enabled wired or wireless switching infrastructure

Infranet Controller

The heart of Juniper's Unified Access Control solution is the Infranet Controller, a hardened policy management server that can push the UAC Agent to the endpoint (or gather information in agentless mode), to get user authentication, endpoint security state and device location. The Infranet Controller combines this information to create dynamic policies, which are then propagated throughout the network to enforcement points, either at the edge of the network prior to granting an IP address via 802.1X, within the network on the firewalls, or both for even greater granularity. The Controllers leverage Juniper's market-leading Secure Access SSL VPN policy control engine to seamlessly integrate with the enterprise's existing AAA/identity and access management infrastructure, and can empower the use of group memberships in authorization directories. These assessments can be repeated at administrator defined times during the session to ensure dynamic policy management and enforcement and also provide granular, policy specific remediation capabilities for non-compliant users. The Infranet Controller can be set up in audit mode to visualize compliance without enforcement.

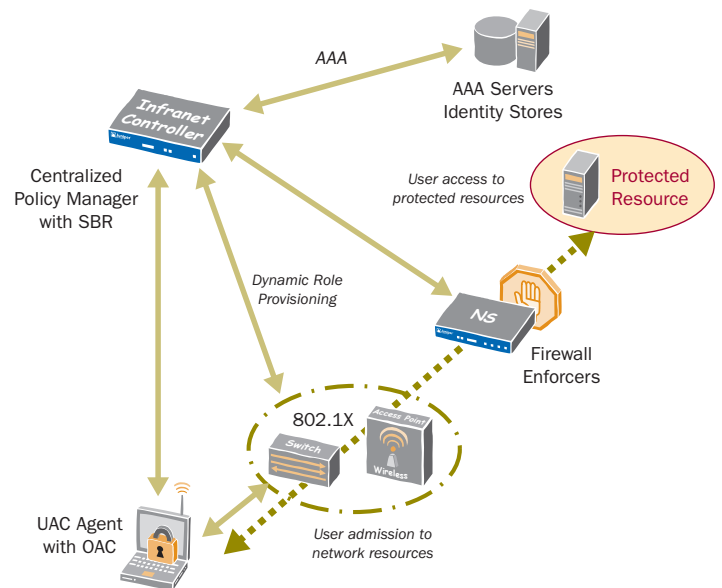
The Infranet Controller is available in two different form factors: Infranet Controller 4000 (IC 4000) and Infranet Controller 6000 (IC 6000). The IC 4000 is designed for the needs of medium enterprises or remote/branch offices. It will scale to handle thousands of concurrent endpoints, and can be deployed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

UAC Agent

The UAC Agent is a dynamically downloadable agent that can be provisioned in real-time by the Controller, installed using Juniper's Installer Service, or deployed by other methods. The Agent includes both integrated 802.1X functionality from Juniper's Odyssey Access Client as well as Layer 3-7 functionality, such as an integrated personal firewall for dynamic client-side enforcement of policies. The Agent also includes specific functionality for Windows devices that includes IPSec VPN (which enables encryption from the endpoint to the firewall) and Single SignOn to Active Directory. The Host Checker functionality enables the administrator to scan endpoints for a variety of security applications/states, including but not limited to antivirus, malware and personal firewalls. UAC also enables custom checks of elements such as registry and port status and can do an MD5 checksum to verify application validity. Deployment is simplified with pre-defined Host Checker policies as well as automatic monitoring of antivirus signature files for the latest definition files for posture assessment.

Enforcement Points

UAC v2.0 enforcement points encompass 802.1X switch/wireless access points and/or overlay enforcement points, which can be any Juniper Networks firewall/VPN platform, including the Secure Services Gateway appliances and Integrated Security Gateways with IDP modules. Support for vendor agnostic 802.1X switches and/or wireless access points enable enterprises to quickly realize the benefits of early access control without requiring a hardware overhaul. The wide variety of Juniper firewalls used as enforcers gives the enterprise both best-in-class firewall functionality and unprecedented access control deployment flexibility. Enforcement points can also be set up in transparent mode, which requires no rework of routing/policies or changes to the network infrastructure. The UAC solution accommodates either 802.1X-based or Layer 3-7 overlay enforcement schemes, and both technologies can also be used together for the most granular access control.



Unified Access Control Solution v2.0

Features and Benefits

Key features and benefits of the Unified Access Control solution can be grouped into three high-level value propositions:

- Combined user identity, device security assessment, network information and policy for dynamic access control
- Standards-based solution
- Leverage existing investments in AAA, switching, and security infrastructure

Combined User Identity, Device Security Assessment, Network Information and Policy for Dynamic Access Control

Feature	Feature Description	Benefit
Infranet Controllers		
Ability to bind endpoint assessment and user identity with real-time network security policy enforcement	Dynamically bind endpoint and user identity to set firewall configurations/rules in real-time	Enables dynamic activation of select Juniper firewall enforcer capabilities, including Intrusion Prevention functionality, Antivirus, logging and Web Filtering, saving time and enforcing security policies
Provisions the UAC Agent	Dynamically provisions the UAC Agent, if required, as well as providing an agentless method for access control	Enables access control for all use cases, including guests, contractors and employees
Leverages Juniper's Secure Access SSL VPN policy engine	Leverages Juniper's Secure Access SSL VPN policy engine	The Secure Access appliance leads the market for SSL VPNs and has been field-tested in thousands of deployments around the world
Leverages Juniper's Steel-Belted Radius	Completes an 802.1X authentication transaction using elements included in the Controller	Does this without the purchase of additional equipment, saving time and money
Two purpose-built, hardened form factors	IC 6000 and IC 4000	Allows the enterprise to choose the best fit for their needs
Single centralized policy engine	Enforces access controls before session login and throughout the session	<ul style="list-style-type: none"> • Pre-authentication assessment, authentication, role mapping and resource controls all in one location • Easy setup and administration of network resource policy rules • No forklift upgrade of existing infrastructure is required to deploy the solution • Dynamic propagation of policy enforcement to the endpoints and the enforcement points, whether they are 802.1X-based, Layer 3 overlay-based, or both • Policy can change as the endpoint or network environment changes
Dynamic authentication policy leverages existing investment in AAA	Support for 802.1X, RADIUS, LDAP, AD, RSA ACE, NIS, Certificate servers (digital certs/PKI), Local login/password, Netegrity SiteMinder (Computer Associates), RSA Cleartrust, and Oblix (Oracle)	Leverages the enterprise's existing investment in directories, PKI, and strong authentication, enabling administrators to establish a dynamic authentication policy for each user session
Dynamic role mapping	Leverages a range of attributes for security requirements that users need to meet before a user login page is presented	Security requirements can be enforced pre-authentication as well as post-authentication throughout the session
Hybrid role- / resource-based policy model	Administrators can tailor access	Ensures that security policies reflect changing business requirements
Granular auditing and logging	Fine-grained auditing and logging capabilities in a clear, easy to understand format	Ensures detailed logging by roles that end 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
Custom instructions for granular quarantine and remediation of non-compliant users	Enables a self-administering platform to intelligently quarantine non-compliant users	Allow users to remediate without any assistance and then they are dynamically mapped to an access role upon remediation
Infranet Agent		
Lightweight agent, dynamically provisioned by the Infranet Controller, if required.	Includes: TNC-compliant for seamless interoperability with any other compliant security solution, Host Enforcer, MS Windows Single SignOn, Native client for IPSEC to the desktop, Agentless enforcement for Mac and Linux	Protects authenticated endpoints from malicious/non-compliant endpoints and allows the enterprise to maintain access control, even if they do not own or manage the endpoint
Endpoint assessment	Can run at login and periodically throughout the user session at administrator-defined intervals	Allows real-time network policy management with pre-defined Host Checks for a wide variety of best-in-class endpoint security solutions; Auto-monitoring of virus signatures
Host Enforcer	Stateful personal firewall, which can also function as a client-side policy enforcer and optional secure transport (authenticated and encrypted) using IPSEC	<ul style="list-style-type: none"> • Provides firewall policy if endpoint is accessing a network segment not protected by 802.1X infrastructure or enforcers • Optional Microsoft IPSEC enforcement provides authenticated and encrypted transport for session integrity and privacy • Authenticated transport ensures that network rules can be enforced in a secure manner • Encrypted transport ensures privacy for communications on the LAN
Agentless deployment	Agentless deployment for cross platform support	Enterprises can secure Mac, Linux, and Solaris platforms by binding endpoint assessment and user identification for source IP-based and continue enforcement of network security policies

Standards-based solution

Feature	Feature Description	Benefit
802.1X-based access control method	802.1X is vendor-agnostic	The enterprise can choose a best fit for equipment without constraints and avoid the dangers of a single vendor solution, which can limit choice in the future
Strong support for the Trusted Computing Group's Trusted Network Connect series of open standards	Strong support for the Trusted Computing Group's Trusted Network Connect series of open standards	Enables the enterprise to choose the security solution that works for them without worrying about interoperability, and ensures maximum choice, which leads to faster return on investment

Leverage existing investments in AAA, switching, and security infrastructure

Feature	Feature Description	Benefit
Leverages existing 802.1X-enabled switches and/or access points	Leverages existing 802.1X-enabled switches and/or access points	Makes it simple for an enterprise to secure a wireless network or 802.1X-based switching infrastructure, without being locked into a single vendor's switching solution
Leverages Juniper's market-leading range of firewalls	Firewalls support throughput ranging from 75 Mbps to 30 Gbps for high performance enforcement of access control policies	<ul style="list-style-type: none"> Enterprise can leverage existing investment in security devices Customers can use UAC to apply security policies such as Intrusion Prevention, Antivirus, and Web Filtering on a per user/session basis. This enables the enterprise to unify the application of access and security policies for comprehensive network access and threat control.
TNC compliant solution	TNC compliant solution	Enables seamless interoperability with any other TNC-compliant product/solution

Product Options

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

Option	Option Description	Applicable Products
Advanced Software Feature Set (includes Central Manager)	Additional sophisticated capabilities that will meet the needs of more complex deployments with diverse audiences and use cases	IC 4000, IC 6000
Redundant hot swappable hard disk	Redundant hot swappable hard disk	IC 6000
Redundant hot swappable power supply	Redundant hot swappable power supply	IC 6000

Specifications

	IC 4000	IC 6000
Dimensions and Power		
Dimensions (W/H/D)	16.7"W x 1.74"H x 15"D (42.42cmW x 4.41cmH x 38.10cmD)	16.7"W x 3.5"H x 16.2"D (42.42cmW x 8.89cmH x 41.15cmD)
Weight	13.6 lb (6.17kg) typical (unboxed)	28.5lb (12.94 kg) typical (unboxed)
A/C Power Supply	100-240VAC, 50-60Hz, 2.5A Max, 260 Watts	100-240VAC, 50-60Hz, 5A Max, 500 Watts
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell
Efficiency	65% minimum, at full load	65% minimum, at full load
MTBF	82 khrs	71 khrs
Material	18 gauge (.048") cold-rolled steel	18 gauge (.048") cold-rolled steel
Fans	3 40mm ball bearing fans, 1 40mm ball bearing fan in power supply	2 externally accessible, hot swappable ball-bearing fans
Panel Display		
Front Panel Power Button	Yes	Yes
Power LED, HD Activity, Temp	Yes	Yes
PS Fail	No	Yes
HDD Activity and RAID Status LEDs	No	Yes
Ports		
Traffic	Two RJ-45 Ethernet - 10/100/1000 full or half-duplex (auto-negotiation)	
Console	One 9-pin serial console port	
Environment		
Operating Temp	50° to 95°F (10°C to 35°C)	
Storage Temp	-40° to 158°F (-40°C to 70°C)	
Relative Humidity (operating)	8% to 90% non-condensing	
Relative Humidity (storage)	5% to 95% non-condensing	
Altitude (operating)	-50 to 10,000 ft (3,000m)	
Altitude (storage)	-50 to 35,000 ft (10,600m)	
Certifications		
Safety Certifications	EN60950-1:2001+A11, UL60950-1:2003, CSA C22.2 No. 60950-1, IEC 60950-1:2001	
Emissions Certifications	FCC Class A, VCCI Class A, CE class A	
Warranty	90 days; Can be extended with support contract	

Ordering Information

Infranet Controller 4000

Base System

IC4000	Infranet Controller 4000 Base System
--------	--------------------------------------

Endpoint Licenses

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

Feature Licenses

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

Clustering Licenses

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

Infranet Controller 6000

Base System

IC6000	Infranet Controller 6000 Base System
--------	--------------------------------------

Endpoint Licenses

IC6000-ADD-250E	Add 250 simultaneous users to IC6000
IC6000-ADD-500E	Add 500 simultaneous users to IC6000
IC4000-ADD-1000E	Add 1000 simultaneous users to IC6000
IC6000-ADD-2000E	Add 2000 simultaneous users to IC6000
IC6000-ADD-3000E	Add 3000 simultaneous users to IC6000
IC6000-ADD-5000E	Add 5000 simultaneous users to IC6000
IC6000-ADD-10000E	Add 10000 simultaneous users to IC6000
IC6000-ADD-15000E	Add 15000 simultaneous users to IC6000
IC6000-ADD-20000E	Add 20000 simultaneous users to IC6000
IC6000-ADD-25000E	Add 25000 simultaneous users to IC6000

Feature Licenses

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

Clustering Licenses

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

Accessories

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

About Juniper

Juniper Networks develops purpose-built, high performance IP platforms that enable customers to support many different services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. 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

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.
Suite 2507-11, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Copyright © 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.