

Juniper UAC 2.1 Channel Partner Frequently Asked Questions (FAQs)

Q: What is Juniper Networks announcing?

On October 8, 2007, Juniper is announcing Unified Access Control (UAC) 2.1, a new software release of our comprehensive network access control solution that advances UAC's ability to meet the evolving access control and security requirements of high-performance businesses.

Q: What are the top messages Juniper is conveying with this launch?

- UAC 2.1 delivers the access control, visibility and monitoring of applications and users needed to more effectively and efficiently sustain regulatory compliance while mitigating risk and exposure to today's rapidly evolving threat landscape.
- UAC 2.1 provides the tools to enable enterprises to quickly, successfully protect their networks and applications for guest networking and from diverse user constituents.
- UAC 2.1 helps reduce the cost and complexity of securing access to networks and applications.
- With UAC 2.1, Juniper is demonstrating continued execution of the company's strategy to provide enterprises with advanced, coordinated visibility and control of applications and users across the extended enterprise.

Q: Why is this announcement important to the industry?

Today, networks and networked applications can no longer be viewed as separate from the business. Access to networks and applications must be pervasive, but remain secure and controlled, with corporate assets – the network and applications – remaining protected. But, as the demand and availability for network and application access has increased, so, too have network risks.

While network access control (NAC) was introduced to handle the threat of managed and unmanaged devices attempting network access, its focus has expanded to address support for unmanageable devices and user based access control, regardless of the user's association (employee, guest, contractor, partner, etc.).

Today, NAC's mission continues to grow, moving beyond preadmission control and endpoint policy assessment to address post admission control, role based application access control, and application and network visibility and monitoring.

By delivering access control, visibility and monitoring of an enterprise's applications and users, Juniper's UAC 2.1 is a comprehensive and cost-effective solution for mitigating exposure to internal and external threats. UAC 2.1 enables different users with varying needs and levels of network and application authorization to access and share resources. UAC 2.1 extends access control to network traffic by implementing security policy enforcement broader and deeper into the network's core and outward to the network's edge, thereby mitigating the risks associated with exposing corporate assets.

Q: What are the most significant enhancements in UAC 2.1?

Juniper UAC 2.1 provides advanced network protection; application visibility, monitoring and control and simplifies network access control deployments. Key innovations and features in Juniper UAC 2.1 include:

- **Coordinated Threat Control:** Leverages the robust features and capabilities of Juniper's Intrusion Detection and Prevention (IDP) platforms to deliver full Layer 3-7

visibility into application traffic, providing IT the ability to isolate a threat down to the user or device level and then employ a specific, configurable policy action against that user or device.

- **Identity-Enabled Profiler:** Ties user identity and role information to network and application usage, enabling enterprise IT to more effectively track and audit network and application access, which in turn helps address regulatory compliance.
- **Unmanageable Device Support:** Dynamically addresses unmanageable endpoint devices, such as printers or voice-over-Internet-Protocol (VoIP) phones, enabling enterprises to leverage existing policy and profile stores or asset discovery solutions for role and resource-based access control.
- **Advanced Security Assessment:** Expands UAC's security assessment capabilities with the integration of Shavlik NetChk® Protect predefined patch management assessment checks, enabling more enhanced, granular endpoint device health and security state assessments.
- **Heterogeneous Endpoint Support:** Extends support for the most popular enterprise computing platforms with a new Layer 2/Layer 3 UAC Agent for the Microsoft® Windows Vista™ platform.
- **Simplified Deployment:** Extends authentication protocol support for supporting phased deployments and provides enhanced automatic remediation capabilities to ensure a seamless end user experience.

Q. What's new in UAC 2.1, and what are the benefits?

Juniper UAC 2.1 delivers coordinated threat control, an identity-enabled profiler, extended support for unmanageable devices and cross-platform endpoints, enhanced endpoint assessment and remediation, and simplified deployment and use.

It also addresses the key network access control (NAC) initiatives of network and application protection, guest user access, and network/application control, visibility, and monitoring, as well as simplifying NAC deployment and usability.

In ensuring the protection of networks and applications, UAC 2.1:

- **Supplies a Layer 2/Layer 3 UAC Agent for the Microsoft® Windows Vista™ platform** providing a unified agent for seamless and comprehensive access control across entire networks, including those with Windows Vista deployments.
- **Dynamically addresses unmanageable endpoint devices**, enabling enterprises to leverage existing policy and profile stores or asset discovery or profiling solutions for role and resource based access control.
- **Delivers coordinated threat control** to enterprises, leveraging full Layer 2 – Layer 7 visibility into application traffic, minimizing downtime and isolating a threat to the user or device level and then employing a configurable policy action against that user or device.
- **Incorporating pre-defined patch management checks** – through its OEM integration of Shavlik NetChk™ Protect – allowing for enhanced, more granular endpoint device health and security state assessments.
- **Delivering a persistent Layer 3 agent for Apple® Macintosh®, Linux, and Solaris platforms**, allowing enterprises to more easily deploy UAC in Layer 3 mode to support heterogeneous endpoint environments.
- **Extending and making automated remediation capabilities** minimizes the number of support calls from noncompliant users.

- **Enabling the integration of 3rd party endpoint compliance checks for non-Windows platforms**, making them more accessible as part of an UAC deployment.

In addressing application control, visibility, and monitoring, UAC 2.1:

- **Delivers an identity enabled profiler**, tying user identity and role information to network and application usage.
- **Leverages deep packet, application level threat intelligence** of Juniper Networks IDP platforms, enabling dynamic threat management.
- **Enables the creation and application of role-based threat management policies**, delivering enterprises the ability to dynamically apply role-based security policies for access and threat control.

And, UAC 2.1 continues to make network access control simple and flexible to deploy and use by:

- **Delivering downloads of the UAC Agent based on role**, linking agent-less or agent-based access dynamically to user and/or device identity.
- **Expanding support to all RADIUS clients**, allowing enterprises to preserve their existing network infrastructure and configurations by supporting value added attributes sent to switches and access points, even those that UAC does not support out-of-the-box.
- **Support for additional authentication protocols and RADIUS processing capabilities** enables enterprises to control access to their network at the Access Layer for a wide variety of deployment scenarios including user authentication for guest users accessing the network with a third party supplicant (not the UAC Agent or OAC).
- **Enabling dynamic downloads of pre-configured UAC Agents** allows enterprises to deploy network access control in their network without the expense of deploying and managing the pre-installation of client software.

UAC 2.1 Pricing, Availability, & Support

Q: When will UAC 2.1 be available?

UAC 2.1 will be announced on Monday, October 8, 2007, and can be ordered now for worldwide delivery at the end of October.

Q: How can enterprises purchase UAC 2.1?

UAC 2.1 can be purchased through standard Juniper distribution and reseller channels.

Q: What level of technical support is available for UAC 2.1?

Juniper offers a suite of services from their J-Care portfolio that offers entitlements from return-to-factory to same-day onsite advanced replacement options. All the support options include 24x7 JTAC, software access, and online tools. Enterprises should work with their J-Partner representatives to determine the best support options to meet their needs. For complete details, please visit

<http://www.juniper.net/products/services/operation/support.html>.

Reseller/Channel Partner Related Questions

Q: Does the UAC solution offer channel partners any opportunities outside of just the product sale? What are they and how are they significant?

Juniper UAC provides channel partners with significant opportunities for additional, add-on product and service sales. For example, additional Juniper products that can be sold with Juniper UAC to increase the size of nearly any deal include:

- Juniper firewall/VPN products
- Odyssey Access Client (OAC)
- Juniper ISG and/or ISG with IDP
- Standalone Juniper IDP appliances
- Steel-Belted Radius (SBR)

There is also an array of pre and post sales services that can be provided by channel partners with sales of Juniper UAC, including, to name just a few:

- NAC/network design and deployment services
- Network/security policy design and integration
- Policy server and client software configuration
- Integration services for existing infrastructure (switches, firewalls, NSM, IDP, etc.)

Q: What does UAC 2.1 offer channel partners that previous versions of UAC could not?

Juniper UAC 2.1 offers several new features and functions that can help channel partners increase their revenues. For instance, UAC 2.1 delivers interoperability with Juniper's standalone IDP and ISG with IDP, which means that channel partners can sell those products as add-ons to a UAC deal. Additionally, UAC 2.1 enables the integration of 3rd party endpoint compliance checks for non-Windows platforms for Java-based Integrity Measurement Collectors (IMCs) and Integrity Measurement Verifiers (IMVs), which are essentially open, standards-based APIs from the Trusted Network Connect (TNC) industry standards. Channel partners can also provide support by developing and integrating these IMC/IMV pairs for platforms other than those that are Windows-based.

Q: What kind of training and tools are available to channel partners to help sell UAC?

Juniper recently launched an Access Control Specialization for our J-Partner channel partners, where they can attain Select or Elite levels in Access Control and the ability to sell the Juniper UAC solution. This Specialization includes certification programs for UAC, with firewall and OAC/802.1X certification programs included as prerequisites. Juniper is working closely with channel partners to address UAC sales and technical training and to inform partners on the ways they can increase UAC-related revenues through services and add-on sales.

Channel partners can contact the Juniper Advanced Technologies (AT) sales and/or Account Management teams for assistance. Juniper also offers:

- A reseller hotline for presales assistance (866-298-6428 extension 2)
- A Partner Center full of information, sales tools, and presentations on or about UAC
(https://www.juniper.net/partners/partner_center/content/reseller/products/uac_kit.jsp)
- A Sales Accelerator for the Controlling Access campaign, which incorporates UAC

(https://www.juniper.net/partners/partner_center/common/sales_tools/controlling_access/controlling_access_kit.jsp)

- Online product demonstrations and labs (ACME Gizmo: Obtain a Login ID and Password from your Channel Account Manager and visit <http://acmegizmo.jnpr.net/>; UAC 2.0 Virtual Training Lab, which provides access to Juniper equipment online to supplement Juniper Technical Certification Programs - https://www.juniper.net/partners/partner_center/common/training/virtual_lab.jsp)
- Specific UAC demonstration incentive programs for partners (J-Partner Demo Bundle (Not for resale): IC4000 with 100 end point license for \$3,000 - https://www.juniper.net/partners/partner_center/content/reseller/nam/selling_tools/promotions.jsp)
- An Access Control advisor, which walks you through what to talk about based on customer attributes (https://www.juniper.net/partners/partner_center/common/sales_tools/aca/index.html)
- J Rewards, which are points for selling Juniper products, where 1 point = \$1; register at www.juniper.net/jrewards

UAC Partner Related Questions

Q: Microsoft Windows Vista™ support is mentioned in the Juniper UAC 2.1 announcement. Does UAC 2.1 address the Juniper UAC/Microsoft NAP interoperability announced in May 2007?

NO. In Juniper UAC 2.1 we are announcing and delivering a Layer 2/Layer 3 UAC Agent for the Windows Vista™ platform that enables deployment of a unified agent for seamless and comprehensive access control – including for Windows Vista deployments – across an entire network.

This announced support for Windows Vista in UAC 2.1 **does not** address the aspects of the May 2007 announcement that Juniper Networks and Microsoft Corporation are working together to provide open standards-based interoperability between Juniper's UAC and Microsoft® Network Access Protection (NAP), based on the NAP primary Statement of Health (SOH) client-server protocol Microsoft contributed to the Trusted Computing Group (TCG), and that the TCG adopted and published as a new Trusted Network Connect (TNC) standard. **A Juniper UAC solution supporting the new TNC standard is expected in the first half of 2008 (1H08).**

Q.: What is the nature of the relationship between Juniper Networks and Shavlik Technologies as it pertains to UAC 2.1?

Juniper Networks has teamed with Shavlik Technologies LLC to integrate advanced security assessment capabilities into UAC 2.1. The two companies have entered into an agreement that enables Juniper to deliver the security scanning capabilities of Shavlik NetChk® Protect as part of Juniper's UAC solution. The integration of a patch management solution based on the scan engine and extensive security patch signature database technology from Shavlik further extends UAC's robust security assessment capabilities and allows more granular endpoint device health and security state assessments. By teaming with Shavlik to deliver integrated, out-of-the-box security assessment capabilities, Juniper is making it easier for customers to better protect their networks and reduce security, regulatory compliance and continuity risks.

Q.: What is the customer benefit of including Shavlik NetChk[®] Protect in UAC 2.1?

Juniper is extending the existing endpoint assessment capabilities of UAC to include support for predefined patch management checks based on the scan engine and extensive security patch signature database technology from Shavlik Technologies' Shavlik NetChk[®] Protect. Shavlik's award-winning patch management solution provides a secure and scalable offering to ensure endpoint security and patch management policy compliance. The predefined patch management checks in UAC 2.1 include the ability to inspect an endpoint device for targeted operating system or application hot fixes. This will enable UAC customers to easily define policies that are directly linked to the presence or absence of specific hot fixes for defined operating systems and/or applications and leveraging this for access control. The predefined patch management checks can be performed according to the severity level of the vulnerability and can be used to enforce or deny access to certain roles.

Q.: Will Juniper's UAC solution support additional patch management solutions moving forward?

YES. Juniper is committed to delivering customers a comprehensive yet flexible solution for network and application access control. We feel that Shavlik has a strong portfolio of patch management and remediation solutions. By providing Shavlik's security assessment capabilities right out of the box, customers can immediately employ comprehensive endpoint assessment as part of their deployment without further cost. If they are currently a Shavlik customer, UAC 2.1 can plug into their existing patch management and remediation environment. Juniper can also support any TNC-compliant patch management solution.

UAC Licensing & Upgrading

Q: Are there any additional licenses required for UAC 2.1?

NO. This is just a software release and can be leveraged by existing customers (under an active maintenance agreement for UAC) free of charge.

HOWEVER, Juniper is introducing two new licenses for UAC 2.1 (IC4000-ADD-TCTRL and IC6000-ADD-TCTRL) that add the ability for UAC 2.1 to communicate with Juniper IDP products for coordinated threat control based on Juniper IDP intelligence.

Q: If I already have UAC 2.0, how can I upgrade to UAC 2.1?

UAC 2.1 is the launch of the next version of UAC software. Existing customers that are under a valid maintenance agreement can upgrade their UAC version and acquire the additional capabilities free of charge.

Q: Will my existing OAC work with UAC 2.1?

YES, your existing version of OAC Enterprise Edition (EE) will work with UAC 2.1.

Q: What are the differences between OAC Enterprise Edition (EE) and the new OAC UAC Edition (UE) for UAC 2.1?

In addition to now supporting Windows Vista as an operating system, the Layer 2/Layer 3 OAC UAC Edition (UE) agent introduces new features and can be preconfigured on Juniper UAC's Infranet Controller policy management appliance, providing tighter control over user-exposed features and settings and allowing access control capabilities to be

introduced without the costly deployment and management issues of preinstalled client software.

The new, downloadable OAC UE now supports:

- Client lock down, where the Infranet Controller can lock down the agent settings that should not be exposed to users
- Configuring profiles that include login names for use, wired and/or wireless adapter configurations, authentication protocols, network SSIDs, and Infranet Controller URLs
- The Infranet Controller can be used to disable the Odyssey Client Administrator and license management settings from being exposed to users

Q: Will my existing Steel-Belted Radius® products work with UAC 2.1?

YES, existing, standalone Steel-Belted Radius (SBR) products will continue to work with UAC 2.1. While UAC 2.1 integrates many of the features that make SBR the most powerful AAA/RADIUS product family available, standalone SBR has still been designed, from the ground up to handle the AAA/RADIUS needs of some of the largest networks in the world, including those of carriers. SBR remains a standalone solution; and, as with UAC 2.0, there is not an upgrade/cross platform fee for SBR to UAC 2.1, as there is for Odyssey Access Client (OAC).

Customer/Market Related Questions

Q. What is the target market for UAC 2.1?

The UAC solution is aimed at enterprises and organizations that are seeking to secure their LAN assets in a scalable and phased manner that does not involve a comprehensive upgrade of their backbone network infrastructure or dictate single vendor lock-in. The UAC 2.1 solution also aids in addressing required regulatory compliance for domestic and international enterprises. Customers can leverage any 802.1X-enabled network infrastructure component or their existing Juniper firewalls as enforcement points for network and application access control through UAC 2.1. This ensures that users who need access to critical resources have to be authenticated and their endpoint security and health state must be deemed compliant by the Infranet Controller before they and/or their device are granted access to any enterprise networks, resources and applications.

Q. What is the typical profile of customers deploying Juniper's UAC solution?

The flexibility, scalability and security afforded by Juniper's UAC solution has broad appeal across industries and continents. For example, Juniper has a number of North American and international UAC wins over an array of industries, including the Consumer/Retail, Education, Financial Services, Public Sector/Government, Healthcare, Service Provider, Technology/Engineering, and Utility industries.

Q. Who are the decision-makers regarding a UAC purchase? At what level of an organization are you selling in and why?

Access control is a unique market category, as evaluation and purchase decisions cross literally all levels of an organization. We have had interest in the solution at levels ranging from CxOs and compliance officers, to network administrators and security teams, and even with teams that manage desktop applications.

Q: Are most UAC customers deploying enforcement points at Layer 2 (802.1X), or at Layers 3 – 7?

Juniper has found that a nearly equal number of UAC customers have deployed using 802.1X/Layer 2 enforcement as are deploying/have deployed with Layer 3 – 7 enforcement. Juniper has also found that many of UAC customers have deployed using both 802.1X/Layer 2 and Layer 3 – 7 enforcement for greater granularity.

Q: How does network access control – and specifically UAC 2.1 – address regulatory compliance?

Industry and government regulations such as the Sarbanes-Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) Data Security Standards (DSS), and others require that enterprises and other affected corporations and entities ensure the security of their networks; assure that devices accessing their networks maintain active, updated antivirus, patch management, and other antimalware tools and controls; control network access; know who is on their network, when; and be able to log and generate reports with this data for compliance audits. Network access control (NAC) solutions aid in compliance with industry and government regulations.

Juniper UAC addresses many of the general and specific requirements of regulations like SOX, HIPAA, PCI DSS, and others. Juniper UAC ensures network protection, assures endpoint device integrity and health, and that endpoint devices maintain active, up-to-date antivirus and antimalware tools; controls network and application access; and logs applicable data, working with existing reporting tools and Security Information and Event Management (SIEM) vendor partners using standards-based interfaces. Juniper UAC 2.1 additionally incorporates pre-defined patch management policies and endpoint device checks; and is able to link user/role information with network and application usage.

Competitive Landscape Questions

Q: How does UAC 2.1 compare against Cisco's NAC?

Juniper UAC compares favorably against Cisco NAC – either their NAC Appliance or NAC Server:

- UAC is standards-based and vendor agnostic, which means no forklift or rip-and-replace upgrades are required to deploy UAC in an existing network
- UAC simplifies deployment and scales easily and quickly
- UAC periodically rechecks the security and health state of an endpoint device
- UAC uses secure communications throughout the solution
- UAC delivers out of the box deployment and integration with identity/access management offerings, endpoint security and network infrastructure

Q: How does UAC compare against other NAC offerings?

When compared against other NAC solutions on the market, Juniper UAC has come out ahead in many categories; UAC:

- Is standards-based and vendor agnostic, able to leverage existing network infrastructure – delivering superior investment protection
- Simplifies deployment, scaling easily and quickly
- Protects the network and applications at Layer 2 – 7, unlike other NAC offerings

- Incorporates both endpoint device and network based access control capabilities; other NAC products do not or cannot offer both
- Based on market leading, field tested components that today are being used, in some cases around-the-clock, in thousands of demanding deployments worldwide
- Is available from Juniper Networks, an established, multi-billion dollar market-leader