

# **Buyer's Guide for Access Control Solutions Juniper's Unified Access Control v2.0**

---

Roslyn Rissler  
Product Marketing



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)  
Part number: 710057-002 Nov 2006

## Contents

Introduction .....	3
Buying Criteria Overview .....	4
Comprehensive Access Control .....	4
Robust Security .....	4
Flexibility and Ease-of-Use .....	5
Administration and Management .....	5
Cost .....	6
Juniper Networks Unified Access Control v2.0 Access Control Without Constraints .....	7
Juniper's Unified Access Control v2.0 .....	7
How UAC Works .....	8
How Juniper Networks Unified Access Control v2.0 Stacks Up Detailed Buyer's Checklist .....	10

## Introduction

Enterprises have been facing the need for access control for some time. This need began in the extended enterprise segment, where remote users, often on unmanaged or unmanageable devices, sought access to vital LAN resources. When such users were not granted access, productivity suffered. When users were granted IPsec VPN access, however, the wide-open tunnel between their endpoint and the LAN often served as a freeway for viruses, worms, spyware, or other malware that the user's endpoint might have contracted.

SSL VPNs have largely solved the problem of safely providing network applications and resources to unknown devices by associating the endpoint security state with user authentication, and by providing specific session-based roles as well as very granular resource policies. As the 3<sup>rd</sup> party populace fast becomes part of the campus LAN audience, however, the same problem is being recreated in the campus LAN. In fact, in some cases, the demand for access control is stronger in the LAN itself, since the user audience can be even more diverse than that seen in the extended enterprise. And as the audiences vary, so too do the endpoints, from mobile devices that transit the network perimeter, to business partner devices that are not managed by the enterprise, to guest user devices that may not be managed at all. Today's campus was built with the presumption that the user's location – on the LAN – was an effective indication of trust, and most LANs today have little to no built-in protection as a result. If you are on the campus, in most cases, you are on the LAN...and so too is whatever security threats or vulnerabilities you have probably unknowingly brought with you.

In response, the access control market is booming. Dozens of vendors, ranging from startups to established networking and security vendors, are using the "access control" buzzword to get your attention. In some cases, these are legitimate, well-thought-out offerings; in others, they are no more than repurposed existing technology with a new name, or multi-vendor "solutions" that, in fact, demand an end-to-end vendor lock-in.

In this document, we will examine some questions that you should consider when looking for the access control solutions that are a best fit for your requirements in your specific deployment, gleaned from customer requests in the real world. We have focused on the following areas:

- • Comprehensive access control
- • Robust security
- • Flexibility and ease-of-use
- • Administration and management
- • Cost

## Buying Criteria Overview

### Comprehensive Access Control

The most innovative access control technologies seek to combine two different concepts – end user identity and endpoint integrity. Some solutions only use part of this combination – such as authentication – and combine it with traffic examination to create something that resembles a check of endpoint security state; but it really isn't. Others rely solely on endpoint security state without any ability to combine it with network-based traffic processing capabilities for access control. A true solution must, at a minimum, have the means to combine user identity, device integrity, and location information with policy, resulting in comprehensive access control.

One of the first questions you need to ask when shopping for an access control solution is this: Does the solution actually handle all the use cases that I will put in front of it? It is one thing to authenticate users and validate endpoint security state when an employee brings his laptop in after a weekend of Internet surfing. It may be something altogether different to check the security state of a contractor's PC, or that of a guest, where you cannot manage the PC and it can accept no downloads. A complete access control solution must be independent of such things as corporate PC images or pre-loaded software, as well as be able to provide cross-platform support. Still another consideration may be branch office users, which can sometimes include all of the same types of users – employees, contractors and guests - that you would find in the campus LAN, needing access to many of the same critical resources, but often without the same security strictures.

A comprehensive access control solution should also be capable of dynamic changes if the endpoint's security state, network information, or user information changes, even if these changes occur mid-session. This dynamic policy should also be enforceable in real time across the network on enforcement points. Given the large investments in enterprise LAN infrastructure across campus and branch offices, the enforcement of policy should ideally leverage existing investments in network infrastructure.

### Robust Security

Access control is, at the end of the day, about security. As such, you should consider whether or not security decisions in your network are being made by devices that were purpose-built to provide security. A consideration at this point is the purpose for which you have purchased (or plan to purchase) a specific piece of your infrastructure. Many different types of equipment can be repurposed for use in an access control scenario, but just because they can fill this position on a network diagram does not mean that they will do so well. This is more often seen in the case of enforcement devices, particularly those that are placed in-line, than anywhere else throughout a typical access control solution. Serious consideration must be given to the throughput, availability, and resiliency of such deployments.

Another consideration includes whether or not the access control solution leverages the investments that you have already made in your security devices. While this can be important when looking at the investment in your firewalls, it is crucial in relation to your AAA infrastructure. Access control must integrate seamlessly with your existing AAA schema, taking advantage of your authentication infrastructure to validate user identity. If it can also utilize your directory servers for user and group membership

information as well, however, the result will be a more secure deployment that is also more cost-effective

## Flexibility and Ease-of-Use

An important consideration when looking at access control solutions is what it will require to deploy the solution in a production network. Most enterprise needs are best suited to a phased approach to access control, where controls can be applied gradually. The fact is that all network segments are not equal; while some portions of the network could benefit from a level of access control, others require it to meet the business' need to show compliance with regulations. In addition, according to leading analysts, many enterprises may not intend to roll access control company-wide ever! The best solution will have several implementation methods, and will ideally use components of your existing infrastructure as building blocks.

Another element to weigh is whether or not the access control solution is flexible. Your network is fluid, not static, and a comprehensive access control solution should be able to change with it. This is another reason to look for solutions that have a variety of deployment methods. This enables you to take advantage of equipment that is specialized, high-ticket technology where you need it, and use more commoditized equipment where it makes sense. Regardless of the deployment method you choose, you should be able to add another enforcement method without having to rip-n-replace what you've already deployed.

One of the best ways to insure this level of interoperability is to seek solutions that are based on open specifications and standards. Some solutions, even those that claim to be "collaborative" or to support "industry-wide" standards, actually hinge on a single vendor's proprietary appliances or protocols. You should consider whether you can use a given access control solution to secure what you have today – including different endpoint vendor security solutions, different auditing/logging solutions, different network infrastructure including switches or routers, different authorization protocols, etc. – or if you are willing to lock your network into one vendor's solution. You should also be mindful that a decision to go with a single vendor today, tempting through it may be for simplicity's sake, could lock you into network infrastructure for the life of the equipment.

## Administration and Management

If ease of deployment is a primary consideration when evaluating a new access control solution, then day-to-day ease of administration and management must be next. After all, it won't matter if a product provides robust access control if you can't manage it. One of the big indicators when probing for the administration factor is to consider whether or not the solution or the components that make it up have been field tested. While no vendor can claim to have a thoroughly vetted access control solution simply because the category is so new, it is possible to consider the elements that make the solution up. If the solution hinges on a dynamically delivered agent, for example, consider whether or not the vendor has experience with products that use this technology.

Another way to determine whether an access control solution will be easy to administer is to consider whether or not you can use your existing infrastructure to manage it. Are the auditing or logging tools proprietary, or can you use what you are accustomed to? Is there a way to import and export the necessary data so that it can be manipulated and reported easily? You may also want to consider to what level the solution simplifies the steps required to create or edit policies or to deploy endpoint security criteria

## Cost

The final consideration – cost – combines considerations of flexibility, ease-of-use, and the day-to-day time spent to administer and manage the access control solution with the actual acquisition cost and the time needed to re-design your network, if required.

Another thing to think about in the area of cost also shows up as a flexibility consideration – whether or not the solution is standards-based. This represents a cost consideration in that implementation of a proprietary solution effectively locks you in to that vendor's solution – and pricing. Standards-based solutions, or those based on open specifications will almost inevitably raise the return on investment and lower total cost of ownership. This is a simple function of market pressures; when the customer has a choice, they will get a better product for less.

For example, if a solution requires an upgrade to your switching infrastructure, you must also factor in the time required to inventory the devices on your network, determine what types of switches are deployed there and what version of code they are running, get hardware and/or software upgrades as required, and test the network.. Another such consideration is the installation of client software, a process that can sometimes be deemed too intrusive.

Cost considerations are another set of criteria that may favor a phased approach to deploying access control. In some cases a phased deployment is preferable and easier to justify as it could save valuable time and expense. Some access control solutions can be easily deployed in a phased manner – others cannot.

## Juniper Networks Unified Access Control v2.0 Access Control Without Constraints

The category of access control has become one of the hottest areas in technology today, offering a variety of benefits, from protecting intellectual property and enabling regulatory compliance to ensuring the productivity of the enterprise itself. Because the category is still evolving, however, many enterprises have been cautious about considering a solution regardless of how badly it is needed. Some vendor solutions lock the enterprise into a single type of infrastructure, while many come from start up companies that have no proven track record. Many vendors' solutions will offer you access control, but the overall solution is constrained by factors that can include switching infrastructure, interoperability issues, user types, device types, or deployment issues

Juniper Networks UAC version 2.0 of its Unified Access Control solution delivers access control without these constraints. Juniper UAC v2.0 solution combines UAC v1.X capabilities which used Juniper's best-selling firewalls as enforcement points – with functionality from Funk's market-leading 802.1X components, including the OAC client-side supplicant and Steel-Belted Radius. The result is an access control solution that can work in a wide variety of deployment scenarios, including those with 802.1X wired or wireless infrastructure, those with Juniper firewalls, or those with both. Every element of the solution has been deployed in literally thousands of enterprises around the world.

UAC 2.0 also embodies Juniper's commitment to open standards. The solution will support any 802.1X infrastructure, whether wired or wireless. And UAC 2.0 is compliant with Trusted Computing Group's Trusted Network Connect, or TNC. The TNC solution is an open architecture that defines several standard interfaces which enable components from different vendors to securely operate together, creating an endpoint integrity and NAC solution from installed equipment and heterogeneous networks. The TNC architecture is designed to build on established standards and technologies, such as 802.1X, RADIUS, IPSec, EAP, and TLS/SSL. This ensures still more choice and flexibility for the enterprise.

Enterprises can use UAC 2.0 to enable access control today, and into the future. They can decide what deployment works best for them, regardless of the switching infrastructure or whether they have Juniper firewalls or not. They can decide what additional security that they want to deploy using TNC-compliant solutions, and rest assured that UAC 2.0 will interoperate seamlessly. For example, many enterprises haven't completely rolled 802.1X-enabled switches yet, and therefore may want to use Juniper firewalls to enable a phased approach. The firewalls can even be deployed in transparent mode behind currently deployed firewalls, if you just want to use them as enforcement points. When 802.1X is deployed, the new policies can simply be pushed, using the same Controller and the same agent. Likewise many enterprises are interested in securing their wireless network; in this case, UAC can be used to provide 802.1X-based access control. If more granular access control is desired, a Juniper firewall can be added at any time.

### Juniper's Unified Access Control v2.0

Juniper's Unified Access Control (UAC) Solution version 2.0 is comprised of several elements, including the Infranet Controller, which serves as a centralized policy manager; the UAC Agent, which is dynamically downloadable endpoint software (please note that an agentless mode is also available for use where a download of any kind is not feasible, such as on guest devices); and several different forms of enforcement points which include both Juniper

firewalls and vendor agnostic 802.1X-compliant switches and/or wireless access points. Both the Controller and the Agent also contain integrated features from Juniper's acquisition of Funk Software in 2005, including the Odyssey Access Client (OAC) 802.1X supplicant and Steel-Belted Radius.

**The Infranet Controller** is a hardened policy management server that consolidates user authentication, endpoint integrity verification and device location, and combines this information with policy to restrict network, resource, and application access. This policy is then passed to Enforcers, either at the edge of the network prior to granting an IP address via 802.1X, within the network on the firewalls, or both. Using both types of enforcement points enables even greater granularity of access control.

**The UAC Agent** is a dynamically downloaded 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 the OAC and Layer 3-7 overlay capabilities. These capabilities include an integrated personal firewall for dynamic client-side enforcement of policies, as well as specific functionality for Windows devices that includes IPSec VPN (which enables encryption from the endpoint to the firewall) and Single Sign On to Active Directory. The Agent also includes Host Checker functionality, familiar from thousands of Juniper Secure Access SSL VPN deployments, which enables the administrator to scan endpoints for a variety of security applications/states, including but not limited to antivirus, malware and personal firewalls. Deployment is simplified with pre-defined Host Checker policies as well as automatic monitoring of AV signature files for the latest definition files for posture assessment. UAC also enables custom checks of elements such as registry and port status and can do an MD5 checksum to verify application validity.

**UAC enforcement points** include vendor agnostic 802.1X switch/wireless access point infrastructure and/or overlay enforcement points, which encompass virtually all Juniper firewall/VPN platforms, including Juniper secure router FW/VPN appliances and Juniper's Integrated Security Gateways with IDP modules. The wide variety of Enforcer platforms allow deployment flexibility from smaller firewalls to protect printer farms to 30Gbps models to enforce policy in the most traffic-intensive settings. Support for vendor agnostic 802.1X switches and/or wireless access points enable enterprises to quickly realize the benefits of access control very early in the user session, without requiring a hardware overhaul. The UAC solution accommodates 802.1X-based or Layer 3-7 overlay enforcement schemes, and both technologies can also be used together for the most granular access control.

## How UAC Works

Before the user even submits credentials to the Controller, the request from the user (in either 802.1X mode or non-802.1x mode, via browser-based agents that are provisioned to the endpoint) has revealed a number of different end user attributes. These include source IP, MAC address, network interface (internal vs external), digital certificate if one exists, browser type, SSL version, and the results of an endpoint security check. Once credentials are submitted, the Controller features a comprehensive authentication, authorization and accounting engine for seamless deployment into almost all popular AAA settings, including existing RADIUS, LDAP, AD, Netegrity SiteMinder, Certificate/PKI servers and Anonymous Authentication servers. The Controller combines the user credentials, and group or attribute information (for example, group membership, if any), to the information gathered before the credentials were entered, including those gathered by Host Checker. This combination allows the Controller to dynamically map the user to the second step of access control - a role for the session. Role attributes can encompass session attributes/parameters, and can also specify restrictions with which the user must comply before they can map to a role, which is

extremely useful in settings where security is vital and compliance must be ensured. The third and final step in access control is the resource policy, which governs network and resource access. Some examples include Layer 2 RADIUS attribute based policies such as VLAN assignments and/or vendor specific attributes, as well as Layer 3 policies that govern access to IP addresses/netmasks, ports, or ranges of the above. Layer 7 policies, such as IDP policies or URL filtering provide additional levels of dynamic threat management.

As you can see, each successive layer of policy can add still more granularity to overall access control, in contrast to some solutions that only have one or two steps in the access control process. At the same time, this level of granularity can be flattened if the customer does not require it or if the level of protection needed does not merit it.

## How Juniper Networks Unified Access Control v2.0 Stacks Up Detailed Buyer's Checklist

Consideration	Juniper Networks Unified Access Control v2.0
<b>Comprehensive Access Control – Unified Access Control v2.0</b>	
<b>Can the solution under consideration handle many different use cases, such as:</b>	
Managed and unmanaged devices?	The UAC v2.0 solution can be run in both agent and agentless modes to provide on-demand validation of endpoint integrity of managed and un-managed endpoints.
Business partner or contractor devices, not owned or managed by the enterprise?	<p>This use case poses several contradictory problems – contractors need granular access control rights, but often have devices that are inherently unmanageable. In cases where an agent cannot be practically downloaded to the endpoint, the UAC agentless mode supports browser-based validation of user credentials and scanning of endpoints for posture assessment both before user authentication and throughout the user session.</p> <p>This use case is best addressed, however by an access control solution that includes a method for providing not only port-based network admission control, but granular access control to specific network resources and applications. The issue can be solved in several ways, including VLAN network segmentation, policy-based network access control using Juniper firewalls as enforcement points, or a combination of both.</p>
Guest access for users with unmanaged devices?	The UAC agentless mode was developed specifically for this use case, and supports browser-based validation of user credentials and scanning of endpoints for posture assessment both before user authentication and throughout the user session. On Windows platforms, agentless mode can check for third party applications, files, process, ports, registry keys, MAC address, IP address, NETBIOS and custom DLLs. The solution can then allow or deny access based on the results of the checks.
Employees with different levels of privileges, including those with administrative or restricted privileges?	Employees typically require very granular access control, but have the advantage of also typically getting to resources via enterprise-owned/managed devices. This use case is best addressed by an access control solution that includes a method for providing not only network admission control, but granular access control to specific network resources and applications. The issue can be solved in several ways, with UAC 2.0 including VLAN network segmentation, policy-based network access control using Juniper firewalls, or a combination of both.

Employees with different roles in an organization?	With UAC 2.0, employees with different roles within an organization can be assigned different modes of endpoint assessment, validating users/endpoints with varied user privileges. UAC 2.0 can also gather user and group membership information from directory stores, making it easy to dynamically assign appropriate access.
Cases where users don't have an agent and such an agent cannot be pre-installed?	The UAC agentless mode was developed specifically for this use case, and supports browser-based validation of user credentials and scanning of endpoints for posture assessment both before user authentication and throughout the user session.
Does the solution enable dynamic agent download?	Yes, UAC v2.0 does feature a dynamically delivered agent. In addition, automatic version control also means that agents are always updated to the latest version of software, minimizing operational costs of troubleshooting and maintenance. UAC uses Active X or Java for flexible delivery of endpoint assessment agent in all connection environments.
Cross platform endpoints, including Mac Linux Solaris	The UAC agentless method is also cross-platform, enabling you to check the status of non-Windows devices as well. On Mac, Linux (SuSE, Fedora, RedHat) and Solaris platforms, the UAC solution supports file, port and process checks to verify endpoint integrity prior to granting network access. The solution also offers the option to simply authenticate users, without posture assessment, on endpoints with supported browsers, which makes it available for PDAs as well.
Users who travel between different offices or jobs that may have varying security requirements?	Using UAC, policies may be set by location, as well as group.
Users attempting access from an unmanaged, offsite device (i.e., Internet kiosk)?	Users attempting access from an unmanaged offsite device may be forced through an SSL VPN gateway, such as Juniper Network's Secure Access appliances. In this case, access control may be provisioned in a very granular fashion, along with the access method. If the SSL VPN is not sufficiently secure, however, or if the deployment requires it, UAC may be used as well. If the user is unable to utilize either agent or agentless function, they may be restricted to a specific area of the network or a specific VLAN only.
Support for environments using 802.1X?	UAC v2.0 will interoperate with any vendor's 802.1X-enabled device
Devices running a variety of security software?	UAC v2.0 is compliant with the Trusted Computing Group's Trusted Network Connect (TNC) specifications. .
<b>Does the solution protect network assets as part of access control? Detailed questions include:</b>	
Does the solution provide network admission control?	UAC 2.0 provides network admission control very early in the session, using 802.1X.
Does the solution provide resource and application access control?	UAC 2.0 can be deployed in a variety of ways to ensure granular resource and application level access control. This level of control can be added to a 802.1X admission control deployment, using Juniper firewalls, or can deployed in an overlay fashion.

<p>Does the solution protect certified endpoints, once they are allowed on the network, from malicious users/devices?</p>	<p>UAC v2.0 provides this level of protection in several ways. First, using the 802.1X deployment method, users are authenticated and their endpoint security stance verified before they even get an IP address on the network. This provides very effective protection from malicious users, or from users who may unknowingly have an infected device. Second, the UAC Agent also contains a stateful personal firewall, which can provide still more protection.</p>
<p><b>Can the solution combine host and network security in a unified fashion for meaningful security? Detailed questions include:</b></p>	
<p>Does the solution rely solely on software on the endpoint to make access control decisions?</p>	<p>The UAC v2.0 solution makes access control decisions on host, via the UAC Agent, as well as network, via 802.1X, Juniper firewalls as enforcers, or both. This enables meaningful policy enforcement.</p>
<p>Can the solution also enforce security policy throughout the network?</p>	<p>UAC v2.0 gives the ability to flexibly enforce policy at the access layer, as well as in front of data center resources, to secure campus wired and wireless networks or to dynamically enforce policy at branch office sites.</p>
<p>Does the solution only assess endpoint integrity prior to user logging in or does it continue to monitor user/endpoint during session for dynamic in-session compliance?</p>	<p>UAC 2.0 will assess the endpoint before login and provide periodic post- login endpoint assessment at administrator-specified intervals during user session. This is a mandatory component in providing complete, dynamic protection.</p>
<p>Can the solution immediately quarantine a previously certified endpoint device that has since been deemed out-of-compliance during the same session?</p>	<p>UAC 2.0 can handle endpoints that are found to be non-compliant during a session in a number of different ways, each of which can be acted upon immediately. Users can be notified of the situation, or re-routed to a remediation VLAN where the non-compliance is explained – this is particularly simple using TNC reason strings – and told what to do to remedy the situation. Or access can simply be denied.</p>
<p>If policies change on the server, can the entire network be dynamically re-assessed and access policies enforced in real-time?</p>	<p>UAC 2.0 features realtime propagation and enforcement of access control policies. New policy will be sent to enforcement points including any vendor's 802.1X-enabled device, Juniper firewall platform or both, as well as to the UAC Agent on the endpoint if deployed.</p>
<p>Does the solution enforce security and access control without compromising network performance?</p>	<p>UAC 2.0 features only one element – the Infranet Controller – that is not a normal part of traffic flow on an average network. The Controller is involved in access control only at the very beginning of the session, when policy is set. After that, traffic flows through switched or wireless infrastructure, as well as through the firewall, just as it always has.</p>
<p><b>Does the solution have the capability to perform remediation on a non-compliant endpoint device?</b></p>	
<p>Can the solution help users remediate?</p>	<p>UAC 2.0 enables policy specific remediation that helps users remediate their machines easily. This is particularly simple if the solution features a TNC-compliant security application, as TNC supports reason strings which will display the problem to the user without requiring the administrator to input custom text. UAC 2.0</p>

	also features auto-remediation features. Upon remediation, the solution dynamically re-assesses the endpoint and grants them network access.
--	--

**Robust Security – Unified Access Control v2.0**

**Is the solution under consideration truly secure? Detailed questions include:**

Can the solution be bested by malicious users?	UAC v2.0's enforcement of policies in the network means that the security enforcement cannot easily be circumvented by malicious users, and policy assessment/enforcement is done over encrypted channels.
Is it easy for users to spoof the solution?	UAC v2.0 can use a native IPSec client, included with the UAC Agent and compatible with any other IPSec client, to ensure validation of endpoint/user prior to granting access to network resources and authenticity of user traffic. IPSec session can be set at 3DES, DES or null encryption. While this might be overkill in some situations, it can be very useful
Is the policy server secure?	UAC's policy server is a purpose built appliance with hardened services to protect from known vulnerabilities and attack vectors. In addition, the Controller uses AES disk encryption for protecting confidential data.
Can the client prevent a user from changing or adding settings?	UAC v2.0's network-based security means that solution can detect malicious behavior on endpoint and take appropriate action.
Does the solution incorporate existing security standards and investments, such as anti-virus, deep packet inspection, intrusion prevention, or URL filtering, for protection of mission-critical LAN assets?	In addition to the security features within the UAC v2.0 solution itself, the choice of deployment option can enable several additional security features. When deployed with Juniper firewalls, the solution is able to take advantage of all of the robust features of these market-leading security devices, including Juniper's Intrusion Detection and Prevention functionality, network-based antivirus, anti spam, and URL filtering capabilities. All of these capabilities can be dynamically leveraged as part of the UAC v2.0 solution, which enables the enterprise to not only enforce access control policies but also to apply security policies such as deep packet inspection, anti virus, and URL filtering on a per user/session basis.

**Flexibility and Ease of Use – Unified Access Control v2.0**

**Does the solution have features that enable flexible, simple deployment and use, including:**

A centralized policy store that maps users to roles that dynamically control network access	The Infranet Controller functions as the dedicated policy management server within the Unified Access Control v2.0 solution. The UAC solution overall incorporates policy elements that are the result of real world experience in the access control area (from SSL VPN) as well as the AAA world (OAC and SBR). Instead of simply authenticating users once and providing relatively crude access controls based on network segmentation only, the UAC solution incorporates three different levels of policy, including authentication/authorization, roles, and resource
---	--

	policies.
1. Does the solution leverage information gathered to dynamically set access policy, including information such as:	
A. Endpoint posture evaluation	With UAC v2.0, endpoint integrity is validated not just prior to login but also during the entire duration of the session for continual posture evaluation. The fact that the solution is also compliant with open specifications from the TNC enables the enterprise to deploy the solutions seamlessly, and enable simple user remediation if necessary.
B. User profiles	The Controller interoperates with a wide variety of authentication methods and schemes, as well as directory stores. The Controller evaluates detailed attributes including user attributes, certificate attributes, and group memberships and uses them to map users to roles that control network access.
C. Network information	Like the Juniper's SSL VPN, UAC v2.0 can be configured to perform network specific checks
D. Ports and applications	Like the Juniper's SSL VPN, the UAC can be configured to perform checks on port activity and the presence of certain applications.
E. Operating systems	UAC 2.0's predefined checks for different OS versions make it easy to setup the checks.
F. Patch compliance	UAC 2.0 checks for presence of patches and leverages these results for dynamic access control.
Does the solution leverage existing policy stores and use these profiles/attributes to control network access?	UAC 2.0 supports a wide variety of IAM solutions, authentication methods, and directory stores, including dual factor authentication, Active Directory, digital certificates/PKI solutions, LDAP, Netegrity Siteminder, NTLM, Radius, RSA ACE, UNIX NIS, and anonymous auth.
How does the solution help meet regulatory compliance?	UAC v2.0 is an excellent step toward compliance, as it combines strong authentication with differentiated user access and a check of the endpoint's security state at login and throughout the session. A wide variety of auditing and logging features are included in the solution to make this easy.
Does the solution support the ability to flexibly run in a combination of audit and enforcement modes?	UAC v2.0 provides this flexibility, and can be deployed in evaluate mode to gain visibility to network compliance and traffic patterns of LAN users for regulatory requirements while providing logging and auditing data.
High availability options to reduce chances of a single point of failure	The solution supports flexible enforcement of access control policies in campus, branch office or data center deployments, where high availability is mission critical. The UAC v2.0 solution's Infranet Controllers can be deployed in cluster pairs or in multi-unit clusters. Stateful clustering supports active-active or active-passive deployments across WAN and LAN.

<p>Does the solution allow a means to deploy enforcement points without reconfiguring the surrounding network?</p>	<p>This can easily be accomplished with UAC v2.0, using the overlay firewall deployment method. Enforcement points can be deployed in transparent mode – behind existing firewalls, if desired - for easy deployment without additional configuration. The combination of this feature with the ability to deploy the solution in audit mode enables you to become comfortable with the solution without risking mission critical traffic.</p>
<p><b>Can you easily deploy the solution? Detailed questions include:</b></p>	
<p>Does it leverage existing network/security infrastructure, security devices and/or software?</p>	<p>UAC v2.0 supports access control using any vendor's 802.1X-enabled switched or wireless infrastructure, existing Juniper firewalls, or both. The solution interoperates seamlessly with virtually all AAA and IAM solutions. And UAC v2.0 is TNC compliant, which ensures interoperability across a wide range of security applications/solutions.</p>
<p>Are there predefined checks for AV, firewall, anti-spyware, OS versions</p>	<p>UAC v2.0 features predefined checks for AV software, virus definition files, firewall, anti-spyware, and OS versions that make it very easy for administrators to set up the security policy checks and bind them to access control policy. UAC also has auto monitoring/ enforcement of the latest AV signature files, making it easy to keep signatures up to date</p>
<p><b>Does solution support a phased deployment? Detailed questions include:</b></p>	
<p>Can the solution start by protecting critical parts of the network and incorporate additional enforcement points over time?</p>	<p>UAC v2.0 features more deployment flexibility than virtually any solution on the market. The solution can be deployed using any vendor's 802.1X-enabled switches or wireless access points, so if an enterprise already has those elements in place, access control is easy and doesn't require a single vendor lockin. If more granular access control is desired, a Juniper firewall can be added at any time, without requiring a redeployment of the Controller or the Agent. In the case where an enterprise hasn't completely rolled 802.1X-enabled infrastructure yet, it is simple to use existing Juniper firewalls to enable a phased approach. The firewalls can even be deployed in transparent mode behind currently deployed firewalls, if you just want to use them as enforcement points. When 802.1X is deployed, the new policies can simply be pushed, using the same Controller and the same agent.</p>
<p>Does the solution allow an organization to provide custom messages for compliance or noncompliance?</p>	<p>In UAC v2.0, custom messages, including remediation instructions, can be tied very granularly to security policies enforced by the solution and users can be given an easy path to remediation. This is made particularly simple in the case of TNC-compliant security applications, which take advantage of reason strings.</p>
<p>Does the solution allow an organization to provide only warning messages for noncompliant endpoints, without quarantining the offending devices?</p>	<p>The UAC v2.0 solution can be deployed in evaluation mode to gain visibility into network compliance and traffic patterns of LAN users for regulatory requirements. This can be an excellent pilot deployment to get visibility into the level of protection that will be required by examining the true security state of endpoints.</p>

<p>Are solution components compliant with industry standards?</p>	<p>Juniper Networks actively supports the efforts of the Trusted Computing Group (TCG) in defining broad access control standards via the Trusted Network Connect (TNC) initiative. UAC v2.0 is also compliant with 802.1X, enabling unmatched flexibility.</p>
<p><b>Administration and Management – Unified Access Control v2.0</b></p>	
<p>How does the solution handle policy setup?</p>	<p>UAC also makes policy easy to set up and maintain. Policy definitions can be duplicated, inherited, and edited for streamlined administration. Each time there is a need to create new policies based those in use, administrators may re-use those which have been already set, including: dynamic authentication policies; role definitions; role settings; and resource authorization policies, including multiple resource groupings which can be associated with the same role, and additional roles which can be easily added to existed resource groupings.</p>
<p>What standard reports does the solution feature?</p>	<p>The Controller provides a range of standard reports, making it easy to properly provision the solution, watch performance thresholds, ensure compliance, and more. Standard reports include Users/ Session reports, Compliance reports, resource access tracking, and system reports</p>
<p>Can reports be filtered or customized?</p>	<p>Logs can be filtered in a variety of formats, including standard formats such as Syslog, WELF and W3C, as well as in custom formats. This enables the enterprise to leverage existing investments in reporting packages, and view the information in the format that they are accustomed to. This information can also be sent to security event management solutions to generate custom reports.</p>
<p>Can different administrative teams control the portion of the solution that reflects their expertise (such as security, networking, etc)? Can administrators in charge of various segments control access to that segment?</p>	<p>UAC v2.0 provides delegated administration to enable different teams to (security, networking, applications) have granular read/write privileges to different segments of the solution. This gives each team the ability to granularly control policy in their configuration. The same is true in the case of distributed network segments.</p>
<p>Do you own the core technology for the policy server and related functions, or do you license it from a partner?</p>	<p>The core technology of the Infranet Controller leverages several distinct technologies, all of which are owned by Juniper Networks. They include the core policy management server, which was developed as part of Juniper's Secure Access SSL VPN product lines and integrated RADIUS capabilities from Juniper's Steel-Belted Radius servers. In addition, the UAC Agent now includes integrated Odyssey Access Client 802.1X supplicant functions.</p> <p>Policy Management Server (from Juniper's Secure Access SSL VPN)</p> <p>Integrated RADIUS Capabilities (from Juniper's Steel-Belted Radius)</p> <p>Integrated 802.1X Supplicant Features (from Juniper's Odyssey Access Client)</p>

<b>Cost – Unified Access Control v2.0</b>	
<b>Are all costs of the solution under consideration explicit, or are there hidden costs?</b>	
Does the solution lock you into a single vendor solution?	UAC v2.0 is specifically designed to overcome this common roadblock to deployment. With UAC, enterprises can utilize their existing investment in any vendor's 802.1X-enabled switch or wireless infrastructure, AAA infrastructure, and security applications. Those that have Juniper firewalls in place may also use that equipment as enforcement points, but it is not mandatory for the solution.
Does the solution require an upgrade of network infrastructure?	No, UAC 2.0 is specifically designed to drop into existing infrastructure, whether it is 802.1X-based or uses Juniper firewalls. In the case where the enterprise has neither types of enforcement points, using Juniper firewalls to provide chokepoint control can enable granular access with minimal investment and no upgrade to the switching infrastructure. Juniper firewalls can be installed in transparent mode behind existing firewalls to act as enforcers only, if there is no desire to change these devices. The use of audit mode can also help to aid further access control decisions.
Does the solution make use of open standards?	UAC 2.0 makes use of two important open standards – the IEEE 802.1X standard, and open specifications developed by TNC. This combination gives the enterprise the ability to choose the equipment and security applications that best fit their particular needs, lowering total cost of ownership, and speeding return on investment.

Copyright © 2006, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

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.