

Read on to learn about CyberGatekeeper enforcement options, and how to check a computer's posture.

**Issue Highlights:**

[Enforcement Options](#)

[Vetting Visitors](#)

[Vulnerability Management](#)



**CyberGatekeeper Enforcement Options**

*Alcatel-Lucent OmniAccess Integration*

In the March/April newsletter, we kicked-off our series on CyberGatekeeper (CGK) enforcement options by starting with an overview of CGK functionality, the common components that comprise InfoExpress' NAC solution, and the various enforcement methods available to an organization. In this issue, we'll continue our series on CGK enforcement options by highlighting CGK integration with Alcatel-Lucent's OmniAccess solution (Aruba wireless) which is part of Alcatel-Lucent's Safe NAC offering.

As a refresh, the various approaches available are peer-based, in-line, 802.1x, and Alcatel-Lucent (ALU) integration (VitalQIP & OmniAccess). And, regardless of which enforcement method(s) an organization uses, the four common components are Policy Manager, Policy Server, Agent, and Reporting/Management Server.

With ALU integration, all the same functionalities exist (pre & post connection assessment, quarantine, remediation, and reporting). Quarantining is done by leveraging the strengths of the Aruba controller—basically assigning different roles based on authentication and compliance status.

Here is how it works:

1. An employee, contractor or guest connects to the wireless network.
2. The OmniAccess Controller provides authentication, and identifies the role the user should be assigned based on credentials (802.1x, Captive Portal).
3. The OmniAccess Controller restricts traffic to the CyberGatekeeper Policy Server and the remediation servers.
4. The CGK Policy Server receives a HIC (host integrity check, AKA posture assessment) report from the CGK Agent.
5. The CGK Policy Server will set the endpoint role on the OmniAccess controller based on the results from the HIC check using the specific integration with the controller.
6. If the HIC fails (audit status=FAIL), the Policy Server will alter set the endpoint role to restrict traffic to remediation resources only.
7. If the HIC passes (audit status=PASS), the Policy Server will set the endpoint role on the controller to the production role the

**Quick Links**

**Solutions**

[LAN Security](#)

[Remote Access](#)

[Diverse Users](#)

[Endpoint Security](#)

[AV/Software Updates](#)

[Demo](#)

[Support](#)

[Contact InfoExpress](#)

[Subscribe to this newsletter](#)

**Watch a demo:**

Seeing is believing. Watch a demonstration of how the Dynamic NAC solution works, and see first-hand the DNAC end-user experience.

[Watch Demo](#)

Or request a personal webcast to learn more about Dynamic NAC.

[Request Webcast](#)

**Customer Corner**

Welcome to Customer Corner, where we publish an interesting question from one of our customers. In this installment we handle the increasingly common case of an organization taking on new employees through a merger or acquisition:

**Q:** We are in the process of integrating new employees as a result of a merger. These employees already use CyberGatekeeper in their own implementation and have their own security policies in place. At least initially, can we continue to use different policies, even if we share the same infrastructure? Are there any

The integration with the OmniAccess Controller builds on 802.1x enforcement to give more functionality and flexibility to NAC by setting the role of the endpoint dynamically on the wireless controller using a specific API with the controller.

The strengths of this approach are:

1. No supplicant required.
2. Works with both managed and unmanaged (e.g., guest) endpoints.
3. Change between roles is immediate (no VLAN switching)—no need to wait for a timeout.
4. Works with all agent types—desktop, web, Linux, and Mac.

In our summertime edition, we'll examine DHCP enforcement.



### Checking a Computer's Posture

It's one thing to check out a computer that's directly under your control—that is owned and administered by your organization. It's another to try to determine whether a computer you don't manage meets your admittance criteria. Here are areas that warrant your scrutiny on both managed and unmanaged computers:

- *Antivirus/Anti-malware*  
Does this machine have anti-virus or other anti-malware software installed. If so, what version of the software? What version of the scan engine? Is the machine running with real-time scanning turned on? Is it up to date with the most recent malware definitions? Has the machine been scanned recently?
- *Personal firewall*  
Does this machine have a firewall installed? What version of software is it running? Is the firewall enabled?
- *Patches*  
What operating system and applications is this machine running? Are the system and applications up to date?

These are some of the requirements our CyberGatekeeper customers determine in checking a computer's posture in allowing access to their network. One of the key strengths of CyberGatekeeper is the policy manager, which allows you to develop policies that are granular and flexible to meet these requirements.



### Using CyberGatekeeper for Vulnerability Management, Part 4

CyberGatekeeper policies are built from rules, which are based on tests and

other 'gotchas'?

**A:** Yes, it's definitely possible to use distinct policy sets for each group, even if they share a CyberGatekeeper infrastructure. To do this, you first need to find something that distinguishes one group from the other ... that can be just about anything, including the address range they are assigned on connect, an installed application, a configuration setting, etc. You then create a test to detect this item, and add it to the WHEN conditions of the policies for the new employees. Now simply order these policies above the existing policies in your export set. As newly integrated employees connect and audit, these new policies will apply to them, while all other users would fall through to the same policies they audit against today.

Down the road, if you want to apply the same policies to all users, simply remove the "new" policies from your export set.

The only 'gotcha' that may arise is that the new employees may use a different shared key, which could prevent them from auditing against your infrastructure. There are several ways to synchronize keys, but it's best to contact InfoExpress support to discuss which options may be best for your environment.

### InfoExpress in the News

"Dynamic NAC can be a cost-effective solution for organizations that have many sparsely populated branch offices, because it

piece of information on the target endpoint should be present or not, such as the operating system version, a running process, machine name, machine identifier or registry key, etc.

Conditions are grouped into *Basic tests*, where all conditions within the Basic test must be met on the target endpoint for the test to be true. In other words, conditions are logically AND'ed together in a Basic test. A *Compound test* is a collection of one or more Basic tests, where only one needs to be true for a target endpoint to pass the inspection element: these are logically OR'ed.

Policies consist of two sections: a *When* section and a *Requirements* section. The When section is populated typically with a rule created from a Compound and/or Basic test and it determines whether or not the policy should be applied to the connecting endpoint. (Effectively the "When" wakes up the agent on the appropriate connecting endpoint: at all other times the agent remains dormant and consumes no endpoint resources.)

The Requirements section contains the rules that specify which conditions must be met for the endpoint to be verified compliant. They comprise the integrity inspection policy.

Multiple policies may be applied to the end-configuration or vulnerability control security strategy that you wish CyberGatekeeper to exercise control over.

*When* is the management entry that governs the selection of the appropriate Requirements tests applied on the network-connecting endpoint. ("When" and "When not" are operands that can be used.)

Examples:

- When the endpoint is a "Windows XP" device, use the set of requirements making up policy A.
- When "this particular Machine Identifier is detected," apply the set of requirements making up policy B, irrespective of other endpoint considerations.

More sophisticated assessments can be devised using conditions that apply for the detection of specific software patches, service pack levels, applications, and other custom criteria.

Requirements section conditional rules are interlinked to the When section and are similarly arranged, making up the inspection policy. A test condition in this section are executed by a "Required" or "Prohibited" operand, and those operands are self explanatory, i.e. it is Required that this particular vendors AV software is present and working.

There is a third and fourth conditional operand and they are "Desired" and "Not-Desired": both are powerful options. With "Desire" administrators can monitor and produce audit trails for certain endpoint conditions that they wish to know about but not enforce. As an example of its use, during the roll-out of new endpoint software the project manager can use a Desire test to check on progress throughout the organisation to the point where confidence has been obtained that enforcing its presence will not disrupt user

doesn't require additional hardware ... customer satisfaction with InfoExpress remains high."  
—Gartner, 2009 NAC report

[Hot Security Products at Interop 2010](#)  
CRN, 4/27/2010

[Georgia Legal Services Deploys InfoExpress NAC](#)  
Law Technology News, April 2010

[Nonprofit Boosts Network Security with InfoExpress Dynamic NAC](#)  
eSecurityPlanet, 3/31/2010

[Nonprofit secures guest access with network access control](#)  
SearchNetworking.com, 3/30/2010

---

#### Customers Talk:

**International manufacturer** security chief says "We now have secure remote access, and the security of our internal network is enforced continually." [Read case study](#)

**Financial institution** chief security officer says "With InfoExpress' CyberGatekeeper integrated into our network, we have created a superior level of network security and visibility. CyberGatekeeper used in conjunction with 802.1x gives us the ability to verify that every machine talking to our network is compliant and allows us to avoid dangerous rogue machines that can get in and damage corporate assets." [Read case study](#)

**Rainy River School Board** head of IT says "With Dynamic NAC from InfoExpress, we can protect our network and data from the risks associated with

is to verify that a vulnerability patch roll-out to all the whole endpoint community has actually occurred.

Further, it's through the Requirements section that IT administrators may specify what remediation (*Fix*) actions should be applied when the endpoint fails a conditional test. A Fix is a scripted action, such as an executable that turns back-on the windows firewall, for example. It could also be a process that kicks-off the downloading and installing of a vulnerability patch, the turning off of the wireless port when wired LAN connected, and so on.

This functional capability makes CyberGatekeeper a highly flexible and very valuable tool in combating many forms of vulnerabilities, especially outside the scope of purely vulnerability patch management. Any endpoint condition that leaves a testable footprint on the endpoint can be inspected for, checked and automatically corrected, ensuring that network connectivity is controlled and the user informed as directed by your security governance controls.



### About InfoExpress

[InfoExpress](#) network security solutions protect enterprise networks and the endpoints connecting to them. The company has provided network access control solutions since 2000. At the core of InfoExpress' solution is the award-winning CyberGatekeeper NAC Suite, which ensures endpoints are safe and compliant with security policies by performing real-time audits and quarantining of all network-attached endpoints. InfoExpress products have received numerous awards for innovation. The privately-held company in its 11th year of profitability is headquartered in Mountain View, California.

Visit InfoExpress at [www.infoexpress.com](http://www.infoexpress.com)

rogues and badly configured computers while providing students, teachers, and administrators access to services that enrich the educational process." [Read press release](#)

**Iona College** IT executive says "The CyberGatekeeper made the first day of school a pleasure. We cut nearly four hours out of our typical first day as the CyberGatekeeper simplified access and allowed the students to do the majority of the install and registration for network access themselves, while we provided support staff." [Read press release](#)

**Kelly College** network manager says "While we must ensure the protection of our students and the network, Kelly College cannot commit IS resources to complex system changes, and the InfoExpress solution solves the dilemma for us." [Read press release](#)

This e-newsletter is published bimonthly by InfoExpress. If you are not yet a subscriber, we invite you to [opt-in](#). [InfoExpress Privacy Policy](#)

© Copyright 2010 InfoExpress