

Lumension® NAC Integrator

Integrate with Network Access Control Solutions

With an increasingly mobile workforce and the growth in outsourcing, there are more unmanaged endpoints than ever before that now require access to enterprise networks. Even with the deployment of a vast array of endpoint security solutions, all it takes is one non-compliant endpoint to compromise your network. By enforcing security policies at the point of entry and quickly and automatically bringing endpoints back into policy compliance, you can significantly strengthen your security posture – without impacting business productivity.

Automated Assessment and Remediation of Endpoints for NAC Solutions

Lumension NAC Integrator is an add-on component to *Lumension®* Patch and Remediation that ensures non-compliant endpoints blocked by your access control solution can be automatically reformed back into policy compliance, allowing end users to quickly gain access to the resources and information they need to remain productive.

Lumension's NAC integration solution supports current and emerging NAC frameworks and enables you to define the minimum vulnerability management policies that must be attained on each endpoint before it is granted network access. These access control policies can be enforced globally across the enterprise or down to individual group levels.

Lumension NAC Integrator enables:

- » Definition of policies that must be attained by all machines before network access is granted
- » Policy compliance assessment for endpoints attempting to gain network access
- » Automatic remediation of endpoints that are not compliant with the policy
- » Post-remediation granting of network access
- » Reduced network risk and minimized cost and NAC implementation time

Key Features

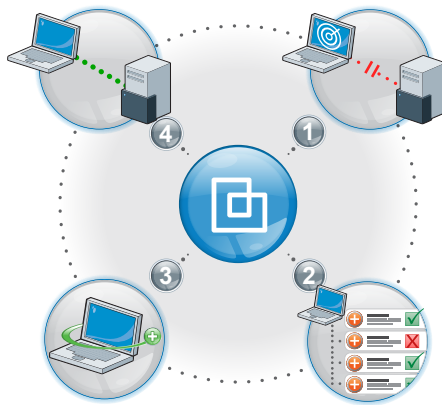
- » Supports Leading NAC Solutions
- » Comprehensive Assessment of IT Assets
- » Automated Remediation Across Heterogeneous Environments
- » Enforce Mandatory Baselines
- » Flexible Policy Definitions
- » Rapid Implementation
- » Flexible Reporting
- » Highly Scalable

Datasheet

Key Benefits

- » Ensures Policy Compliance for All Endpoints Accessing the Network
- » Automatically Remediate Any Endpoints Not in Compliance
- » Minimizes End User Downtime from Network
- » Reduces TCO by Saving IT Operations Time and Effort

How Lumension NAC Integrator Works



1. Endpoints attempt to gain access to the network.
2. Comprehensive agent-based scan proactively assesses applications, operating systems and configurations before access is granted. Endpoints blocked from gaining access due to non-compliance with network access policies.
3. If network access is denied, endpoints are automatically remediated based on defined policies.
4. Endpoints that have been remediated back into policy compliance can now access the network.

Key Features

Supports Leading NAC Solutions: Designed to support current and emerging NAC frameworks, ensuring seamless integration with Cisco NAC Appliance, Cisco Clean Access or Cisco NAC Framework 2.0, Bradford Networks NAC Director or Campus Manager, Forescout CounterACT, Juniper Unified Access Control (UAC), Nortel and all policy based solutions that can read the local registry or pull information via a web service.

Comprehensive Assessment of IT Assets: Provides comprehensive understanding of security posture for managed endpoints via in-depth assessment of vulnerabilities, patch status, security configurations, installed software, and hardware inventory.

Automated Remediation Across Heterogeneous Environments: Vulnerability audits and remediation of security configurations, OS and application vulnerabilities, null passwords, patch-level related vulnerabilities, known hacking tools, malware, common worms, and P2P software checks across major OS platforms (Windows, Linux, MacOS, Sun Solaris, HP, etc.), POSIX and infrastructure devices.

Enforce Mandatory Baselines: Ensures that

all your systems meet a mandatory baseline policy – a key aspect of corporate security and regulatory compliance.

Flexible Policy Definitions: Creates enterprise-wide policies that must be met by every machine attempting to access your network, or group level policies to meet the unique needs of various departments within the organization.

Rapid Implementation: By leveraging your existing Lumension Patch and Remediation implementation, you can significantly reduce the set-up and deployment period for your NAC solution.

Flexible Reporting: More than 20 reports that provide detailed information about the patch and remediation management process, including agent policy status, vulnerability deployments, asset inventory and more.

Highly Scalable: Complete coverage for the largest worldwide networks with high-availability topologies and distribution point architecture. Packages are cached locally, minimizing network traffic and optimizing bandwidth utilization.

www.lumension.com

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Mgmt.

System Requirements

- » **Server:** Windows Server 2003 with Microsoft SQL Server 2005 and .NET Framework
- » **Client (Agents):** Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008

[Complete Requirements](#)

Online Resources

- » [FREE TRIAL](#)
- » [Vulnerability Management Blog](#)
- » [Vulnerability Scanner](#)
- » [Automating the Vulnerability Management Lifecycle](#)

OTIKA

OTIKA

Phone: 01 71 11 31 45

lumension@otika.fr

www.otika.fr

 **Lumension**
IT Secured. Success Optimized.™

LNAC-DS-EN-12-16-09