

Unified Secure Access Solution for Network Access Control

McAfee Unified Secure Access Solution

McAfee® Unified Secure Access is the world's first network access control (NAC) solution to unify endpoint and network security with access control and policy auditing.

Key Advantages

Leverages existing infrastructure

- Easy to acquire and add on components to create a complete NAC solution

Integrates with McAfee ePO

- Uses one unified console for endpoint security, compliance auditing, and access control

Controls admission of employees, partners, and guests

- Provides the right level of network access for different types of users

Reduces errors and cuts support overhead by adapting controls to the situation

- Matches the control to the situation and avoids locking out users by mistake

Controls pre- and post-admission

- Assesses endpoint health and remediates policy violations before or after admission

Detects rogue or unknown machines and devices anywhere on your network

- Detects smartphones, medical devices, game consoles, and more

Offers complete reporting and control

- Detects and reports on endpoint changes, user identity, accessed applications, and malicious behavior

Unlike many existing NAC solutions, McAfee's integrated solution secures against threats inside and outside the network while remaining simple, cost-effective, accurate, scalable, and secure. It expands your security posture with Adaptive Policy Technology that combines multiple assessment and control features into one NAC solution. It controls access and protects against broad threats with application-based and identity-based technologies, which control who has access to your specific critical network resources. Furthermore, Unified Secure Access protects your investment by leveraging your existing network and system components and taking advantage of McAfee's integrated management through McAfee ePolicy Orchestrator® (ePO™).

- McAfee NAC Appliance supports guest access and offers in-line identity and application-based network access control
- McAfee NAC Software supports managed users and offers endpoint health assessment and local access control
- McAfee NAC Module for McAfee Network Security Platform supports guest access by combining NAC and Network Intrusion Prevention



Solution Brief McAfee Unified Secure Access

McAfee Unified Secure Access includes three main components: *McAfee NAC Appliance*, *McAfee NAC Software*, and *McAfee NAC Module for Network Security Platform*. Mix and match these optional products to create a complete Unified Secure Access Solution.

	1 McAfee NAC Appliance	2 McAfee NAC Software	3 McAfee NAC Module for Network Security Platform	Unified Secure Access Solution
Pre-admission control	X		X	X
Post-admission monitoring and control via IPS			X	X
Local access control and remediation		X		X
Guest access portal	X		X	X
Identity- and application-based control	X		X	X
Endpoint health assessment		X		X
Rogue system detection		X		X
Host quarantine	X	X	X	X
ePO integrated	X	X	X	X

Specifications

Model N-450

- 2 Gbps throughput
- Support for in excess of 5,000 concurrent hosts. Note: Actual requirements will vary depending on environment.
- 20 10/100/1000 ports
- Can support 10 in-line segments simultaneously
- SFP supported
- DHCP Servers supported—Microsoft, Infoblox, and Lucent QIP
- VPNs supported—Cisco, Juniper SSL, and Nortel
- Supports high-availability configuration when paired with another appliance
- Active failover support

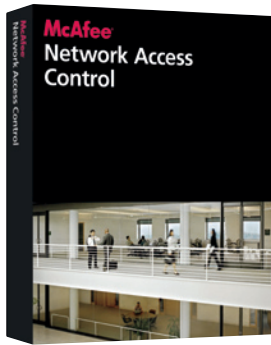
McAfee NAC Appliance

The McAfee NAC Appliance offers the same NAC features as the add-on to the Network Security Platform without the intrusion prevention system (IPS) features. These NAC features, when married with purpose-built hardware, create the most cost-effective enterprise-class platform for NAC. The powerful industry-leading platform provides in-line NAC at line speeds ranging from 100 Mbps to 2 Gbps for 5,000 or more concurrent users.



The NAC module provides the following capabilities:

- **Flexible deployment**—Choice of deploying in Dynamic Host Configuration Protocol (DHCP) mode or in-line behind a VPN or LAN or behind a wireless access point on the network
- **Access control for unmanaged hosts**—Mitigation of unmanaged hosts via secure guest access portal, host posture assessment, and time-based pre-provisioning for guest access
- **Identity-based access control**—Integrates with Microsoft Active Directory to provide network access based on organizational role
- **Comprehensive post-admission control**—Network access control by application protocol, source/destination addresses, and ports
- NAC monitoring and reporting that enable regulatory compliance and risk management
- Simulation mode that allows testing in pilot mode without actual enforcement
- **Risk management**—Integration of NAC monitoring with McAfee Vulnerability Manager to determine if a vulnerable host is attempting frequent network access



Specifications

Note: Actual requirements will vary depending on environment.

McAfee Network Access Control Server

Hardware Requirements:

- Use the same hardware as specified for the ePolicy Orchestrator 4.0 server. When adding McAfee Network Access Control, we suggest using the recommended hardware configuration rather than the minimum configuration. For details, see the ePolicy Orchestrator 4.0 documentation.
- ePolicy Orchestrator 4.0 with patch 2 installed, Rogue System Detection 2.0 or later, and McAfee Network Access Control Client

System Requirements:

- Memory: 512 MB or higher RAM
- Operating System: Windows 2000 Professional, Service Pack 4; Windows 2000 Advanced Server, Service Pack 4; Windows 2000 Server, Service Pack 4; Windows 2000 Terminal Services, Service Pack 4; Windows XP Professional, Service Pack 2 or later; Windows Server 2003 Enterprise, Service Pack 1 or later; Windows Server 2003 Standard, Service Pack 1 or later; Windows Server 2003 Web, Service Pack 1 or later; Windows Vista, all versions; and McAfee Agent 3.6 patch 2 or later

McAfee NAC Software

A key component of McAfee Total Protection for Endpoint—Advanced, McAfee NAC software is the complete solution for managed hosts, such as employees, contractors, and remote users. It has everything you need to define policy, detect rogue or unknown devices, assess health, enforce policy, and remediate.

Key Features

- Policy definition through integrated, centralized McAfee ePolicy Orchestrator version 4.0: simple, flexible, and scalable
- Integrated with the McAfee Network Security Platform and NAC Appliance for enforcement of unmanaged systems
- Simplified compliance and fewer errors by sharing user interface and check library with McAfee Policy Auditor
- Over 3,000 checks based on eXtensible Configuration Checklist Description Format (XCCDF) and Open Vulnerability and Assessment Language (OVAL) policy documents for third-party applications, common software, and OS patches as well as custom checks
- Tightly integrated with Microsoft Network Access Protection (NAP) for control of Windows endpoints
- Complete support for custom checks greatly expands policy flexibility
- Detection and control of managed and unmanaged systems using various techniques: Agent (pre-installed or dissolvable), rogue system detection, Network Security Platform, and Microsoft NAP framework
- Leverages your investment in Microsoft products, including Windows Server 2008, NAP, Windows XP, and Windows Vista
- Easy upgrade from existing McAfee products

Specifications

- Requires v5.1 software
- DHCP servers supported—Microsoft, Infoblox, and Lucent QIP
- VPNs supported—Cisco, Juniper SSL, and Nortel
- Available on all I-Series and M-Series Platforms, with the exception of the M-8000

McAfee NAC Module for Network Security Platform

The NAC Module for Network Security Platform works alongside the intrusion prevention software on purpose-built hardware and integrates with ePolicy Orchestrator for an easily managed NAC solution. The powerful industry-leading platform provides in-line NAC at line speeds ranging from 100 Mbps to 2 Gbps.

The add-on NAC module provides the following capabilities:

- **Flexible deployment**—Choice of deploying in DHCP mode or in-line behind a VPN or LAN or behind a wireless access point on the network
- **Access control for unmanaged hosts**—Mitigation of unmanaged hosts via secure guest access portal, host posture assessment, and time-based pre-provisioning for guest access
- **Identity-based access control**—Integrates with Microsoft Active Directory to provide network access based on organizational role
- **Comprehensive post-admission control**—Network access control by application protocol, source/destination addresses, ports, changing host posture, and IPS-detected malicious behavior
- NAC monitoring and reporting enabling regulatory compliance and risk management
- Simulation mode that enables testing in pilot mode without actual enforcement
- **Risk management**—Integration of NAC monitoring with McAfee Vulnerability Manager to determine if a vulnerable host is attempting frequent network access



Learn More

Visit www.mcafee.com, or call us at 888.847.8766, 24 hours a day, seven days a week. McAfee Network Access Control is part of the McAfee family of business security products and services. McAfee provides a comprehensive portfolio of dynamic risk management and mitigation solutions that secure your business advantage.

Professional Services

Along with our partners, McAfee offers a wide variety of services to help you assess, plan, deploy, tune, and manage your security. For more information, visit www.mcafee.com/us/enterprise/services/index.html.

Technical Support

Make sure that everything runs smoothly during and after installation with flexible programs from McAfee Technical Support. Our highly skilled and certified security specialists possess a wealth of knowledge and resources to meet your security needs. Visit www.mcafee.com/us/enterprise/support/index.html for more information.

