

## Cisco NAC

Cisco® Network Admission Control (NAC) solutions allow network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether networked devices such as laptops, desktops, and other corporate assets are compliant with an organization's security policies, and it repairs vulnerabilities before permitting access to the network.

### Product Overview

Cisco NAC is an easy-to-deploy, end-to-end network registration and enforcement solution. This advanced network security product:

- Recognizes users, their devices, and their roles in the network. This first step occurs at the point of authentication, before malicious code can cause damage.
- Evaluates whether machines are compliant with security policies. Security policies can vary by user type, device type, or operating system.
- Enforces security policies by blocking, isolating, and repairing noncompliant machines. The machines are redirected into a quarantine area, where remediation occurs at the discretion of the administrator.

Cisco NAC can apply posture assessment and remediation services to all devices, regardless of:

- **Device type.** Cisco NAC can enforce security policies on all networked devices, including Windows, Mac, or Linux machines; laptops; desktops; personal digital assistants (PDAs); and corporate assets such as printers and IP phones.
- **Device ownership.** Cisco NAC can apply security policies to systems owned by the corporation, employees, contractors, and guests.
- **Device access method.** Cisco NAC applies network admission control to devices connecting through the LAN, WLAN, WAN, or VPN.

Cisco NAC is unique in its ability to enforce policies for all operating scenarios without requiring separate products or additional modules.

### Features and Benefits

Cisco NAC solutions can benefit organizations in numerous ways:

- NAC addresses compliance requirements by enforcing security policies.
- Unauthorized network access is prevented to protect valuable information assets.
- NAC helps proactively mitigate network threats, such as viruses, worms, spyware, and other malicious applications.
- Vulnerabilities on user machines are minimized through periodic evaluation and remediation.
- Significant cost savings can be achieved by automating the process of identifying, tracking, repairing and updating endpoint machines.

### Authentication Integration with Single Sign-On

Cisco NAC serves as an authentication proxy for most forms of authentication, natively integrating with Kerberos, Lightweight Directory Access Protocol (LDAP), RADIUS, Active Directory, S/Ident, and others. To minimize the inconvenience to end users, Cisco NAC supports single sign-on for VPN clients, wireless clients, and Windows Active Directory domains. Administrators can maintain multiple user profiles with different permission levels through the use of role-based access control.

### Vulnerability Assessment

Cisco NAC supports scanning of all Windows, Mac OS, and Linux-based operating systems and machines, as well as non-PC networked devices such as game consoles, PDAs, printers, and IP phones. It conducts network-based scans or can use custom-built scans as required. Cisco NAC can check for any application as identified by registry key settings, services running, or system files.

### Device Quarantine

Cisco NAC can place noncompliant machines into quarantine, which prevents the spread of infection while enabling the machines to maintain access to remediation resources. Quarantine can be accomplished by using subnets as small as /30, or by using a quarantine VLAN.

### Automatic Security Policy Updates

Automatic security policy updates that are part of Cisco's standard software maintenance package provide predefined policies for the most common network access criteria, including policies that check for critical operating system updates, common antivirus software virus definition updates, and common antispymware definition updates. This eases the management cost for network administrators, who can rely on Cisco NAC to constantly maintain updated policies.

### Centralized Management

The Cisco NAC web-based management console allows administrators to define the types of scans required for each role, as well as the related remediation packages necessary for recovery. One management console can manage multiple servers.

### Remediation and Repair

Quarantining gives devices access to remediation servers that can provide operating system patches and updates, virus definition files, or endpoint security solutions such as Cisco Security Agent. Administrators can enable automated remediation through the optional agent, or specify a series of remediation instructions. In addition, Cisco NAC delivers user-friendly features, such as the monitoring mode and silent remediation, to minimize user impact.

### Flexible Deployment Modes

Cisco NAC offers the broadest array of deployment modes to fit into any customer network. Customers can deploy the product as a virtual or real IP gateway, at the edge or centrally, with Layer 2 or Layer 3 client access, and in-band or out-of-band with network traffic.

### Deployment Modes

Cisco NAC can be deployed in several ways to best accommodate a customer's network. Table 1 illustrates the options for deployment:

**Table 1.** Cisco NAC Deployment Options

Deployment Model	Options
------------------	---------

Deployment Model	Options
Passing traffic mode	<ul style="list-style-type: none"> <li>Virtual gateway (bridged mode)</li> <li>Real IP gateway/NAT gateway (routed mode)</li> </ul>
Physical deployment model	<ul style="list-style-type: none"> <li>Edge</li> <li>Central</li> </ul>
Client access mode	<ul style="list-style-type: none"> <li>Layer 2 (client is adjacent to the Cisco NAC Server)</li> <li>Layer 3 (client is multiple hops from the Cisco NAC Server)</li> </ul>
Traffic flow model	<ul style="list-style-type: none"> <li>In-band (Cisco NAC Server is always in line with user traffic)</li> <li>Out-of-band (Cisco NAC Server is in line only during authentication, posture assessment, and remediation)</li> </ul>

## Product Architecture

Cisco NAC has several core components, with additional optional components for enhanced capabilities.

- Cisco NAC Server:** This device initiates assessment and enforces access privileges based on endpoint compliance. Users are blocked at the port layer and restricted from accessing the trusted network until they successfully pass inspection. The Cisco NAC Server is available in seven sizes based on the number of online, concurrent users: 100, 250, 500, 1500, 2500, 3500, and 5000 users. A single company can have several servers of differing sizes; for example, a headquarters building would require a 1500-user Cisco NAC Server, while a branch office for the same company might only require a 100-user server.
- Cisco NAC Manager:** A centralized, web-based console for establishing roles, checks, rules, and policies. The Cisco NAC Manager is available in three sizes: the Cisco NAC Lite Manager manages up to three Cisco NAC Servers; the Cisco NAC Standard Manager manages up to 20 Cisco NAC Servers; and the Cisco NAC Super Manager manages up to 40 Cisco NAC Servers or 80 Cisco NAC Network Modules.
- Cisco NAC Agent:** A thin, read-only agent that enhances posture assessment functions and streamlines remediation. Cisco NAC Agents are optional and are distributed free of charge.

## Additional NAC Services

In addition to the core Cisco NAC Manager and Server functions of user authentication, device compliance assessment, and role-based access control, several advanced Cisco NAC services yield even greater operational benefits and policy control.

- Cisco NAC Profiler:** The optional Cisco NAC Profiler provides non-PC device profiling by keeping a real-time, contextual inventory of all devices in a network, including non-authenticating devices such as IP phones, printers, and scanners. It significantly reduces the Cisco NAC deployment and management tasks associated with endpoint device discovery and tracking. For the Cisco NAC Profiler data sheet, see [http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product\\_data\\_sheet0900aecd806b7d4e.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806b7d4e.html).
- Cisco NAC Guest Server:** The optional Cisco NAC Guest Server simplifies the provisioning, notification, management, and reporting of guest users on wired and wireless networks, offloading from IT staff much of the challenges commonly associated with supporting corporate visitors. The Secure Guest service enhances IT's ability to protect its own organization's assets, employees, and information while providing secure and flexible network access to meet visitors' business needs. For the Cisco NAC Guest Server data sheet, see [http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product\\_data\\_sheet0900aecd806e98c9.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/product_data_sheet0900aecd806e98c9.html).

Figure 1 is a logical diagram of Cisco NAC in an in-band deployment mode. This configuration works with any 802.11 wireless access point, including Cisco Aironet® access points. The in-band mode is also the preferred deployment mode for VPN traffic.

**Figure 1.** Cisco NAC Architecture in In-Band Mode

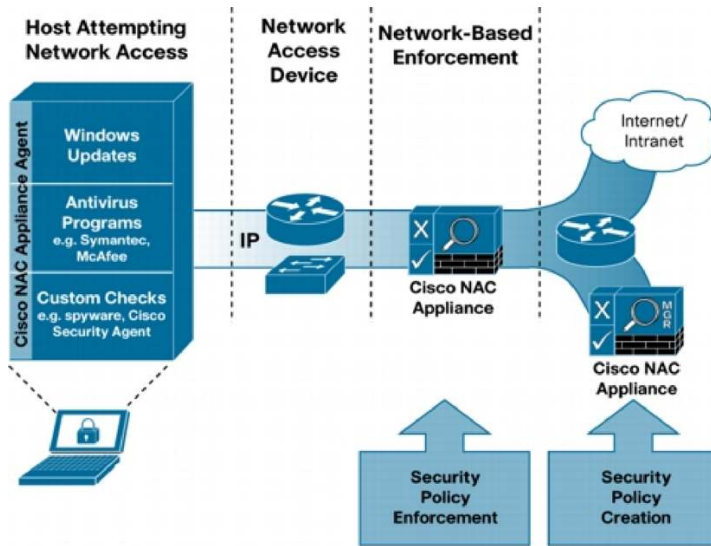
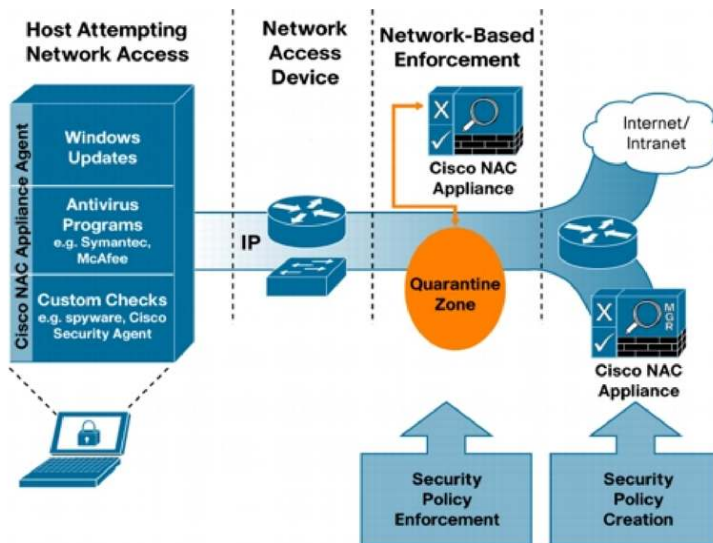


Figure 2 is a logical diagram of Cisco NAC in out-of-band deployment mode. In this mode, the Cisco NAC Server is in-band only during the process of authentication, posture assessment, and remediation. Once a user's device has successfully logged on, its traffic traverses the switch port directly.

**Figure 2.** Cisco NAC Architecture in Out-of-Band Mode



In addition to the traffic flow modes, customers also have a variety of other deployment options to best fit NAC into their network. Table 2 lists additional deployment options.

**Table 2.** Cisco NAC Network Module Deployment Options

Deployment Model	Options
Passing traffic mode	<ul style="list-style-type: none"> <li>Virtual gateway (bridged mode)</li> <li>Real IP gateway (routed mode)</li> </ul>
Client access mode	<ul style="list-style-type: none"> <li>Layer 2 (client is adjacent to the Cisco NAC Server)</li> <li>Layer 3 (client is multiple hops from the Cisco NAC Server)</li> </ul>

Deployment Model	Options
Traffic flow model	<ul style="list-style-type: none"> <li>In-band (Cisco NAC Server is always in line with user traffic)</li> <li>Out-of-band (Cisco NAC Server is in line only during authentication, posture assessment, and remediation)</li> </ul>

While the Cisco NAC in in-band mode supports any network infrastructure, the out-of-band mode communicates with switches using Simple Network Management Protocol (SNMP). Please visit [http://www.cisco.com/en/US/docs/security/nac/appliance/support\\_guide/switch\\_spt.html](http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html) for the most recent list of supported switches. This list is updated frequently.

## Product Specifications

There are three new hardware options that form the bases of the NAC Server and NAC Manager. Table 3 lists the specifications for the hardware appliance versions of Cisco NAC.

**Table 3.** Cisco NAC Hardware Specifications

	Cisco NAC Appliance 3315	Cisco NAC Appliance 3355	Cisco NAC Appliance 3395
<b>Product</b>	<ul style="list-style-type: none"> <li>Cisco NAC Server for 100, 250, and 500 users</li> <li>Cisco NAC Lite Manager</li> </ul>	<ul style="list-style-type: none"> <li>Cisco NAC Server for 1500, 2500, 3500, and 5000 users</li> <li>Cisco NAC Standard Manager</li> </ul>	Cisco NAC Super Manager
<b>Processor</b>	Quad-core Intel Xeon (Core 2 Quad)	Quad-core Intel Xeon (Nehalem)	2 x Quad-core Intel Xeon (Nehalem)
<b>Memory</b>	4 GB	6 GB	8 GB
<b>Hard disk</b>	250-GB SATA drive	2 x 300-GB SAS RAID drives	4 x 300-GB SFF SAS RAID drives
<b>Removable media</b>	CD/DVD-ROM drive	CD/DVD-ROM drive	CD/DVD-ROM drive
<b>Network Connectivity</b>			
<b>Ethernet network interface cards (NICs)</b>	<ul style="list-style-type: none"> <li>2 x Integrated NICs</li> <li>2 x Gigabit NICs (PCI-X)</li> </ul>	<ul style="list-style-type: none"> <li>2 x Integrated NICs</li> <li>2 x Gigabit NICs (PCI-X)</li> </ul>	<ul style="list-style-type: none"> <li>2 x Integrated NICs</li> <li>2 x Gigabit NICs (PCI-X)</li> </ul>
<b>10BASE-T cable support</b>	Category (Cat) 3, 4, or 5 unshielded twisted pair (UTP) up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)
<b>10/100/1000BASE-TX cable support</b>	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)
<b>Secure Sockets Layer (SSL) accelerator card</b>	None	Cavium CN1120-NHB-E	Cavium CN1120-NHB-E
<b>Interfaces</b>			
<b>Serial ports</b>	1	1	1
<b>USB 2.0 ports</b>	4 (two front, two rear)	4 (one front, one internal, two rear)	4 (one front, one internal, two rear)
<b>Keyboard ports</b>	1	1	1
<b>Video ports</b>	1	1	1
<b>Mouse ports</b>	1	1	1
<b>External SCSI ports</b>	None	None	None
<b>System Unit</b>			
<b>Form factor</b>	Rack-mount 1 RU	Rack-mount 1 RU	Rack-mount 1 RU
<b>Weight</b>	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured
<b>Dimensions</b>	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)	1.70 x 16.78 x 27.75 in. (4.32 x 42.62 x 70.49 cm)
<b>Power supply</b>	350W	Dual 675W (redundant)	Dual 675W (redundant)
<b>Cooling fans</b>	6; non-hot plug, nonredundant	9; redundant	9; redundant
<b>BTU rating</b>	2661 BTU/Hr (at 120V)	2661 BTU/Hr (at 120V)	2661 BTU/Hr (at 120V)
<b>Regulatory and Standards Compliance</b>			
<b>Industry certifications</b>	FIPS 140-2 Level 2 Common Criteria EAL2	FIPS 140-2 Level 2 Common Criteria EAL2	FIPS 140-2 Level 2 Common Criteria EAL2

## System Requirements

The optional Cisco NAC Agent works on systems with the characteristics listed in Table 4.

**Table 4.** Cisco NAC Agent System Requirements

Feature	Minimum Requirement
<b>Supported OS</b>	Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC, Windows 2000, Windows 98, Windows SE, Windows ME, Mac OS X
<b>Hard drive space</b>	Minimum of 10 MB of free hard drive space
<b>Hardware</b>	No minimum hardware requirements (works on various client machines)

Cisco NAC also supports single sign-on for wireless and remote-access users using certain IP Security (IPsec) VPN and WebVPN clients. These are outlined in Table 5.

**Table 5.** VPN and Wireless Components Supported with Single Sign-On

Product	Clients
<b>Cisco wireless LAN controllers</b>	–
<b>Cisco ASA 5500 Series Adaptive Security Appliances</b>	<ul style="list-style-type: none"> <li>• Cisco SSL VPN (tunnel)</li> <li>• Cisco IPsec VPN Client</li> </ul>
<b>Cisco WebVPN Service Modules for Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers</b>	
<b>Cisco VPN 3000 Series Concentrators</b>	
<b>Cisco PIX® Security Appliances</b>	

Cisco NAC is preconfigured to offer policy checks for more than 350 applications from 50 vendors. This list is constantly being expanded; please visit [http://www.cisco.com/en/US/products/ps6128/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html) for the latest supported applications (listed under “Cisco NAC Appliance Supported AV/AS Product List”).

**Note:** Not all check types are supported for all products, and some vendors do not support Windows 9x. In addition to the preconfigured checks, the customer has full access to the Cisco NAC rules engine and can create any custom check or rule for any other third-party application.

## Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, see [Cisco Technical Support Services](#) or [Cisco Advanced Services](#).

Warranty information is available at <http://www.cisco.com/go/warranty>. Licensing information is available at [http://www.cisco.com/en/US/docs/security/nac/appliance/support\\_guide/license.html](http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html).

## For More Information

For more information about Cisco NAC, visit <http://www.cisco.com/go/nac/> or contact your local Cisco account representative.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSE, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumina, Cisco Nexus, Cisco Nitro Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mini, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), CiscoFinance (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Register, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCR, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Connum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, ILYN, Internet Quotient, IOS, IPPhone, iQuickStudy, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanel, PowerTV, PowerTV (Design), PowerVu, Prime, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TennaPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (09080)