

## Cisco Network Admission Control for Wireless LANs

This document presents the Cisco<sup>®</sup> Network Admission Control (NAC) support available for Cisco wireless LANs (WLANs) via the NAC Appliance.

### Challenge

Networks must be protected from security threats, such as viruses, worms, and spyware. These security threats disrupt business, causing downtime and continual patching. Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

### Solution

[Network Admission Control](#) is a set of technologies and solutions built on an industry initiative led by Cisco Systems<sup>®</sup>. NAC has been designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices coming into the network. By ensuring that every endpoint device complies with corporate security policy and is running the latest and most relevant security protections, organizations can significantly reduce or eliminate endpoint devices as a common source of infection or network compromise. NAC is part of the Cisco Self-Defending Network, a strategy to dramatically improve the network's ability to automatically identify, prevent, and adapt to security threats.

Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network. The NAC Appliance is a "turn key, self-contained" version of NAC that is an all-in-one, bundled solution.

Networks with Cisco NAC Appliance can realize benefits such as:

- Minimized network outages
- Enforcement of security policies
- Significant cost savings with automated device repairs and updates

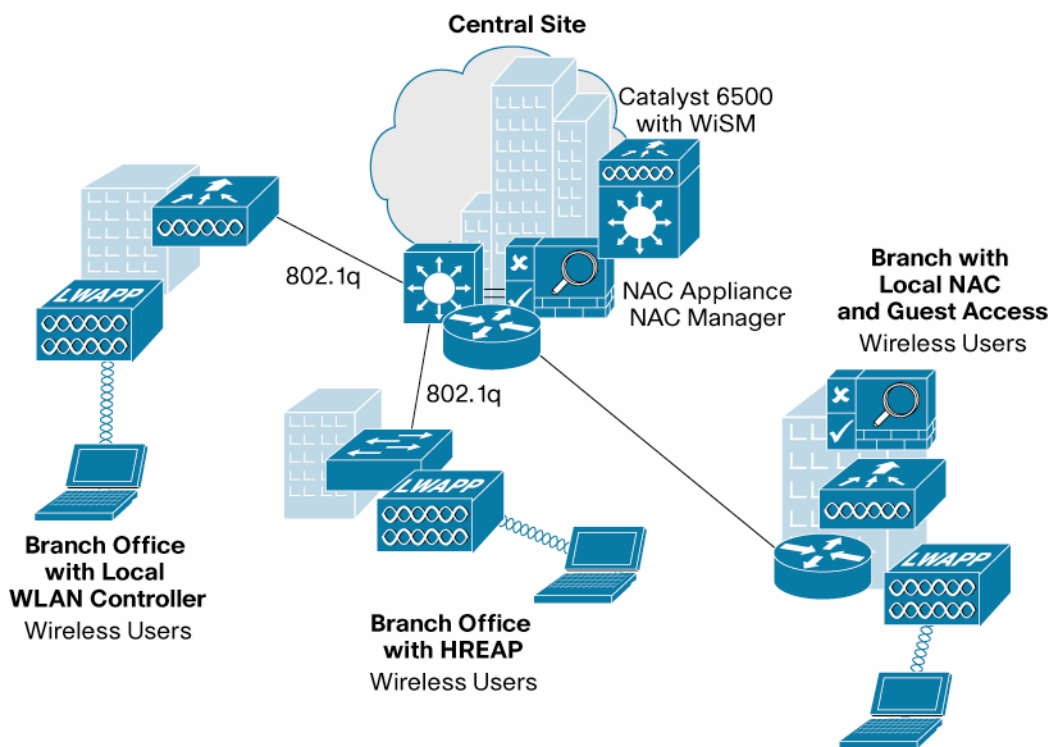
### NAC Appliance for WLANs

WLANs need to be protected from security threats such as viruses, worms, and spyware. The NAC Appliance provides security threat protection for WLANs by enforcing device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine non-compliant WLAN clients and provide remediation services to help ensure compliance. The solution is fully interoperable with the [Cisco Unified Wireless Network](#).

NAC Appliance can apply posture assessment and remediation to any 802.11 wireless user device including [Cisco Aironet®](#) and [Cisco Compatible](#) client devices.

NAC Appliance can be deployed for WLANs as an in-band deployment for full-time endpoint scanning or out-of-band with a central site for periodic scanning to confirm posture compliance. The NAC Appliance server performs authentication, posture assessment, and remediation. The server securely controls authenticated and unauthenticated user traffic by managing traffic policies based on protocol/port or subnet, providing bandwidth policy management based on shared, or per-user bandwidth, or using time-based sessions and heartbeat controls. (Figure 1)

**Figure 1.** NAC Appliance Architecture for Wireless Networks



All wireless users can be subject to NAC Appliance compliance when connecting through any Wi-Fi access point. The following wireless products are supported by NAC Appliance:

- Any 802.11 Wi-Fi access point including:
  - Cisco Aironet access points deployed in stand alone mode—Cisco Aironet [350](#), [1100](#), [1130AG](#), [1200](#), [1230AG](#), [1240AG](#), and [1300](#) series access points.
  - Cisco Aironet lightweight access points deployed with a Cisco Wireless LAN Controller (Access points—Cisco Aironet [1000](#), [1130AG](#), [1200](#)<sup>1</sup>, [1230AG](#), [1240AG](#), [1250](#) and [1500](#) series access points and Cisco—[2100](#) or [4400](#) series wireless LAN controllers as well as the [Cisco Catalyst 6500 Series Wireless Services Module \(WiSM\)](#), the [Cisco Catalyst 3750G Integrated Wireless LAN Controller](#) and the [Cisco Wireless LAN Controller Module](#) for Integrated Services Routers). Cisco Aironet lightweight access points are configured for NAC Appliance compliance via Web-based setup on the wireless LAN controller.

<sup>1</sup> Cisco Aironet 1200 Series access points that contain 802.11g (AIR-MP21G-x-K9) and/or second-generation 802.11a radios (AIR-RM21A-x-K9 or AIR RM22A x K9)

- Any 802.11 Wi-Fi client device including:
  - Cisco Aironet client devices
  - Cisco Compatible client devices

## Summary

Virus and worm invasions continue to disrupt business, causing downtime and continual patching. NAC helps organizations reduce this risk by preventing vulnerable hosts from obtaining and retaining normal network access. NAC helps ensure that all hosts comply with the latest corporate antivirus, security software, and operating system patch policies prior to obtaining normal network access. Vulnerable and noncompliant hosts may be isolated and given reduced network access until they are patched and secured, thus preventing them from being the targets of—or the sources for—worm and virus infections.

NAC is useful to any organization focused on limiting damage from emerging security threats, such as viruses, worms, and spyware. It is beneficial to organizations that are intent upon restricting access to their environments only to approved and compliant assets, or with requirements to audit and monitor all endpoint access within the networked environment. NAC is beneficial to all enterprise organizations, especially those having difficulty managing desktop and server compliance, including contractor and business partner systems. For the same reasons, NAC is also beneficial to smaller organizations. Virtually all industry segments—including financial, healthcare, government, and manufacturing—can benefit from NAC. To achieve comprehensive network coverage, NAC spans across all of the access methods that hosts use to connect to the network—including wireless LANs.

## For More Information

Contact your local account representative or visit the locations below for more information.

For more information about Cisco NAC, visit: <http://www.cisco.com/go/nac>

For more information about Cisco Wireless products, visit: <http://www.cisco.com/go/wireless>

For more information about the Cisco Unified Wireless Network, visit:  
<http://www.cisco.com/go/unifiedwireless>



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).

CCDF, CCENT, Cisco Eos, Cisco StadiumView, the Cisco logo, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn is a service mark and Access Register. Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IQ Experience, the IQ logo, IQ Net, Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MBX, NetScout, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SNAFUTest, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (080239)