

Cisco Network Admission Control (NAC) Solution

New: Updated to include the Cisco Secure Network Server (SNS)

Cisco® Network Admission Control (NAC) solutions allow you to authenticate wired, wireless, and VPN users and devices to the network; evaluate and remediate a device for policy compliance before permitting access to the network; differentiate access based on roles; and then audit and report on who is on the network.

Product Overview

The Cisco NAC Solution is a powerful, easy-to-deploy admission control and compliance enforcement component of the Cisco TrustSec® solution. With comprehensive security features, in-band or out-of-band deployment options, user authentication tools, and bandwidth and traffic filtering controls, the Cisco NAC Solution is a comprehensive offering for controlling and securing networks. You can implement security, access, and compliance policies through a central management point rather than configure policies throughout the network on individual devices.

Features and Benefits

The Cisco NAC Solution is an integral component of the Cisco TrustSec. The Cisco NAC Solution:

- Prevents unauthorized network access to protect your information assets
- Helps proactively mitigate network threats such as viruses, worms, and spyware
- Addresses vulnerabilities on user machines through periodic evaluation and remediation
- Brings you significant cost savings by automatically tracking, repairing, and updating client machines
- Recognizes and categorizes users and their devices before malicious code can cause damage
- Evaluates security policy compliance based on user type, device type, and operating system
- Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention
- Applies posture assessment and remediation services to a variety of devices, operating systems, and device access methods including LAN, WLAN, WAN, and VPN
- Enforces policies for all operating scenarios without requiring separate products or additional modules
- Supports seamless single sign-on through an agent with automated remediation
- Provides clientless web authentication for guest users

Authentication Integration with Single Sign-On

Cisco NAC works with existing authentication sources, natively integrating with Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, Kerberos, S/Ident, and others. For the convenience of 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.

Device Quarantine

Cisco NAC places noncompliant machines into quarantine, preventing the spread of infection while giving the machines access to remediation resources. Through DHCP, inline traffic filters, or a quarantine VLAN, quarantine is achieved.

Automatic Security Policy Updates

Automatic updates in Cisco's standard software maintenance package provide predefined policies for common network access criteria. These include policies that check for critical operating system updates, virus definition updates for antivirus software, and antispyware definition updates. This eases the management cost for network administrators, who can rely on Cisco NAC for constantly updated policies.

Centralized Management

The Cisco NAC web-based management console allows you to define a policy for the entire network, as well as the related remediation packages necessary for recovery. The management console manages the Cisco NAC Servers and network switches from a central interface.

Remediation and Repair

Quarantining allows remediation servers to provide operating system patches and updates, virus definition files, or endpoint security solutions to compromised or vulnerable devices. You enable automated remediation through the optional agent, or specify your own remediation instructions. And Cisco NAC delivers user-friendly features, such as monitoring mode and silent remediation, to minimize user impact.

Flexible Deployment Modes

Cisco NAC offers the right deployment mode to fit your network. The Cisco NAC Solution can be deployed in an in-band or out-of-band configuration. It can be deployed as a Layer 2 bridge and as a Layer 3 router. You can deploy it adjacent to the client on the same subnet or multiple router hops away.

Product Architecture

The Cisco NAC solution is comprised of the following components.

- **Cisco NAC Server:** The NAC Server enforces access privileges based on endpoint compliance and user authentication. A user cannot gain access to the network until they authenticate and the device meets defined posture requirements. The Cisco NAC Server is available in sizes for 100, 250, 500, 1500, 2500, 3500, and 5000 concurrent online users. The NAC Server is available as a standalone appliance. Appliances are available in different configurations and software licenses.
- **Cisco NAC Manager:** This centralized, web-based console for establishing roles, checks, rules, and policies 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. A single Cisco NAC Manager can manage up to 50,000 endpoints.
- **Cisco NAC Agent:** This thin, read-only agent enhances posture assessment functions and streamlines remediation. Cisco NAC Agents are optional and are distributed free of charge.

Additional NAC Services

The Cisco NAC Solution can be optionally deployed with the Cisco Identity Services Engine for profiling services and the NAC Guest Server.

- **Cisco Identity Services Engine (ISE):** Cisco ISE provides profiling capabilities that can discover, analyze, and classify in real time all the endpoints connecting to the network. Cisco ISE comes with hundreds of built-in profiles for devices such as IP phones, printers, mobile devices (IPads, iPhones), scanners, and more, making it possible to identify the type of device connecting to the network. Cisco ISE provides the administrator full visibility into everything connected to the network in real time. It allows the administrator to control the access privileges associated with each type of endpoint.

Starting the Cisco ISE Version 1.0 MR and Cisco NAC Version 4.9, the Cisco ISE can integrate with the Cisco NAC to provide profiler capabilities to a NAC deployment. The combined deployment of the Cisco NAC with the Cisco ISE is the replacement for the Cisco NAC Profiler, which has reached end-of-life status.

To find out more about Cisco ISE, please visit:

http://www.cisco.com/en/US/products/ps11640/products_data_sheets_list.html.

- **Cisco NAC Guest Server:** The optional Cisco NAC Guest Server streamlines the provisioning, notification, management, and reporting of guest users on wired and wireless networks. It offloads resources from IT staff who are charged with supporting corporate visitors. The secure NAC Guest Server enhances your ability to protect your assets, employees, and information while providing network access that fully meets your visitors' business needs. For more information about the Cisco NAC Guest Server data sheet, visit:

http://www.cisco.com/en/US/products/ps10160/products_data_sheets_list.html.

In addition to the traffic flow modes, you have several other deployment options to best fit NAC into your network (see Table 1).

Table 1. Cisco NAC Network Module Deployment Options

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

The Cisco NAC 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 for the most recent list of supported switches.

Product Specifications

The Cisco NAC family now utilizes the Cisco Secure Network Server (SNS), taking advantage of a common hardware platform across NAC Server, NAC Manager, NAC Guest Server, the Identity Services Engine (ISE), and Cisco Secure Access Control Server (ACS) to create a flexible deployment environment.

The Cisco Secure Network Server family is based on the Cisco UCS C220 M3 Rack Server and is configured specifically to support security applications. The Secure Network Server is an innovative platform that supports these applications in two server configurations: SNS-3415 and SNS-3495. The SNS-3415 is designed to be deployed in small and medium-sized deployments, while the SNS-3495 has several redundant components making it suitable for large deployments needing highly reliable system configuration. Table 2 highlights both the SNS-3415 and SNS-3495 in NAC Server and NAC Manager roles.

Table 2. Cisco NAC Hardware Specifications

	Cisco Secure Network Server 3415	Cisco Secure Network Server 3495
Product	<ul style="list-style-type: none"> • Cisco NAC Server for 100, 250, and 500 users • Cisco NAC Lite Manager 	<ul style="list-style-type: none"> • Cisco NAC Server for 1500, 2500, 3500, and 5000 users • Cisco NAC Standard Manager • Cisco NAC Super Manager
Processor	1 x QuadCore Intel Xenon E5-2609 @ 2.4 GHz	2 x QuadCore Intel Xenon E5-2609 @ 2.4 GHz
Memory	4 x 4 GB (16 GB)	8 x 4 GB (32 GB)
Hard disk	1 x 600 GB 6 Gbps SAS 10,000 RPM	2 x 600 GB 6 Gbps SAS 10,000 RPM - Level 1 RAID
Hardware RAID	No	Level 0 & 1 LSI 2008 SAS RAID Mezzanine Card
Network Interfaces	4 x 1 Gb	4 x 1 Gb
Power Supplies	1 x 650 Watts	2 x 650 Watts
Trusted Platform Module	Yes	Yes
SSL Acceleration Card	No	Yes

System Requirements

The optional Cisco NAC Agent works on systems with the characteristics listed in Table 3.

Table 3. Cisco NAC Agent System Requirements

Feature	Minimum Requirement
Supported OS	Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, 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 (v10.5.x, v10.6.x)
Hard drive space	Minimum of 10 MB free hard drive space
Hardware	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 (see Table 4).

Table 4. VPN and Wireless Components Supported with Single Sign-On

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

Cisco NAC is preconfigured to offer policy checks for more than 350 applications from 50 vendors. This list is constantly being expanded; visit 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, you have 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 your success. These innovative programs are delivered through a combination of people, processes, tools, and partners that results 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.

For More Information

For more information about Cisco NAC products and the Cisco TrustSec solution, 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)