# Cisco NAC Appliance with Identity Services Engine Profiler

## Positioning

**Q.** What is the Cisco® NAC Appliance?

**A.** The Cisco NAC Appliance (formerly Cisco Clean Access) is a product that allows 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, IP phones, personal digital assistants, or printers are compliant with an organization's security policies, and repairs any vulnerabilities before permitting access to the network.

**Q.** Why would an organization need the Cisco NAC Appliance?

**A.** One of the greatest inadvertent threats to network security is the end user. Because each endpoint is a potential conduit into the network, it is increasingly important for users to bring their machines into compliance with their organizations' security policies. The Cisco NAC Appliance uses the incentive of network access to ensure compliance, and uses the capabilities of the network to bring noncompliant machines up to requirements.

**Q.** What is the relationship between the Cisco NAC Appliance and Network Admission Control (NAC)?

**A.** The Cisco NAC Appliance is a self-contained solution that delivers Cisco's industry-leading NAC initiative. The Cisco NAC Appliance is easily deployed to mitigate security threats posted by noncompliant machines and unauthorized users.

**Q.** What is the difference between the Cisco NAC Appliance and NAC-like products from companies such as Symantec, Trend Micro, and NAI/McAfee?

**A.** Desktop security companies, including Symantec, Trend Micro, and McAfee, have recently introduced solutions that enforce policies on individual endpoints. The Cisco NAC Appliance is different. It covers the entire lifecycle of policy enforcement: authentication, posture assessment, network quarantine, and remediation. Cisco can offer this robust, integrated set of features because the NAC Appliance uses the network as the enforcement point rather than individual endpoints. As a result, Cisco NAC solutions are more effective, and integrate into the network fabric with greater ease than an endpoint-based approach.

**Q.** Is the Cisco NAC Appliance specific to LAN users? Do I need a separate product to enforce policies on my remote-access users?

**A.** The Cisco NAC Appliance applies a uniform set of policies to all incoming devices, regardless of device ownership, access method, or operating system. Organizations need only one instance of the NAC Appliance to enforce policies on devices coming through LANs, WLANs, VPNs, and WANs.

**Q.** How does the Cisco NAC Appliance fit with Cisco Security Agent?

**A.** Cisco Security Agents reside on each endpoint, protecting them from day-zero attacks through host intrusion prevention technology. The Cisco NAC Appliance focuses on security policy enforcement - making sure that each endpoint meets the security policy requirements before access is granted. The two solutions are complementary: The Cisco NAC Appliance can help enforce that Cisco Security Agent is running on the endpoint device.

**Q.** How can I talk to a Cisco NAC Appliance customer?

**A.** Please contact your Cisco sales representative to facilitate a conversation with a customer.

## Cisco NAC Appliance Components

**Q.** What are the components of the Cisco NAC Appliance?

**A.** The Cisco NAC Appliance comprises three components: the Cisco NAC Server, Cisco NAC Manager, and optional Cisco NAC Agent. As part of the product, customers also receive constant updates of the latest rule sets and checks.

**Q.** Which components do I need for a deployment? Are Cisco NAC Agents sold on a per-seat basis?

**A.** You will need at least one Cisco NAC Manager and one Cisco NAC Server. One Manager can manage multiple Servers. Cisco NAC Agents are not sold on a per-seat basis - they are free.

**Q.** How do I size a Cisco NAC Appliance deployment?

**A.** The number of online, concurrent users in a deployment determines the type and quantity of Cisco NAC Servers required. In turn, the type and quantity of Cisco NAC Servers determines the type of Cisco NAC Manager required.

**Q.** Is there an ongoing cost to receive new updates, vulnerability lists, etc.?

**A.** For a customer that holds a valid Cisco support contract, the updates are included in the current maintenance cost.

**Q.** What is a "failover bundle"? How should it be used?

**A.** A failover bundle contains two Cisco NAC Servers or Managers. This provides redundancy in the event that the production server experiences a disruption. Cisco recommends that all NAC Appliance products include failover.

**Q.** Are both the Manager and Server required even for small installations?

**A.** Yes. Both components are required for all installations. Cisco NAC Managers are available to support 3, 20, or 40 NAC Servers. Servers are available in 100-, 250-, 500-, 1500-, 2500-, 3500-, and 5000-user sizes.

## How the Cisco NAC Appliance Works: General

**Q.** How does the Cisco NAC Appliance work?

**A.** When a device attempts to log onto the network, the Cisco NAC Appliance requests authentication credentials and identifies what kind of device it is. Depending on the role of the user, a posture assessment is performed based on the requirements of the network. If the device is found to be noncompliant, the Cisco NAC Appliance redirects the machine to a quarantine area where the user can perform the necessary downloads to update the machine. The machine is then rescanned and, if compliant, is granted access to the network.

**Q.** Is the Cisco NAC Appliance sold as hardware or as software?

**A.** The Cisco NAC Appliance is available as a rack-mountable hardware appliance. Cisco SMARTnet® support applies.

**Q.** Does the Cisco NAC Appliance work for remote or branch office users using a VPN connection?

**A.** Yes. The Cisco NAC Appliance can be deployed behind other Layer 3 network access devices, including VPN concentrators, dialup servers, and other routers. When the Cisco NAC Appliance detects a new IP address, it will start the authentication-assessment-remediation process.

**Q.** How is a noncompliant machine blocked?

**A.** The Cisco NAC Appliance blocks by either logical or physical means. When deployed inline, the Cisco NAC Appliance is IP-independent and controls admission of noncompliant wireless or wired users by restricting them to a particular subnet and even generating a nonbroadcast, multiaccess topology for virtual segmentation. When deployed out-of-band, the Cisco NAC Appliance blocks noncompliant users at a port layer, preventing them from accessing the network until they pass inspection.

**Q.** Does the Cisco NAC Appliance require administrator rights on end-user computers?

**A.** The Cisco NAC Appliance network scanning component does not require administrator rights. Installing the Cisco NAC Agent requires administrator or power user rights, with capability embedded to enable future Agent updates without requiring administrator or power user rights.

**Q.** Is the Cisco NAC Appliance "choke-point" based? That is, does all traffic have to pass through the Cisco NAC Appliance?

**A.** Cisco offers both in-band and out-of-band versions of the Cisco NAC Appliance. In the out-of-band version, the NAC Appliance communicates directly with the switches to allow or quarantine incoming devices. The specifics of a customer's network may require in-band, out-of-band, or a combination of both.

**Q.** Does an in-band deployment require the placement of multiple Cisco NAC Servers at the access layer?

**A.** No. The Server is logically in-line, not physically. This permits the placement of the Server at the core.

**Q.** Which is better: in-band or out-of-band?

**A.** It depends on what the customer needs. The Cisco NAC Appliance offers customers the flexibility to connect users with either in-band or out-of-band, depending on specific requirements (Table 1).

**Table 1.** In-Band and Out-of-Band Versions of the Cisco NAC Appliance

| | In-Band | Out-of-Band |
|---|---|---|
| **Pros** | • Switch/router platform-independent<br>• Switch/router version-independent<br>• Appropriate for wired and wireless networks<br>• Full network access control<br>• Bandwidth management control | • Inline only for quarantined traffic<br>• Full network access control for quarantined traffic<br>• Switch control using Simple Network Management Protocol (SNMP)<br>• Port- or role-based VLAN assignment<br>• Appropriate for wired networks |
| **Cons** | • Inline dependency<br>• No switch port level control | • Switch platform and version dependencies<br>• Limited bandwidth management controls after remediation |

**Q.** When the Cisco NAC Appliance is deployed out-of-band, how is access prevented?

**A.** As an out-of-band solution, the Cisco NAC Appliance prevents access at the port level by containing noncompliant computers in an authentication/quarantine VLAN.

**Q.** What switches does the Cisco NAC Appliance support when deployed in out-of-band mode?

**A.** The Cisco NAC Appliance currently supports numerous Cisco switches. The latest list can be viewed in the most recent Cisco NAC Appliance release notes at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

**Q.** Can the Cisco NAC Appliance perform roles-based VLAN retagging when deployed in in-band mode?

**A.** Yes. The Cisco NAC Appliance can retag users on the trusted side of the network from one VLAN to another, based on the user's role.

**Q.** Does the Cisco NAC Appliance require exclusively Cisco devices in the access layer?

**A.** No.

**Q.** What happens if a computer on the network is not power-cycled more often than once a week?

**A.** Administrators can set a heartbeat time for inactivity, where inactive machines will be logged off. There are also other options for limiting the user's session time.

**Q.** What happens if a user comes on the network with a static IP address that conflicts with a certified address?

**A.** Actual certification of the user is done based on MAC address. If the user spoofs an IP address, his or her traffic will be dropped.

## How the Cisco NAC Appliance Works: Authentication and Authorization

**Q.** Why is authentication a critical part of Network Admission Control?

**A.** Without authentication, administrators lose a significant degree of control over incoming devices. Authentication helps administrators determine what kind of policies to apply to different types of users, helps ensure confidentiality of data by authorizing access to certain places only to those in the correct role, and prevents unauthorized users from hijacking certified devices.

**Q.** Does the Cisco NAC Appliance support single sign-on?

**A.** Single sign-on is supported for remote-access/VPN users, wireless users, and Windows Active Directory users. When users enter their credentials into the VPN client, wireless Q&A authentication screen, or Windows login prompt, they do not need to re-enter those credentials for the machine to be evaluated for compliance.

**Q.** What forms of authentication are supported by the Cisco NAC Appliance?

**A.** All major forms of authentication are supported, including RADIUS, Lightweight Directory Access Protocol (LDAP), Kerberos, and Windows NT. Since the Cisco NAC Appliance works as an authentication proxy, there is no need to synchronize or replicate an authentication database.

**Q.** Does the Cisco NAC Appliance work with Cisco Secure Access Control Server (ACS)?

**A.** Yes. The Cisco NAC Appliance works with Cisco Secure ACS using RADIUS. The Cisco NAC Appliance also provides detailed RADIUS accounting and failover support.

**Q.** Does the Cisco NAC Appliance use 802.1x for authentication?

**A.** The Cisco NAC Appliance does not require 802.1x for authentication, though it can act as an 802.1x overlay.

## How the Cisco NAC Appliance Works: Scanning and Evaluation

**Q.** What kind of scans does the Cisco NAC Appliance perform?

**A.** The Cisco NAC Appliance performs network- and agent-based scans. Network-based scans look for network vulnerabilities such as remote-procedure call (RPC) buffer overflows or messenger buffer overflows. Agent-based scans check a user's system registry, file system, and system memory for specific services and applications.

**Q.** Can the Cisco NAC Appliance rescan and reevaluate user devices after they have been put onto the certified devices list?

**A.** Yes. The administrator can set the length of time after which all users on the certified devices list will need to be rescanned. Most customers require rescanning between once daily and once weekly. Administrators can also manually reset the certified devices list in the event of high worm and virus activity.

**Q.** Can the Cisco NAC Appliance scan and evaluate non-Windows machines or PDAs, such as those that run on MacOS, Linux, or UNIX?

**A.** Yes. Non-Windows machines and PDAs can undergo network-based scanning. The Cisco NAC Agent also supports Windows and Mac operating systems.

**Q.** Does the Cisco NAC Appliance support networked noncomputer devices such as IP phones, networked printers, and gaming consoles?

**A.** Yes. The Cisco NAC Appliance can enforce security policies as long as the devices have MAC addresses.

**Q.** What happens if an end user has installed a personal firewall that blocks the network scanning?

**A.** This is configurable by the end user, who can either open a port to allow scanning, disable the firewall, or keep it enabled. If the firewall remains enabled, scanning will time out. The administrator can configure what actions to take with timeouts, such as informing the end user about network policy. A personal firewall does not impact agent-based scanning.

**Q.** Does the Cisco NAC Appliance detect only specific antivirus software packages?

**A.** No. The Cisco NAC Appliance has the flexibility to be configured to detect any antivirus software; in fact, it can be configured to look for any application or file. Currently, the Cisco NAC Appliance is pre-packaged with automatic checks from most major antivirus and antispyware vendors, as well as with Microsoft updates.

**Q.** How long does the scanning process take on the client?

**A.** The latency depends on how rigorously you configure your policies. In general, for network scanning, the process takes between 5 and 60 seconds, and the frequency of scans is a configuration option. For agent scanning, the process takes no more than 5 seconds.

**Q.** Can the help desk and/or administrator see scan results for a particular user to assist in remediation?

**A.** Yes. The Cisco NAC Appliance has separate help desk and administrator views for monitoring scan results on end-user machines. As a result, staff can help users remediate if users run into any issues.

**Q.** How is the Cisco NAC Appliance updated with the latest Internet threats and vulnerabilities?

**A.** Cisco conducts automatic, periodic downloads to the Cisco NAC Appliance so that administrators do not have to manually configure dynamic data, such as virus signatures.

## How the Cisco NAC Appliance Works: Quarantine and Remediation

**Q.** How does the Cisco NAC Appliance accomplish quarantining?

**A.** The Cisco NAC Appliance can affect a quarantine in two ways: by placing the noncompliant machine in a specific user role that has restricted access, or by containing the noncompliant machine in a quarantine VLAN or 30 subnet.

**Q.** Does the Cisco NAC Appliance actually clean, or does it just make sure programs are installed and updated so that machines remain clean?

**A.** In the case of a failed Windows hotfix, the Cisco NAC Appliance can automatically launch the Windows AutoUpdate tool. If the Cisco NAC Appliance detects an infection or vulnerability, it can push a fix tool to the user (Symantec's MyDoom Fix Tool, for example) and require that user to use it before accessing the network. In addition, any registry setting that is detected can trigger the download of software or scripts that secure the user's device to meet established security policies.

**Q.** Is the remediation system included in the Cisco NAC Appliance?

**A.** Yes. The remediation system is part of the Cisco NAC Appliance product. It can launch third-party remediation applications, such as IBM's Tivoli or BigFix.

**Q.** Can customers deploy patches and updates through the Cisco NAC Appliance?

**A.** Yes. Customers can provision and deploy patches and updates through the Cisco NAC Appliance, or they can use an existing patch management service.

**Q.** What happens if a Windows-based system is not legally registered and cannot download Windows updates?

**A.** The Cisco NAC Appliance can work with a local Microsoft SUS server.

## How the Cisco NAC Appliance Works: Agent

**Q.** What does the Cisco NAC Agent do?

**A.** The Cisco NAC Agent is an optional, on-device agent that enhances the scanning and compliance mechanisms of the Cisco NAC Appliance.

**Q.** What are the main differences between using the Cisco NAC Appliance with and without a client agent?

**A.** The Cisco NAC Agent enhances two functional areas: device scanning and remediation. In scanning, the Agent enables a scan of the Windows registry, file systems, and system memory to identify compliance with security policies. Policies can include installation of required software (such as antivirus), removal of prohibited programs (such as spyware), or date of latest operating system patch. On the remediation part, the Agent can act as a remediation "wizard," automating the otherwise web-based "click-through" process of cleaning a machine.

**Q.** On which operating systems is the Cisco NAC Agent supported?

**A.** Currently, the Agent supports machines running Windows, beginning with Windows 98, and Macintosh OSX.

**Q.** Can users bypass or disable the Cisco NAC Agent?

**A.** The Agent is a light and robust read-only agent that scans system registries, file systems, and system memories. If it is required as a condition of network access, it must be downloaded to proceed. If users disable the Agent, it does not permit them access to the network; instead, they will need to enable it to log onto the network.

## Deployment Considerations

**Q.** What are the primary deployment considerations for potential customers?

**A.** Determining what kind of solution the customer needs involves four considerations:

- What kind of deployment fits the customer's network best?
- Does the customer need an agent-based solution, an agentless solution, or both?
- Does customer have existing policies to enforce, or will policies need to be created?
- To what methods of network access will customer apply NAC?

Most customers follow a phased approach. For example, they will deploy NAC for remote-access users first, then extend it to wireless users, and finally extend it to users on the LAN. Please consult Cisco NAC Appliance documentation at http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html for more details.

**Q.** I have a network with a typical "star" configuration, where the router sits in the middle. Will I require a Cisco NAC Server on every "leg" of my network?

**A.** Since the Cisco NAC Appliance supports 802.1q trunking, you can direct incoming traffic through the server by configuring the leg on the trunk port. This allows you to deploy the Cisco NAC Appliance in a centralized manner.

**Q.** If I want to deploy "in-band", do I need a Cisco NAC Server at every access point in my network?

**A.** No. The Server is logically in-band, not physically in-band. As a result, you do not need multiple Servers at the edge.

**Q.** Is onsite installation available for the Cisco NAC Appliance?

**A.** Yes. Cisco offers combined onsite installation and training.

**Q.** What browsers are compatible with the Cisco NAC Appliance?

**A.** The Cisco NAC Appliance is compatible with any browser that supports Secure Sockets Layer (SSL) and redirects.

**Q.** What is the average time to set up and install the Cisco NAC Appliance?

**A.** Installation can take as little as one day, and as many as five days.

**Q.** How large of an enterprise, in terms of the number of users, can the Cisco NAC Appliance support?

**A.** Currently, the largest Cisco NAC Appliance deployment supports 63,000 users. The average number of users in a Cisco NAC Appliance deployment is around 8500.

**Q.** How many VLANs does the Cisco NAC Appliance support?

**A.** There is no theoretical limit to the number of VLANs supported by the Cisco NAC Appliance. Practically speaking, deployments should plan about 60 subnets per server.

**Q.** Can I try out the Cisco NAC Appliance?

**A.** Yes. You can download a free copy of the Cisco NAC Manager and Cisco NAC Server from http://www.cisco.com/public/sw-center/ciscosecure/cleanaccess.shtml. (This requires a Cisco.com login. Registration is available at http://tools.cisco.com/RPF/register/register.do.) To obtain a trial license, please visit http://www.cisco.com/go/license, where a 30-day license is available. (This also requires a Cisco.com login.)

## How Cisco NAC Appliance Works with the Identity Services Engine Profiler

**Q.** What is the current status of the Cisco NAC Profiler (Great Bay OEM)?

**A.** The end of life of the NAC Profiler was announced in March 2011, and the Profiler reached end-of-sale status in May 2011. Current customers running the NAC Profiler will be supported until September 2014.

**Q.** Is there a replacement for Cisco NAC Profiler?

**A.** Yes. The Cisco Identity Services Engine 1.0MR2, released in October 2011, provides a profiler service that can be integrated with Cisco NAC Appliance 4.9. This combined integrated offering will replace the Cisco NAC Profiler.

**Q.** Where does the profiling service reside?

**A.** The Cisco Identity Services Engine deployment is separate from a NAC Appliance deployment. The profiling software and components are installed on a separate Identity Services Engine appliance and cannot be installed on existing NAC Appliances.

**Q.** Which Cisco Identity Services Engine license do I need for the profiler service to work?

**A.** Customers will need to purchase both BASE and ADVANCED licenses for the profiler service to work on the Cisco Identity Services Engine.

**Q.** How many Cisco Identity Services Engine endpoint licenses will I need to purchase to deploy the profiling service?

**A.** The total endpoint license count required for Cisco Identity Services Engine licenses to support profiling integration is based on the total count of endpoints added to the device filter list.

**Q.** What type of license is required for the Cisco Identity Services Engine profiling service?

**A.** The Cisco Identity Services Engine profiling service license is a subscription-based license (3 or 5 years). It is not a perpetual license.

**Q.** I understand that the Cisco Identity Services Engine can be sold only by Authorized Technology Providers (ATPs). Is it necessary to use an ATP provider to deploy the Identity Services Engine?

**A.** Yes. The combined profiler solution must be deployed by a Cisco ATP Partner.

**Q.** Can I migrate the configuration from my Cisco NAC Profiler (Great Bay OEM) to the Cisco Identity Services Engine?

**A.** Yes. An existing profiled endpoint configuration can be migrated to the Cisco Identity Services Engine via LDAP or file import.

**Q.** Is the Cisco Identity Services Engine profiler service on par with the NAC Profiler?

**A.** No. The Cisco Identity Services Engine was designed independently; differences do exist between the Cisco NAC Profiler (Great Bay OEM) and the profiler service in the Identity Services Engine.

**Q.** How is the Cisco Identity Services Engine profiler service different from the Cisco NAC Profiler?

**A.** The Cisco Identity Services Engine provides a full-featured wired and wireless profiling solution that integrates with AAA posture services using a RADIUS control plane.

**Q.** Where do I get more information on the Cisco Identity Services Engine ATP Program?

**A.** Go to http://www.cisco.com/web/partners/pr11/atp/index.html.

**Q.** Where do I get more information on the Cisco Identity Services Engine product?

**A.** Information is available at http://www.cisco.com/go/ise.

## For More Information

For more information about the Cisco NAC Appliance, please visit http://www.cisco.com/go/nac/appliance or contact your local account representative. You may also send specific questions to cca-questions@external.cisco.com.