



CHAPTER 1

Introduction

This chapter introduces the Clean Access Server. Topics include:

- [What Is Cisco NAC Appliance \(Cisco Clean Access\)?, page 1-1](#)
- [Cisco NAC Appliance Components, page 1-2](#)
- [Clean Access Server Features, page 1-3](#)
- [Installation Requirements, page 1-4](#)
- [CAS Management Pages Summary, page 1-6](#)
- [Global vs. Local Administration Settings, page 1-7](#)

What Is Cisco NAC Appliance (Cisco Clean Access)?

The Cisco Network Admission Control (NAC) Appliance (also known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, in-band or out-of-band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks. As the central access management point for your network, Cisco NAC Appliance lets you implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices.

The security features in Cisco NAC Appliance include user authentication, policy-based traffic filtering, and Clean Access vulnerability assessment and remediation (also referred to as posture assessment). Clean Access stops viruses and worms at the edge of the network. With remote or local system checking, Clean Access lets you block user devices from accessing your network unless they meet the requirements you establish.

Cisco NAC Appliance is a network-centric integrated solution administered from the web console of the Clean Access Manager (CAM) administration server and enforced through the Clean Access Server (CAS) and (optionally) the Clean Access Agent. You can deploy the Cisco NAC Appliance in the configuration that best meets the needs of your network. The Clean Access Server can be deployed as the first-hop gateway for your edge devices providing simple routing functionality, advanced DHCP services, and other services. Alternatively, if elements in your network already provide these services, the CAS can work alongside those elements without requiring changes to your existing network by being deployed as a “bump-in-the-wire.”

Other key features of Cisco NAC Appliance include:

- Standards-based architecture— Uses HTTP, HTTPS, XML, and Java Management Extensions (JMX).

- User authentication—Integrates with existing back end authentication servers, including Kerberos, LDAP, RADIUS, and Windows NT domain.
- VPN concentrator integration—Integrates with Cisco VPN concentrators (e.g. VPN 3000, ASA) and provides Single Sign-On (SSO).
- Clean Access compliance policies—Allows you to configure client vulnerability assessment and remediation via use of Clean Access Agent or Nessus-based network port scanning.
- L2 or L3 deployment options—The Clean Access Server can be deployed within L2 proximity of users, or multiple hops away from users. You can use a single CAS for both L3 and L2 users.
- In-band (IB) or out-of-band (OOB) deployment options— Cisco NAC Appliance can be deployed in-line with user traffic, or out-of-band to allow clients to traverse the Clean Access network only during vulnerability assessment and remediation while bypassing it after certification (posture assessment).
- Traffic filtering policies—Role-based IP and host-based policies provide fine-grained and flexible control for in-band network traffic.
- Bandwidth management controls—Limit bandwidth for downloads or uploads.
- High availability—Active/Passive failover (requiring two servers) ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) servers and/or CAS servers in high-availability mode.

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the Clean Access Agent. Cisco NAC Appliance checks client systems, enforces network requirements, distributes patches and antivirus software, and quarantines vulnerable or infected clients for remediation **before** clients access the network. Cisco NAC Appliance consists of the following components (in [Figure 1-1](#)):

- **Clean Access Manager (CAM)**—Administration server for Clean Access deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASes if installing a Super CAM). For Out-of-Band (OOB) deployment, the web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP.



Note The CAM web admin console supports Internet Explorer 6.0 or above only, and requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and Clean Access Agent authentication.

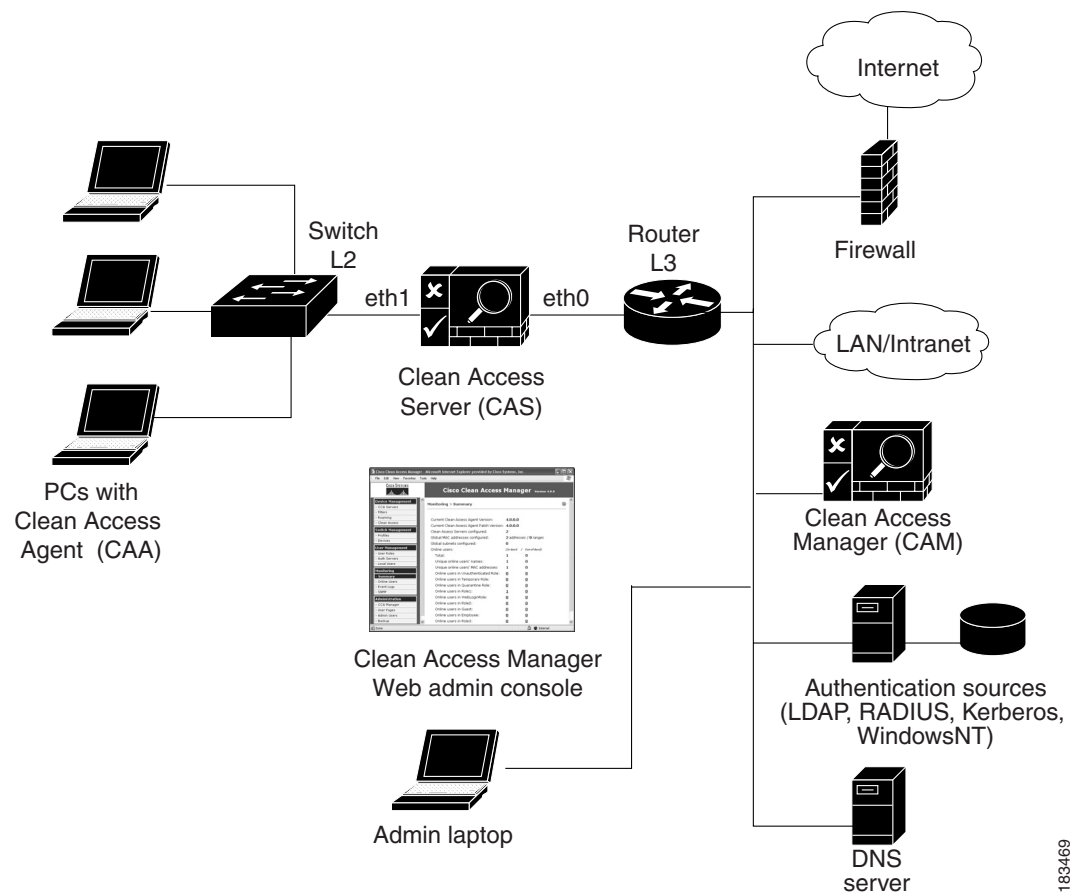
- **Clean Access Server (CAS)**—Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Clean Access system requirements. It can be deployed in-band (always inline with user traffic) or out-of-band (inline with user traffic only during authentication/posture assessment). It can also be deployed in Layer 2 mode (users are L2-adjacent to CAS) or Layer 3 mode (users are multiple L3 hops away from the CAS).
- **Clean Access Agent (CAA)**—Optional read-only agent that resides on Windows clients. The Clean Access Agent checks applications, files, services or registry keys to ensure that clients meets your specified network and software requirements prior to gaining access to the network.



Note There is no client firewall restriction with Clean Access Agent vulnerability assessment. The Agent can check the client registry, services, and applications even if a personal firewall is installed and running.

- **Clean Access Policy Updates**—Regular updates of pre-packaged policies/rules that can be used to check the up-to-date status of operating systems, antivirus (AV), antispyware (AS), and other client software. Provides built-in support for 24 AV vendors and 17 AS vendors.

Figure 1-1 Cisco NAC Appliance Deployment (L2 In-Band Example)



Clean Access Server Features

The following are key features and benefits of the Clean Access Server:

- In-Band or Out-of-Band deployment
- Layer 2 or Layer 3 deployment
- Integration with Cisco VPN concentrators
- Secure user authentication
- Clean Access network-based and agent-based scanning and remediation

- Role-based access control
- DHCP address allocation for untrusted (managed) clients, or DHCP relay or passthrough modes
- Network address translation (NAT) services, with support for dynamic or 1:1 NAT (non-production only)
- Bandwidth management
- Event logging and reporting services
- VLAN support in which the Clean Access Server can be a VLAN termination point, provide VLAN passthrough, and provide VLAN-based access control.
- Flexible deployment options enabling the Clean Access Server to be integrated into most network architectures
- High availability—Active/Passive failover (requiring two servers) that ensures services continue if an unexpected shutdown occurs. You can configure pairs of Clean Access Manager (CAM) servers and/or CAS servers in high-availability mode.

Installation Requirements

This section describes the following:

- [Product Licensing and Service Contract Support](#)
- [Upgrading the Software](#)
- [Cisco NAC Appliance Hardware Platforms](#)
- [Supported Server Hardware Platforms](#)
- [Minimum System Requirements](#)
- [Important Release Information](#)

Product Licensing and Service Contract Support

**Note**

Refer to *Cisco NAC Appliance Service Contract / Licensing Support* for complete step-by-step instructions for how to obtain and install product licenses and obtain service contract support for Cisco NAC Appliances.

Upgrading the Software

Refer to “Upgrading to 4.1(x)” in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(x)* for complete instructions on upgrading your CAM/CAS to the latest software release.

Cisco NAC Appliance Hardware Platforms

The Cisco NAC Appliance 3300 Series provides Linux-based network hardware appliances which are pre-installed with either the CAM (MANAGER) or CAS (SERVER) application, the operating system and all relevant components on a dedicated server machine. The operating system comprises a hardened Linux kernel based on a Fedora core. Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAM or CAS dedicated machine.

**Note**

You can upgrade Cisco NAC Appliance 3300 Series hardware platforms to release 4.1(1) and later. However, the 4.1(0) release is not available for and cannot be installed on NAC 3300 Series platforms. Refer to the applicable [Release Notes](#) for details.

**Note**

The Cisco NAC Appliance 3100 Series includes the Cisco Clean Access 3140 (CCA-3140-H1) NAC Appliance (soon to be EOL). The CCA-3140-H1 requires CD installation of either the Clean Access Server or Clean Access Manager software.

Refer to [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) and the [Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.1\(1\)](#) for complete details on the Cisco NAC Appliance 3300 Series and 3100 Series hardware appliances.

Supported Server Hardware Platforms

If providing your own server hardware on which to install the Cisco NAC Appliance software, the Clean Access Manager is available as software that can be installed on the supported platforms described in [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#).

Minimum System Requirements

Refer to “System Requirements” in the [Supported Hardware and System Requirements for Cisco NAC Appliance \(Cisco Clean Access\)](#) document for details on minimum system requirements to run the Clean Access Manager and Clean Access Server software and Clean Access Agent client software.

Important Release Information

Refer to the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.1\(x\)](#) for additional and late-breaking information on 4.1(x) software releases.

CAS Management Pages Summary

A Clean Access Server must be added to the Clean Access Manager domain before it can be managed from the web admin console, as described in [Add the CAS to the CAM, page 5-2](#). Once you have added the Clean Access Server, you access it from the admin console as shown in the following steps. In this document, *CAS management pages* refers to the set of pages, tabs, and forms accessed as shown below.

1. Click the **CCA Servers** link in the **Device Management** module. The **List of Servers** tab appears by default.

IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.240.10	Out-of-Band NAT Gateway	Dell350	Connected				
10.201.240.12	NAT Gateway	DellPowerEdge750	Connected				

2. Click the **Manage** button for the Clean Access Server you want to access.



Note

For high-availability Clean Access Servers, the Service IP is automatically listed first, and the IP address of the currently active CAS is shown in brackets.

3. The CAS management pages are shown in [Figure 1-2](#). The **Status** tab of appears by default.

Figure 1-2 CAS Management Pages

Module	Status
IP Filter	Started
DHCP Server	Stopped
DHCP Relay	Stopped
IPSec Server	Started
Active Directory SSO	Stopped
Windows NetBIOS SSO	Stopped

Global vs. Local Administration Settings

The Clean Access Manager web admin console has the following types of settings:

- **Clean Access Manager administration settings** are relevant only to the Clean Access Manager. These include its IP address and host name, SSL certificate information, and High-Availability (failover) settings.
- **Global administration settings** are set from the Clean Access Manager and applied to **all** Clean Access Servers. These include authentication server information, global device/subnet filter policies, user roles, and Cisco NAC Appliance configuration.
- **Local administration settings** are set in the CAS management pages of the admin console and apply only to that Clean Access Server. These include CAS network settings, SSL certificates, VPN concentrator integration, DHCP and 1:1 NAT configuration, IPSec key changes, local traffic control policies, and local device/subnet filter policies.

The global or local scope of a setting is indicated in the **Clean Access Server** column in the web admin console, as shown in [Figure 1-3](#).

Figure 1-3 Scope of Settings

Clean Access Server	MAC Address	User	Provi
GLOBAL	00:11:5B:22:27:CF	exempt	exempt
GLOBAL	00:0F:1F:1E:CS:28	exempt	exempt
GLOBAL	00:0C:76:0E:1E:28	exempt	exempt
192.168.0.100	00:08:D8:DC:8F:A8	user1	Local

- **GLOBAL** — The entry was created using a global form in the CAM web admin console and applies to all Clean Access Servers in the CAM's domain.
- **<IP Address>** — The entry was created using a local form from the CAS management pages and applies only for the Clean Access Server with this IP address.

In most cases, global settings are added, edited, and deleted from the global forms used to create them, and local settings are added, edited, and deleted from the local forms used to create them.

Some pages may display global settings (referenced by GLOBAL) and local settings (referenced by IP address) for convenience. Usually, the local settings may be edited or deleted from the global pages but can be **added** only from the local CAS management pages for a particular CAS.

Priority of Settings

Global (defined in CAM for all CASes) and local (CAS-specific) settings often coexist on the same CAS. If a global and local setting conflict, the local setting always overrides the global setting. Note the following:

- For device/subnet filter policies (in which authentication requirements can be bypassed), local (CAS-specific) settings override global (CAM) settings.
- For other settings, such as traffic control policies, the priority of the policy (higher or lower) determines which global or local policy is enforced.
- Some features must be enabled on the CAS first (via the CAS management pages) before being configured in the CAM, for example:

- L3 support for the Clean Access Agent (for multi-hop L3 deployments)
- Bandwidth Management
- Use of VPN policy between CAS and users in user role
- Clean Access requirements and network scanning plugins are configured globally from the CAM and apply to all CASes.