



CHAPTER 1

Introduction

This chapter provides a high-level overview of the Cisco NAC Appliance solution. Topics include:

- [What Is Cisco NAC Appliance \(Cisco Clean Access\)?, page 1-1](#)
- [Cisco NAC Appliance Components, page 1-2](#)
- [Managing Users, page 1-6](#)
- [Installation Requirements, page 1-7](#)
- [Overview of Web Admin Console Elements, page 1-9](#)
- [Clean Access Server \(CAS\) Management Pages, page 1-10](#)
- [Admin Console Summary, page 1-13](#)

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 the Clean Access Agent/Cisco NAC Web 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 backend 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).
- Active Directory SSO—Integrates with Active Directory on Windows Servers to provide Single Sign-On for Clean Access Agent users logging into Windows systems. (Cisco NAC Web Agent does not support 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. The Cisco NAC Web Agent performs vulnerability assessment, but does not provide a medium for remediation. The user must manually fix/update the client machine and “Re-Scan” to fulfill posture assessment requirements with the Web Agent.
- 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) machines and/or CAS machines in high-availability mode.



Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

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 or Cisco NAC Web 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 CASs if installing a SuperCAM). 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/Cisco NAC Web 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.

You can install a CAS as either a stand-alone appliance (like the Cisco NAC-3300 series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis and deploy it In-Band (always inline with user traffic) or Out-of-Band (inline with user traffic only during authentication/posture assessment). The CAS 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).

You can also deploy several CASs of varying size/capacity to fit the needs of varying network segments. You can install Cisco NAC-3300 series appliances in your company headquarters core, for example to handle thousands of users and simultaneously install one or more Cisco NAC network modules in ISR platforms to accommodate smaller groups of users at a satellite office, for example.

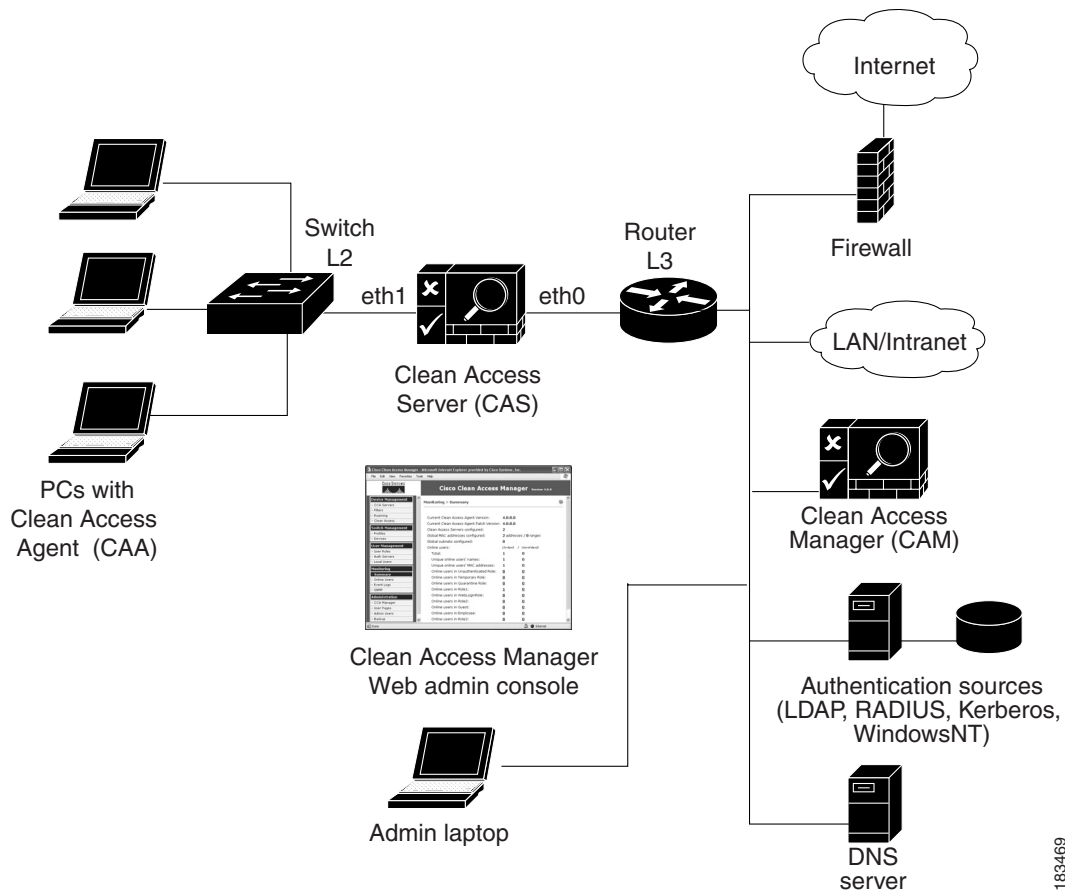
- **Clean Access Agent (CAA)**—Optional read-only Agent that resides on Windows clients. The Clean Access Agent checks applications, files, services or registry keys to ensure that clients meets your specified network and software requirements prior to gaining access to the network.



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.

- **Cisco NAC Web Agent**—The Cisco NAC Web Agent provides temporal vulnerability assessment for client machines. Users launch the Cisco NAC Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet. When the user terminates the Web Agent session, the Web Agent logs the user off of the network and their user ID disappears from the Online Users list.
- **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), antispysware (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)

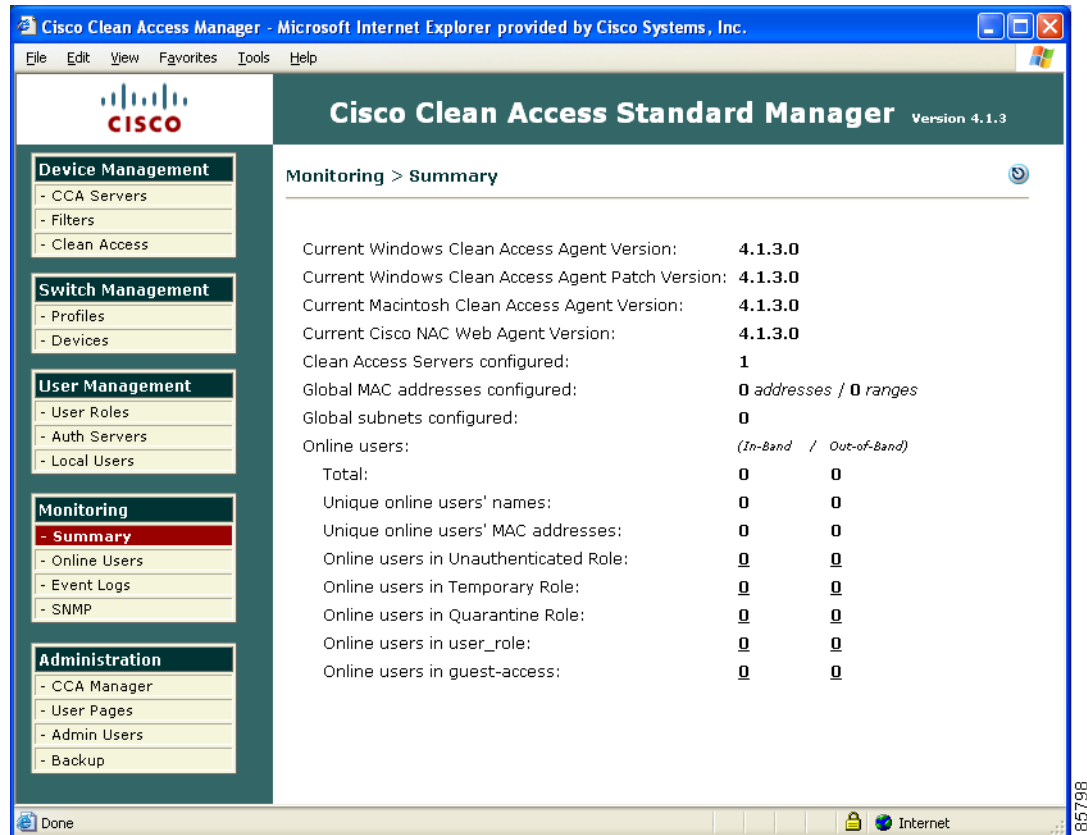


183469

Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface (Figure 1-2). See [Admin Console Summary, page 1-13](#) for a brief introduction to the modules of the web console. For out-of-band (OOB) deployment, the web admin console provides the **Switch Management** module to add and control switches in the Clean Access Manager's domain and configure switch ports.

Figure 1-2 CAM Web Admin Console



Clean Access Server (CAS)

The Clean Access Server (CAS) is the gateway between an untrusted and trusted network. The Clean Access Server can operate in one of the following In-Band (IB) or Out-of-Band (OOB) modes:

- IB Virtual Gateway (L2 transparent bridge mode)
- IB Real-IP Gateway
- IB NAT Gateway (IP router/default gateway with Network Address Translation services)
- OOB Virtual Gateway
- OOB Real-IP Gateway
- OOB NAT Gateway



Note

NAT Gateway (IB or OOB) is not supported for production deployment.

This guide describes the global configuration and administration of Clean Access Servers and Cisco NAC Appliance deployment using the Clean Access Manager web admin console.

For a summary of CAS operating modes, see [Add Clean Access Servers to the Managed Domain](#), page 3-2. For complete details on CAS deployment, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

For details on OOB implementation and configuration, see [Chapter 4, “Switch Management: Configuring Out-of-Band \(OOB\) Deployment.”](#)

For details on options configured locally on the CAS, such as DHCP configuration, Cisco VPN Concentrator integration, CAS High-Availability implementation, or local traffic policies, see the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1\(3\)](#).

Clean Access Agent

When enabled for your Cisco NAC Appliance deployment, the Clean Access Agent can ensure that computers accessing your network meet the system requirements you specify. The Clean Access Agent is a read-only, easy-to-use, small-footprint program that resides on Windows user machines. When a user attempts to access the network, the Clean Access Agent checks the client system for the software you require, and helps users acquire any missing updates or software.

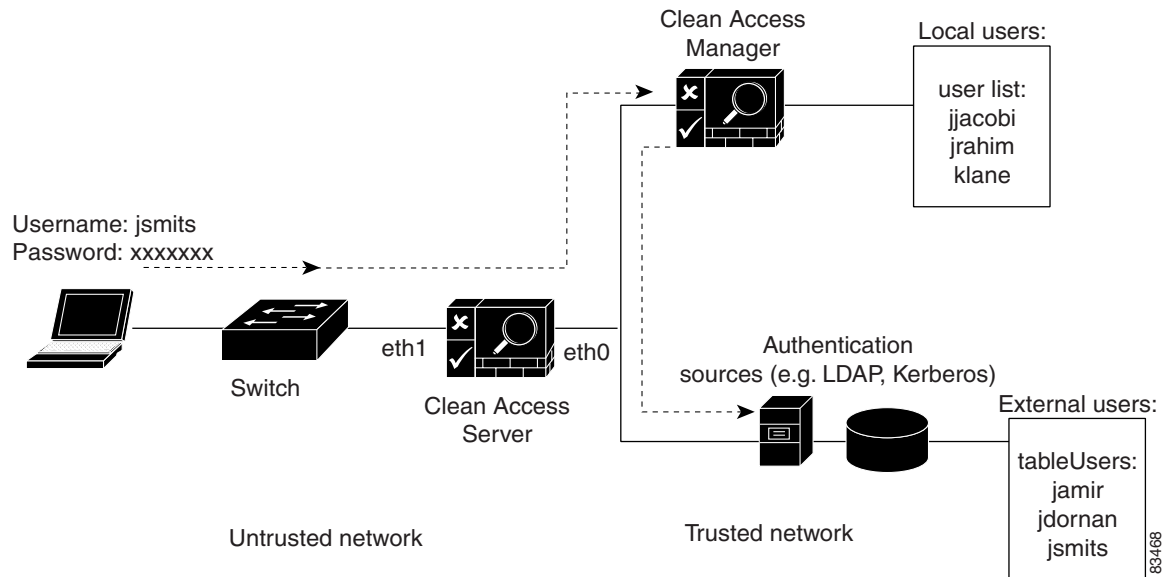
Agent users who fail the system checks you have configured are assigned to the Clean Access Agent Temporary role. This role gives users limited network access to access the resources needed to comply with the Clean Access Agent requirements. Once a client system meets the requirements, it is considered “clean” and allowed network access.

Managing Users

The Clean Access Manager makes it easy to apply existing authentication mechanisms to users on the network ([Figure 1-3](#)). You can customize user roles to group together and define traffic policies, bandwidth restrictions, session duration, Clean Access vulnerability assessment, and other policies within Cisco Clean Access for particular groups of users. You can then use role-mapping to map users to these policies based on VLAN ID or attributes passed from external authentication sources.

When the Clean Access Server receives an HTTP request from the untrusted network, it checks whether the request comes from an authenticated user. If not, a customizable secure web login page is presented to the user. The user submits his or her credentials securely through the web login page, which can then be authenticated by the CAM itself (for local user testing) or by an external authentication server, such as LDAP, RADIUS, Kerberos, or Windows NT. If distributing the Clean Access Agent or Cisco NAC Web Agent, users download and install the Agent after the initial web login, then use the Agent after that for login/posture assessment.

Figure 1-3 Authentication Path



You can configure and apply Clean Access vulnerability assessment and remediation (posture assessment) to authenticated users by configuring requirements for the Clean Access Agent and/or network port scanning (via the Clean Access module of the web admin console).

**Note**

The Cisco NAC Web Agent performs vulnerability assessment, but does not provide a medium for remediation. The user must manually fix/update the client machine and “Re-Scan” to fulfill posture assessment requirements with the Web Agent.

With IP-based and host-based traffic policies, you can control network access for users before authentication, during posture assessment, and after a user device is certified as “clean.”

With IP-based, host-based, and (for Virtual Gateway deployments) Layer 2 Ethernet traffic policies, you can control network access for users before authentication, during posture assessment, and after a user device is certified as “clean.”

**Note**

Layer 2 Ethernet traffic control only applies to Clean Access Servers operating in Virtual Gateway mode.

Finally, you can monitor user activity from the web console through the Online Users page (for L2 and L3 deployments) and the Certified Devices List (L2 deployments only).

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.

When you add the initial CAM license, the top of the CAM web console will display the type of Clean Access Manager license installed:

- **Cisco Clean Access Lite Manager** supports 3 Clean Access Servers
- **Cisco Clean Access Standard Manager** supports 20 Clean Access Servers
- **Cisco Clean Access Super Manager** supports 40 Clean Access Servers (SuperCAM runs only on the NAC-3390 platform)

Additionally, the **Administration > CCA Manager > Licensing** page will display the types of licenses present after they are added. See [Licensing, page 15-21](#) for further details.

Upgrading the Software

Refer to “Upgrading to 4.1(3)” in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(3)* 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 Cisco NAC network module is a CAS you can install in a Cisco 2800 and 3800 Series ISR chassis that features all of the same features and functionality as a stand-alone CAS appliance with one exception; the Cisco NAC network module does not support high availability.



Note

For more information on the Cisco NAC network module, see *Getting Started with NAC Network Modules in Cisco Access Routers* and *Installing Cisco Network Modules in Cisco Access Routers*.

The Cisco NAC Appliance operating system is comprised of 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 the [Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.1\(3\)](#) for further details on the Cisco NAC Appliance 3300 Series 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/Cisco NAC Web Agent client software.

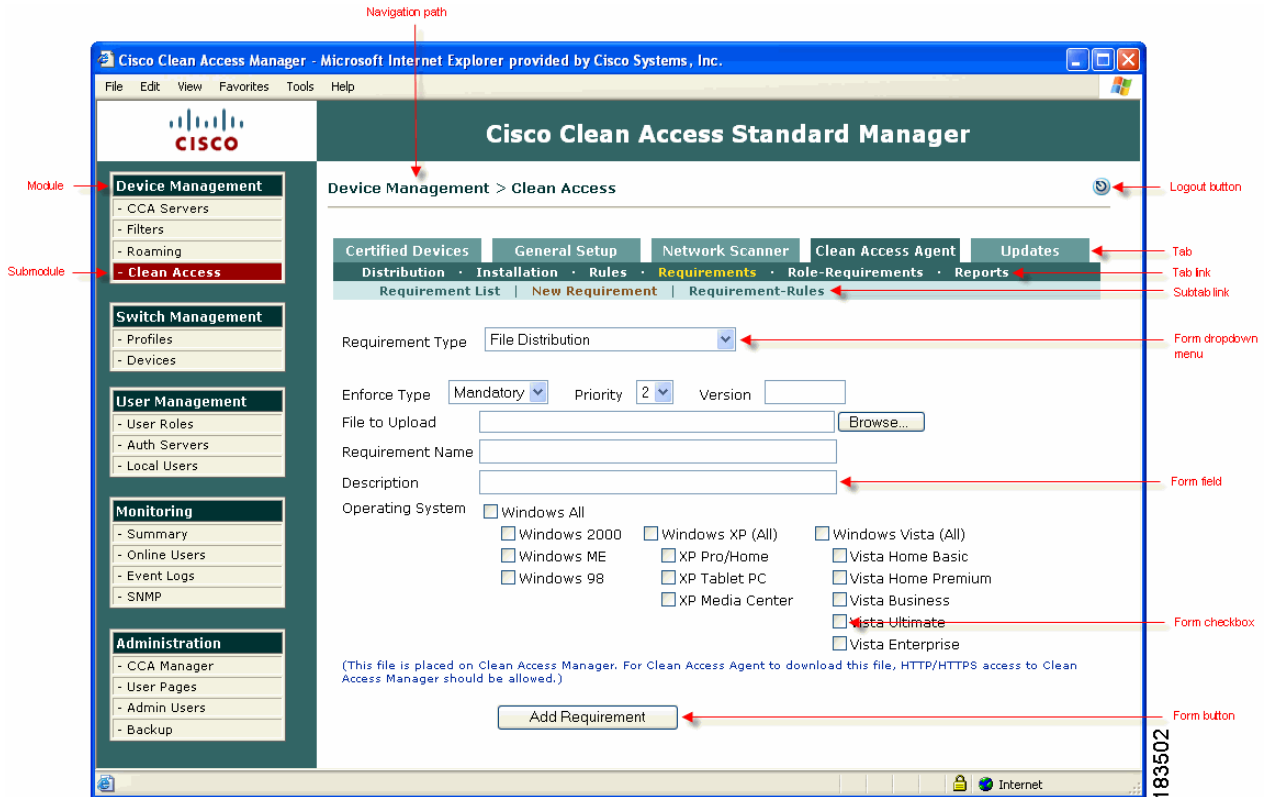
Important Release Information

Refer to the [Release Notes for Cisco NAC Appliance \(Cisco Clean Access\), Version 4.1\(3\)](#) for additional and late-breaking information on 4.1(3) software releases.

Overview of Web Admin Console Elements

Once the Cisco NAC Appliance software is enabled with a license, the web admin console of the CAM provides an easy-to-use interface for managing Cisco NAC Appliance deployment. The left panel of the web console displays the main modules and submodules. The navigation path at the top of the web console indicates your module and submodule location in the interface. Clicking a submodule opens the tabs of the interface, or in some cases configuration pages or forms directly. Configuration pages allow you to perform actions, and configuration forms allow you to fill in fields. Web admin console pages can comprise the following elements shown in [Figure 1-4 on page 1-10](#).

Figure 1-4 Web Admin Console Page Elements

**Note**

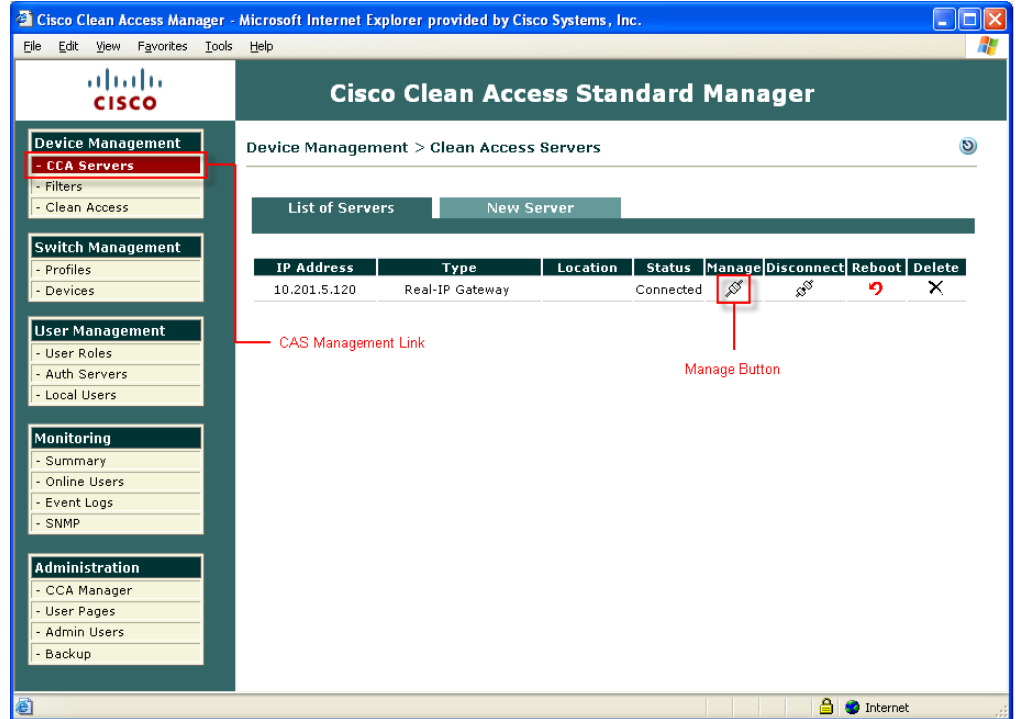
This document uses the following convention to describe navigational links in the admin console:
Module > Submodule > Tab > Tab Link > Subtab link (if applicable)

Clean Access Server (CAS) Management Pages

The Clean Access Server must be added to the Clean Access Manager domain before it can be managed from the web admin console. Chapter 3, “Device Management: Adding Clean Access Servers, Adding Filters,” explains how to do this. Once you have added a Clean Access Server, you access it from the admin console as shown in the steps below. In this document, “CAS management pages” refers to the set of pages, tabs, and forms shown in Figure 1-6.

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

Figure 1-5 CAS List of Servers Page



2. Click the **Manage** button for the IP address of 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 for the Clean Access Server appear as shown in [Figure 1-6](#).

Figure 1-6 CAS Management Pages

Cisco Clean Access Standard Manager

Device Management > Clean Access Servers > 10.201.5.120

Status Network Filter Advanced Authentication Misc

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

Done Internet

186287

Admin Console Summary

Table 1-1 summarizes the major functions of each module in the web admin console.

Table 1-1 Summary of Modules in Clean Access Manager Web Admin Console



Module	Module Description
	<p>The Device Management module allows you to:</p> <ul style="list-style-type: none"> • Add, configure, manage, and perform software upgrade on Clean Access Servers via the CAS management pages (shown in Figure 1-6). See Chapter 3, “Device Management: Adding Clean Access Servers, Adding Filters”. For details on local CAS configuration including AD SSO, DHCP, Cisco VPN Concentrator integration, and CAS High-Availability (failover), see the Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3). For upgrade information, see the “Upgrading to a New Software Release” section of the Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(3). • Configure device or subnet filters to allow devices on the untrusted side to bypass authentication and posture assessment (referred to as “Clean Access certification” in this document) See Global Device and Subnet Filtering, page 3-7 for details. • Configure Clean Access (Network Scanning/Clean Access Agent/Cisco NAC Web Agent) vulnerability assessment and/or remediation per user role and OS. See: <ul style="list-style-type: none"> – Chapter 9, “Clean Access Implementation Overview” – Chapter 13, “Configuring Network Scanning” – Chapter 11, “Configuring Agent Requirements” <p>Note User sessions are managed by MAC address (if available) or IP address, as well as the user role assigned to the user, as configured in the User Management module.</p>
	<p>The Switch Management module is used for Cisco NAC Appliance Out-of-Band deployment. It allows you to:</p> <ul style="list-style-type: none"> • Configure out-of-band Group, Switch, and Port profiles, as well as the Clean Access Manager’s SNMP Receiver. • Add supported out-of-band switches, configure the SNMP traps sent, manage individual switch ports via the Ports (and Port Profile) page and monitor the list of Discovered Clients. <p>See Chapter 4, “Switch Management: Configuring Out-of-Band (OOB) Deployment”</p>

Table 1-1 Summary of Modules in Clean Access Manager Web Admin Console (continued)




Module	Module Description
	<p>The User Management module allows you to:</p> <ul style="list-style-type: none"> • Create normal login user roles to associate groups of users with authentication parameters, traffic control policies, session timeouts, and bandwidth limitations. If using role-based configuration for OOB Port Profiles, you can configure the Access VLAN via the user role. • Add IP and host-based traffic control policies to configure network access for all the user roles. Configure traffic policies/session timeout for Clean Access Agent//Cisco NAC Web Agent Temporary role and quarantine role(s) to limit network access if a client device fails requirements or is found to have network scanning vulnerabilities. • Add Auth Servers to the CAM (configure external authentication sources on your network). • Add auth sources such as Active Directory SSO and Cisco VPN SSO to enable Single Sign-On (SSO) when the CAS is configured for AD SSO or Cisco VPN Concentrator integration. • Create complex mapping rules to map users to user roles based on LDAP or RADIUS attributes, or VLAN IDs. • Perform RADIUS accounting. • Create local users authenticated internally by the CAM (for testing) <p>For details see:</p> <ul style="list-style-type: none"> – Chapter 6, “User Management: Configuring User Roles and Local Users” – Chapter 7, “User Management: Configuring Auth Servers” – Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule” <p>For additional details on Cisco VPN Concentrator integration, see the Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(3).</p>
	<p>The Monitoring module allows you to:</p> <ul style="list-style-type: none"> • View a status summary of your deployment. • Manage in-band and out-of-band online users. • View, search, and redirect Clean Access Manager event logs. • Configure basic SNMP polling and alerting for the Clean Access Manager <p>See Chapter 14, “Monitoring Online Users and Event Logs”.</p>

Table 1-1 Summary of Modules in Clean Access Manager Web Admin Console (continued)

Module	Module Description
	<p>The Administration module allows you to:</p> <ul style="list-style-type: none"> • Configure Clean Access Manager network and high availability (failover) settings. See Chapter 16, “Configuring High Availability (HA)”. • Configure CAM SSL certificates, system time, CAM /CAS product licenses, create or restore CAM database backup snapshots, and download technical support logs. See Chapter 15, “Administering the CAM” • Perform software upgrade on the CAM. See the “Upgrading to a New Software Release” section of the Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(3). • Add the default login page (mandatory for all user authentication), and customize the web login page(s) for web login users. See Chapter 5, “Configuring User Login Page and Guest Access”. • Configure multiple administrator groups and access privileges. See Admin Users, page 15-25.

