Cisco NAC Appliance - Clean Access Server Installation and Administration Guide

Release 4.1
December 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-12213-01

Cisco NAC Appliance - Clean Access Server Installation and Administration Guide

CONTENTS

About This Guide

This preface includes the following sections:

Audience

This guide is for network administrators who are implementing the Cisco NAC Appliance solution to manage and secure their networks. Cisco NAC Appliance comprises the Clean Access Manager (CAM) administration appliance, Clean Access Server (CAS) enforcement appliance, and Clean Access Agent end-user client software. Use this document along with the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* to install and administer your Cisco NAC Appliance deployment.

Purpose

The *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide* describes how to install and configure the Clean Access Server to implement the Cisco NAC Appliance (Cisco Clean Access) solution on your network. The Clean Access Server is the enforcement server between the untrusted and trusted sides of a Cisco NAC Appliance network. This guide provides additional information specific to the Clean Access Server, such as how to configure DHCP, perform CAS-specific (local) configuration tasks, and implement High Availability.

See Product Documentation for further details on the document set for Cisco NAC Appliance.

Document Conventions

Item	Convention
Indicates command line output.	`Screen` font
Indicates information you enter.	**`Boldface screen`** font
Indicates variables for which you supply values.	*`Italic screen`* font
Indicates web admin console modules, menus, tabs, links and submenu links.	**Boldface** font
Indicates a menu item to be selected.	**Administration > User Pages**

Product Documentation

Table 1 lists documents are available for Cisco NAC Appliance on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

Tip To access external URLs referenced in this document, right-click the link in Adobe Acrobat and select "Open Weblink in Browser."

Table 1 Cisco NAC Appliance Document Set

Refer to This Document For Information On:	Document Title
• Which server hardware supports which versions of CAM/CAS software (if using your own server hardware) • CAM/CAS/Agent system requirements • NIC card troubleshooting	Supported Hardware and System Requirements for Cisco NAC Appliance
• Which switches and NMEs support OOB deployment • Known issues/troubleshooting for switches and WLCs	Switch Support for Cisco NAC Appliance
Details on the latest 4.1(x) release, including: • New features and enhancements • Fixed caveats • Upgrade instructions • Supported AV/AS product charts • CAM/CAS/Agent compatibility and version information	Release Notes for Cisco NAC Appliance - Clean Access Version 4.1(x)

Table 1 Cisco NAC Appliance Document Set

Refer to This Document For Information On:	Document Title
Complete CAM details, including: • How to install the CAM software • Overviews of major concepts and features of Cisco NAC Appliance • How to use the CAM web console to perform global configuration of Cisco NAC Appliance (applying to all CASes in the deployment) • How to configure CAM pairs for High Availability	Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide
CAS-specific details, including: • How to install the CAS software • Where to deploy the CAS on the network (general information) • How to perform local (CAS-specific) configuration using the CAS management pages of the CAM web console, or the CAS direct access console. • How to configure CAS pairs for High Availability	Cisco NAC Appliance - Clean Access Server Installation and Administration Guide
Summary of features for release 4.1(0)	What's New in Cisco NAC Appliance 4.1

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Introduction

This chapter introduces the Clean Access Server. Topics include:

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 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 authentication.

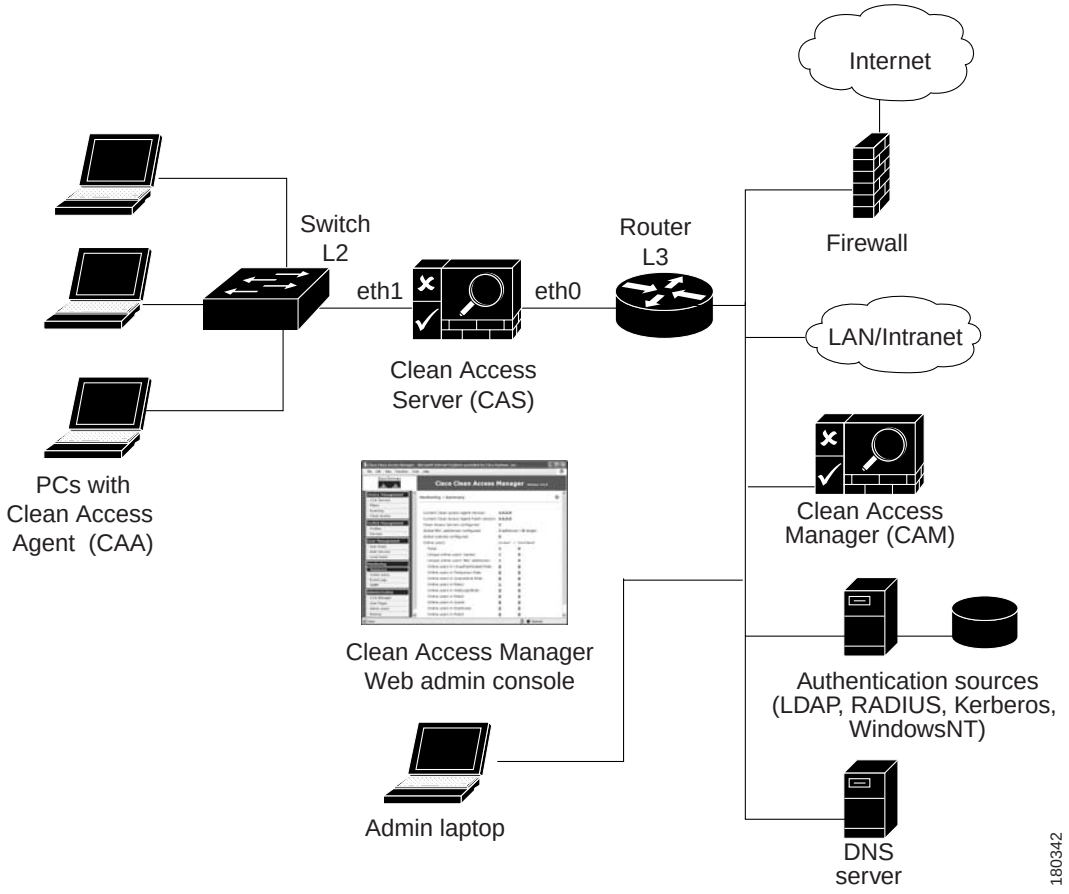
- **Clean Access Server (CAS)**—Enforcement server between the untrusted (managed) network and the trusted network. The CAS enforces the policies you have defined in the CAM web admin console, including network access privileges, authentication requirements, bandwidth restrictions, and Clean Access system 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 will be able to upgrade Cisco NAC Appliance 3300 Series hardware platforms to release 4.1(x). 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.

The Cisco NAC Appliance 3100 Series comprises the Cisco Clean Access 3140 (CCA-3140-H1) NAC Appliance. The CCA-3140-H1 requires CD installation of either the Clean Access Server or Clean Access Manager software. See Installing CCA-3140 Cisco NAC Appliance for instructions.

Refer to Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access) and the Cisco NAC Appliance Quick Start Guide 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.

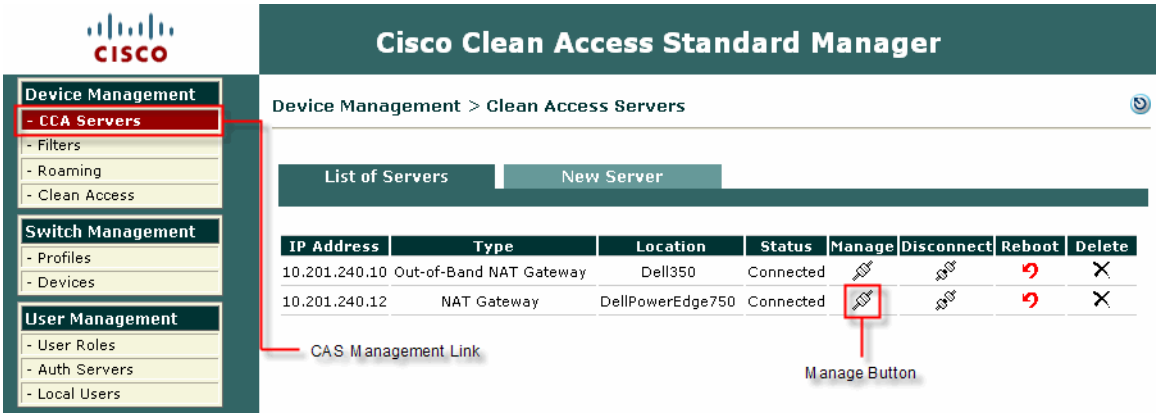
Important Release Information

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.

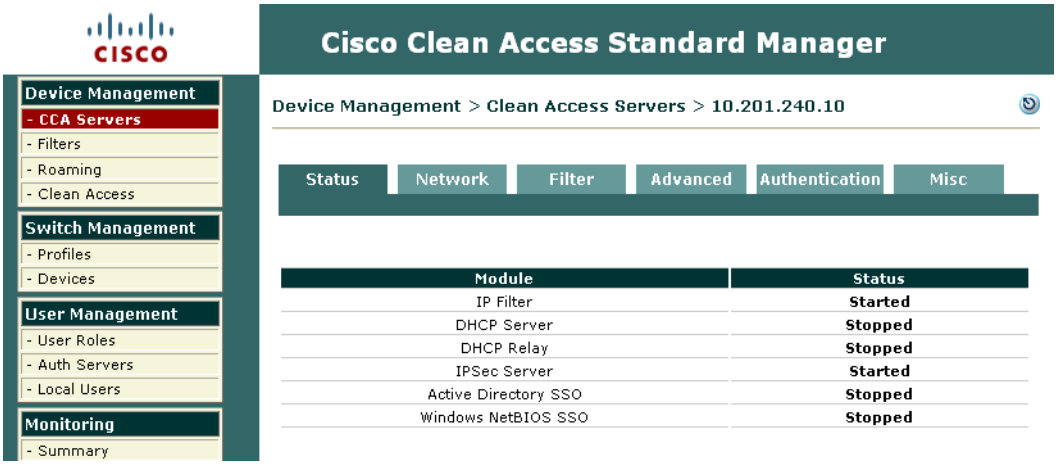


2. Click the **Manage** button ( ) for the Clean Access Server you want to access.

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



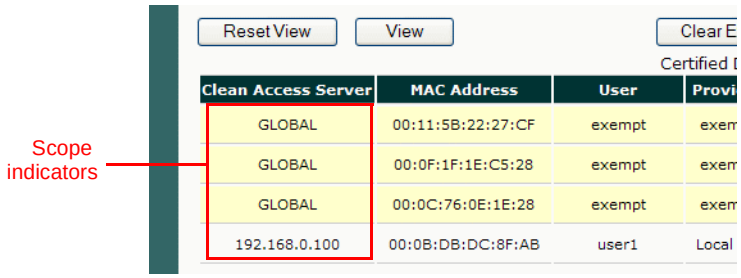
Global vs. Local Administration Settings

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 Clean Access 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



- **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.

Planning Your Deployment

This chapter discusses planning considerations for deploying the software. Topics include:

Overview

Before installing the Clean Access Server (CAS), you should consider how the Clean Access Server will fit into your existing network:

- Choose the operating mode for the Clean Access Server—The operating mode determines the services the Clean Access Server will provide. For example, the CAS can operate as a bridge between the untrusted and trusted network, or it can operate as a gateway for the untrusted network.
- Deploy the Clean Access Server centrally or at the edge of your network.

This chapter describes operating modes and deployment options for the Clean Access Server. It also provides an overview of how the deployment options affect configuration of the Clean Access Server as well as any external elements in your network, such as routers.

Clean Access Server Operating Modes

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) – Operates as a bridge between the untrusted network and an existing gateway, while providing IPSec, filtering, and other services.
- **IB Real-IP Gateway** – Operates as the default gateway for the untrusted network.
- **IB NAT Gateway (for testing only)**– Operates as an IP router/default gateway and performs NAT (Network Address Translation) services for the untrusted network.
- **OOB Virtual Gateway** (L2 transparent bridge mode)— Operates as a Virtual Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).
- **OOB Real-IP Gateway** — Operates as a Real-IP Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

- **OOB NAT Gateway (for testing only)**— Operates as a NAT Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

Note NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because NAT Gateway is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is NOT supported for production deployment. Cisco NAC Appliance uses ports 20000-65535 (45536 connections) for NAT Gateway mode.

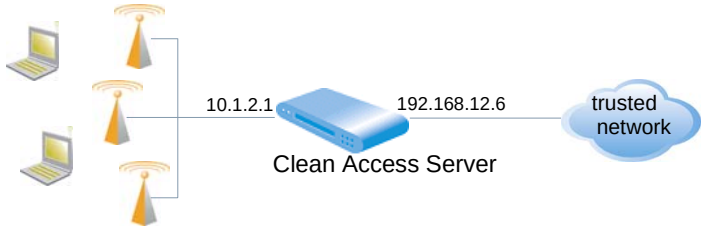
The Clean Access Manager can control both in-band and out-of-band CASes in its domain. However, the Clean Access Server itself must be *either* in-band or out-of-band.

For more information on OOB configuration in the CAM, see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*. The following sections further describe each CAS operating mode.

Real-IP Gateway

In the Real-IP Gateway configuration, the Clean Access Server operates as the default gateway for untrusted network (managed) clients. All traffic between the untrusted and trusted network passes through the Clean Access Server, which applies the IP filtering rules, access policies, and any other traffic handling mechanisms you configure.

Figure 2-1 Real-IP Gateway Configuration



When using the Clean Access Server as a Real-IP Gateway, you need to specify the IP addresses of its two interfaces: one for the trusted side and one for the untrusted side. The two addresses should be on different subnets. The Clean Access Server can manage one or more subnets, with its untrusted interface acting as a gateway for the managed subnets. For details on setting up managed subnets, see Configuring Managed Subnets or Static Routes, page 5-18.

The Clean Access Server does not advertise routes. Instead, static routes must be added to the next hop router indicating that traffic to the managed subnets must be relayed to the Clean Access Server's trusted interface.

Note In Real IP Gateway mode, the CAS can send traffic out of the trusted port in one VLAN only. You cannot configure the switch port connecting to the trusted port of the CAS as a trunk port.

Additionally, when the Clean Access Server is in Real-IP Gateway mode, it can act as a DHCP server or relay. With DHCP server functionality enabled, the CAS provides the appropriate gateway information to the clients, that is, the appropriate gateway IP held by the CAS for the particular managed subnet. If the CAS is working as a DHCP relay, then the DHCP server must be configured to provide the managed

clients with the appropriate gateway information (that is, the appropriate gateway IP held by the CAS for the particular managed subnet). For further details, refer to Configuring Managed Subnets or Static Routes, page 5-18 and Chapter 6, “Configuring DHCP”.

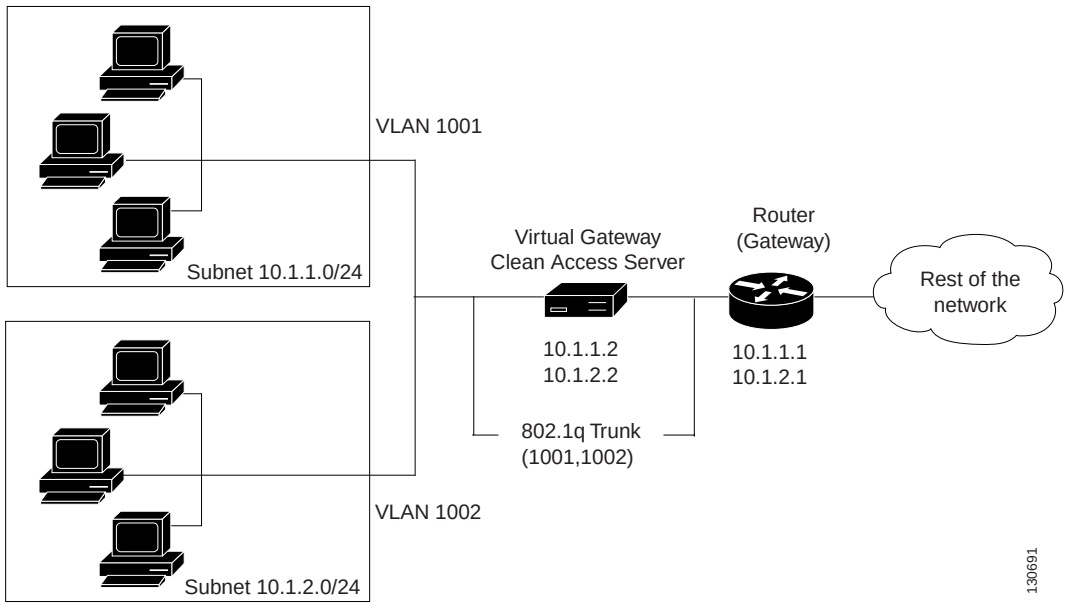
Virtual Gateway

In Virtual Gateway deployment, the Clean Access Server operates as a standard Ethernet bridge, but with the added functionality provided by the IP filter and IPSec module. This configuration is typically used when the untrusted network already has a gateway and you do not wish to alter the existing configuration.

For example, if there are two untrusted subnets, 10.1.1.0/24 and 10.1.2.0/24, with gateways 10.1.1.1 and 10.1.2.1, respectively, the CAS in Virtual Gateway mode is deployed between the untrusted subnets and their gateways (Figure 2-2). The untrusted subnets are configured as “Managed Subnets” in the CAS. Note especially that:

- The CAS needs to have an IP address on each managed subnet.
- Traffic from clients **must** pass through the CAS before hitting the gateway.

Figure 2-2 Virtual Gateway Configuration



When the CAS is a Virtual Gateway:

- The CAS and CAM **must** be on different subnets.
- eth0 and eth1 of the Clean Access Server can have the same IP address.
- All end devices in the bridged subnet must be on the untrusted side of the CAS.
- The CAS should be configured for DHCP forwarding.
- Make sure to configure managed subnets for the CAS. For the example in Figure 2-2, you would configure two managed subnets:
  - 10.1.1.2 / 255.255.255.0 1001
  - 10.1.2.2 / 255.255.255.0 1002

When the CAS is an Out-of-Band Virtual Gateway, the following also applies:

- The CAS and CAM must be on different VLANs.
- The CAS should be on a different VLAN than the user or Access VLANs.

Note

- For Virtual Gateway (In-Band or OOB), it is recommended to connect the untrusted interface (eth1) of the CAS to the switch only **after** the CAS has been added to the CAM via the web console.
- For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See Configure VLAN Mapping for Out-of-Band, page 5-30.

NAT Gateway

In the NAT Gateway configuration, the Clean Access Server functions similarly to the Real-IP Gateway configuration, but adds Network Address Translation (NAT) services. With NAT, clients are assigned IP addresses dynamically from a private address pool. The Clean Access Server performs the translation between the private and public addresses as traffic is routed between the untrusted (managed) and external network. The Clean Access Server supports standard, dynamic NAT and 1:1 NAT. In 1:1 NAT, there is a one-to-one correlation between public and private addresses. With 1:1 NAT, you can map port numbers as well as IP addresses for translation.

Note NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because it is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is not supported for production deployment. See CAM/CAS Connectivity Across a Firewall, page 4-18 for details.

Central Versus Edge Deployment

The Clean Access Server can be deployed either centrally or at the edge of your network. A central deployment reduces the number of Clean Access Servers you need to deploy, facilitating management and scalability. In a central deployment, the Clean Access Server can be configured to perform either routing or bridging for the untrusted network.

Cisco NAC Appliance allows you to achieve multi-hop L3 deployment if you want to move the CAS several hops away from users.

Routed Central Deployment (L2)

In a routed central deployment, the Clean Access Server is configured to act as the Real-IP Gateway for each of the subnets that you wish to manage.

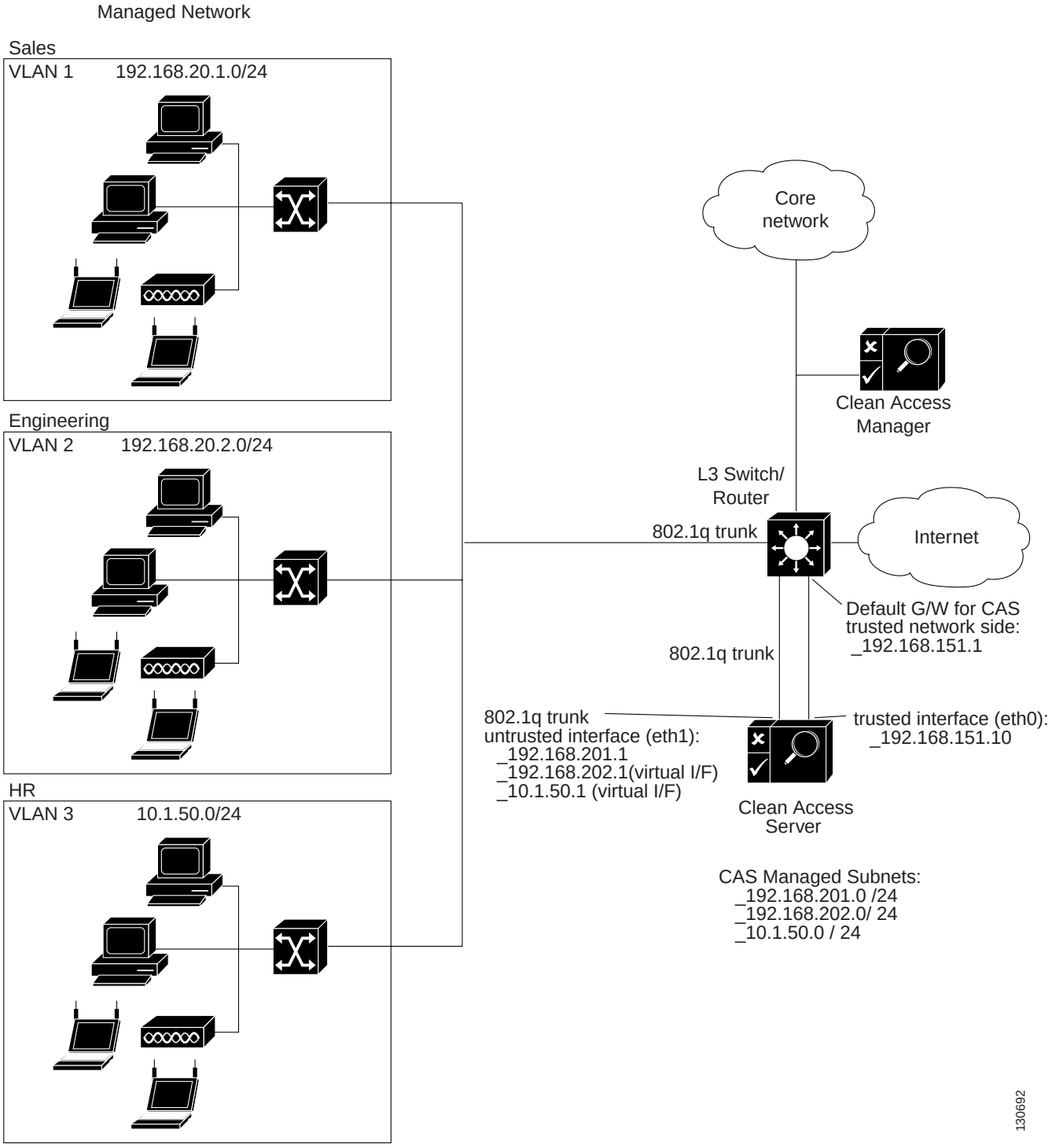
Deployment Steps

The specific steps to deploy a centrally routed Clean Access Server in a typical network include:

1. Turn off routing on your existing Layer 3 switch or router for the subnets that you wish to manage through the CAS.
2. Configure the untrusted interface of the CAS to be the gateway for the managed subnets.
3. Configure the default gateway of the CAS's trusted interface to be the L3 switch or the router.
4. Add static routes on the L3 switch or router to route traffic for the managed subnets to the CAS's trusted interface.
5. If using your own DHCP server, modify its configuration so that the default gateway address that the DHCP server passes to clients with the lease is the address of the CAS's untrusted interface.

In a VLAN-enabled environment, multiple VLANs are trunked through a single Clean Access Server. Aggregating multiple VLANs—organized by location, wiring, or shared needs of users—through a single CAS (by VLAN trunking) can help to simplify your deployment. Figure 2-3 shows a centrally-routed deployment:

Figure 2-3 Routed Central Deployment in a VLAN-Enabled Network



Multi-Hop L3 Deployment

You can choose to deploy the CAS either closer to the edge of the network or several hops away from the network. With centralized L3 deployment, the CAS(es) may be placed several hops away from users. Multi-hop L3 deployment allows:

- Easier deployment. The CAS(es) are deployed between routers, spanning VLANs is not necessary and fewer CASes are needed.
- Not every packet has to go through the CAS. User traffic only needs to traverse the CAS for trusted network access.

However, note that Cisco NAC Appliance policies are enforced at the CAS only. Traffic which does not reach the CAS is not subject to policy enforcement.

Deployment Steps

The specific steps to deploy a centrally routed Clean Access Server in a typical network include:

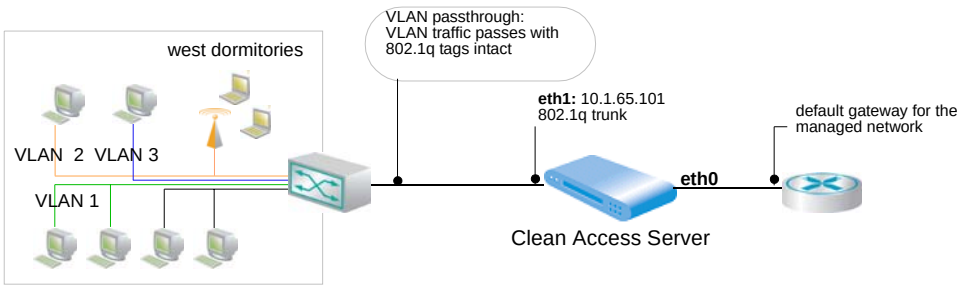
1. Enable L3 on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Network** and clicking the checkbox for "**Enable L3 support for Clean Access Agent**"
2. Managed subnets should be configured for user subnets that are Layer 2 adjacent to the CAS. For user subnets that are one or more hops away from the CAS, static routes should be configured. Hence if enabling L3 support on the CAS, for the L3 users configure their subnets under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes** and NOT under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnets**
3. Set the **Discovery Host** field under **Device Management > Clean Access > Clean Access Agent > Installation**.
4. If enabling the L3 multi-hop feature for VPN concentrator integration, perform all the configuration described in Chapter 8, "Integrating with Cisco VPN Concentrators."

Bridged Central Deployment

In a central deployment with the Clean Access Server configured as a bridge (Virtual Gateway), VLAN trunks are used to aggregate the traffic from the managed subnets to the CAS before being forwarded to their respective gateways on the L3 switch or router.

To ensure that no path exists from the clients to the gateway, it is recommended that you deploy a switch that aggregates all VLANs to the untrusted interface of the CAS, while the trusted interface of the CAS is directly connected to the L3 switch or the router, as shown in Figure 2-4. Note that the Clean Access Server interfaces will be connected to trunked ports and should provide VLAN passthrough.

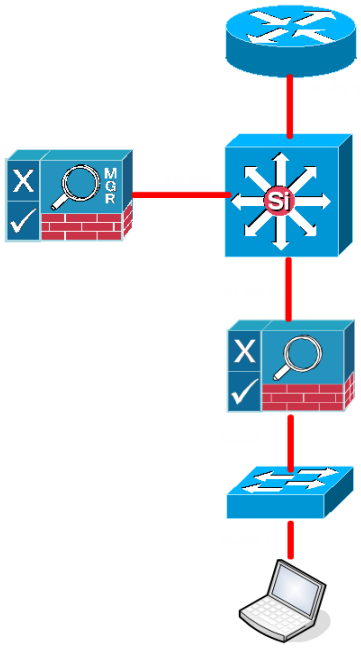
Figure 2-4 Bridged Central Deployment in a VLAN-Enabled Network



Edge Deployment

While central deployment has advantages in terms of reducing the number of required Clean Access Servers, a central deployment is not always possible. For example, if using gigabit throughput to your network's edge, an edge deployment is required. In edge deployment, the Clean Access Server is placed between each managed subnet and router in the network, as illustrated in Figure 2-5. This allows the Clean Access Server to continue to capture MAC addresses for the devices to be managed. In edge deployment, the CAS can act as either a Virtual Gateway or a Real-IP Gateway.

Figure 2-5 Edge Deployment



CAS Operating Mode Summary

Table 2-1 summarizes the features and advantages for each operating mode.

Table 2-1 CAS Operating Mode Summary

CAS Type	Features	Advantages
Virtual Gateway	• CAS acts like a bridge for the managed network • CAS acts as a DHCP passthrough.	• CAS acts in an unobtrusive manner. • Good if you do not want to modify the existing network. • There is no need to define static routes on the main router.
Real-IP Gateway	• CAS acts as a gateway for the managed subnet. • CAS is designated as a static route for the managed subnet. • CAS can perform DHCP services, or act as a DHCP relay.	• Good for situations in which a new subnet can be used for the managed network. • Clients are assigned real IP addresses. • Takes advantage of the CAS's advanced DHCP services.
NAT Gateway	• CAS performs NAT (Network Address Translation) or PAT (Port Address Translation) services, so that clients can use private addresses • Performs DHCP address allocation for managed clients. • All traffic originating from managed clients appears on the trusted side as originating from the Clean Access Server.	• Allows the use of a private address range for managed clients. • Setup is easy: does not involve setting up routes or creating subnets. • Only requires two IP addresses.
OOB Virtual Gateway	• CAS acts like a bridge for the managed network only during the authentication, posture assessment and remediation process. • CAS acts as a DHCP passthrough for Authentication VLAN.	• Once successfully logged on, user traffic bypasses the CAS and traverses the switch ports directly. • User can be logged out via role-based session timer or link-down SNMP traps. • Can be deployed in Edge or Core (central) switches. • No need to bounce client ports. • Recommended configuration if sharing ports between IP phones and PCs.

Table 2-1 CAS Operating Mode Summary

CAS Type	Features	Advantages
OOB Real-IP Gateway	• CAS acts as an inline L3 router for the managed network only during the authentication, posture assessment and remediation process. • CAS can perform DHCP services, or act as a DHCP relay. • User obtains DHCP address from Authentication VLAN. • L3 Switch/router configuration: Configure CAS as default gateway for managed subnets.	• Clients are assigned real IP addresses. • Once successfully logged on, user traffic bypasses the CAS and traverse the switch ports directly. • Port bouncing not required. DHCP release/renew is triggered by 4.1.0.0+ Agent or Active X/ Java Applet downloaded from web login page.
OOB NAT Gateway	• CAS acts as an inline L3 router for the managed network only during the authentication, posture assessment and remediation process. • CAS can perform DHCP services, or act as a DHCP relay. • User obtains DHCP address from Authentication VLAN. • Allows private address range via NAT configuration. • L3 Switch/router configuration: Turn off routing for managed network on L3 Switch or router	• Clients are assigned NAT IP addresses while on Authentication VLAN. • Once successfully logged on, user traffic bypasses the CAS and traverses the switch ports directly. • Need to bounce interface for client to acquire new DHCP address from Access VLAN.

Configuring Layer 3 Out-of-Band (L3 OOB)

This chapter provides a general overview of the configuration needed for Layer 3 Out-of-Band deployment.

For general information on configuring the Cisco NAC Appliance for out-of-band deployment, see "Switch Management and Configuring Out-of-Band (OOB) Deployment" and "Enable the Login Page for L3 OOB" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Overview

Multi-hop L3 support for **in-band** (wired) deployments enables administrators to deploy the Clean Access Server (CAS) in-band centrally (in core or distribution layer) to support users behind L3 Switches (e.g. routed access) and remote users behind VPN Concentrators or remote WAN routers.With L3 IB, users more than one L3 hop away from the CAS are supported and their traffic always goes through Cisco NAC Appliance.

Multi-hop L3 support for **out-of-band** (wired) deployments enables administrators to deploy the CAS out-of-band centrally (in core or distribution layer) to support users behind L3 Switches (e.g. routed access) and remote users behind WAN routers in some instances. With L3 OOB, users more than one L3 hop away from the CAS are supported and their traffic only has to go through Cisco NAC Appliance for authentication/posture assessment only.

Administrators have the option of deploying a remote CAS or L3 IB CAS for remote WAN users, and in some instances using L3 OOB.

Client MAC Address Detection—Clean Access Agent or ActiveX/Java Applet

The MAC detection mechanism of the Clean Access Agent will automatically acquire the client MAC address in L3 OOB deployments.

Users performing web login will download and execute either an Active X control (for IE browsers) or Java applet (for non-IE browsers) to the client machine prior to user login to determine the user machine's MAC address. This information is then reported to the CAS and the CAM to provide the IP address/ MAC address mapping.

ActiveX/Java Applet and Browser Compatibility

- ActiveX is supported on IE 6.0 for Windows XP and Windows 2000 systems.
- **IE 7.0 Beta is not supported when the Clean Access Agent is installed**. For the Agent to login and perform other operations, users must uninstall IE 7.0 Beta 2.

- Java applets are supported for major browsers including Safari 1.2+, Mozilla (Camino, Opera), and Internet Explorer on Windows XP, Windows 2000, MacOS 10, and Linux operating systems.
- Due to Firefox issues with Java, Java applets are not supported for Firefox on Mac OS X. See the Firefox release notes (http://www.mozilla.com/firefox/releases/1.5.0.3.html) for details.

Note **For MAC OS Clients:** On Apple MacOS, the browser settings to bypass proxy must have the full CAS IP address (e.g. 10.201.217.93) in order for the client machine to load the Java Applet and login successfully.

Note **For Linux OOB Clients:**

Because Linux machines behave differently than Windows/Mac OS clients (i.e. do not release IP address when NIC is down and renew IP address when NIC is up), use the following steps for OOB Linux clients:

1. Set a short lease time (e.g. 60 seconds) for the DHCP server on the Auth VLAN.
2. In the **Port Profile**, disable (uncheck) the **"Remove out-of-band online user when SNMP linkdown trap is received**" option.

   This will cause the Linux client to renew its IP address shortly after authentication/certification.

   Note Because Linux shuts down/restarts the NIC when renewing the IP address, if this option is enabled (checked) in the Port Profile, the renewal will set the port back to the Auth VLAN.

3. Alternatively, you can set the Port Profile to: "**Change to [Access VLAN] if the device is certified but not in the out-of-band user list**." This ensures the port stays on the Access VLAN for an authenticated/certified Linux client that is reconnecting to the port after renewing its DHCP lease.

This new feature modifies the following web admin console pages:

- A new checkbox and dropdown menu is added for "**Use Active X or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address**" in the following user login configuration pages:
  - CAM web console: **Administration > User Pages > Login Page > List [Edit] | General**
  - CAS management pages: **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page > List [Edit] > General**
- **Device Management > Clean Access > Updates** (version information for updates to L3 Java Applet Web Client and L3 ActiveX Web Client)

In addition, the web login pages for L3 OOB users will reflect status information related to loading the Active X control or Java applet, and renewing the client IP address.

Layer 3 Out-of-Band Deployment Use Cases

- OOB is for wired deployments only
- L3 OOB is best used in Routed Access deployments
- L3 OOB can also be used for Remote WAN sites but considerations/tradeoffs with other deployments, such as:
  - Remote CAS to WAN sites
  - L3 IB CAS in Central site to support WAN sites

Layer 3 Out-of-Band L2 vs L3 OOB Implementation

In L2 OOB:

- Users are Layer 2 adjacent to the CAS
- User device connects to switch, switch sends SNMP trap to CAM
- CAM gets device mac and port information from switch
- CAS receives packets and sends source IP/MAC info to CAM
- CAM now has complete mapping IP/MAC/Port
- Once device is certified to be compliant, CAM knows which port to change VLAN

In L3 OOB

- Users are one or more hops away from the CAS
- CAM still gets device MAC and port information from switch
- CAS receives packets with user's IP
- CAS gets MAC information from either Agent or web-login page enabled for ActiveX/Java Applet to determine device MAC address and report it back to CAS
- CAS informs CAM of IP/MAC of device
- CAM has complete IP-MAC-Port mapping

Layer 3 Out-of-Band L3 OOB Details

Using the CCA Agent

The Agent will inform CAS of the device MAC address.

Without the CCA Agent (using weblogin)

- Web-login page will download Active-X Control or Java Applet to determine device MAC address and report it back to CAS
- CAS informs CAM of IP/MAC of device
- CAM has complete IP-MAC-Port mapping

Layer 3 OOB: Configuration

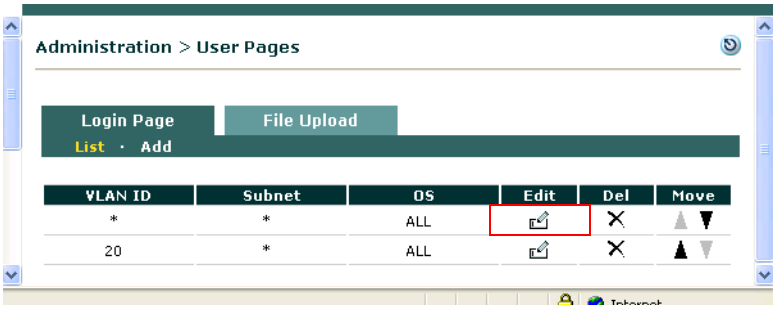
With CCA Agent

- CCA Agent will inform CAS of MAC address
- No additional configuration is needed

Without CCA Agent (using Web Login)

Configure the Login Page

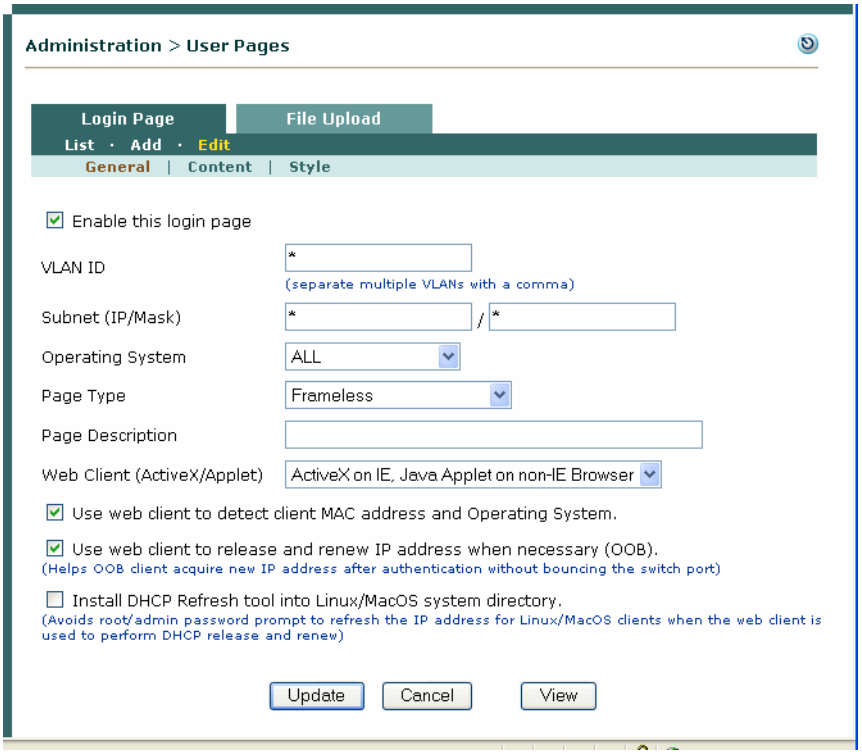
- On CAM: **Administration > User Pages > Login Page > Add/Edit**
- Or CAS: D**evice Management > CCA Servers > Manage [CAS_IP] > Authentication > Login Page | [Override Global Settings]**



Layer 3 OOB: Configuration

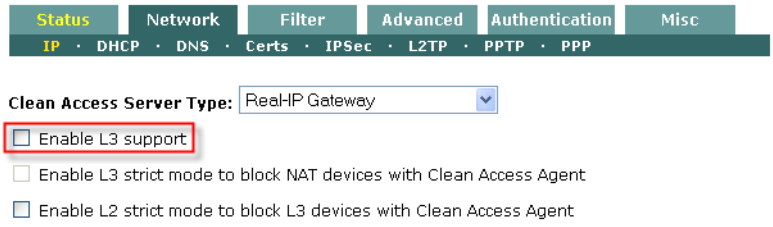
- On Login Page, there is a new checkbox and dropdown menu “Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address” with the following options:
  - ActiveX Only
  - Java Applet Only
  - ActiveX Preferred
  - Java Applet Preferred
  - ActiveX on IE, Java Applet on non-IE Browser
- For “Preferred” options, the preferred option is loaded first; if it fails, the other option is loaded
  - ActiveX is fastest with IE
  - ActiveX is preferred and faster than applet
- ActiveX supported on IE 6.0 on Windows XP/2000
- Java Applet supported on most browsers

Note With release 4.1, DHCP IP addresses can be refreshed for client machines using the 4.1.0.0+ Clean Access Agent, or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. See “ Enable Web Client for Login Page” in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for further details.



Layer 3 OOB: Important Configuration Notes

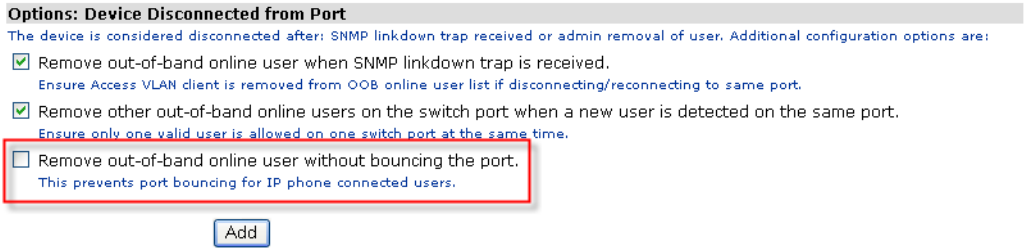
- If a Managed Subnet is configured, NAC Appliance will not use L3 OOB for those subnets.
- Managed subnets are for L2 users only.
- You must click the "**Enable L3 support**" checkbox under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.



- Client machine should be able to execute either ActiveX or Java Applet.

- When the CAM changes the VLAN on the switch port from the Auth VLAN to the Access/User Role VLAN, port bouncing is required.
  - In Port profiles (**Switch Management > Profiles > Port > New/Edit**), make sure "**Bounce the port after VLAN is changed**" is checked

  - In Port profiles, make sure "**Remove out-of-band online user without bouncing the port**" is unchecked.



Layer 3 OOB: Networking

- L3 OOB will typically be used in Routed Access environments.
- With OOB, the goal is to make user traffic flow through the CAS during Authentication, Posture Assessment and Remediation only.
  - CAS challenges user for credentials and also acts as policy enforcement device in the Unauthenticated and Quarantine/Temporary roles.
- Once the user is certified to be compliant, it bypasses the CAS.
- Use networking technologies (such as PBR or VRF) to achieve this goal.

Installing the Clean Access Server NAC Appliance

This chapter describes how to install the Clean Access Server (CAS). Topics include:

Overview

The Cisco NAC Appliance is a Linux-based network hardware appliance.

Cisco NAC Appliance software is distributed as an installation CD-ROM that will install either the Clean Access Manager or Clean Access 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. Once the software is installed (either CAM or CAS) on a dedicated server, the Cisco NAC Appliance does not support the installation of any other packages or applications onto a CAS or CAM.

If you received the Clean Access Server on the distribution CD-ROM, you will need to install it on the target machine as follows:

Step 1 Physically connect the server machine to the network. If intending to configure the CAS in Virtual Gateway mode, see Virtual Gateway Mode Connection Requirements, page 4-4 first before physically connecting the server to the network.

Step 2 Connect a monitor and keyboard to the server machine, or connect to the machine from a workstation by serial cable.

Step 3 For the CD-ROM installation, mount the CD-ROM and run the installation program.

Step 4 Perform the initial configuration. For CD-ROM installation, the initial configuration is part of the installation sequence.

Step 5 Add the Clean Access Server to the list of managed servers in the Clean Access Manager, as described in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Step 6 Configure the Clean Access Server using the Clean Access Manager web administration console.

These steps are described in the following sections. When finished, you will be able to administer the Clean Access Server through the Clean Access Manager's web admin console.

Tip Install the Clean Access Server(s) first, prior to installing the Clean Access Manager, to quickly continue to web admin console configuration after Clean Access Manager installation. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details on CAS configuration.

Caution Cisco NAC Appliance (Cisco Clean Access) software is not intended to coexist with other software or data on the target machine. The installation process formats and partitions the target hard drive, destroying any data or software on the drive. Before starting the installation, make sure that the target machine does not contain any data or applications that you need to keep.

Note

- The Clean Access Server does not advertise routes. Instead, static routes must be added to the next hop router indicating that traffic to the managed subnets must be relayed to the Clean Access Server's trusted interface.
- When the Clean Access Server is in Real-IP Gateway mode, it can act as a DHCP Server or DHCP Relay. With DHCP functionality enabled, the CAS provides the appropriate gateway information (that is, the CAS's untrusted interface IP address) to the clients. If the CAS is working as a DHCP Relay, then the DHCP server in your network must be configured to provide the managed clients with the appropriate gateway information (that is, the Clean Access Server's untrusted interface IP address).

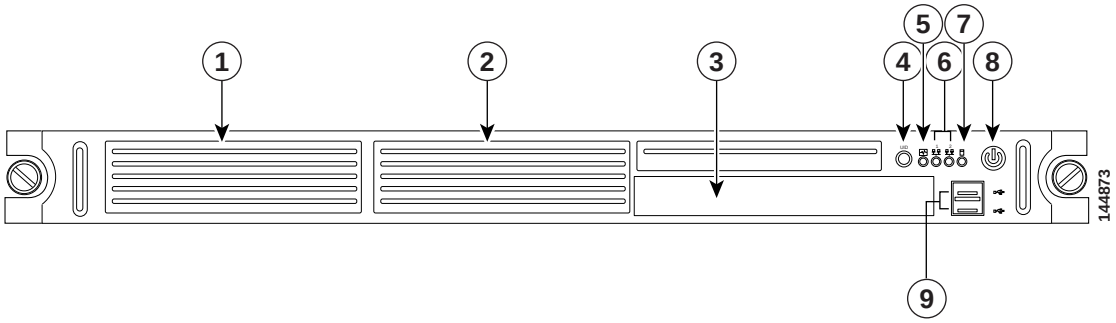
Set Up the Clean Access Server NAC Appliance

These instructions describe how to set up the Clean Access Server on the CCA-3140-H1 Cisco Clean Access NAC Appliance server hardware. If you are using different hardware, the connectors on your machine may not match those shown. If needed, refer to the documentation that came with your server machine to find the serial and Ethernet connectors equivalent to those described here.

1. The Clean Access Server machine uses one of the two 10/100/1000BASE-TX interface connectors on the back panel. Connect the network interface (number 7 in Figure 4-3) on the server machine to your local area network (LAN) with a CAT5 Ethernet cable.
2. Connect the power by plugging one end of the AC power cord into the back of the server machine and the other end into an electrical outlet.

3. Power on the server machine by pressing the power button on the front of the server. The diagnostic LEDs will flash a few times as part of an LED diagnostic test. Status messages are displayed on the console as the server boots up.

Figure 4-1 Front View— CCA-3140-H1



1	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	6	NIC activity LEDs
2	1-inch Non-Hot Plug SATA or SCSI Hard Drive Bay	7	Disc activity LED
3	Optional CD-ROM or DVD drive	8	Power Switch
4	UID LED	9	USB ports
5	System Health Monitor LED		

Figure 4-2 Front View Detail— CCA-3140-H1

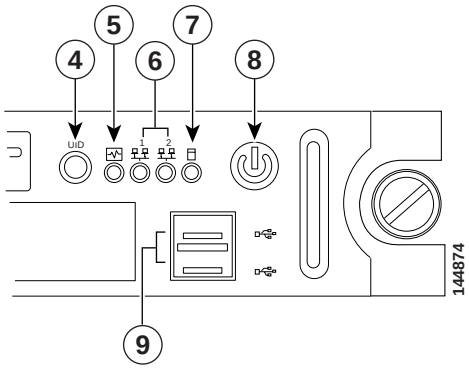
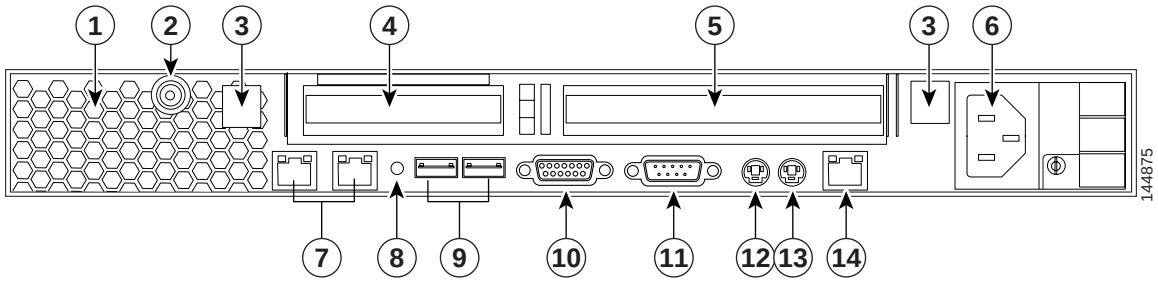


Figure 4-3 Back View— CCA-3140-H1



1	Ventilation holes	8	UID button with LED indicator (blue) This button mirrors the function of the UID button located on the front panel.
2	Thumbscrew for the top cover	9	USB 2.0 ports (black)
3	Thumbscrews for the PCI riser board assembly	10	Video port (blue)
4	Low profile 64-bit/133 MHz PCI-X riser board slot cover	11	Serial port (teal)
5	Standard height/ full-length 64-bit/133 MHz PCI-X riser board slot cover	12	PS/2 keyboard port (purple)
6	Power supply cable socket	13	PS/2 mouse port (green)
7	GbE LAN ports for NIC 1 (eth0) on the left-hand side and NIC 2 (eth1) on the right-hand side (RJ-45).	14	10/100 Mbps LAN port for IPMI management (RJ-45)

Note The CCA-3140-H1 Cisco Clean Access NAC Appliance is based on the HP ProLiant DL140 G2 server.

Virtual Gateway Mode Connection Requirements

If intending to configure the Clean Access Server in Virtual Gateway mode (IB or OOB), you must disable or unplug the untrusted interface (eth1) of the CAS until after you have added the CAS to the CAM from the web admin console. Keeping the eth1 interface connected while performing initial installation and configuration of the CAS for Virtual Gateway mode can result in network connectivity issues.

When setting up a CAS in Virtual Gateway mode, you specify the same IP address for the trusted (eth0) and untrusted (eth1) network interfaces during the initial installation of the CAS via CLI. At this point in the installation, the CAS does not recognize that it is a Virtual Gateway. It will attempt to connect to the network using both interfaces, causing collisions and possible port disabling by the switch. Unplugging or disabling the untrusted interface until after adding the CAS to the CAM in Virtual Gateway mode prevents these connectivity issues. Once the CAS has been added to the CAM in Virtual Gateway mode, you can re-enable or reconnect the untrusted interface.

Administrators must use the following procedure for correct configuration of a Virtual Gateway Central Deployment. To prevent looping on any central/core switch as you plug both interfaces of the Clean Access Server into the switch, perform the following steps:

1. Before you connect both interfaces of the CAS to the switch, physically disconnect the eth1 interface.
2. Physically connect the eth0 interface of the CAS to the network.
3. Add the CAS to the CAM in the CAM web console under **Device Management > CCA Servers > New Server**, as described in Add the CAS to the CAM, page 5-2.
4. Physically connect the eth1 interface of the CAS to the switch.

5. Manage the CAS by accessing the CAS management pages, via **Device Management > CCA Servers > Manage [CAS_IP]** as described in Navigating the CAS Management Pages, page 5-7.
6. Configure VLAN mapping (for Central Deployment only). After you have added the CAS to the CAM web console, make sure to set the VLAN to be mapped under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. Also make sure you check the "**Enable VLAN Mapping**" checkbox and click **Update**. See VLAN Mapping in Virtual Gateway Modes, page 5-28.
7. For the 802.1q ports configuration on the switch, make sure to prune all other VLANs for switches trunking to eth0 and eth1 of the CAS except those used for the CAS Management VLAN and the User VLANs.
8. Prune VLAN 1 on the switch ports connecting to the CAS eth0 and eth1 interfaces. For details, see: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12122ea7/scg/swvlan.htm#wp1150302
9. Once the preceding steps are completed, SSH to the CLI of the CAS and enable eth1 on CAS using the CLI command:

```
ifconfig eth1 up
```

Switch Support for CAS Virtual Gateway/VLAN Mapping (IB and OOB)

For details on Cisco Catalyst switch model/NME support for the Virtual Gateway VLAN Mapping feature of the Clean Access Server for either in-band (IB) or out-of-band (OOB) deployments., refer to Switch Support for Cisco NAC Appliance.

Access the CAS Over a Serial Connection

To install the Clean Access Server software from the CD-ROM or to perform its initial configuration, you will need to access the server machine's command line. This can be done in one of two ways:

1. Connect a monitor and keyboard directly to the machine via the keyboard connector and video monitor/console connector on the back panel, or
2. Connect a serial cable from an external workstation (PC/laptop) to the server machine and open a serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) on the external workstation.

This section describes how to access the server machine over a serial connection.

Note The steps described here for accessing the server directly through a serial connection can be used later for troubleshooting. If the server cannot be reached through the web admin console, you can serially connect to the server to restore the server to a reachable state, usually by correcting its network settings.

To use a serial connection, first connect the computer you will be using as the workstation to an available serial port on the server machine with a serial cable.

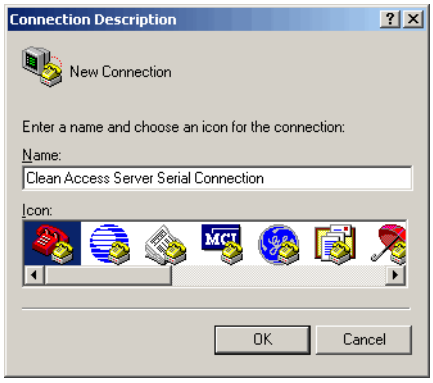
Note If the server is already configured for high availability, its serial port may already be in use for the peer connection. In this case, the computer needs to have at least two serial ports to be able to manage the server over a serial connection. If it does not, you have the option of freeing the serial port by using an Ethernet connection for the peer connection. For more information, see Chapter 13, "Configuring High Availability (HA)."

After physically connecting the workstation to the server, you can access the serial connection interface using any terminal emulation software. The following steps describe how to connect using Microsoft® HyperTerminal. If you are using different software, the steps may vary.

Set Up the Terminal Emulation Console Connection

The following steps describe how to connect using Microsoft® HyperTerminal. If you are using different software, the steps may vary.

1. Open the HyperTerminal window by clicking **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**
2. Give any name to the session and click **OK**:



3. In the **Connect using** dropdown list, choose the COM port on the workstation to which the serial cable is connected, generally either `COM1` or `COM2` and click **OK**.

4. Configure the **Port Settings** as follows:
   - **Bits per second** – `9600`

- **Data bits** – `8`
- **Parity** – `None`
- **Stop bits** – `1`
- **Flow control** – `None`

5. Go to **File > Properties**, or click the Properties icon ( ) to open the Properties dialog for the session. Change the **Emulation** setting to:
   - **Emulation**– `VT100`

You should now be able to access the command interface for the server. You can now:

- Install the Clean Access Server Software from CD-ROM, page 4-7
- Perform the Initial Configuration, page 4-9
- If you already performed the initial installation, but need to modify the original settings, you can log in as user **`root`** and run the **`service perfigo config`** command.

Install the Clean Access Server Software from CD-ROM

This section describes how to install the software from the distribution CD-ROM. It is assumed that you have already connected the server to the network, as described in Set Up the Clean Access Server NAC Appliance, page 4-2 and are working on the server either directly from a console or from terminal emulation software over a serial connection, as described in Access the CAS Over a Serial Connection, page 4-5

Caution The Clean Access Server software is not intended to coexist with other software or data on the target machine. The installation process formats and partitions the target hard drive, destroying any existing data or software on the drive. Before starting the installation, make sure that the target computer does not contain any data or applications that you need to keep.

CD Installation Steps

The entire installation process, including the configuration steps described in Perform the Initial Configuration, page 4-9 should take about 15 minutes.

1. Insert the distribution CD-ROM that contains the Clean Access Server .iso file into the CD-ROM drive of the target server machine.
2. Reboot the machine. The Cisco Clean Access Installer welcome screen appears after the machine restarts:

```
Cisco Clean Access Installer (C) 2006 Cisco Systems, Inc.

                Welcome to the Cisco Clean Access Installer!

 -  To install a Cisco Clean Access device, press the <ENTER> key.

 -  To install a Cisco Clean Access device over a serial console,
  enter serial at the boot prompt and press the <ENTER> key.

boot:
```

3. Depending on your specific NAC Appliance platform and type of connection, at the "`boot`:" prompt:

   For Cisco NAC-3350:

   - Press the Enter key if your monitor and keyboard are directly connected to the target machine.
   - Type **`serial`** and press enter in the terminal emulation console if you are accessing the target machine over a serial connection.

   For Cisco NAC-3310:

   - Type **`DL140`** if you are directly connected (monitor, keyboard, and mouse) to the target machine.
   - Type **`serial_DL140`** if you are installing the software via serial console connection.

4. The Package Group Selection screen appears next to prompt you to choose CCA Manager software installation or CCA Server software installation. At the following screen prompt, you MUST choose **`CCA Server`** and select **`OK`** to begin the Clean Access Server installation. Use the space bar and the "+" and "-" keys to select the appropriate type. Use the Tab key to tab to the OK field, and press the Enter key when done to start the installation of the package type selected.

```
Welcome to Cisco Clean Access

                  ++ Package Group Selection ++
                  |                           |
                  | Total install size: 606M  |
                  |                           |
                  |    [ ] CCA Manager #      |
                  |    [*] CCA Server  #      |
                  |                    #      |
                  |                    #      |
                  |                    #      |
                  |                    #      |
                  |                    #      |
                  |                    #      |
                  |                           |
                  |   +-----+     +-------+   |
                  |   | OK |      | Back |    |
                  |   +-----+     +-------+   |
                  |                           |
                  |                           |
                  +---------------------------+


<Space>,<+>,<-> selection   |   <F2> Group Details   |   <F12> next screen
```

Caution Only one CD is used for installation of the Clean Access Server or Clean Access Manager software. The installation script does not automatically detect CAS or CAM installation for the target server. The Package Group Selection is set by default to **`CCA Manager`**.You must select the appropriate type, **either** CAS or CAM, for the target machine on which you are performing installation, then tab to the OK field and press Enter to start the installation.

Note Do not select the "Back" option from the Package Group Selection screen.

5. The Clean Access Server Package Installation then executes. The installation takes a few minutes. When finished, the welcome screen for the Clean Access Server quick configuration utility appears, and a series of questions prompt you for the initial server configuration, as described in the next section, Configuration Utility Script, page 4-9.

If after installation you need to reset the configuration settings for the Clean Access Server (such as the eth0 IP address), you can modify these values by connecting to the Clean Access Server machine serially or via SSH and running the `service perfigo config` command. See Configuration Utility Script, page 4-9 for details.

Note Most other settings can also be modified later from the web admin console.

Perform the Initial Configuration

When installing the Clean Access Server from CD-ROM, the Configuration Utility Script automatically appears after the software packages install to prompt you for the initial server configuration.

Note If necessary, you can always manually start the Configuration Utility Script as follows:

1. Over a serial connection or working directly on the server machine, log onto the server as user **root** with default password **cisco123**.
2. Run the initial configuration script by entering the following command:

   service perfigo config

You can run the **service perfigo config** command to modify the configuration of the server if it cannot be reached through the web admin console. For further details on CLI commands, see Using the Command Line Interface (CLI), page 4-17.

Configuration Utility Script

1. The configuration utility script suggests default values for particular parameters. To configure the installation, either accept the default value or provide a new one, as described below.
2. After the software is installed from the CD and package installation is complete, the welcome script for the configuration utility appears:

   ```
   Welcome to the Cisco Clean Access Server quick configuration utility.
   Note that you need to be root to execute this utility.
   The utility will now ask you a series of configuration questions.
   Please answer them carefully.
   ```

3. The script first asks for settings for the trusted interface (eth0). The trusted interface is the interface to the protected, backend network.

   ```
   Configuring the network interfaces:
   Please enter the IP address for the interface eth0 [10.0.2.15]: 10.201.240.12
   You entered 10.201.240.12 Is this correct? (y/n)? [y] y
   ```

   At the prompt, type the eth0 IP address of the CAS and press Enter. At the confirmation prompt, type **y** to accept the entry or type **n** to change it and enter another address for the trusted eth0 network interface. When prompted, press Enter to confirm the value.

Note The eth0 IP address of the CAS is the same as the Management IP address.

4. Type the subnet mask of the eth0 interface or press Enter to accept the default of 255.255.255.0. Confirm the value at when prompted.

   ```
   Please enter the netmask for the interface eth0 [255.255.255.0]:
   You entered 255.255.255.0, is this correct? (y/n)? [y]
   ```

5. Specify the default gateway address for the trusted interface and press Enter. Confirm the value at when prompted.

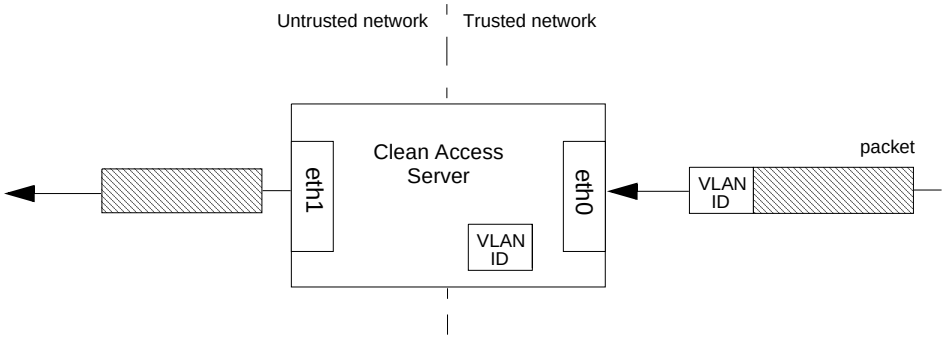
   ```
   Please enter the IP address for the default gateway [10.201.240.1]:
   You entered 10.201.240.1 Is this correct? (y/n)? [y]
   ```

6. Specify VLAN ID passthrough behavior. At the prompt, type `n` and press Enter (or just press Enter) to accept the default behavior (VLAN passthrough is disabled and VLAN IDs are stripped from traffic passing through the interface) or enter `y` to enable VLAN ID passthrough for traffic passing from the trusted network to the untrusted network.

```
[Vlan Id Passthrough] for packets from eth0 to eth1 is disabled.
Would you like to enable it? (y/n)? [n]
```

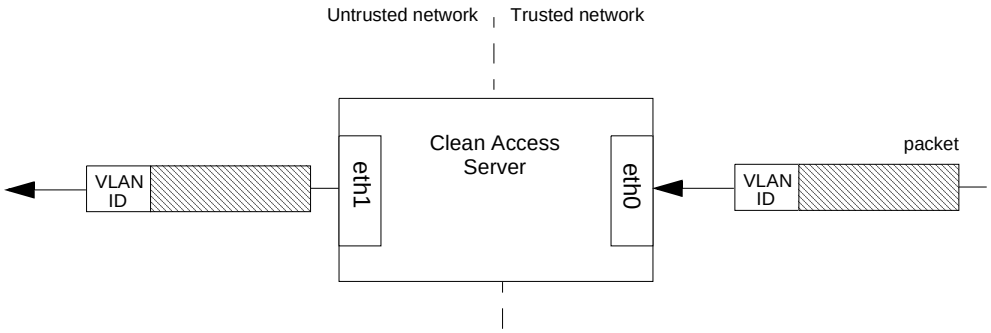
By default, the VLAN ID is not passed through, that is, the VLAN ID is stripped from packets passed through the CAS, as illustrated in Figure 4-4. The IDs are retained by the Clean Access Server and attached to response messages passed from the untrusted network back to the trusted network.

Figure 4-4 VLAN ID Termination



In VLAN ID passthrough, the identifier is retained on traffic that passes through the interface.

Figure 4-5 VLAN ID Passthrough



Note

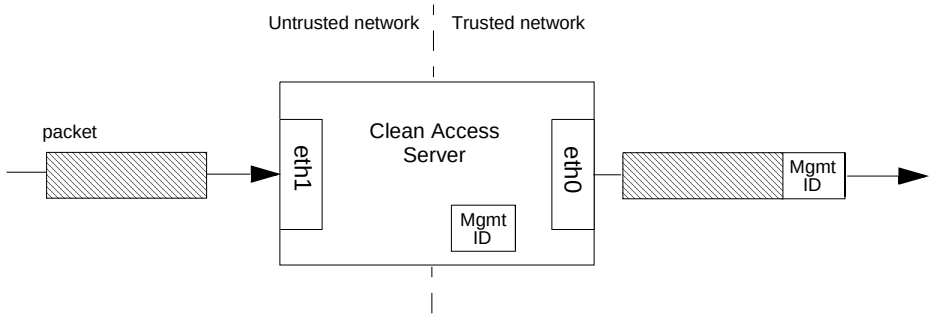
- In most cases, enabling VLAN passthrough is not needed. Only enable passthrough if you are sure you need it. If you choose not to enable it at this time, you can change the option later in the web console or using the `service perfigo config` utility.
- Faulty VLAN settings can render the Clean Access Server unreachable from the Clean Access Manager, so use caution when configuring VLAN settings.

7. Specify Management VLAN Tagging behavior at the next prompt. Type `N` and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default), or type `Y` and press Enter to enable Management VLAN tagging and type the VLAN ID to use.

```
[Management Vlan Tagging] for egress packets of eth0 is disabled.
Would you like to enable it? (y/n)? [n]
```

A Management VLAN identifier is a default VLAN identifier that is added to a packet if it does not have its own VLAN identifier or if the identifier was originally stripped by the adjacent interface. The setting at the prompt applies to traffic passing from the untrusted network to the trusted network.

Figure 4-6 Eth0 Egress Packets with Management VLAN ID Tagging



Note

- In most cases, enabling Management VLAN tagging is not needed. You should only enable it if you are sure it is necessary. If you choose not to enable it at this time, you can change the option later in the web console or using **`service perfigo config`** utility.
- Also note that faulty VLAN settings can render the Clean Access Server unreachable from the Clean Access Manager, so be sure to use care when configuring VLAN settings.

8. Next configure the untrusted interface. This is the interface to the untrusted (managed) network. At the prompt type the address you want to use for the untrusted interface (eth1) and press Enter. Unless deploying the Clean Access Server in a bridge (Virtual gateway) configuration, the trusted and untrusted interfaces must be on separate subnets. Confirm the value when prompted.

```
Please enter the IP address for the untrusted interface eth1 [192.168.0.1]:
You entered 192.168.0.1 Is this correct? (y/n)? [y]
```

9. Type the subnet mask of the eth1 interface or press Enter to accept the default of 255.255.255.0. Confirm the value at when prompted.

```
Please enter the netmask for the interface eth1 [255.255.255.0]: 255.255.0.0
You entered 255.255.0.0, is this correct? (y/n)? [y]
```

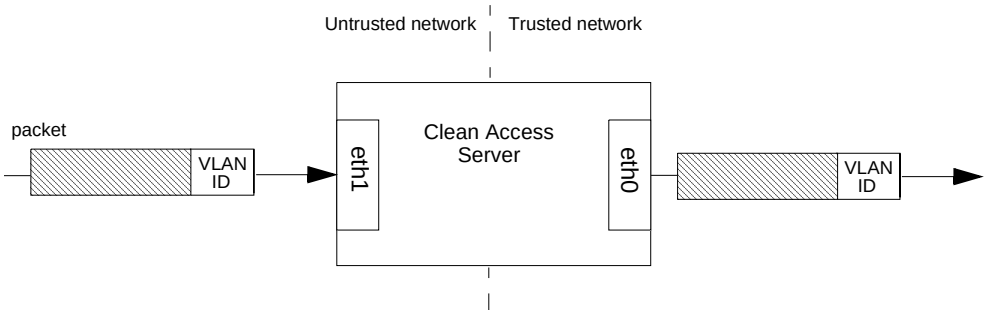
10. Enter the default gateway address for the untrusted interface:
    - If the Clean Access Server will act as a Real-IP gateway or NAT gateway, this should be the IP address of the CAS's untrusted interface eth1.
    - If the Clean Access Server will act as a Virtual gateway (i.e., a bridge), this can be the same default gateway address used for the trusted side.

```
Please enter the IP address for the default gateway [192.168.0.1]:
You entered 192.168.0.1 Is this correct? (y/n)? [y]
```

11. Specify VLAN passthrough behavior for traffic passing from the untrusted to the trusted network. At the prompt, type **`n`** and press Enter (or just press Enter) to accept the default behavior (disabled) or enter **`y`** to enable VLAN ID passthrough for traffic from the untrusted network.

```
[Vlan Id Passthrough] for packets from eth1 to eth0 is disabled.
Would you like to enable it? (y/n)? [n]
```

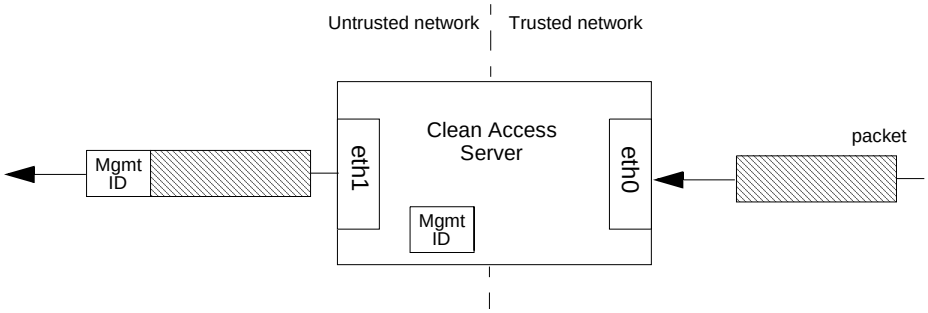
Figure 4-7 VLAN ID Passthrough



12. At the next prompt, specify Management VLAN Tagging behavior for traffic passing from the trusted to the untrusted network. Type **N** and press Enter (or just press Enter) to keep Management VLAN tagging disabled (default), or type **Y** and press Enter to enable Management VLAN tagging and type the VLAN ID to use.

```
[Management Vlan Tagging] for egress packets of eth1 is disabled.
Would you like to enable it? (y/n)? [n]
```

Figure 4-8 Eth1 Egress Packets with Management VLAN ID Tagging



13. Specify the host name for the Clean Access Server (**caserver** is the default). Type and confirm the address when prompted:

```
Please enter the hostname [caserver]: caserver10
You entered caserver10 Is this correct? (y/n)? [y]
```

14. Specify the IP address of the Domain Name System (DNS) server in your environment. Type and confirm the address when prompted:

```
Please enter the IP address for the name server: [172.68.226.120]:
You entered 172.68.226.120 Is this correct? (y/n)? [y]
```

15. The Clean Access Manager and Clean Access Servers in a deployment authenticate each other through a shared secret. The shared secret serves as an internal password for the deployment. Type and confirm the shared secret when prompted:

```
The shared secret used between Clean Access Manager and Clean Access Server is the
default string: cisco123.

This is highly insecure. It is recommended that you choose a string that is unique to
your installation.

Please enter the shared secret: cisco123
You entered: cisco123
Is this correct? (y/n)? [y]
```

Caution The shared secret must be the same for the Clean Access Manager and all Clean Access Servers in the deployment. If they have different shared secrets, they cannot communicate.

16. Specify time settings for the Clean Access Server.

a. Choose the timezone location from the continents and oceans list. Type the number next to your location on the list, such as **2** for the Americas, and press enter. Enter 11 to enter the time zone in Posix TZ format, such as `GST-10`.

```
>>> Configuring date and time:

The timezone is currently not set on this system.
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 2
```

b. Choose a country for the chosen timezone. Select your country from the country list, such as **45** for the United States, and press Enter.

```
Please select a country.
 1) Anguilla              18) Ecuador               35) Paraguay
 2) Antigua & Barbuda     19) El Salvador           36) Peru
 3) Argentina             20) French Guiana         37) Puerto Rico
 4) Aruba                 21) Greenland             38) St Kitts & Nevis
 5) Bahamas               22) Grenada               39) St Lucia
 6) Barbados              23) Guadeloupe            40) St Pierre & Miquelon
 7) Belize                24) Guatemala             41) St Vincent
 8) Bolivia               25) Guyana                42) Suriname
 9) Brazil                26) Haiti                 43) Trinidad & Tobago
10) Canada                27) Honduras              44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica               45) United States
12) Chile                 29) Martinique            46) Uruguay
13) Colombia              30) Mexico                47) Venezuela
14) Costa Rica            31) Montserrat            48) Virgin Islands (UK)
15) Cuba                  32) Netherlands Antilles  49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
#? 45
```

c. If the country contains more than one time zone, time zone regions for the country appear. Choose the appropriate time zone region from the list and press enter (for example, **16** for Pacific Time).

```
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Standard Time - Indiana - most locations
 6) Eastern Standard Time - Indiana - Crawford County
```

```
 7) Eastern Standard Time - Indiana - Starke County
 8) Eastern Standard Time - Indiana - Switzerland County
 9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands
22) Hawaii
#? 16
```

d. Confirm your choices or cancel your choices and start over, by entering 1 to confirm or 2 to start over.

```
The following information has been given:

        United States
        Pacific Time

Is the above information OK?
1) Yes
2) No
#? 1

Updating timezone information...
```

17. Confirm the current date and time at the next prompt by pressing enter, or provide the correct date and time in the format shown. Confirm the values when prompted.

```
Current date and time hh:mm:ss mm/dd/yy [04:08:29 02/15/06]: 18:08:29 02/15/06
You entered 18:08:29 02/15/06 Is this correct? (y/n)? [y]
Wed Feb 15 18:08:29 PST 2006
```

18. Press Enter to configure the temporary SSL certificate. The certificate secures the login exchange between the Clean Access Server and untrusted (managed) clients. Configure the certificate as follows:

a. At the following prompt, type the IP address or domain name for which you want the certificate to be issued.

```
You must generate a valid SSL certificate in order to use the Clean Access Serv
er's secure web console.
Please answer the following questions correctly.
Information for a new SSL certificate:
Enter fully qualified domain name or IP: 10.201.240.12
```

b. For the organization unit name, enter the group within your organization that is responsible for the certificate (for example, `IT` or `engineering`).

```
Enter organization unit name: engineering
```

c. For the organization name, type the name of your company or organization for which you would like to receive the certificate, and press enter.

```
Enter organization name: Cisco Systems
```

d. Type the name of the city or county in which your organization is legally located, and press enter.

```
Enter city name: San Jose
```

e. Enter the two-character state code in which the organization is located, such as CA or NY, and press enter.

```
Enter state code: CA
```

f. Type the two-letter country code and press enter.

```
Enter 2 letter country code: US
```

g. A list of the values you entered appears. Press enter to accept the values or `N` to restart.

```
You entered the following:
Domain: 10.201.240.12
Organization unit: qa
Organization name: Cisco Systems
City name: San Jose
State code: CA
Country code: US
Is this correct? (y/n)? [y]
Generating SSL Certificate...
CA signing: /root/.tomcat.csr -> /root/.tomcat.crt:
CA verifying: /root/.tomcat.crt <-> CA cert
/root/.tomcat.crt: OK

Done
```

When you confirm your values, the certificate is generated and the Clean Access Server database is initialized.

19. Now configure passwords on the CAS for the root user account (SSH users), and the CAS direct access web console. The CAS web console gives you direct access to limited CAS-specific settings, and is primarily used to set up High Availability. The specific passwords to set are as follows:

a. The first password is for the **`root`** user of the installed Linux operating system. You can use this account when accessing the CAS over a serial connection.

```
For security reasons, it is highly recommended that you change the default
password for the root user.
User: root
Changing password for user root.
New UNIX password:
```

b. Next type the password for the **`admin`** user for the CAS direct access web console. Note that **`admin`** web user account is different than the **`admin`** Linux OS user account.

```
Would you like to change the default password for the web console admin user pas
sword? (y/n)? [y]
Please enter an appropriately secure password for the web console admin user.

New password for web console admin:
Confirm new password for web console admin:
Web console admin password changed successfully.
```

20. If installing from the CD-ROM, press the Enter key to reboot the CAS when configuration is complete:

```
Configuration is complete.
Done
Install has completed. Press <ENTER> to reboot.
```

21. If running the `service perfigo config` configuration utility, run the following command to reboot the server:

    ```
    service perfigo reboot
    ```

22. The initial configuration is now complete. Once the Clean Access Manager is also installed and initially configured, use the CAM web administration console to add the CAS to the CAM as described in Chapter 5, "Clean Access Server Managed Domain."

Important Notes for SSL Certificates

- You must generate the SSL certificate during CAS installation or you will not be able to access your server as an end user.
- After CAM and CAS installation, make sure to synchronize the time on the CAM and CAS via the web console interface before regenerating a temporary certificate on which a Certificate Signing Request (CSR) will be based. For further details on the CAS, see:
  - Synchronize System Time, page 12-16
  - Manage CAS SSL Certificates, page 12-3
  - For details on the CAM, see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.
- Before deploying the server in a production environment, you can acquire a trusted certificate from a Certificate Authority to replace the temporary certificate (in order to avoid the security warning that is displayed to end users during user login).

Using the Command Line Interface (CLI)

The CAM web admin console allows you to perform most of the tasks required for administering Cisco NAC Appliance deployment. However, in some cases you may need to access the CAS configuration directly, for example if the web admin console is unavailable due to incorrect network or VLAN settings. You can use the Cisco NAC Appliance command line interface (CLI) to set basic operational parameters directly on the CAS.

To run the CLI commands, access the CAS using SSH and log in as user **root** (default password is **cisco123**) If already serially connected to the server, you can run CLI commands from the terminal emulation console after logging in as **root** (see Access the CAS Over a Serial Connection, page 4-5). The format `service perfigo <command>` is used to enter a command from the command line. Table 4-1 lists the commonly used Cisco NAC Appliance CLI commands.

Table 4-1 CLI Commands

Command	Description
service perfigo start	Starts up the server. If the server is already running, a warning message appears. The server must be stopped for this command to be used.
service perfigo stop	Shuts down the Clean Access service. **Note** When the management VLAN is set, this command will cause the CAS to lose network connectivity when issued.
service perfigo maintenance	This CAS-only command brings the CAS to maintenance mode. In maintenance mode, only the basic CAS router runs and continues to handle VLAN-tagged packets. The command allows communication through the management VLAN and is intended for environments where the CAS is in trunk mode and the native VLAN is different than the management VLAN.
service perfigo restart	Shuts down the Clean Access service and starts it up again. This is used when the service is already running and you want to restart it. **Note** **service perfigo restart** should not be used to test high availability (failover). Instead, Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, if a CLI command is preferred, **service perfigo stop** and **service perfigo start**
service perfigo reboot	Shuts down and reboots the machine. You can also use the Linux **reboot** command.
service perfigo config	Starts the configuration script to modify the server configuration. After completing **service perfigo config**, you must reboot the server. For instructions on using the script, see Perform the Initial Configuration, page 4-9
service perfigo time	Use to modify the time zone settings.

CAM/CAS Connectivity Across a Firewall

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details on which ports to open in a firewall to allow communication between the Clean Access Manager and Clean Access Server(s).

Configuring the CAS Behind a NAT Firewall

If deploying the Clean Access Server behind a firewall (there is a NAT router between CAS and CAM), you will need to perform the following steps to make the CAS accessible:

1. Connect to the CAS by SSH or use a serial console. Log in as **root** user.
2. Change directories to `/perfigo/agent/bin/`.
3. Edit the file `startagent`.
4. Locate the `JAVA_OPTS` variable definition in the file.
5. Add **`-Djava.rmi.server.hostname=<`***`caserver1_hostname`***`>`** to the variable, replacing *`caserver1_hostname`* with the host name of the server you are modifying. For example:

   ```
   JAVA_OPTS="-server
   -Djava.util.logging.config.file=/perfigo/agent/conf/logging.properties
   -Dperfigo.jmx.context= ${PERFIGO_SECRET} -Xms40m -Xmx40m -Xincgc
   -Djava.rmi.server.hostname=caserver1"
   ```

6. Restart the CAS by entering the **`service perfigo restart`** command.
7. Repeat the preceding steps for each Clean Access Server in your deployment.
8. Connect to the Clean Access Manager by SSH or using a serial console. Login as **`root`**.
9. Change directories to `/etc/`.
10. Edit the hosts file by appending the following line:

    `<public_IP_address> <caserver1_hostname> <caserver2_hostname>`
    where:

    - *`<public_IP_address>`* – The address that is accessible outside the firewall.
    - *`<caservern_hostname>`* – The host name of each Clean Access Server behind the firewall.

The CASes should now be addressable behind the firewall.

Configuring Additional NIC Cards

The Configuration Utility script assumes that the CAM and CAS machines come with eth0 (NIC1) and eth1 (NIC2) interfaces by default and allows you to configure these during initial installation. If your system has additional network interface cards (e.g. NIC3, NIC4), you can use the following instructions to configure the additional interfaces (e.g. eth2, eth3) on those cards. Typically, eth2 needs to be configured when setting up Clean Access Server systems for High Availability. For HA, once the eth2 (NIC3) interface is configured with the proper addressing, it can then be configured as the dedicated UDP heartbeat interface for the HA-CAS.

Note

- For Cisco NAC Appliance hardware, the following instructions assume that the NIC is plugged in and "working" (i.e. recognized by BIOS and by Linux).
- If the NIC card is not recognized by BIOS (for example, for a non-appliance server machine), you may need to adjust IRQ/memory settings as per the manufacturer's recommendations.
- Once the NIC is recognized by BIOS, it should be automatically recognized by the software (Linux). If for some reason, the NIC is recognized by BIOS, but not by Linux, then login to the system and run "kudzu". This will bring up a utility that helps you configure the NIC.

To Configure an Additional NIC

1. To verify that the NIC has been recognized by Linux, type `ifconfig eth<n>` (where `<n>` is the interface number). For example, <n> will be 2 if adding a NIC to a system that already has two built-in Ethernet interfaces; therefore, you would type:

   ```
   ifconfig eth2
   ```

2. You should see information about the interface including MAC address, transmit and receive counters. This means the interface has been recognized by Linux and can be used.
3. Change to the following directory:

   ```
   cd /etc/sysconfig/network-scripts
   ```

4. Use vi to edit the `ifcfg` file for the interface, for example:

   ```
   vi ifcfg-eth2
   ```

5. Add the following lines into the file—replacing `IPADDR`, `NETMASK`, `BROADCAST` and `NETWORK` values with the actual values suitable for your network:

   ```
   DEVICE=eth2
   IPADDR=192.168.0.253
   NETMASK=255.255.255.252
   BROADCAST=192.168.0.255
   NETWORK=192.168.0.252
   BOOTPROTO=static
   ONBOOT=yes
   TYPE=Ethernet
   ```

6. Save the file and reboot the system.
7. The network interface is now ready to be used for HA.

Note See CAS High Availability Requirements, page 13-4 for additional details.

Troubleshooting the Installation

Note For further troubleshooting information, see the latest version of the *Release Notes for Cisco NAC Appliance*: http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html.

Network Interface Card (NIC) Driver Not Supported

For complete details, refer to the "Troubleshooting Network Card Driver Support Issues" section of the Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access).

Resetting the Clean Access Server Configuration

If incorrect network, shared secret, or VLAN settings have rendered the Clean Access Server unreachable from the Clean Access Manager, you can reset the Clean Access Server's configuration. Note that resetting the configuration restores the Clean Access Server configuration to its install state. Any configuration settings made since installation will be lost.

To reset the configuration:

1. Connect to the Clean Access Server by SSH.
2. Delete the `env` file:

   ```
   # rm /perfigo/access/bin/env
   ```

3. Then reboot using:

   ```
   # service perfigo reboot
   ```

You can now add the CAS to the CAM. See Chapter 5, "Clean Access Server Managed Domain."

Clean Access Server Managed Domain

This chapter describes how to set up the Clean Access Server's managed domain. Topics include:

Overview

After installing the Clean Access Server, it needs to be added to the Clean Access Manager's domain. You can then configure the Clean Access Server's managed (untrusted) network.

Configuring the Clean Access Server managed network involves setting up passthrough policies, specifying managed subnets (subnets you want to manage that are not within the address space specified at the untrusted network interface), setting up static routes, along with other tasks described here.

Add the CAS to the CAM

This section describes the following topics:

The Clean Access Server gets almost all of its runtime parameters from the Clean Access Manager, and cannot operate unless it is added to the domain of a Clean Access Manager. Once it is added to the CAM, the CAS can be configured and monitored through the admin console.

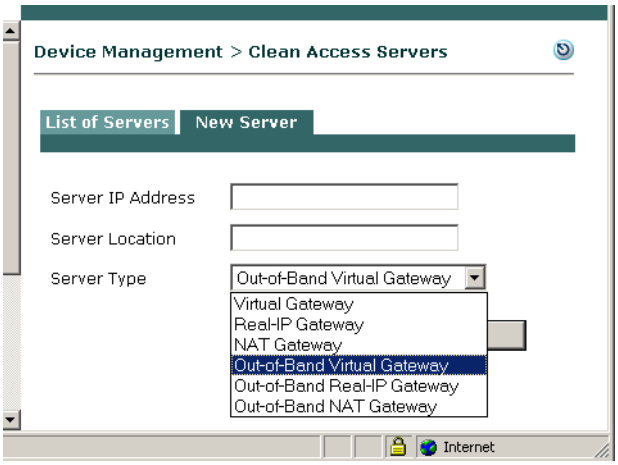
Add New Server

Note If intending to configure the Clean Access Server in Virtual Gateway mode (IB or OOB), you must disable or unplug the untrusted interface (eth1) of the CAS until after you have added the CAS to the CAM from the web admin console. Keeping the eth1 interface connected while performing initial installation and configuration of the CAS for Virtual Gateway mode can result in network connectivity issues.
For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**.
See Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments), page 5-5 for details.

1. Open a web browser and type the IP address of the CAM as the URL to access the CAM web admin console.
2. Go to the **Device Management** module and click **CCA Servers**.

3. Click the **New Server** tab to add a new CAS.

Figure 5-1 New Server



4. In the **Server IP address** field, type the IP address of the Clean Access Server's eth0 trusted interface.

Note The eth0 IP address of the CAS is the same as the Management IP address.

5. The **Server Type** dropdown menu determines whether the Clean Access Server operates as a bridge or a gateway. For in-band operation, choose one of the following CAS operating modes as appropriate for your environment:
   - **Virtual Gateway** —CAS operates as a bridge between the untrusted network and an existing gateway

Note See Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments), page 5-5.

   - **Real-IP Gateway** — CAS operates as a gateway for the untrusted network
   - **NAT Gateway** — CAS operates as a gateway and performs NAT services for the untrusted network

Note NAT Gateway mode is primarily intended to facilitate testing, as it requires the least amount of network configuration and is easy to initially set up. However, because it is limited in the number of connections it can handle, NAT Gateway mode (in-band or out-of-band) is not supported for production deployment. See Configuring the CAS Behind a NAT Firewall, page 4-18 and NAT Session Throttle, page 5-38 for additional details.

6. The Out-of-Band Server Types appear in the dropdown menu when you apply an OOB-enabled license to a Clean Access deployment. For OOB, the CAS operates as a Virtual, Real-IP, or NAT Gateway while client traffic is in-band (in the Clean Access network) during authentication and certification. Once clients are authenticated and certified, they are considered "out-of-band" (no longer passing through the Clean Access network) and allowed directly onto the trusted network. Choose one of the following operating modes for the CAS:
   - **Out-of-Band Virtual Gateway** — CAS operates as a Virtual Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

- **Out-of-Band Real-IP Gateway** — CAS operates as a Real-IP Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).
- **Out-of-Band NAT Gateway** — CAS operates as a NAT Gateway during authentication and certification, before the user is switched out-of-band (i.e., the user is connected directly to the access network).

Note NAT Gateway (in-band or out-of-band) is not supported for production deployment.

Note that the CAM can control both in-band and out-of-band Clean Access Servers in its domain. However, the **CAS** itself must be **either** in-band or out-of-band.

For details on in-band operating modes, see Clean Access Server Operating Modes, page 2-1. For details on OOB operating modes, see "Switch Management and Configuring Out-of-Band (OOB) Deployment" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

7. Click **Add Clean Access Server**. The Clean Access Manager looks for the CAS on the network, and adds it to its list of managed Clean Access Servers.

IP Addressing Considerations

Note

- eth0 and eth1 generally correlate to the first two network cards—NIC 1 and NIC 2—on most types of server hardware.
- For Virtual Gateway (In-Band or OOB), do not connect the untrusted interface (eth1) of the CAS to the switch until **after** the CAS has been added to the CAM via the web console, and VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**.

Real-IP:

- The trusted (eth0) and untrusted (eth1) interfaces of the CAS must be on different subnets.
- You must add static routes on the L3 switch or router to route traffic for the managed subnets to the trusted interface of the respective CASs.
- If using DHCP relay, make sure the DHCP server has a route back to the managed subnets.

NAT Gateway Mode:

- The trusted (eth0) and untrusted (eth1) interfaces of the CAS must be on different subnets.

Virtual Gateway Mode:

- The CAS and CAM **must** be on different subnets (or VLANs).
- The trusted (eth0) and untrusted interfaces (eth1) of the CAS can have the same IP address. (Note: this is equivalent to an L3 switched virtual interface (SVI) IP address)
- All end devices in the bridged subnet must be on the untrusted side of the CAS.
- Managed subnets must be configured on the CAS for all the user subnets that are managed by the CAS. When configuring the Managed subnet, make sure that you type an **unused** IP address in that subnet (for the CAS to use), and not a subnet address.

- The CAS is automatically configured for DHCP Passthrough when set to Virtual Gateway mode.
- Traffic from clients **must** pass through the CAS before hitting the gateway.

OOB Virtual Gateway Mode:

When the CAS is an OOB VGW, the following also applies:

- The CAS interfaces must be on a separate subnet (or VLAN) from the CAM.
- The CAS management VLAN must be on a different VLAN than the user or Access VLANs.

Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments)

1. There should be a management VLAN setting on the CAS **IP** page (and in your network configuration) to allow communication to the CAS's trusted and untrusted IP addresses.
2. The Native VLAN ID on the switch ports to which CAS eth0 and eth1 are connected should ideally be two otherwise unused VLAN IDs (e.g. 999, 998). Choose any two VLAN IDS from a range that you are not using anywhere on your network.
3. Do **not** connect eth1(untrusted interface) of the CAS until after you have configured and enabled VLAN Mapping entries in the CAS (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**). See Configure VLAN Mapping for Out-of-Band, page 5-30 for detailed steps.

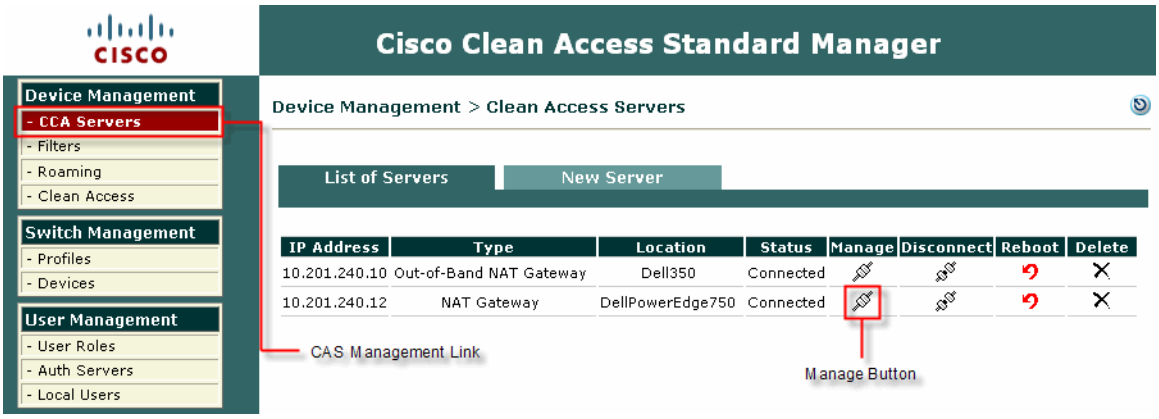
Caution To avoid switch errors, make sure to correctly set VLAN Mapping in the CAS before connecting the eth1 interface of the CAS. Failure to do so could cause spanning tree loops and shut down the switch.

Note The Clean Access Server needs to receive Ethernet frames and only supports Ethernet as the LLC (Logical Link Control) protocol. For any non-IP protocol, such as SNA or IPX, the CAS can support it only if Ethernet is used as the LLC protocol, the CAS is a Virtual Gateway, and there is no VLAN mapping (i.e. the CAS is in Edge Deployment mode).

List of Clean Access Servers

Once you add the CAS to the Clean Access Manager, the CAS appears in the **List of Servers** tab.

Figure 5-2 List of Servers



Each Clean Access Server entry lists the IP address, server type, location, and connection status of the CAS. In addition, four management control icons are displayed: **Manage** ( ), **Disconnect** ( ), **Reboot** ( ), and **Delete** ( ). You access the management pages of a Clean Access Server by clicking the **Manage** icon next to the CAS.

Troubleshooting when Adding the Clean Access Server

If the Clean Access Server cannot be added to Clean Access Manager, check the following:

1. Ping connectivity from the CAS to the CAM and from the CAM to the CAS.
   a. If the CAS is not pingable, network settings may be incorrect. Reset them using `service perfigo config`. See Using the Command Line Interface (CLI), page 4-17 for details.
   b. If the CAS is pingable but cannot be added to the CAM:
   – Physically disconnect the eth1 interface of the CAS.
   – Wait 2 minutes, then add the CAS again from the CAM web console.
   – When the CAS is successfully added, physically connect the eth1 interface of the CAS.
2. SSH from the CAM to the CAS and from the CAS to the CAM and check for any errors.
3. Check the shared secret key on both the CAM and CAS under: `cat /root/.secret`. If this is the problem, reset the shared secret with `service perfigo config`.
4. Check the SSL certificates. For details, see Typical Steps for CAS New Installs, page 12-5 and Troubleshooting Certificate Issues, page 12-13 in this guide, and the corresponding sections of the CAS guide.
5. Check the product license. Make sure you have a license for OOB if using OOB. If running OOB, the “Switch Management” module will be present in left hand pane of the web admin console. When upgrading, your previous license must already enable OOB, or you must obtain a new license to use OOB features. See Product Licensing and Service Contract Support, page 1-4.
6. Check the date/time on both the CAM and CAS via SSH. The date/time difference cannot be more than 3 minutes.

- To check the time on the CAS/CAM, issue: `date`
- To change the time on the CAS/CAM, issue: `service perfigo time`

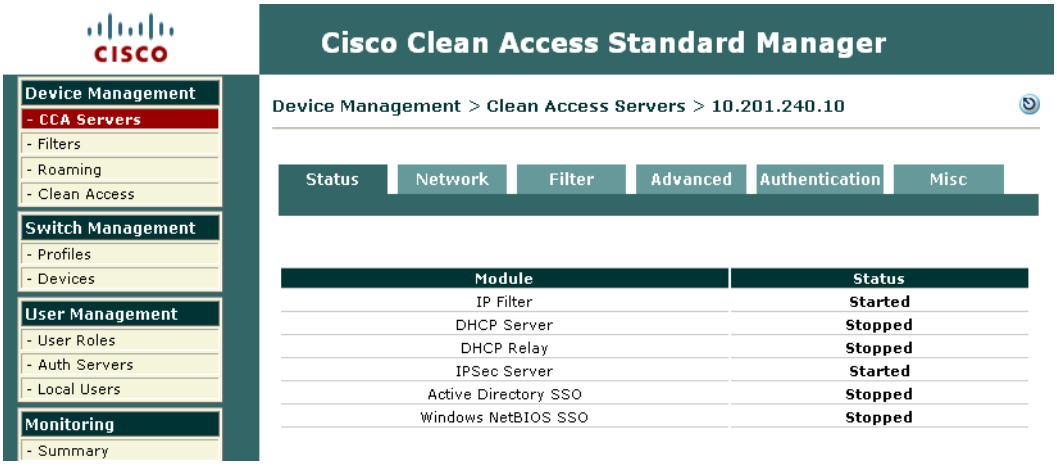
7. If the CAS is a Virtual Gateway, make sure the CAM and CAS are on different subnets (or VLANs).
8. If the CAS is a Virtual Gateway, and both ports of the CAS are connected to the same switch:
   a. Physically reconnect the eth1 interface of the CAS.
   b. Configure VLAN mapping (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**)
   c. Wait 2 minutes.
   d. Physically connect the eth1 interface of the CAS.
9. Check the CAM Event Log (under **Monitoring > Event Logs**). This can help pinpoint license and other issues.
10. Make sure there are no firewall rules blocking RMI ports (see CAM/CAS Connectivity Across a Firewall, page 4-18 for details):
11. Perform `service perfigo restart` on both the CAM and CAS.
12. Perform `service perfigo reboot` on both CAM and CAS.
13. Contact TAC. See Obtaining Technical Assistance, page -vi.

For further details on disconnecting, rebooting or deleting a Clean Access Server see "Working with Clean Access Servers" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Navigating the CAS Management Pages

When you click the **Manage** icon for a Clean Access Server in the **List of Servers** tab, the Clean Access Server management pages appear with a default view of the CAS **Status** tab, as shown in Figure 5-3.

Figure 5-3 Clean Access Servers Management Pages

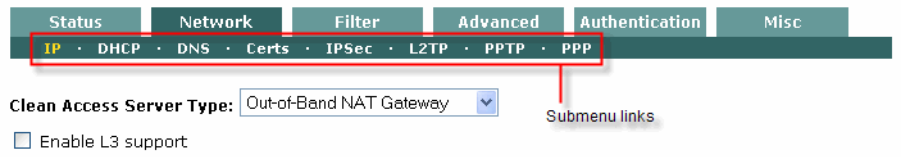


The tabs in the Clean Access Server management pages are as follows:

- **Status** – Status of Clean Access Server modules (Started or Stopped)

- **Network** – Operating mode and interface settings (IP address, VLAN, L2/L3) for the CAS itself, DNS settings, SSL certificate management, and DHCP configuration for managed subnets.
- **Filter** – Local (per CAS) device and subnet access policies, local traffic control and bandwidth policies (by role), and local Certified Device and Floating Device lists.
- **Advanced** – Routing settings for the CAS, such as Managed Subnets (L2) or Static Routes (L3), VLAN mapping for Virtual Gateways, NAT, 1:1 NAT, ARP, and Proxy server settings.
- **Authentication** – Enable and configuration settings for local login page, OS detection, VPN concentrator SSO and Windows AD SSO.
- **Misc** – CAS software upgrade, system time, and heartbeat timer for all users.

Within each tab, click the submenu links to access individual configuration forms.



Configure Network Settings for the CAS

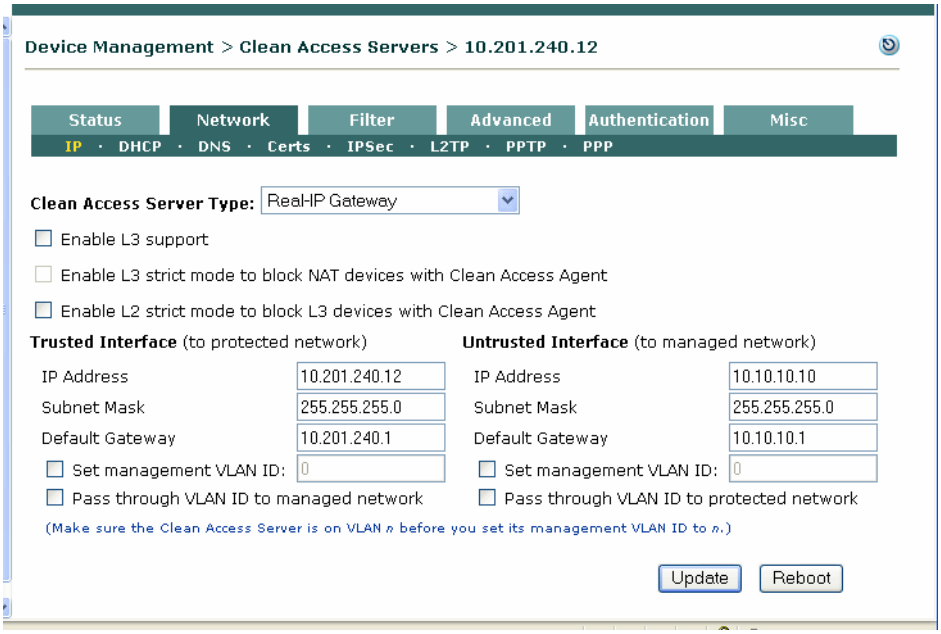
This section describes the following:

IP Form

The **IP** form in the **Network** tab (Figure 5-4) contains the network settings of the CAS configured at initial installation (or using the **service perfigo config** utility), as well as the CAS operating mode chosen when the CAS was added to the CAM. You must use the **IP** form to configure the CAS for L3 or L2 strict deployment, and you can use this form to view or change the IP address and network settings of the CAS as described below.

1. Access the **IP** form by navigating in the web console to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Network > IP**.

Figure 5-4 CAS Network IP Settings



2. The CAS **IP** form includes the following settings:

- **Clean Access Server Type** —This is the operating mode of the CAS, set when you Add the CAS to the CAM, page 5-2. See Change Clean Access Server Type, page 5-12 for additional details.
  - In-Band: Virtual Gateway, Real-IP Gateway, or NAT Gateway
  - OOB: Out-of-Band Virtual Gateway, Out-of-Band Real-IP Gateway, Out-of-Band NAT Gateway

Note NAT Gateway (in-band or out-of-band) is not supported for production deployment.

- **Enable L3 support**: When this option is enabled, the CAS allows all users from any hops away. For multi-hop L3 in-band deployments, this setting enables/disables L3 discovery of the CAS for web login users and Clean Access Agent users at the CAS level. When set, the CAS is forced to use the routing table to send packets. See Enable L3 Support, page 5-13 for details.
- **Enable L3 strict mode to block NAT devices with Clean Access Agent** — When this option is checked (in conjunction with "Enable L3 support"), the CAS verifies the source IP address of user packets against the IP address sent by the Clean Access Agent and blocks all L3 Agent users with NAT devices between those users and the CAS. See Enable L3 Strict Mode (Clean Access Agent Only), page 5-15 for details.
- **Enable L2 strict mode to block L3 devices with Clean Access Agent** — When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the Clean Access Agent and blocks all L3 Agent users (those more than one hop away from the CAS). The user is forced to remove any router between the CAS and the user's client machine to gain access to the network. See Enable L2 Strict Mode (Clean Access Agent Only), page 5-15 for details.
- All L3 or L2/L3 strict options left unchecked (Default setting)— The CAS performs in L2 mode and expects that all clients are one hop away. The CAS will not be able to distinguish if a router is between the CAS and the client and will allow the MAC address of a router as the machine of the first user who logs in and any subsequent users. Checks will not be performed on the actual client machines passing through the router as a result, as their MAC addresses will not be seen.

Note

- If using L2 deployment only, make sure the **Enable L3 support** option is not checked.
- L3 and L2 strict options are mutually exclusive. Enabling one option will disable the other option.
- Enabling or disabling L3 or L2 strict mode ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.

- **Trusted Interface—**The trusted interface (eth0) connects the CAS to the trusted backend network.
  - **IP Address**: The IP address of the trusted (eth0) interface of the CAS.
  - **Subnet Mask**: The subnet mask for the trusted interface.
  - **Default Gateway**:

    For Real-IP Gateway—This is the address of the default gateway on the trusted network, such as a network central router address.

    For Virtual Gateway—This is the address of the existing gateway on the trusted network side of the CAS.
  - **Set management VLAN ID**: When set at the trusted interface, the specified VLAN ID is added to packets destined to the trusted network.

    Note See also Native VLAN, Management VLAN, Dummy VLAN, page 5-28 for additional information needed for Virtual Gateway.

  - **Pass through VLAN ID to managed network**: If selected, VLAN IDs in the packets are passed through the interface unmodified.
- **Untrusted Interface**—The untrusted interface (eth1) connects the CAS to the untrusted managed network.

- **IP Address**: The IP address of the untrusted (eth1) interface of the CAS.
- **Subnet Mask: The** subnet mask for the untrusted interface.
- **Default Gateway**:

  For Real-IP Gateway—The default gateway is the untrusted interface IP address of the CAS.

  For Virtual Gateway—The default gateway is the address of the existing gateway on the trusted network side of the CAS.
- **Set management VLAN ID**: When set at the untrusted interface, the specified VLAN ID to is added to packets destined to clients.
- **Pass through VLAN ID to managed network**: If selected, VLAN IDs in the packets are passed through the interface unmodified.

3. After modifying settings, click **Update** and **Reboot**.
   Update causes the web console to retain the changed setting until the next reboot.
   Reboot causes the process to start in the CAS. The CAS will restart with the new settings.

Note Modified CAS **IP** settings ALWAYS require an **Update** and **Reboot** of the CAS to take effect.

Note For High Availability CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the standby CAS unit through its direct access web console. These settings include updating the SSL certificate, system time/time zone, DNS, or Service IP. See Clean Access Server Direct Access Web Console, page 12-2 and Modifying High Availability Settings, page 13-23 for details.

Note If you do not have a CA-signed certificate based on the DNS name of the CAS, when changing the IP address of the CAS, you must also regenerate the certificate as described in Manage CAS SSL Certificates, page 12-3.

Change Clean Access Server Type

When you add the CAS to the Clean Access Manager, you specify its operating mode: In-Band or Out-of-Band Real-IP, NAT, or Virtual Gateway. This section describes how to change the Server Type of the CAS after it has been added to the CAM as a different operating mode.

Note You must have an OOB-enabled license to change the CAS from In-Band to Out-of-Band mode.

Switching Between NAT and Real-IP Gateway Modes

To switch between NAT and Real IP Gateway modes, simply make the necessary configuration changes within the CAM admin console (for example, choose the type in the IP form, configure NAT behavior and DHCP properties, and so on).

Switching Between Virtual Gateway and NAT/ Real-IP Gateway Modes

To switch between Virtual and Real IP/NAT Gateway modes, you will need to change the topology of the network to reflect the modification. You must also modify the routing table on the upstream router to reflect the change. For more information on possible topology changes that are required, see Chapter 2, "Planning Your Deployment." The general steps for switching between these types are:

1. Delete the CAS from the list of managed Clean Access Servers in the CAM.
2. Modify the network topology as appropriate. Change the cable connections to the CAS, if needed.
3. Access the CAS via SSH console and execute the `service perfigo config` utility to change the IP address of the CAS (see Perform the Initial Configuration, page 4-9). You must change the eth1 IP address of the CAS.
4. Ping the CAS from the CAM's subnet to make sure that the topology is correctly changed.
5. Add the CAS in the CAM admin console.
6. Add or re-add managed subnets with the address that the CAS will represent. The managed subnet entries must specify the CAS as the default gateway for each of the managed subnets.
7. Add static routes in the upstream router for the subnets managed by the CAS.
8. Change the CAS configuration on the CAM from the **Device Management > CCA Servers > Manage [CAS_IP]> Network** page, and **Update** and **Reboot** the CAS.
9. Set up the CAS as either a DHCP server or relay.
10. Update relevant configuration settings such as certificates.
11. If changing to an Out-of-Band Real-IP Gateway, make sure to enable Port Bouncing (**Switch Management > Profiles > Port | "Bounce the port after VLAN is changed"**) to help Real-IP or NAT gateway clients get a new IP address after successful authentication and certification.

Enable Network Access (L3, L3 Strict or L2 Strict)

By default, Cisco NAC Appliance supports in-band web login and Clean Access Agent users within L2 proximity of the Clean Access Server.

For L2 deployments, you can optionally restrict L2 access so that Agent users cannot use home-based wireless routers or NAT devices to connect to the network.

If deploying for VPN/L3, you must **enable** L3 support for web login or Agent users that are multiple L3 hops away from the CAS.

You can additionally enable the "L3 strict" option, in conjunction with L3 support, to restrict L3 Clean Access Agent clients from connecting to the Clean Access Server through NAT devices.

For L2 discovery, the Agent sends discovery packets to all the default gateways of all the adapters on the machine on which the Agent is running. If a CAS is present either as the default gateway (Real-IP/NAT Gateway) or as a bridge before the default gateway (Virtual Gateway), the CAS will respond.

If the CAS does not respond via L2 discovery, the Agent will perform L3 discovery (if enabled). The Agent attempts to send packets to the Discovery Host, an IP address on the trusted side of the CAS. This IP address is set in the **Discovery Host** field of the **Device Management > Clean Access > Clean Access Agent > Installation** page and is set by default to the IP address of the CAM (which is always assumed to be on the trusted side of the CAS). When these packets reach a CAS (if present), the CAS intercepts the packets and responds to the Agent.

Note To discover the CAS, the Clean Access Agent sends SWISS (proprietary CAS-Agent communication protocol) packets on UDP port 8905 for L2 users and on port 8906 for L3 users. The CAS always listens on UDP port 8905 and 8906 and accepts traffic on port 8905 by default. The CAS will drop traffic on UDP port 8906 unless L3 support is enabled.The Agent performs SWISS discovery every 5 seconds.

Note As a best practice recommendation, when users are L2 adjacent to the CAS, it is recommended to use the Enable L2 strict mode to block L3 devices with Clean Access Agent. It is possible for a single CAS to support both L3 and L2 (non-restricted) Agent users. However, L2 strict mode and L3 support are mutually exclusive. Therefore, Cisco recommends against using the same CAS for L2 and L3 in-band deployment.

Enable L3 Support

To support multi-hop L3 deployments, you need to enable L3 support on each CAS. L3 support is disabled by default after upgrade or new install, and enabling L3 support requires an update and reboot of the Clean Access Server.

To Enable L3 Support:

1. Go **Device Management > CCA Servers > Manage [CAS_IP] > Network** and click the checkbox for "**Enable L3 support**" (see Figure 5-4 on page 5-9).
2. Click **Update**.
3. Click **Reboot**.

Note For Clean Access Agent users, the **Discovery Host** field (under **Device Management > Clean Access > Clean Access Agent > Installation**) automatically populates with the IP address of the CAM by default after new install or upgrade.

To Disable L3 Capability:

To disable L3 discovery of the Clean Access Server at the CAS level for web login and Clean Access Agent users:

1. Go **Device Management > CCA Servers > Manage [CAS_IP] > Network** and uncheck the option for "**Enable L3 support**" (see Figure 5-4 on page 5-9).
2. Click **Update**.
3. Click **Reboot**.

VPN/L3 Access for Clean Access Agent

The CAM/CAS/Agent support in-band multi-hop L3 deployment and VPN/L3 access from the Clean Access Agent. The Agent will:

1. Check the client network for the Clean Access Server (L2 deployments), and if not found,
2. Attempt to discover the CAS by sending discovery packets to the CAM. This causes the discovery packets to go through the CAS even if the CAS is multiple hops away (multi-hop deployment) so that the CAS will intercept these packets and respond to the Agent.

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the Agent from the CAS (via download web page or auto-upgrade). Either method allows the Agent to acquire the IP address of the CAM in order to send traffic to the CAM/CAS over the L3 network. Once installed in this way, the Agent can be used for both L3/VPN concentrator deployments or regular L2 deployments.

Acquiring and installing the Agent on the client by means other than direct download from the CAS (e.g. from Cisco Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.

To support VPN/L3 Access, you must:

- Check the option for "Enable L3 support" and perform an Update and Reboot under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.
- There must be a valid **Discovery Host** under **Device Management > Clean Access > Clean Access Agent > Installation** (set by default to the trusted IP address of the CAM).
- Clients must initially download the Agent from the CAS, in one of two ways:
  - "Download Clean Access Agent" web page (i.e. via web login)
  - Auto-Upgrade to 4.1.0.0 Agent (3.5.1+ Agent is required for auto-upgrade).
- SSO is only supported when integrating Cisco NAC Appliance with Cisco VPN Concentrators.

Note

- Uninstalling the Agent while still on the VPN connection does not terminate the connection.
- For VPN-concentrator SSO deployments, if the Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. Cisco Downloads), the Agent will not be able to get the runtime IP information of the CAM and will not pop up automatically nor scan the client.

3. If a 3.5.0 or prior version of the Agent is already installed, or if the Agent is installed through non-CAS means (e.g. Cisco Downloads), you must perform web login to download the Agent setup files from the CAS directly and reinstall the Agent to get the L3 capability.

Enable L3 Strict Mode (Clean Access Agent Only)

Administrators with L3 deployments can optionally restrict L3 Clean Access Agent clients from connecting to the Clean Access Server through NAT devices using the "**Enable L3 strict mode to block NAT devices with Clean Access Agent**" option.

When this feature is enabled in conjunction with "Enable L3 support," the CAS will check the client IP information automatically sent by the Clean Access Agent against source IP information to ensure no NAT device exists between the CAS and the client. If a NAT device is detected between the client device and the CAS, the user is not allowed to log in.

This provides administrators with the following options when enabling network access for clients on the CAS:

- **Enable L3 support** —The CAS allows all users from any hops away.
- **Enable L3 strict mode to block NAT devices with Clean Access Agent** — When this option is checked (in conjunction with "Enable L3 support"), the CAS verifies the source IP address of user packets against the IP address sent by the Clean Access Agent and blocks all L3 Agent users with NAT devices between those users and the CAS.
- **Enable L2 strict mode to block L3 devices with Clean Access Agent** — When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the Clean Access Agent and blocks all L3 Agent users (those more than one hop away from the CAS). The user will be forced to remove any router between the CAS and the user's client machine to gain access to the network.
- **All options left unchecked** (Default setting)— The CAS performs in L2 mode and expects that all clients are one hop away. The CAS will not be able to distinguish if a router is between the CAS and the client and will allow the MAC address of router as the machine of the first user who logs in and any subsequent users. Checks will not be performed on the actual client machines passing through the router as a result, as their MAC addresses will not be seen.

Enable L2 Strict Mode (Clean Access Agent Only)

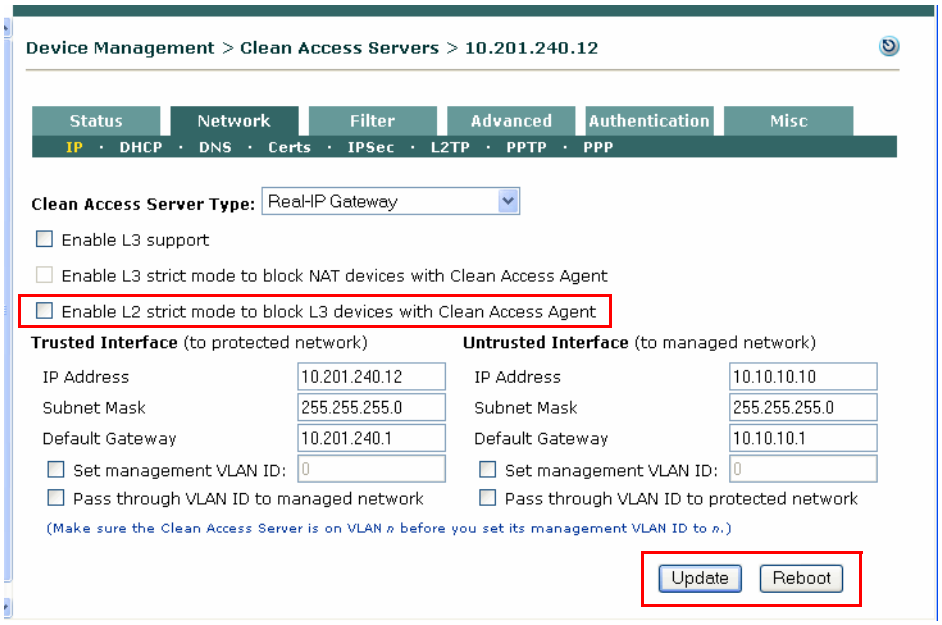
Administrators can optionally restrict Clean Access Agent clients to be connected to the Clean Access Server directly as their only gateway using the "Enable L2 strict mode to block L3 devices with Clean Access Agent" option.

When this feature is enabled, the Clean Access Agent will send the MAC addresses for all interfaces on the client machine with the login request to the CAS. The CAS then checks this information to ensure no NAT exists between the CAS and the client. The CAS verifies and compares MAC addresses to ensure that the MAC address seen by the CAS is the MAC address of the Agent client machine only. If user home-based wireless routers or NAT devices are detected between the client device and the CAS, the user is not allowed to log in.

To Enable L2 strict mode to block L3 devices with Clean Access Agent

1. **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**. The management pages appear for the chosen Clean Access Server appear.

Figure 5-5 CAS Network Tab



2. Click the checkbox for **Enable L2 strict mode to block L3 devices with Clean Access Agent**.
3. Click **Update**.
4. Click **Reboot**.

Note

- Enabling or disabling L3 or L2 strict mode ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.
- L3 and L2 strict options are mutually exclusive. Enabling one option will disable the other option.

See also the "Clean Access Agent" chapter of the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for additional information.

Configure DHCP

You can configure the CAS to be a DHCP server when the CAS is in Real-IP/NAT Gateway mode, if a DHCP server does not already exist on your network. For complete details, see Chapter 6, "Configuring DHCP."

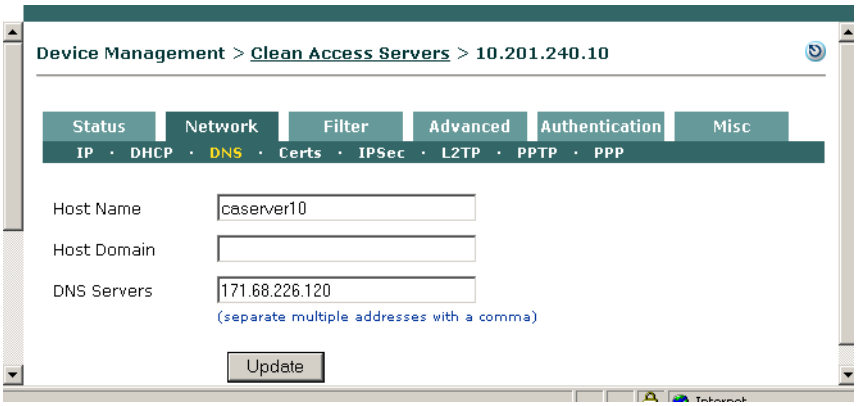
Configure DNS Servers on the Network

The **DNS** form lets you specify the Domain Name Service (DNS) servers to be queried for host name lookups.

To configure a DNS for your environment:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network >DNS**.

Figure 5-6 DNS Form



2. Type the IP addresses of one or more domain name servers in the **DNS Servers** field. If entering multiple servers, use commas to separate the addresses. The Clean Access Server attempts to contact the DNS servers in the order they appear in the list.
   - **Host Name —**The host name you want to use for the Clean Access Server.
   - **Host Domain—**The domain name applicable in your environment.
   - **DNS Servers —**The IP address of the DNS server in your environment. Separate multiple addresses with commas. If you specify more than one DNS server, the Clean Access Server tries to contact them sequentially, until one of them returns a response.
3. Click **Update**.

Note For High Availability CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the standby CAS unit through its direct access web console. These settings include updating the SSL certificate, system time/time zone, DNS, or Service IP. See Clean Access Server Direct Access Web Console, page 12-2 and Modifying High Availability Settings, page 13-23 for details.

Configuring Managed Subnets or Static Routes

This section describes the following:

Overview

For all CAS modes in L2 deployment (Real-IP/NAT/Virtual Gateway) when configuring additional subnets, you must configure **Managed Subnets** in the CAS so that the CAS can send ARP queries with appropriate VLAN IDs for client machines on the untrusted interface.

Managed Subnets are only for user subnets that are **Layer 2 adjacent** to the CAS.

For all CAS modes in L3 deployment, **Static Routes** must be configured for the user subnets that are one or more hops away. Managed subnets should not be configured for these subnets. See Configure Static Routes for L3 Deployments, page 5-22 for details.

Note In the case of a multi-hop L3 deployment where the VPN concentrator performs Proxy ARP for client machines, managed subnets can be used instead of static routes and should be created in the CAS.

Table 5-1 summarizes the steps required for each deployment. Forms mentioned below are located in the CAS management pages under **Device Management > CCA Servers > Manage [CAS_IP]**.

Note

- For IPs with VLAN restrictions, all IPs must be in a managed subnet, and you must create a managed subnet first before creating an IP range (DHCP pool).
- For IPs with relay restrictions, all IPs should typically be in static routes, but can be in managed subnets if integrating the CAS with Aironet devices or other non-RFC 2131/2132 compliant devices. Note that these IP address pools must be in either a static route or a managed subnet, and IPs with relay restrictions should only be put in a managed subnet for these non-compliant devices.

See Configuring IP Ranges (IP Address Pools), page 6-5 for details.

Table 5-1 Guidelines for Adding Managed Subnets vs. Static Routes

<table>
<tr><th>Layer 2—In-Band or Out-of-Band
(CAS has L2 proximity to users)</th><th colspan="2">Layer 3 (Multi-Hop) —In-Band Only
(e.g. CAS is behind VPN Concentrator or Router or L3 Switch)</th></tr>
<tr><td>For Real-IP and NAT Gateways:</td><td colspan="2">For Real-IP and NAT Gateways:</td></tr>
<tr><td></td><td>If the router below the CAS performs proxy ARP:</td><td>If the router below the CAS does NOT perform proxy ARP:</td></tr>
<tr><td>Add a managed subnet under Advanced > Managed Subnet to assign the gateway IP address of the subnet to the CAS.

For example, to configure the CAS to be the gateway (10.10.10.1) for VLAN 10 /subnet 10.10.10.0, specify the following managed subnet:

IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
VLAN ID: 10</td><td>Always add a managed subnet under Advanced > Managed Subnet</td><td>1. Always add static routes for the subnets on the untrusted side under Advanced > Static Routes. For example:
<pre>Network   Mask   Interface Gateway
10.10.10.0 /24   eth1   10.10.10.1
10.10.20.0 /24   eth1   10.10.20.1</pre>Note /24 subnet mask = 255.255.255.0

2. Specify an ARP entry for the gateway IP that the CAS needs to hold under Advanced > ARP. For example:
<pre>10.10.10.0 255.255.255.255 eth1</pre>See Figure 5-7 on page 5-20.</td></tr>
<tr><td>For Virtual Gateways:</td><td colspan="2">For Virtual Gateways:</td></tr>
<tr><td></td><td>If the router below the CAS performs proxy ARP:</td><td>If the router below the CAS does NOT perform proxy ARP:</td></tr>
<tr><td>Add a managed subnet under Advanced > Managed Subnet to assign an IP address to the CAS that is otherwise unused on the subnet.

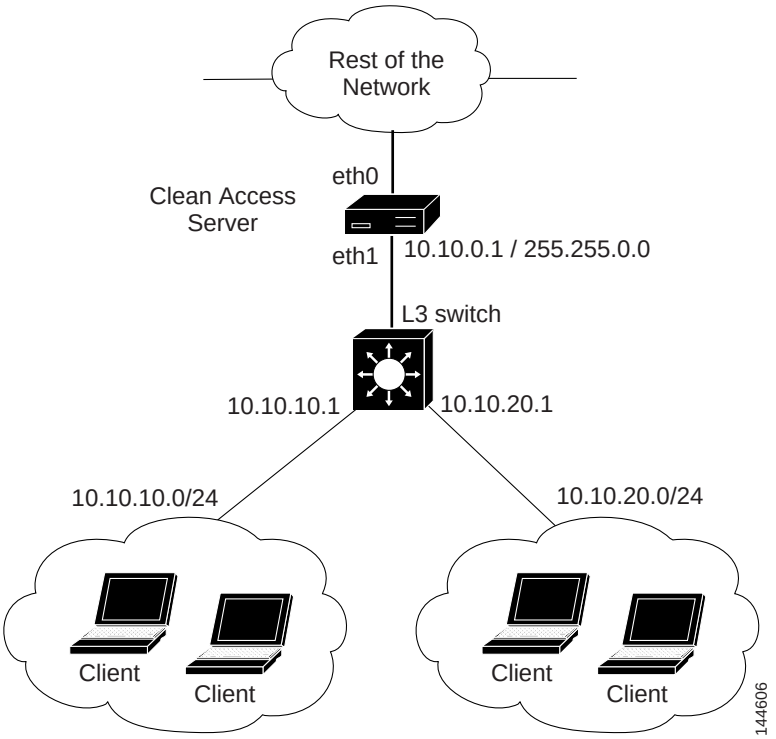
For example, to have the CAS manage subnet 10.10.10.0/24 on VLAN 10 where the gateway for this subnet is 10.10.10.1, you will need to reserve an IP address for the CAS, such as 10.10.10.2. Specify the following managed subnet:

IP Address: 10.10.10.2
Subnet Mask: 255.255.255.0
VLAN ID: 10

The CAS is not the gateway, but owns the 10.10.10.2 address for this VLAN/subnet.</td><td>Always add a managed subnet under Advanced > Managed Subnet</td><td>1. Add static route for the subnets on the untrusted side under Advanced > Static Routes. For example:
<pre>Network   Mask   Interface Gateway
10.10.10.0 /24   eth1   10.10.10.1</pre>Note When deploying the CAS in L3 VGW mode, the gateway is not optional and you must specify the gateway for the static route.</td></tr>
</table>

Note In general, when the CAS is in Virtual Gateway mode for Layer 2 or Layer 3, you cannot ping the gateways of the subnets being handled by the CAS. This should not affect the connectivity of the users on these subnets.

Figure 5-7 Configuring Static Routes for CAS in L3 Real-IP Gateway Deployment



Configure Managed Subnets for L2 Deployments

When the Clean Access Server is first added to the Clean Access Manager, the untrusted IP address provided for the CAS is automatically assigned a VLAN ID of -1 to denote a Main Subnet. By default, the untrusted network the Clean Access Server initially manages is the Main Subnet.

You can configure the CAS to manage additional subnets by adding them under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**. In this case, the Clean Access Server acts as the virtual default gateway for the managed subnets, and puts a virtual IP for the added managed subnet on the untrusted interface.

Note If the Clean Access Server is a Real-IP Gateway, you will need to add a static route on the upstream router to send traffic to the CAS. For example, for managed subnet 10.0.0.0/24, you will need to add static route 10.0.0.0/255.255.0.0 gateway <CAS_trusted_IP> to the upstream router.

To modify the Main Subnet of the CAS, go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**. To change the VLAN ID of the Main Subnet, enter it in the **Set management VLAN ID** field in the **Untrusted Interface** side of the form. If modifying the IP Address, Subnet Mask, Default Gateway, or management VLAN ID for the untrusted interface of the CAS, you must click **Update** then **Reboot** for the new settings to take effect on the CAS and on the network.

When you create a managed subnet, an ARP entry is automatically generated for the gateway of the subnet. Therefore, to manage a subnet of 10.1.1.0/255.255.255.0, configure the managed subnet with the following values:

- IP Address: 10.1.1.1 (if 10.1.1.1 is the desired default gateway)

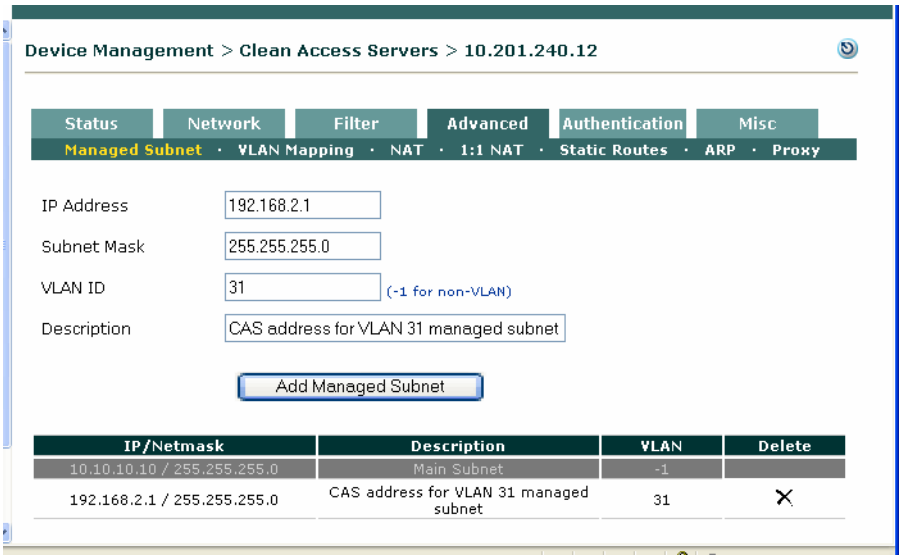
- Subnet Mask: 255.255.255.0

An ARP entry is automatically generated for the 10.1.1.1 address, the presumed gateway. However, if using a non-standard gateway address (such as 10.1.1.213 for the 10.1.1.0/255.255.255.0 subnet), you will need to create the managed subnet as 10.1.1.213/255.255.255.0.

Adding Managed Subnets

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**.

Figure 5-8 Managed Subnet



2. In the **IP Address** field, type the IP address that the CAS will own for the managed subnet (the CAS will perform ARP for this IP address):
   - For Real-IP/NAT Gateways, the CAS will own the gateway IP address of the managed subnet (for example, 10.10.10.1).
   - For Virtual Gateways, the CAS will own an IP address on the managed subnet that is otherwise unused (for example, 10.10.10.2)

   See Table 5-1 on page 5-19, "Guidelines for Adding Managed Subnets vs. Static Routes" for details.
3. In the **Subnet Mask** field, type the mask for the network address. The CAM calculates the network address by applying the subnet mask to the **IP Address** field.
4. In the **VLAN ID** field, type the VLAN ID associated with this subnet. Use -1 if the subnet is not on a VLAN.

Note The VLAN column for the main subnet displays the eth1 Management VLAN of the CAS (if available) or "-1" if no eth1 Management VLAN is set for the CAS.

5. Click **Add Managed Subnet** to save the subnet.

If you need to provide an ARP entry for the managed subnet other than the one created by default, use the instructions in Add ARP Entry, page 5-24. For the entry, use the gateway address for the subnet and set the **Link** value to **Untrusted (eth1)**.

Configure Static Routes for L3 Deployments

L3 deployments (and some VPN concentrators deployments) should not use Managed Subnets and should only use Static Routes to configure how the CAS should route packets. The **Static Route** form (Figure 5-11) lets you set up routing rules in the Clean Access Server. Static Routes have the form:

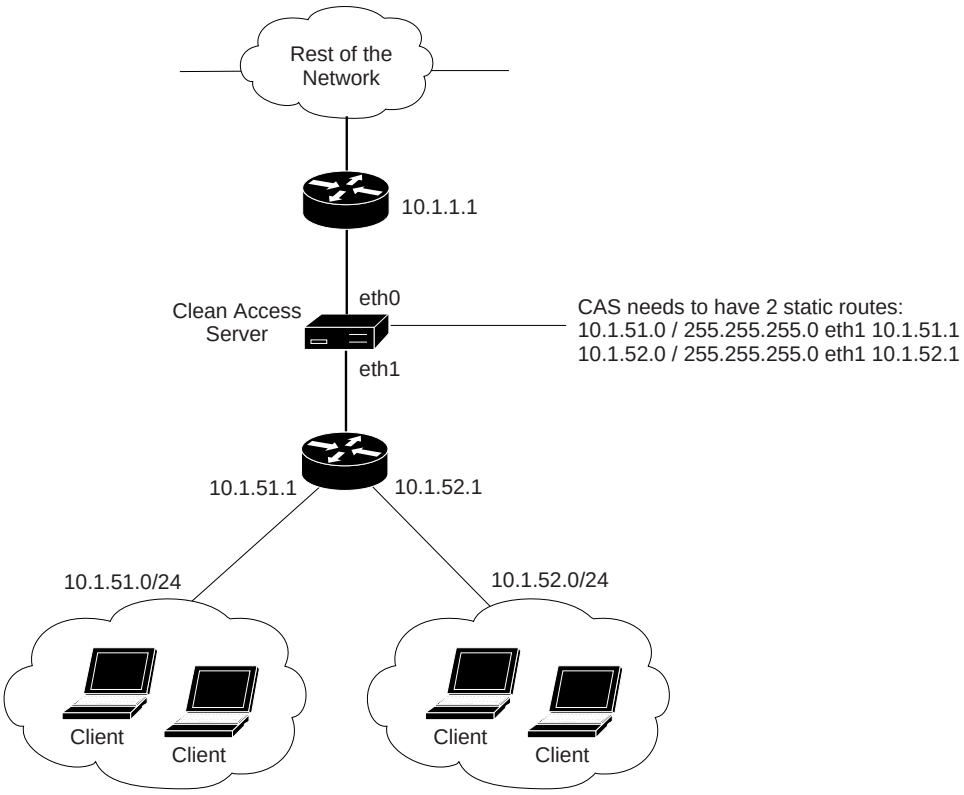
Network / subnet mask / send packets to interface (trusted or untrusted) / Gateway IP address (optional)

Any packet that comes into the CAS is evaluated based on static routes, then routed appropriately to the router. When the CAS receives a packet, it looks through its static route table, finds the most specific match, and if that route has a gateway specified, the CAS sends packets through that gateway. If no gateway is specified, then the CAS puts packets on the interface specified for the route (eth0 or eth1).

Note If converting from L2 to L3 deployment, remove managed subnets and add static routes instead.

Figure 5-9 illustrates a Layer 3 deployment scenario that requires a static route.

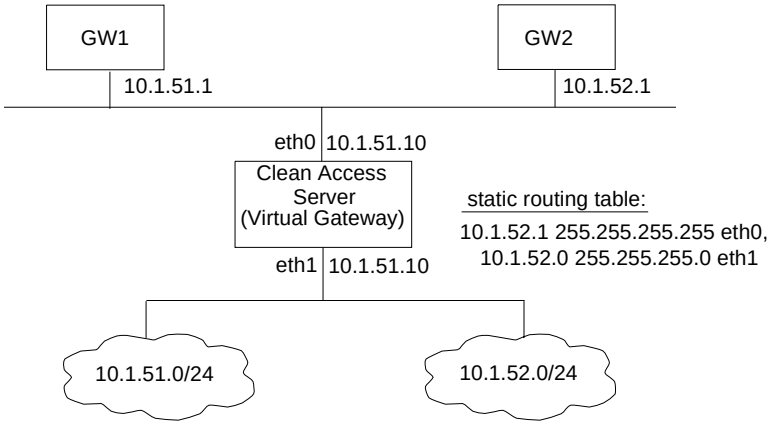
Figure 5-9 Static Route Example (Layer 3)



Configuring Static Routes for Layer 2 Deployments

Figure 5-10 illustrates a Layer 2 deployment scenario that requires a static route. In this case, the Clean Access Server operates as a Virtual Gateway. Two gateways exist on the trusted network (GW1 and GW2). The address for the second gateway, GW2, is outside the address space of the first gateway, which includes the Clean Access Server interfaces. The static route ensures that traffic intended for GW2 is correctly passed to the Clean Access Server's trusted interface (eth0).

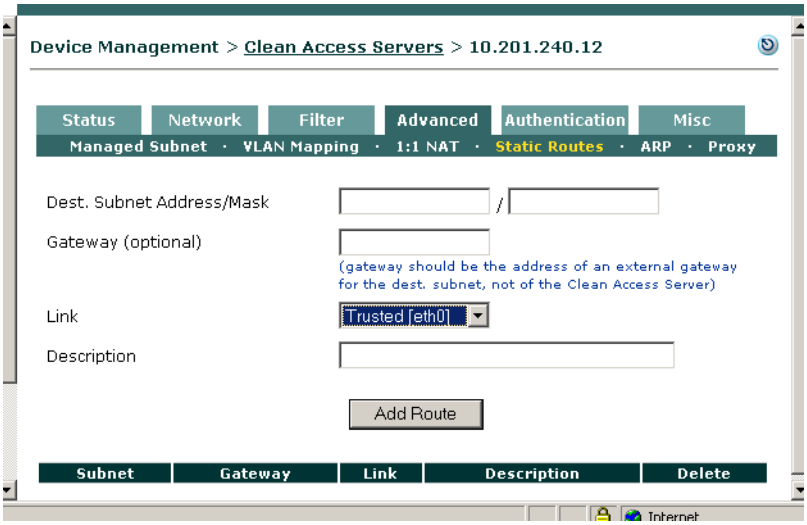
Figure 5-10 Static Route Example (Layer 2)



Add Static Route

1. Open the **Static Routes** form in the **Advanced** tab of the CAS management pages.

Figure 5-11 Static Routes



2. In the **Static Routes** form, type the destination IP address and subnet mask (in CIDR format) in the **Dest. Subnet Address/Mask** fields. If the destination address in the packet matches this address, the packet is routed to the specified interface.
3. If needed, type the external, destination **Gateway** address (such as 10.1.52.1 in Figure 5-10).

Note For Virtual Gateway mode, the **Gateway** address is not optional and must always be specified.

4. Choose the appropriate interface of the Clean Access Server machine from the **Link** dropdown list. In most cases this is eth0, since most static routing scenarios involve directing traffic from the untrusted to the trusted network.
5. Optionally, type a **Description** of the route definition.
6. Click **Add Route**.

Configure ARP Entries

An ARP (Address Resolution Protocol) entry allows you to associate IP addresses with one of the Clean Access Server's interfaces. An ARP entry is typically used to advertise to the trusted network that certain addresses are within the Clean Access Server's managed domain, so that traffic for the managed clients can be directed to the Clean Access Server's untrusted interface.

ARP entries are automatically created for:

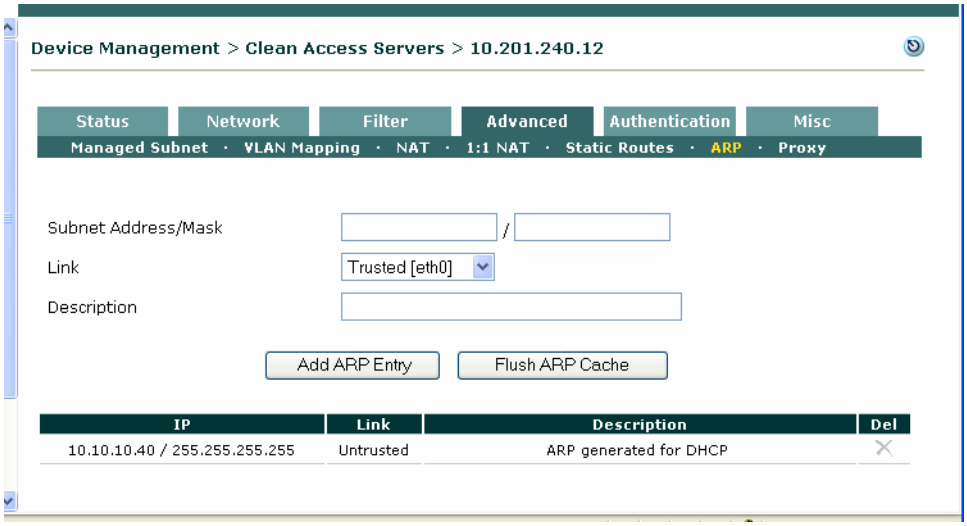
- The untrusted network specified for the Clean Access Server in the **IP** form.
- Any managed subnets you added (see Configuring Managed Subnets or Static Routes, page 5-18).
- Auto-generated subnets created during DHCP configuration. These entries are identified by the description "ARP Generated for DHCP." (see Figure 6-12 on page 6-13)

Add ARP Entry

Use the following steps to manually create an ARP entry.

1. Open the **ARP** form in the **Advanced** tab.

Figure 5-12 Create ARP Entry



2. Type the IP address of the network or machine to be associated with the interface along with the subnet mask in the **Subnet Address/Mask** fields. If creating an ARP entry for a single address, such as a virtual default gateway address, specify the address and use 255.255.255.255 as the subnet mask.
3. Choose the interface from the **Link** dropdown menu (usually eth1, the untrusted interface).
4. Optionally, type a **Description** of the ARP entry.
5. Click **Add ARP Entry** to save the settings.
6. Clicking the **Flush ARP Cache** button clears cached MAC-to-IP address associations.

Note Due to Roaming feature deprecation in release 4.1(0), the **Continuously broadcast gratuitous ARP with VLAN ID** option is removed.

Understanding VLAN Settings

The Clean Access Server can serve either as a VLAN termination point or it can perform VLAN passthrough. In a Virtual Gateway configuration, VLAN IDs are passed through by default.

In a Real-IP or NAT Gateway configuration, by default the VLAN identifiers are terminated at the CAS (that is, identifiers are stripped from packets received at the trusted and untrusted interfaces). However, if you enable VLAN ID passthrough, packets retain their VLAN identifiers.

Note If you are unsure of which mode to use, you should use the default behavior of the CAS.

For the VLAN identifier to be retained, passthrough only needs to be enabled for the first of the two interfaces that receives the message. That is, if VLAN ID passthrough is enabled for the untrusted interface, but terminated for the trusted interface, packets from the untrusted (managed) clients to the trusted network retain identifiers, but packets from the trusted network to the untrusted (managed) clients have their identifiers removed. Note, however, that in most cases you would enable or disable VLAN ID passthrough on both interfaces.

A management VLAN identifier is a default VLAN identifier. If a packet does not have its own VLAN identifier, or if the identifier was stripped by the adjacent interface, a management VLAN identifier specified at the interface is added to the packets (in order to route them properly through VLAN enabled equipment on the network).

Note The Clean Access Server is typically configured such that the untrusted interface is connected to a trunk port with multiple VLANs trunked to the port. In such a situation, the management VLAN ID is the VLAN ID of the VLAN to which the IP address of the CAS belongs.

Use care when configuring VLAN settings. Incorrect VLAN settings can cause the CAS to be inaccessible from the CAM web admin console. If you cannot access the CAS from the CAM after modifying the VLAN settings, you will need to access the CAS directly to correct its configuration, as described in Access the CAS Over a Serial Connection, page 4-5.

VLAN settings for the CAS eth0 and eth1 interfaces are set under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**. The settings are as follows:

- **Set management VLAN ID** – The default VLAN identifier value added to packets that do not have an identifier. Set at the untrusted (eth1) interface to add the VLAN ID to packets directed to managed clients, or at the trusted (eth0) interface to add the VLAN ID to packets destined for the trusted (protected) network.
- **Pass through VLAN ID to managed network** / **Pass through VLAN ID to protected network** – If selected, VLAN identifiers in the packets are passed through the interface unmodified.

As mentioned, by setting the management VLAN ID value for the managed network, you can add VLAN ID tags to the outbound traffic of the entire managed network. You can also set VLAN IDs based on other characteristics. Specifically, the CAS can tag outbound traffic by:

- Managed network
  (under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**)
- Managed subnet
  (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**)
- User role
  (under **User Management> User Roles > User Roles > New** or **Edit Role**)

For example, if you set the VLAN ID for the *faculty* role to 1005, the CAS would set that VLAN ID on every packet belonging to a user in that role as the packet went from the untrusted side to the trusted side of the Clean Access Server.

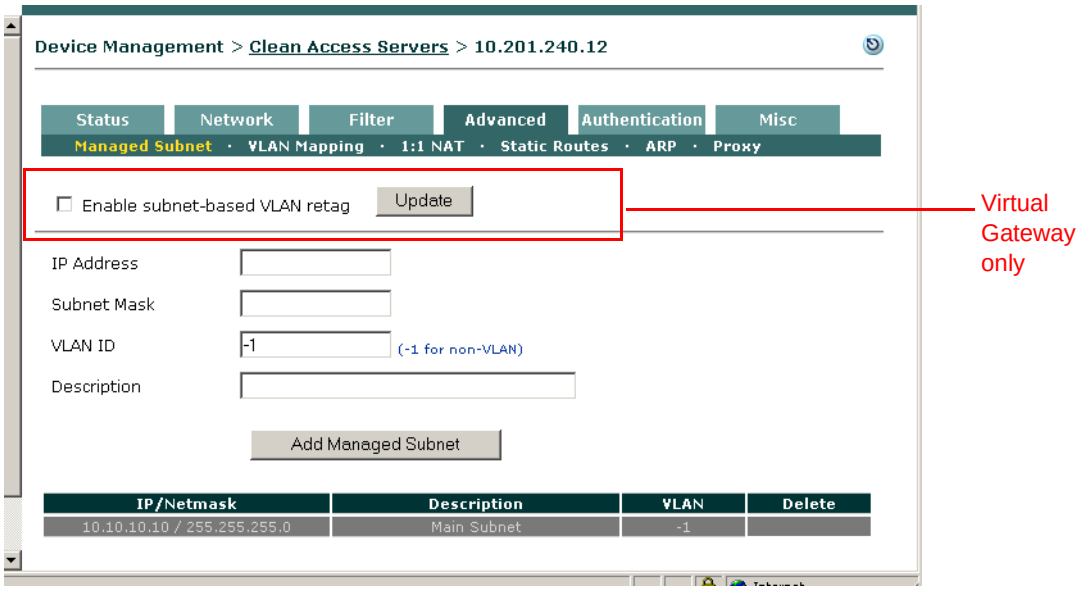
In addition, once VLAN tagging is configured, traffic from users on a particular VLAN ID and authenticated by an external authentication source can be mapped to a specific user role (under **User Management> Auth Servers > Mapping Rules**). Role mapping rules can use the user's VLAN ID as one of the attributes when assigning a user to a role. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Enable Subnet-Based VLAN Retag in Virtual Gateway Mode

The Managed Subnet form (**Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**) allows you to add managed subnets for Clean Access Servers in Real-IP, NAT and Virtual Gateway modes as described in Configure Managed Subnets for L2 Deployments, page 5-20. Traffic originating from the untrusted interface of the CAS is tagged according to the VLAN ID set for the managed subnet.

For CASes in Virtual Gateway mode only, the **Enable subnet-based VLAN retag** option appears at the top of the **Managed Subnet** form, as shown in Figure 5-13.

Figure 5-13 Enable Subnet-Based VLAN Retag for Virtual Gateway



This feature is more useful on wireless networks than on wired networks. For example, assume that a single CAS in Virtual Gateway mode is managing multiple subnets/VLANs, where each subnet is a separate VLAN. If a user is initially connected to an Access Point on VLAN A, the user will receive an IP address on subnet A. Assume that due to overlapping wireless signals, the user is subsequently connected to an AP on VLAN B. If the **Enable subnet-based VLAN retag** feature is not enabled, the user's traffic will not be routed correctly since their address is on subnet A (i.e. VLAN A) but their packets are tagged with VLAN B. This feature allows the CAS to retag packets based on the subnet to which they belong, thus enabling the packets to be routed correctly.

VLAN Mapping in Virtual Gateway Modes

For Clean Access Servers in Virtual Gateway mode only, the VLAN mapping form appears under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. This forms allows you to map an untrusted interface VLAN ID to a trusted network VLAN ID.

Traffic going through the CAS will be VLAN-retagged according to this VLAN Mapping setting.

Native VLAN, Management VLAN, Dummy VLAN

For best practice purposes, and to prevent trunking configuration issues for Virtual Gateway deployments, Cisco NAC Appliance requires differentiating native, management, and dummy VLANs when configuring your switches.

Caution Do not put the Clean Access Server on VLAN 1.

A native VLAN is present whether or not one is declared; the default is VLAN 1. By default all Cisco switches have their ports configured to be in VLAN 1, and a trunk link has the native VLAN set as VLAN 1. In addition to the well-known vulnerabilities associated with VLAN 1, as a security appliance, Cisco explicitly recommends setting the native VLAN to a VLAN **other than VLAN 1**. This ensures that no traffic is unknowingly passed to or through the CAS on this VLAN. For example, if there is a misconfiguration on the trunk link or any unknown traffic on VLAN 1 (such as a user connecting a laptop on an unused port on default VLAN 1) this will not cause any problems on the CAS.

Note The VLAN 1 restriction is required for the CAS, and highly recommended for the CAM. Because of the configuration requirements on the CAS in Virtual Gateway mode, where no common VLANs should exist between the trusted and untrusted port, VLAN 1 should not be used at all on either the trusted port or the untrusted port. This ensures that a Layer 2 loop cannot occur on VLAN 1 due to misconfiguration.

Although the management VLAN could be the native VLAN, setting the management VLAN to another value also ensures that **all traffic** that passes to or through the CAS is tagged and that there is no question that the CAS properly associates the traffic either to the Management VLAN of the CAS or to the VLAN mappings from the untrusted to trusted interface of the CAS. For this reason, the “dummy” VLAN is also used so that any untagged packet is correctly dropped.

Note The Management VLAN for the CAS is set under **Network > IP.** VLAN mappings are set on the CAS under **Advanced > VLAN Mapping.**

Best practice dictates the use of **different** dummy VLAN IDs, for example 998 and 999, for the native VLANs on the eth0 and eth1 interfaces of the CAS. This ensures that untagged traffic is dropped and is never passed unknowingly between the Untrusted and Trusted CAS interfaces. The CAS should not pass the traffic in either case without a VLAN mapping. However, the use of different dummy VLAN IDs prevents the possibility of manual/administrator errors resulting in the incorrect passing of traffic to or through the CAS via the native VLAN.

VLAN Mapping for In-Band

When a Clean Access Server operates in Virtual Gateway mode, it passes network traffic from its eth0 interface to eth1 and from eth1 to eth0 without changing the VLAN tag.

For In-Band configurations, in order to pass traffic from both interfaces through the same Layer 2 switch without creating a loop, it is necessary to place incoming traffic to the Clean Access Server on a different VLAN from the outgoing traffic of the Clean Access Server.

VLAN Mapping for Out-of-Band

In Out-of-Band Virtual Gateway mode, the OOB Clean Access Server uses VLAN mapping to retag an unauthenticated client's allowed traffic (e.g. DHCP/DNS) from the Authentication VLAN to the Access VLAN and vice versa.

Note See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for all other details on OOB configuration.

Switch Configuration for Out-of-Band Virtual Gateway Mode

Obtain the following VLAN IDs for Cisco NAC Appliance:

- VLAN for the Clean Access Manager (the management VLAN, e.g. 64)
- VLAN for the Clean Access Server (a new management VLAN, e.g. 222)

Note For a Virtual Gateway, the management VLAN for the CAS must be different from the CAM.

- VLAN(s) for Access (e.g., 10, 20, 30, 40)
- VLAN(s) for Authentication (e.g. 610, 620, 630, 640)
- Dummy (unused) VLAN for native VLAN settings on switch interfaces connected to the CAS interfaces (e.g. 998, 999)

Example switch configuration on the switch interfaces connecting to eth0 of the CAS:

- switchport trunk encapsulation dot1q
- switchport trunk native vlan 998
- switchport trunk allowed vlan 10,20,30,40,222

Example switch configuration on the switch interfaces connecting to eth1 of the CAS:

- switchport trunk encapsulation dot1q
- switchport trunk native vlan 999
- switchport trunk allowed vlan 610,620,630,640

CAS eth0 and eth1 network settings:
(Device Management > CCA Servers > Manage [CAS_IP] > Network > IP):

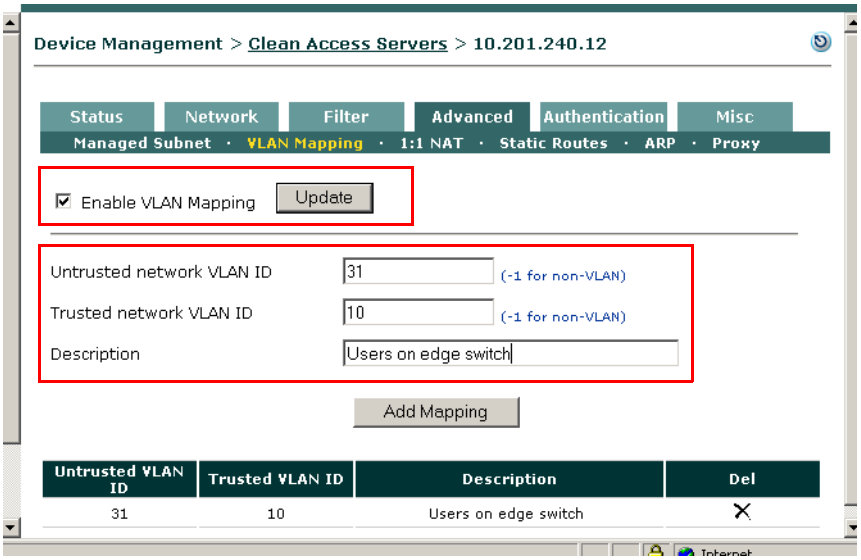
- Set Trusted management VLAN ID (e.g. 222)

Note You must prune VLANs on both the trusted and untrusted sides to only the VLANs that the CAS needs to manage. You must also prune VLAN 1 out of the trunk on both sides.

Configure VLAN Mapping for Out-of-Band

1. Go to **Device Management > CCA Servers > List of Servers** and click the **Manage** button (🔧) for the Out-of-Band Virtual Gateway CAS you added. The CAS management pages appear.
2. Click the **Advanced** tab.
3. Click the **VLAN Mapping** link.

Figure 5-14 Enable VLAN Mapping

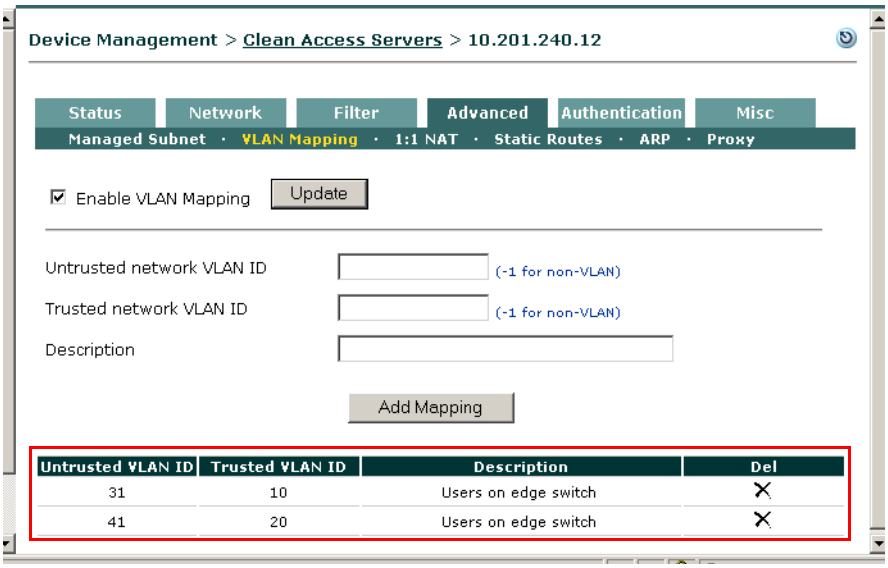


4. Click the checkbox for **Enable VLAN Mapping**.
5. Click **Update**.
6. Enter the Auth VLAN ID for the **Untrusted network VLAN ID** field.
7. Enter the Access VLAN ID for the **Trusted network VLAN ID** field.
8. Type an optional **Description (**such as **Users on edge switch**).
9. Click **Add Mapping**.

To Verify VLAN Mapping for Out-of-Band

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Advanced > VLAN Mapping.**
2. The VLAN mappings you configured should be listed at the bottom of the page.

Figure 5-15 Verify VLAN Mapping



Local Device and Subnet Filtering

As typically implemented, Cisco NAC Appliance enforces authentication requirements on clients attempting to access the network. Device and subnet filters allow you to define specialized access privileges or limitations for particular clients.

Note Access policies set in the CAS management page apply only to the CAS being administered. To configure global passthrough policies for all Clean Access Servers, go to the **Device Management > Filters** module in the CAM web console. Note that local policies override global settings.

An device/subnet filter can:

- Allow all traffic for a device/subnet without requiring authentication.
- Block a device/subnet from accessing the network.
- Exempt a device/subnet from authentication while applying other policies of a role for the device(s)

An filter policy is one way that a Cisco NAC Appliance role can be assigned to a client. The order of priority for role assignment as follows:

1. MAC address
2. Subnet / IP address
3. Login information (login ID, user attributes from auth server, VLAN ID of user machine, etc.)

Therefore, if a MAC address associates the client with “Role A”, but the user’s login ID associates him or her to “Role B”, “Role A” is used.

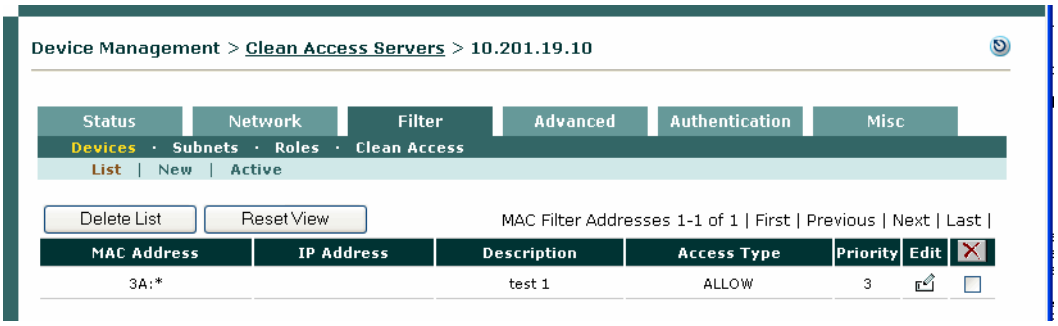
Note The Clean Access Manager respects the global Device Filters list for Out-of-Band deployments (does not apply to CAS-specific filters). See “Global Device and Subnet Filtering” in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Configure Local Device Access Filter Policies

You can configure local device filter polices for in-band deployments.

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Filter > Devices**.

Figure 5-16 Local Device Filters List



2. Click **New**. The New local filter form appears as shown in Figure 5-17.
3. In the **Devices** Filter form, enter the MAC address of the device(s) for which you want to create a policy in the **MAC Address/IP Address Description** text field. Type one entry per line using the following format:

   <MAC>/<optional_IP> <optional_entry_description>

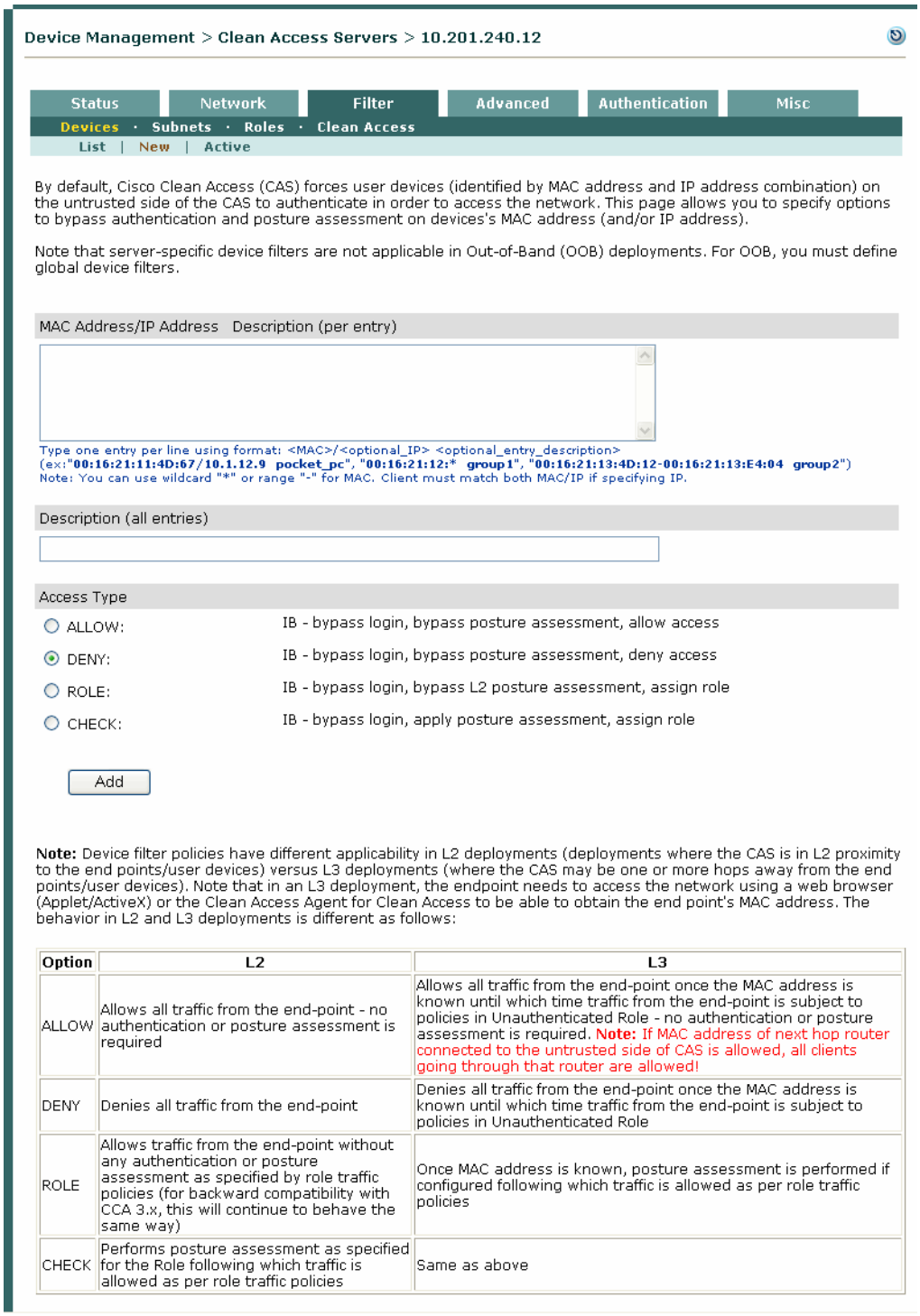
   Note the following:

   - You can use wildcards "*" or a range "-" to specify multiple MAC addresses
   - Separate multiple devices with a return.
   - If you enter both a MAC and an IP address, the client must match both for the rule to apply.
   - You can specify a description by device or for all devices. A description specific to a particular device (in the MAC Address field) supersedes a description that applies all devices in the **Description (all entries)** field. There cannot be spaces within the description in the device entry.
4. Choose the policy for the device from the **Access Type** choices:
5. Choose the policy for the device from the **Access Type** choices:
   - **ALLOW —** IB - bypass login, bypass posture assessment, allow access
   - **DENY —** IB - bypass login, bypass posture assessment, deny access
   - **ROLE—** IB - bypass login, bypass L2 posture assessment, assign role
   - **CHECK—** IB - bypass login, apply posture assessment, assign role
6. If using **CHECK** or **ROLE**, choose a role from the **User Role** dropdown menu.
7. Click **Add** to save the policy. The policy appears in the list at the bottom of the page

The following examples are all valid entries (that can be entered at the same time):

```
00:16:21:11:4D:67/10.1.12.9 pocket_pc
00:16:21:12:* group1
00:16:21:13:4D:12-00:16:21:13:E4:04 group2
```

Figure 5-17 New Local Filter



Option	L2	L3
ALLOW	Allows all traffic from the end-point - no authentication or posture assessment is required	Allows all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role - no authentication or posture assessment is required. **Note:** If MAC address of next hop router connected to the untrusted side of CAS is allowed, all clients going through that router are allowed!
DENY	Denies all traffic from the end-point	Denies all traffic from the end-point once the MAC address is known until which time traffic from the end-point is subject to policies in Unauthenticated Role
ROLE	Allows traffic from the end-point without any authentication or posture assessment as specified by role traffic policies (for backward compatibility with CCA 3.x, this will continue to behave the same way)	Once MAC address is known, posture assessment is performed if configured following which traffic is allowed as per role traffic policies
CHECK	Performs posture assessment as specified for the Role following which traffic is allowed as per role traffic policies	Same as above

Note If bandwidth management is enabled, devices allowed without specifying a role will use the bandwidth of the Unauthenticated Role.

You can sort the columns of the filter list by clicking on the column heading label (MAC Address, IP Address, Description, Access Type).

You can edit a device access policy by clicking the **Edit** button. Note that the MAC address is not an editable property of the filter policy. To modify a MAC address, create a new filter policy and delete the existing policy.

You can remove any number of device access policies by clicking the checkbox next to the policy and clicking the **Delete** button.

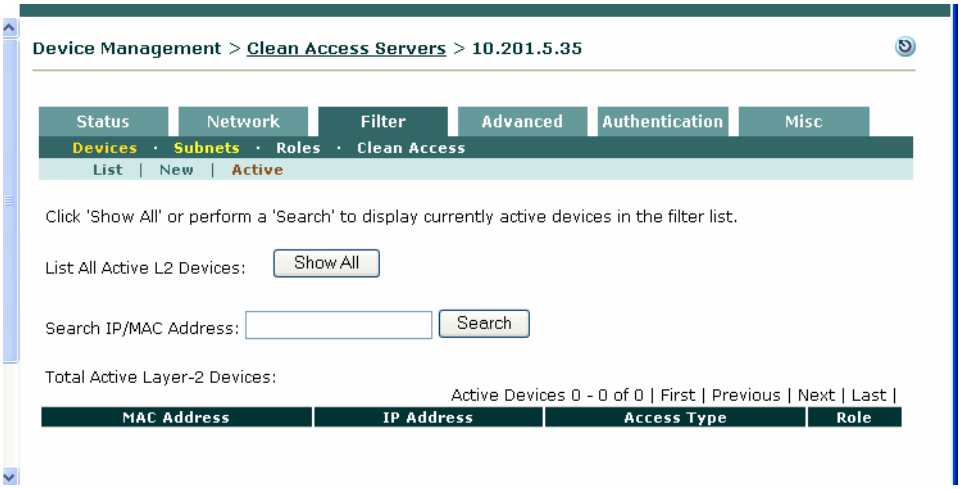
View Active L2 Device Filter Policies

To view active L2 devices in filter policies for a particular Clean Access Server:

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Filter > Devices > Active**
2. Click the **Show All** button first to populate the **Active** page with the information from all clients currently connected to the CAS, sending packets, and with their MAC addresses in a device filter.
3. You can also perform a **Search** on a client IP or MAC address to populate the page with the result. By default, the **Search** parameter performed is equivalent to "contains" for the value entered in the **Search IP/MAC Address** field.

Note that for performance considerations, the **Active** page only displays the most current device information when you refresh the page by clicking **Show All** or **Search**.

Figure 5-18 Active



Note To view active devices for all CASes from the CAM, go **Device Management > Filters > Devices > Active**.

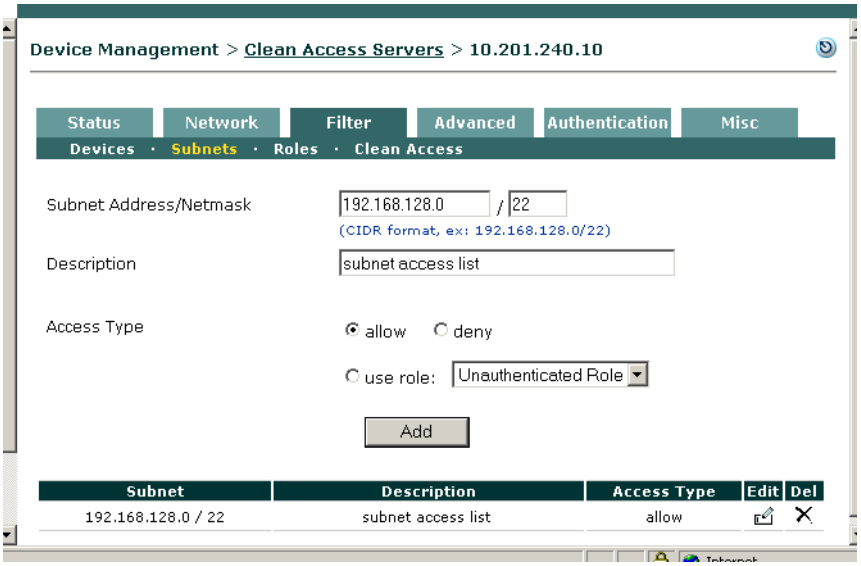
Configure Subnet Access Filter Policies

The **Subnets** form allows you to specify access rules for an entire subnet. All devices accessing the network from the subnet are subject to the rule.

To set up subnet-based access controls:

1. Click the **Subnets** link in the **Filter** tab.
2. In the **Subnet address/netmask** fields, enter the address of the subnet and the netmask identifying the significant bits of the subnet address.

Figure 5-19 Local Subnet Filter



3. Optionally, type a description of the policy or device in the **Description** field.
4. Choose the network access policy for the device from the **Access Type** choices:
   - **allow** – Enables the device to access the network without authentication.
   - **deny** – Prevents the device from accessing the network. If applicable, the user is blocked and an HTML page appears notifying the user that access is denied.
   - **use role** – Applies a role to users with the specified device. If you select this option, also select the role to be applied. The user will not need to be authenticated.
5. Click **Add** to save the policy.

The policy, which takes effect immediately, appears in the filter policy list. From there you can remove a subnet policy using the delete (✕) button or edit it by clicking the edit button (). Note that the subnet address is not an editable property of the filter policy. To modify an address, you need to create a new filter policy and delete the existing one.

You can sort the filter list by column by clicking the heading label (e.g. Subnet, Description).

CAS Fallback Policy

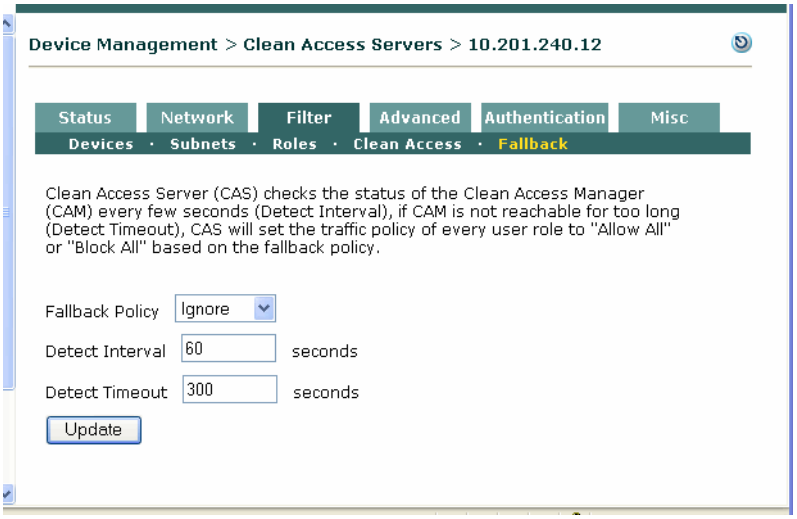
The CAS Fallback policy feature allows administrators to configure the level of user access permitted by the Clean Access Server when the Clean Access Manager becomes unreachable to the CAS. For example, if a remote CAS attempts to reach the CAM, but the WAN link fails, CAS Fallback can be used to specify the user access policy: allow all user traffic, block all user traffic, or only allow traffic for already-authenticated users (default CAS behavior).

The CAS checks the status of the CAM periodically, according to the Detect Interval specified. If the CAM is not reachable before the specified Detect Timeout, the CAS declares the CAM as dead, and sets the traffic policy of every user role to “Allow All, “Block All” or “Ignore” based on the Fallback Policy chosen.

Note The CAS fallback feature is for situations where communication between the CAS and CAM is lost. For protection against CAS failure itself in a Central Deployment, the CAS failover bundle is recommended.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Fallback**

Figure 5-20 CAS Fallback



2. From the **Fallback Policy** dropdown menu, select one of the following options:
   - **Ignore** (default)—Allow traffic only for authenticated users but block new users. This allows existing (authenticated) users to access local and remote site resources, but new (unauthenticated) users will be blocked.
   - **Allow All**—Allow all traffic for all users (authenticated and new). This allows new and existing users to access local and remote site resources.
   - **Block All**—Block all traffic for all users (authenticated and new). This blocks all users from accessing local and remote site resources.
3. Type a **Detect Interval** (default is 60 seconds). The Detect Interval determines how often the CAS verifies if the CAM is still connected.
4. Type a **Detect Timeout** (default is 300 seconds). The Detect Timeout determines the time of “no response” after which the CAS declares the CAM as dead.

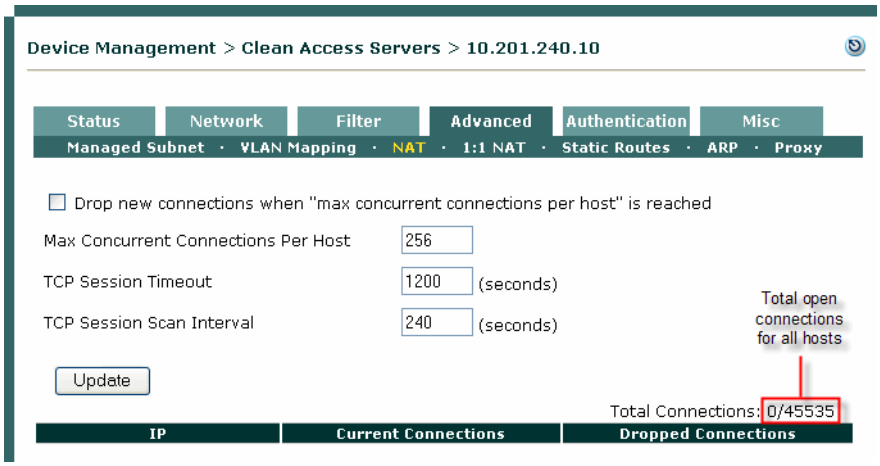
5. Click **Update**.

NAT Session Throttle

You can configure a throttle/threshold on a per-host basis when the Clean Access Server operates as a NAT Gateway. This allows the CAS to restrict the maximum number of connections each host can open at any one time and eliminate the chance of one host consuming all the connections (for example due to a malicious user or a user with a worm).

1. Go to **Device Management > CCA Servers > Manage[CAS_IP] > Advanced > NAT**

Figure 5-21 NAT Page



2. Click the checkbox for **Drop new connections when "max concurrent connections per host" is reached** to enable the NAT session throttle feature for new user connections.
When this option is checked, all new sessions will be dropped for a user if the total number of current connections for the host exceeds the threshold set in the **Max Concurrent Connections Per Host** field. For example, if an existing user has 300 connections open, then the administrator enables this feature for a maximum of 100 connections per host, the user's existing connections will not be affected, but the user will not be able to open any **new** connections until the total number of connections is less than 100.
3. Configure the following options:
   - **Max Concurrent Connections Per Host** —You can configure this threshold up to the maximum value of 45535 connections. Typically, 256 or 512 connections should be sufficient per host. If there are a lot of dropped connections for a user, you can increase the maximum number of connections allowed per host in this field.
   - **TCP Session Timeout (seconds)**—This field sets the idle time for each connection. If the user opens a connection (e.g. for Telnet) and the connection is idle past the number of seconds configured in this field, the connection will be dropped.
   - **TCP Session Scan Interval (seconds)**—This field sets the interval to scan the entire table of NAT connections (up to 45,535 entries) to check which connections have timed out. For example, if this value is 90 seconds, the table will be scanned every 90 seconds.
4. Click **Update** to save and activate settings on the CAS NAT gateway.
5. For troubleshooting, the bottom of the page lists the current connection table for each host:

- **Total Connections—(x/45535)**—This shows the total number of open connections out of the the 45,535 maximum number of concurrent connections available for a CAS in NAT gateway mode (for example, 33/45535 means 33 connections are open).
- **IP**—IP address of the host
- **Current Connections**—The total number of connections currently being consumed by this host, for example: 2, 10, etc. If the checkbox is NOT checked for **Drop new connections when "max concurrent connections per host" is reached**, the **Current Connections** value can be greater than the value set for **Max Concurrent Connections Per Host**.
- **Dropped Connections**—The current number of connections that have been dropped for this host. This field can facilitate troubleshooting if a user wants to know why his/her connections are being dropped.

Configure 1:1 Network Address Translation (NAT)

In 1:1 NATing, there is a one-to-one correspondence between the external and internal addresses involved in the translation (in contrast to the default NAT behavior, in which many internal addresses share a single external address).

1:1 NATing conceals your internal network architecture, but does not economize on external IP addresses, since you must have an external address for every host that needs to communicate externally. It can be used in conjunction with the default, dynamic NATing, allowing you to make email servers, web servers or any other services accessible from the Internet.

You can map a range of addresses, or map individual addresses along with port numbers.

For a range, you need to specify the starting point for both the internal and external address ranges and the length of the range. For example, a configuration of:

- public range begin: 11.1.1.2; port: *
- private range begin: 192.168.151.200; port: *
- range: 4

Results in the following address mappings:

- 192.168.151.200 <-> 11.1.1.2
- 192.168.151.201 <-> 11.1.1.3
- 192.168.151.202 <-> 11.1.1.4
- 192.168.151.203 <-> 11.1.1.5

By default, the port numbers are passed through unchanged (as indicated by the asterisk (*) port value).

By specifying an address range of 1, you can map single addresses. This mapping may include port mappings. For example, the following assignment maps incoming traffic for 11.1.1.6:8756 to the internal address 192.168.151.204:80:

- public range begin: 11.1.1.6; port: 8756
- private range begin: 192.168.151.204; port: 80
- range: 1

Caution Make sure you do not include a particular address in more than one mapping at a time, for example, by including it in a range and as an individual mapping.

Configure 1:1 NATing

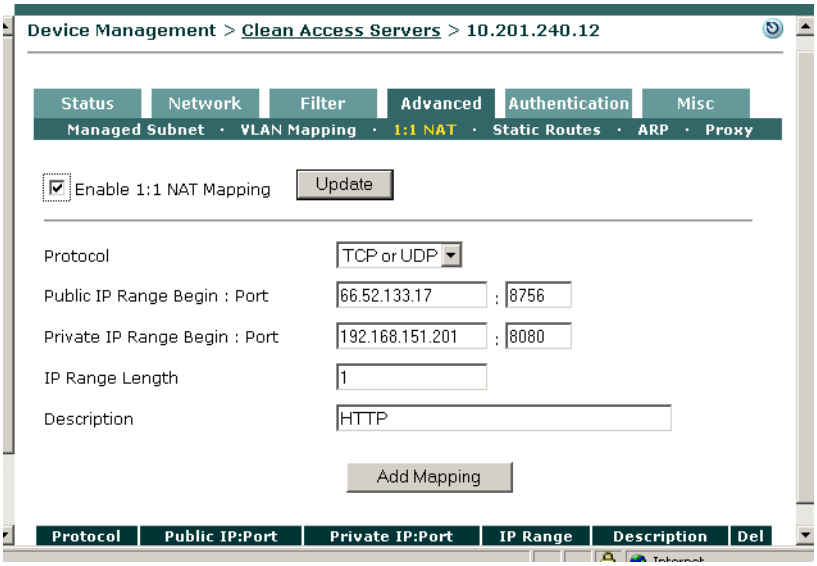
1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > 1:1 NAT**.
2. Select **Enable NAT 1:1 Mapping** and click **Update**.
3. Choose the **Protocol** for which NATing is performed. Options are TCP, UDP, or both.
4. Type the first address in the *public* address range in the **Public IP Range Begin** field. An asterisk in an address or port field results in the value passing translation unchanged.
5. Type the first address in the *private* address range in the **Private IP Range Begin** field.
6. Specify the length of the range, that is, the number of sequentially numbered addresses to be translated.
7. Optionally, type a description of the mapping in the **Description** field.
8. Click the **Add Mapping** button.

The new range mapping appears in the list of mappings.

Configure 1:1 NATing with Port Forwarding

You can use the port field to achieve port forwarding. To create a 1:1 mapping with port forwarding, type the public and private addresses in the appropriate fields, along with corresponding port numbers, and make the **IP Range Length** value 1, as shown in Figure 5-22.

Figure 5-22 1:1 NAT with Port Forwarding



Configure Proxy Server Settings on CAS

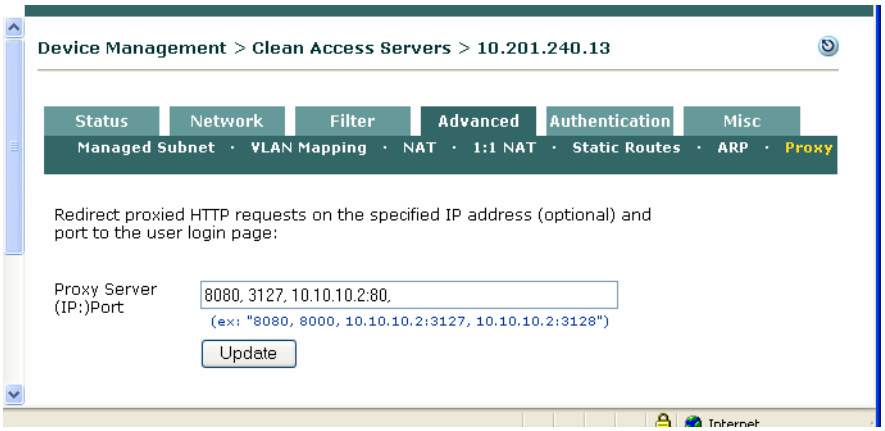
By default, the Clean Access Server redirects client traffic on ports 80 and 443 to the login page. If users on your untrusted network are required to use a proxy server and/or different ports, you can configure the CAS with corresponding proxy server information in order to appropriately redirect HTTP/HTTPS traffic client traffic to the login page (for unauthenticated users) or HTTP/HTTPS/FTP traffic to allowed hosts (for quarantine or Temporary role users). You can specify:

- Proxy server ports only (for example, 8080, 8000)—this is useful in environments where users may go through a proxy server but not know its IP address (e.g. university).
- Proxy server IP address and port pair (for example, 10.10.10.2:80) — this is useful in environments where the IP and port of the proxy server to be used are known (e.g. corporate/enterprise).

To Specify Proxy Server Settings on the CAS

1. Go **Device Management > Clean Access Servers > Manage [CAS_IP] > Advanced > Proxy**.

Figure 5-23 Proxy Settings for Client Traffic



2. Type the port number or IP:port of the proxy server. Separate multiple entries with commas, for example: 3128,8080,8000,10.10.10.2:6588,10.10.10.2:3382.

Note For better security, it is strongly recommended to specify both IP and port for the proxy server. This causes the CAS to intercept only those requests from the IP address specified. Either port or IP:port must be specified for the proxy server; you cannot specify an IP address alone.

Note Port 80 (and 443) are not supported as proxy ports.

3. Click **Update** to save settings.

To Configure the CAS to Parse Host Policy Traffic

When the "**Parse Proxy Traffic for Roles other than Unauthenticated Role**" option is enabled for an individual CAS (under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**), the CAS will check the payloads of GET, POST and CONNECT HTTP/HTTPS/FTP requests to make sure that the host is on the host policy list before allowing traffic to the proxy server

specified on the **Proxy** page. This allows users to access only the host sites enabled for a role (e.g. Temporary or quarantine users that need to meet requirements) when the specified proxy server is used. Note that this "parse proxy traffic" feature is enabled per CAS and you must specify the Proxy server IP and port (as described above) first, then enable the "**Parse Proxy Traffic for Roles other than Unauthenticated Role**" option on the CAS, as described in Enable Proxy Traffic, page 9-7, for this feature to take effect.

Note For the Unauthenticated role, host policies do not work when a proxy server is specified, and the user is always redirected to the login page.

Note When using proxy settings, also make sure DNS settings are properly configured on the CAS under De**vice Management > CCA Servers > Manage [CAS_IP] > Network > DNS**. See Configure DNS Servers on the Network, page 5-17 for details.

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details on the login page.

Configuring DHCP

In the majority of deployments, a DHCP server already exists on the network, and the Clean Access Server needs to be configured in either DHCP Relay or DHCP Passthrough mode. DHCP Relay mode can be used when a CAS is a Real-IP/NAT Gateway, and DHCP Passthrough is used exclusively for a CAS in Virtual Gateway mode. For a lab/test environment, or if a DHCP server is not already set up, you can configure a Real-IP or NAT Gateway CAS to be the DHCP Server for your network. This chapter describes how to configure each of the DHCP modes of the Clean Access Server. Topics include:

Overview

DHCP (Dynamic Host Configuration Protocol) is a broadcast protocol for dynamically allocating IP addresses to computers on a network. When a client computer attempts to join a DHCP-enabled network, the client broadcasts an address request message. A DHCP server on the network responds to the request, and through the course of several exchanges, an IP address is negotiated for and delivered to the client.

In a DHCP-enabled network, the Clean Access Server can operate in one of several modes:

- **DHCP Passthrough** – This is the only mode that can be used when the CAS is configured as a Virtual Gateway. In DHCP Passthrough mode, a Virtual Gateway CAS propagates the DHCP broadcast messages across its interfaces without modification.
- **DHCP Relay** – In this mode, a Real-IP/NAT Gateway CAS forwards messages from clients to another DHCP server.
- **DHCP Server** – In this mode, a Real-IP/NAT Gateway CAS acts as the DHCP server and allocates client IP addresses for the managed (untrusted) network.

When a Real-IP or NAT Gateway CAS is enabled as a **DHCP Server**, it provides the services of a full-featured DHCP server. It can allocate addresses from a single IP pool or from multiple pools across many subnets. It can assign static IP addresses to particular client devices.

The **DHCP Server** configuration interface includes tools for auto-generating IP pools, making it easier to create many pools at once, and provides checking mechanisms to help detect configuration errors.

Auto-generating IP pools as a response to heightened virus activity can help to protect your network. By segmenting your network into many small subnets (such as /30 subnets), you can isolate clients from one another. Since clients cannot communicate directly across subnets, all traffic between them is routed through the Clean Access Server, limiting the ability of worms to propagate over peer-to-peer connections.

When you generate subnetted IP address pools, the Clean Access Server is automatically configured as the router for the subnet. An ARP entry for the subnet is automatically generated as well.

For static addresses, you can reserve a particular IP address for a particular device by MAC address.

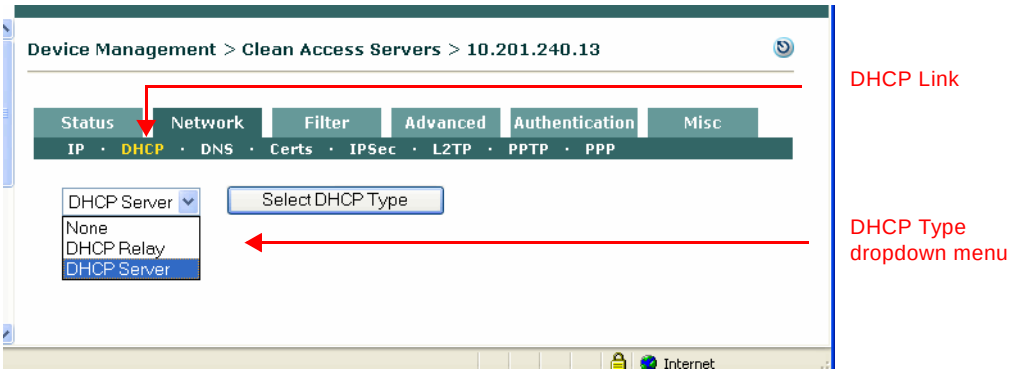
Enable the DHCP Module

You can enable DHCP Relay or DHCP Server mode on a Clean Access Server that is in Real-IP or NAT Gateway mode. When a CAS is a Virtual Gateway, it is always in DHCP Passthrough mode (see Figure 6-4).

Configure DHCP Relay or DHCP Server Mode

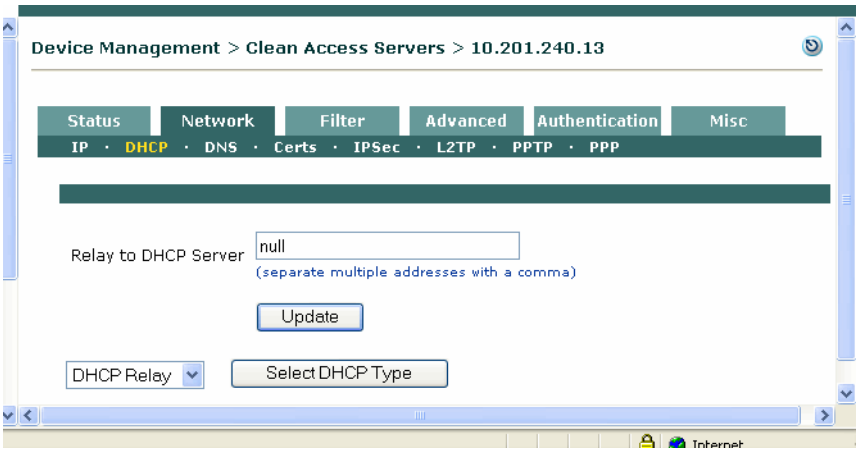
1. From **Device Management > CCA Servers > List of Servers**, click the **Manage** button ( ) next to the Clean Access Server.
2. Click the **DHCP** link to open the DHCP form in the **Network** tab (Figure 6-1).

Figure 6-1 Select DHCP Type (CAS in Real-IP/NAT Gateway Mode)



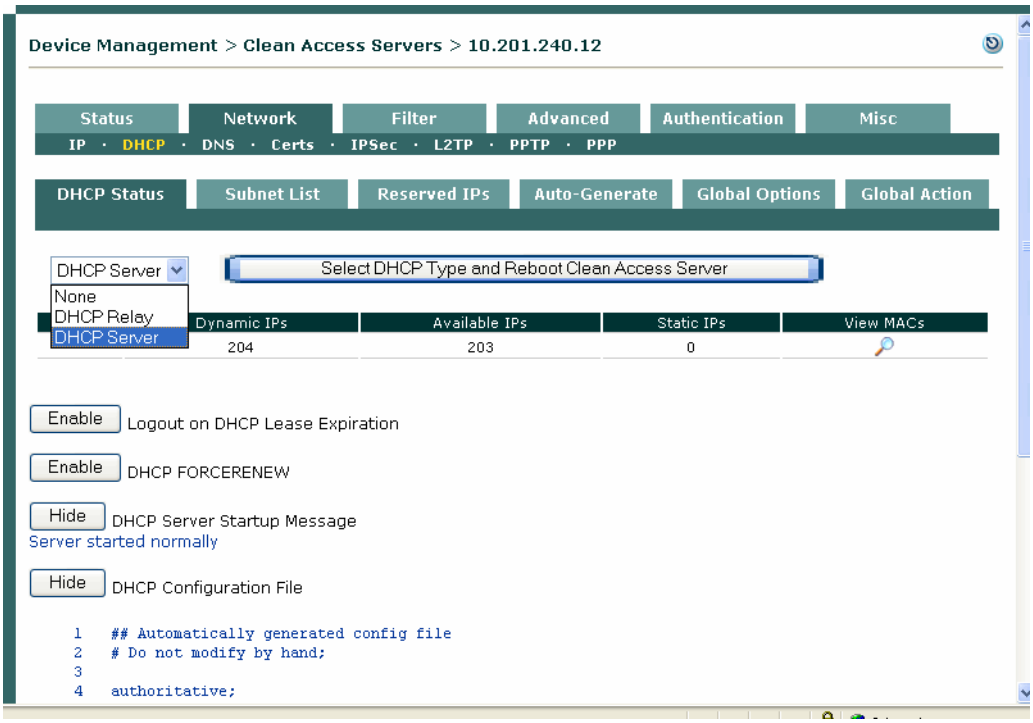
3. From the DHCP Type dropdown menu, select one of the following options and click the **Select DHCP Type** button (note that this button label toggles to **Select DHCP Type and Reboot Clean Access Server** when in DHCP Server mode.) Options are as follows:
   a. **None** – This is the default mode of the CAS, in which the CAS propagates DHCP broadcast messages across its interfaces without change. Leave the CAS in this default mode if a DHCP server already exists on the trusted network.
   b. **DHCP Relay** – In this mode, the CAS forwards DHCP messages between clients and a specific external DHCP server. For DHCP Relay, you need to configure the DHCP server in the environment so that it hands out the Clean Access Server's untrusted (eth1) address as the gateway IP address to managed clients. Selecting **DHCP Relay** mode displays an additional DHCP Relay configuration form (Figure 6-2). Type the IP address of the external DHCP server in the **Relay to DHCP server** field and click the **Update** button.

Figure 6-2 Configuring DHCP Relay



c. **DHCP Server** – This sets the CAS to perform DHCP services for managed clients. Once the CAS is enabled as a **DHCP Server**, the **DHCP Status**, **Subnet List**, **Reserved IPs**, **Auto-Generate**, and **Global Options** subtabs are displayed (Figure 6-3). From there, you can add IP pools manually, auto-generate pools and subnets, or specify reserved IPs, as described in Configuring IP Ranges (IP Address Pools), page 6-5.

Figure 6-3 DHCP Server Mode



Note Once **DHCP Server** is selected, to switch to a different DHCP Type for the Clean Access Server, you must reboot the CAS. To change the type, select **None** or **DHCP Relay** from the dropdown menu and click the button **Select DHCP Type and Reboot Clean Access Server**.

DHCP Status Options

When the CAS is enabled as a DHCP server, the **DHCP Status** tab includes the enable buttons shown in Figure 6-3.

Release 4.1 offers two new DHCP enable/disable enhancements to ensure client IP addresses are renewed properly when the CAS is configured as the DHCP server for your network. These are User Logout on DHCP Lease Expiration and DHCP FORCERENEW, as described below.

Enable/Disable Logout on DHCP Lease Expiration

This toggle button is disabled by default. Clicking the **Enable** button causes the user to be logged out (either Agent logout or web logout) from the Cisco NAC Appliance when the client's DHCP lease expires.

Enable/Disable DHCP FORCERENEW

This toggle button is disabled by default. Clicking the **Enable** button instructs the DHCP server to execute a DHCP NAK command, which releases IP addresses assigned to a client by other DHCP servers. Following the NAK command, the DHCP client will be assigned a valid IP address as configured on the CAS.

Show/Hide DHCP Server Startup Message

When this button is clicked, the last DHCP server startup message is displayed. If the server does not start, an error message is shown here.

Show/Hide DHCP Configuration File

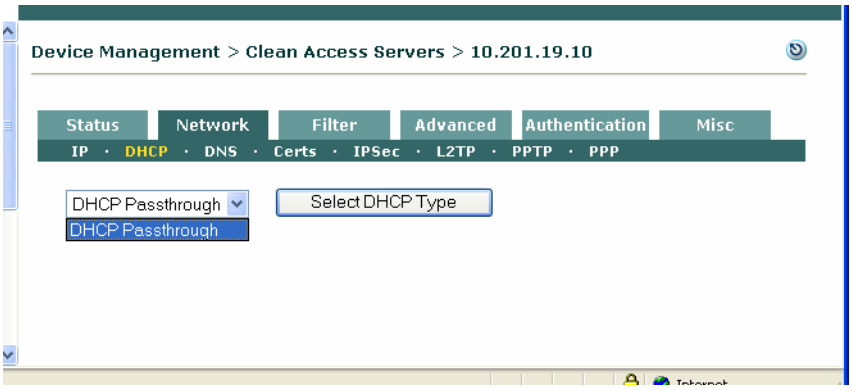
When this button is clicked, the DHCP configuration file is displayed. In some cases, the startup message displays an error for a particular line of the configuration. Clicking this button allows you to view the configuration file line-by-line.

For further information on the **DHCP Status** tab see Working with Subnets, page 6-14.

For additional information on DHCP configuration, see User-Specified DHCP Options, page 6-18.

Note A Virtual Gateway CAS is always in DHCP Passthrough mode (Figure 6-4).

Figure 6-4 CAS VGW DHCP Type



Configuring IP Ranges (IP Address Pools)

To set up the Clean Access Server to provide DHCP services, you first configure the range of IP addresses to be allocated to clients (the IP address pool). In addition, you can specify network information to be handed to clients with the address, such as DNS addresses.

The CAS can allocate addresses from multiple pools and subnets. However, allocated addresses must fall within the ranges specified to be managed by the CAS. This can be either:

- The address space of its untrusted interface managed network (set in the **Network> IP** page)
- A managed subnet specified in the **Managed Subnet** form of the **Advanced** tab

If you try to create an address pool from a subnet that is not managed, an error message notifying you of the condition appears in the admin console and the pool is not created.

Auto-Generated versus Manually Created Subnets

You can automatically generate subnets in order to create many IP address pools at a time. Creating a large number of IP pools of relatively small size (from which only a few addresses can be assigned) can help protect your network. By isolating clients into small subnets, you limit the ability of peers to communicate directly with one another, and thereby prevent events such as worms from proliferating across peer connections.

Alternatively, you can manually create subnets if only a few IP address pools are required for your network.

Subnetting Rules

Whether creating IP pools automatically or manually in the admin console, the subnets you create must follow standard subnetting design rules. Only properly aligned, power-of-two subnet addresses are supported. For example, you cannot start a subnet range at address 10.1.1.57 with a subnet mask of 255.255.255.192, because the final octet of the netmask, 192, corresponds to a “size 64” subnet. There can only be four size-64 subnets, with subnet start address boundaries of .0, .64, .128, and .192. Since .57 is not a power-of-two, it cannot be used as the starting address for a subnet.

You must specify the starting address of the range for either manually-created or automatically-generated subnets. To manually create a pool you specify the end of the range, and to auto-generate a pool you specify the number of subnets to generate.

Addresses in the IP range are assigned as follows:

1. Network address — The first valid number entered for the range is used as the network address for the subnet (or the first subnet, if generating more than one subnet).
2. Router address — The second number is used as the router address (that is, the virtual gateway interface address for the subnet).
3. Host IP address — The third number is the first address that is leasable to clients.
4. Broadcast address — The final address in the range is the broadcast address.

By specifying an IP range of only four addresses, you can create a subnet for a single host.

Table 6-1 shows the number of leasable addresses for each subnet size and number of subnets possible per CIDR (Classless InterDomain Routing) prefix. Each CIDR prefix corresponds to a specific subnet mask. CIDR notation identifies the number of bits masked for the network portion of a 32-bit IP address

in order to produce a specific number of host addresses. For example, a CIDR address of 10.5.50.6 /30 indicates that the first 30 bits of the address are used for the network portion, leaving the remaining 2 bits to be used for the host portion. Two bits of address yield four host addresses: three addresses are automatically allocated for the required network, gateway, and broadcast addresses for the subnet, and the remaining address can be leased. Therefore, a /30 network creates a subnet of one host.

Table 6-1 Addresses per Subnet Size

CIDR Prefix	No. of possible subnets (Class C)	Total number of addresses	No. of leasable host addresses	Example valid start-of-range addresses
/30	64	4	1	10.1.65.0 10.1.65.4 10.1.65.8 ...
/29	32	8	5	10.1.65.0 10.1.65.8 10.1.65.16 ...
/28	16	16	13	10.1.65.0 10.1.65.16 10.1.65.32 ...
/27	8	32	29	10.1.65.0 10.1.65.32 10.1.65.64 ...
/26	4	64	61	10.1.65.0 10.1.65.64 10.1.65.128 10.1.65.192
/25	2	128	125	10.1.65.0 10.1.65.128
/24	1	256	253	10.1.65.0

Table 6-2 shows the addressing for an automatically-generated IP range of four /30 subnets starting at address 10.1.100.12.

Table 6-2 Auto-Generated Subnets

IP Range Entries	1st Subnet	2nd Subnet	3rd Subnet	4th Subnet
Network address	10.1.100.12	10.1.100.16	10.1.100.20	10.1.100.24
Router address	10.1.100.13	10.1.100.17	10.1.100.21	10.1.100.25
Client address range	10.1.100.14 - 10.1.100.14	10.1.100.18 - 10.1.100.18	10.1.100.22 - 10.1.100.22	10.1.100.26 - 10.1.100.26
Broadcast address	10.1.100.15	10.1.100.19	10.1.100.23	10.1.100.27

In general, the admin console enforces rules for properly configured subnets. If you attempt to use an invalid network address for the netmask, the message appears: “Subnet/Netmask pair do not match”. In this case, choose a new value for the address.

Create IP Pools Manually

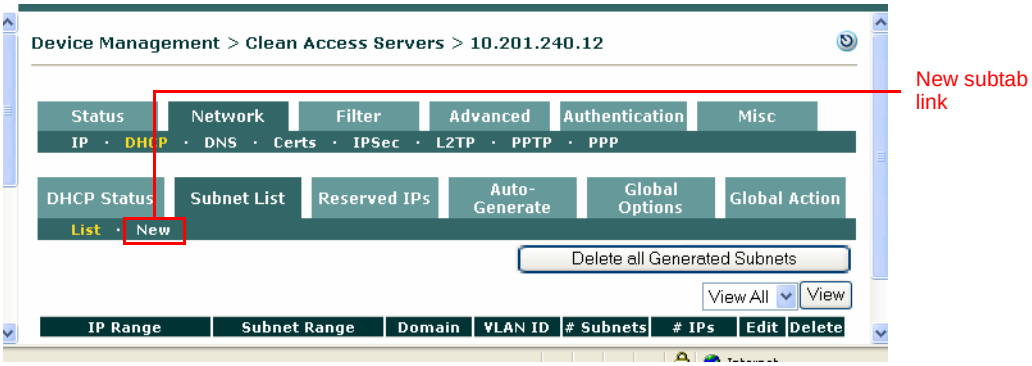
To create an IP pool manually, you also need to define the subnet in which the pool resides. There are three ways to arrive at the subnet address and netmask values for a manually generated pool:

- Enter the subnet address directly, as an IP address and netmask.
- Have the admin console generate the smallest possible subnet based on the IP range you enter.
- Have the admin console calculate the values from the list of subnets currently managed by the Clean Access Server.

To create an IP pool range:

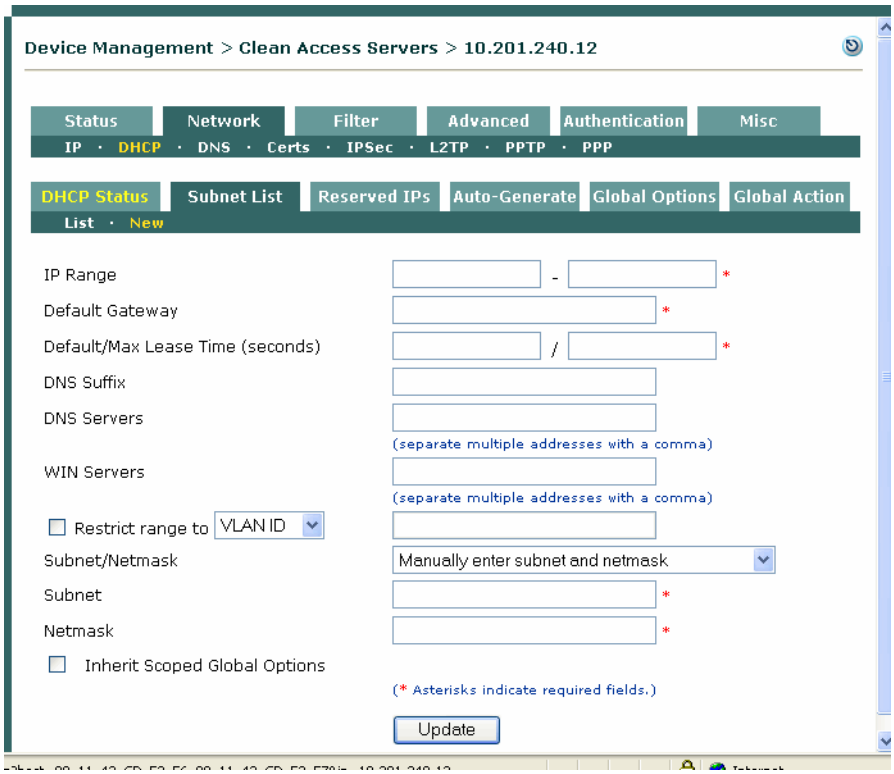
1. In the **DHCP** form, click the **Subnet List** tab, then the **New** link.

Figure 6-5 New Subnet List Subtab Link



2. The new IP pool form appears.

Figure 6-6 New Subnet Form



3. Enter values for these fields:
   - **IP Range** – The IP address pool to be assigned to clients. Provide a range of addresses not currently assigned in your environment.
   - **Default Gateway** – The IP address of the default gateway passed to clients. This should be the untrusted interface address of the Clean Access Server.
   - **Default/Max Lease Time (seconds)** – The amount of time the IP address is assigned to the client, if the client does not request a particular lease time, as well as the maximum amount of time for which a lease can be granted. If the client requests a lease for a time that is greater, the maximum lease time is used.
   - **DNS Suffix** – The DNS suffix information to be passed to clients along with the address.
   - **DNS Servers** – The address of one or more DNS servers in the client's environment. Multiple addresses should be separated by commas.
   - **WIN Servers** – The address of one or more WIN servers in the client's environment. Multiple addresses should be separated by commas.
   - **Restrict range to [VLAN ID | RELAY IP]**

     If choosing **VLAN ID**, type the VLAN ID in the text field. Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.

Note For IPs with VLAN restrictions, all IPs must be in a managed subnet, and you must create a managed subnet first before creating an IP range (DHCP pool). See Configuring Managed Subnets or Static Routes, page 5-18 for details.

If choosing **RELAY IP**, type the Relay IP in the text field. Clients not associated with the specified Relay IP cannot receive addresses from this IP pool.

Note For IPs with relay restrictions, all IPs should typically be in static routes, but can be in managed subnets if integrating the CAS with Aironet devices or other non-RFC 2131/2132 compliant devices. Note that these IP address pools must be in either a static route or a managed subnet, and IPs with relay restrictions should only be put in a managed subnet for these non-compliant devices. See Configuring Managed Subnets or Static Routes, page 5-18 for details.

4. From the **Subnet/Netmask** list, choose how you want the subnet address to be specified, from the following choices:
   - **Calculate from existing managed subnets** – The admin console determines what to use for the subnet and netmask values based on the configuration in the **Managed Subnet** form (in the **Advanced** tab). It calculates the network address by applying the netmask to the gateway address for each managed subnet.
   - **Calculate smallest subnet for IP range entered** – The admin console determines the subnet and netmask values based on the IP address range you entered.
   - **Manually enter subnet and netmask** – To specify the desired network address and netmask manually. If selected, the **Subnet** and **NetMask** fields appear at the bottom of the form.
   - **Inherit Scoped Global Options** — This field is only visible if DHCP options are enabled, and will be checked by default. If this field is disabled (unchecked), the scoped global options configured in the **Global Options** tab are not inherited. See User-Specified DHCP Options, page 6-18 for details.
5. Click **Update** when finished. If there are errors in the configuration, warning messages appear. Follow the instructions to correct the settings.

Auto-Generating IP Pools and Subnets

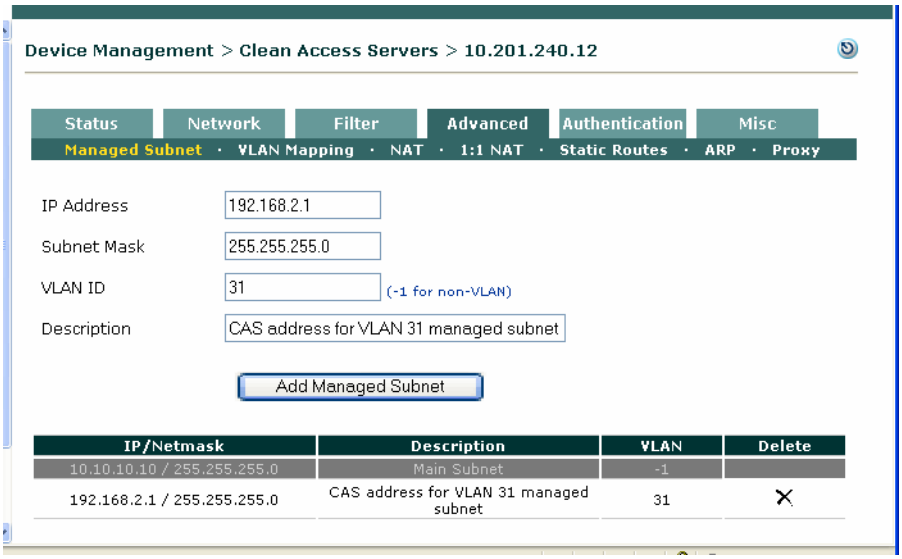
By automatically generating subnets, you can quickly divide your network into small segments. Segmenting your network into small subnets can be an effective security measure in response to a worm attack, since a network comprised of many small subnets (with one host per subnet possible) limits the ability of clients to engage in peer-to-peer interaction.

Caution The recommended maximum number of subnets per Clean Access Server is 1000. If the CAS machine has sufficient memory (>1G), up to 2500 subnets can be configured. Do not exceed the recommended limit if this will place an excessive burden on system resources, particularly server memory.

Add Managed Subnet

1. First, make sure that the IP pools you want to add are in the range of a managed subnet. If needed, add the managed subnet under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet** (for details, see Configure Managed Subnets for L2 Deployments, page 5-20).

Figure 6-7 Add Managed Subnet

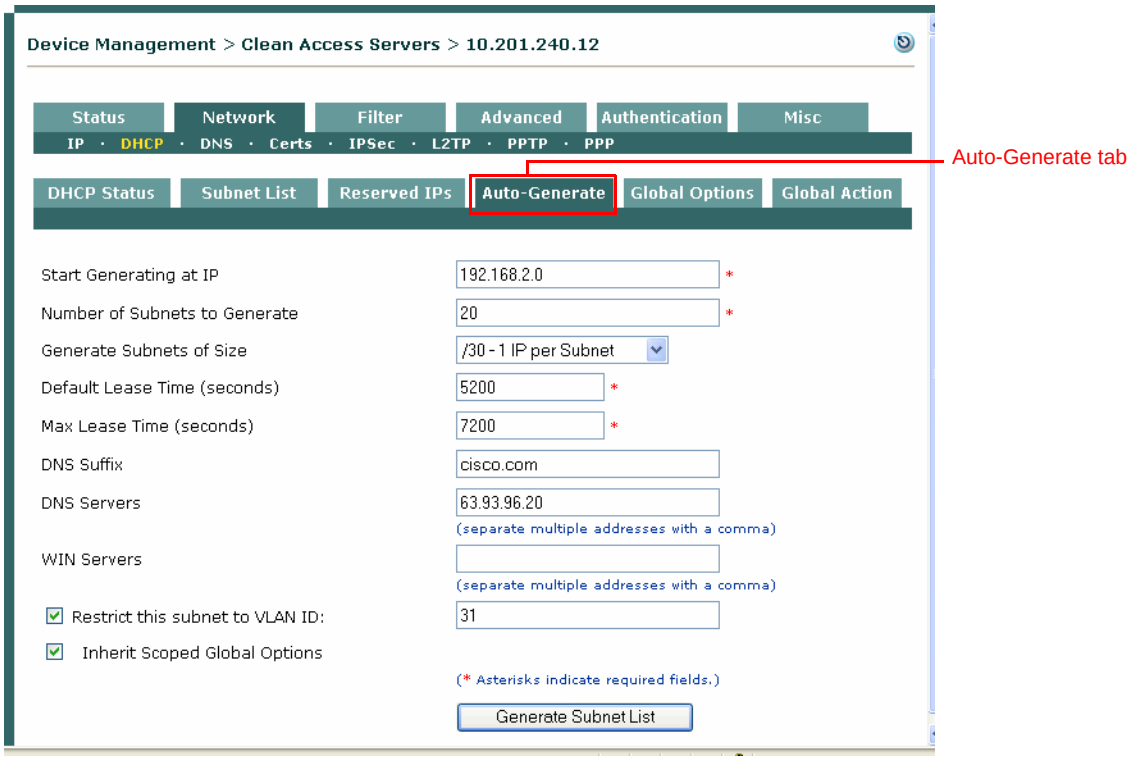


Note When adding a managed subnet, the **IP Address** field you configure should be the gateway address for the subnet—that is the address used by the CAS to route the subnet. The **IP Address** of the managed subnet should not be the network address (which the Clean Access Manager will calculate by applying the Subnet Mask to the gateway address).

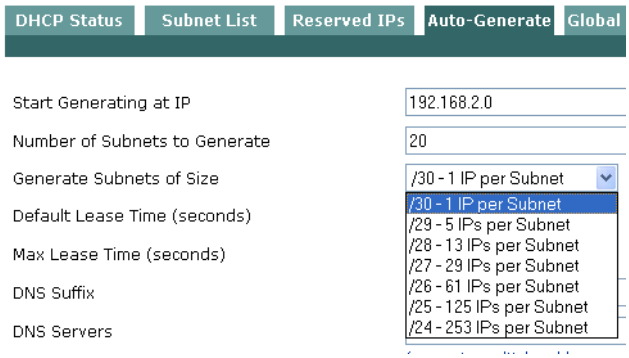
Create Auto-Generated Subnet

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Auto-Generate**. The **Auto-Generate** pane appears as follows:

Figure 6-8 DHCP—Auto-Generate Subnet Form



2. In the **Start Generating at IP** field, type the first IP address of the range to be generated:



The first available valid address for the managed subnet range is used as the network address for the first subnet, the next number is used as the router address, and the next number after that becomes the first address that is leasable to clients.

3. In the **Number of Subnets to Generate** field, type the number of subnets to generate. As mentioned, the maximum recommended size is 1000. Exceeding this number can impose a burden on the server's system resources.

4. From the **Generate Subnets of Size** dropdown list, select the size of each subnet. Subnet sizes are presented in CIDR format (such as /30). The dropdown menu also lists the corresponding number of available host addresses per subnet for each CIDR prefix. For each range, three addresses are automatically reserved and cannot be allocated to clients:

   – The network address of the subnet

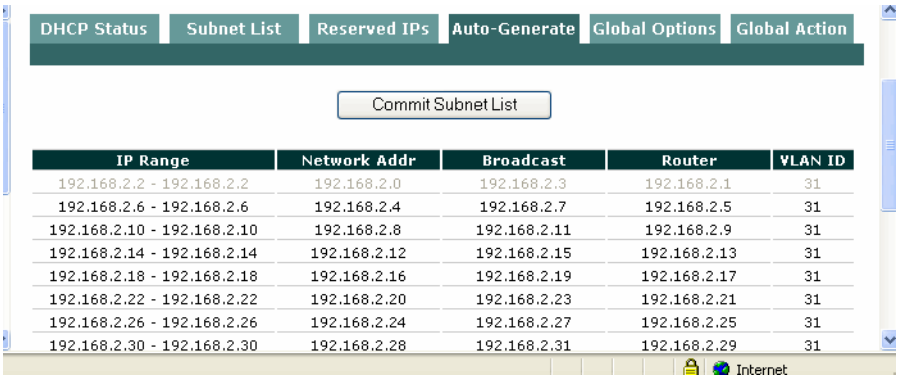
- The router address (for the Clean Access Server)
- The broadcast address

Therefore, a /30 size subnet has four addresses, but only one IP available for hosts.

5. Provide values for the remaining fields:
   - **Default Lease Time (seconds)** – The amount of time the IP address is assigned to the client, if the client does not request a particular lease time.
   - **Max Lease Time (seconds)**– The maximum amount of time a lease can be reserved. If the client requests a lease for a time that is greater, this max lease time is used.
   - **DNS Suffix** – The DNS suffix information to be passed to clients along with the address lease.
   - **DNS Server(s)** – The address of one or more DNS servers in the client's environment. Multiple addresses should be separated by commas.
   - **WIN Server(s)** – The address of one or more WIN servers in the client's environment. Multiple addresses should be separated by commas.
   - **Restrict this Subnet to a specific VLAN ID** – Clients not associated with the specified VLAN cannot receive addresses from this IP pool. A VLAN ID can be any number between 0 and 4095.
   - **Inherit Scoped Global Options** — This field is only visible if DHCP options are enabled and is turned on by default. If this field is disabled, the scoped global options configured in the **Global Options** tab are not inherited. See User-Specified DHCP Options, page 6-18 for details.
6. When finished, generate a preliminary list of subnets by clicking **Generate Subnet List**. If there are errors in the values provided, error messages appear at this time. If the subnet based on your address is not properly aligned, the interface suggests the closest legal starting IP address for your range.

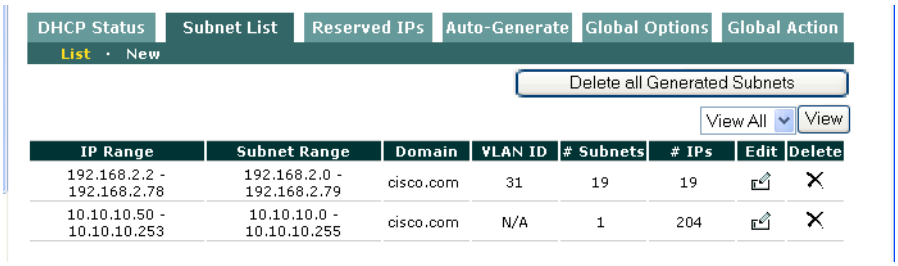
   If successful, a preliminary list of IP ranges appears, allowing you to review the results.

Figure 6-9 Commit Subnet List



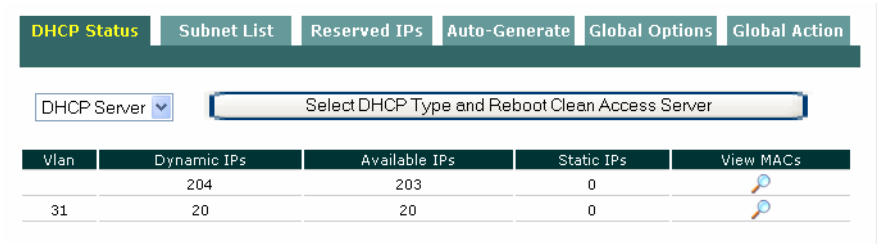
7. Click **Commit Subnet List** to save the IP ranges.
8. The auto-generated subnets appear as a single subnet range under **Subnet List > List**. The **"# of Subnets"** and "**# of IPs"** columns allow you to view how large the auto-generated range is in terms how many subnets have been created as well as the number of IP addresses for the range.

Figure 6-10 Subnet List— List



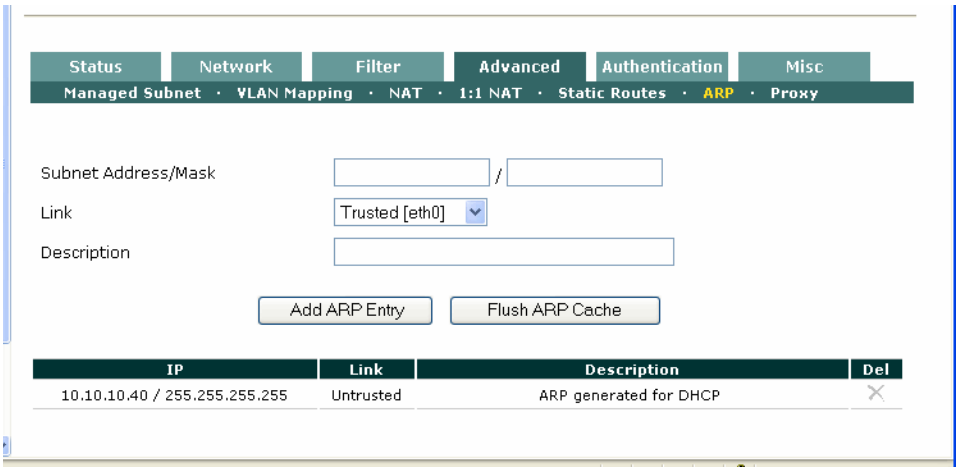
9. The newly-generated list also appears in summary form under **DHCP Status** tab (listing VLAN ID and number of dynamic, available, and static IP addresses).

Figure 6-11 DHCP Status



Note ARP entries are automatically created in the Clean Access Server configuration for the generated subnets (under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > ARP**), as shown in Figure 6-12. Deleting generated subnets also removes the corresponding ARP entries.

Figure 6-12 ARP Entries Generated for DHCP

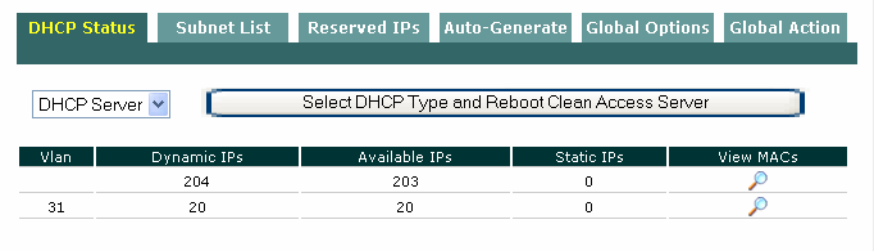


Working with Subnets

View Users by MAC Address/VLAN

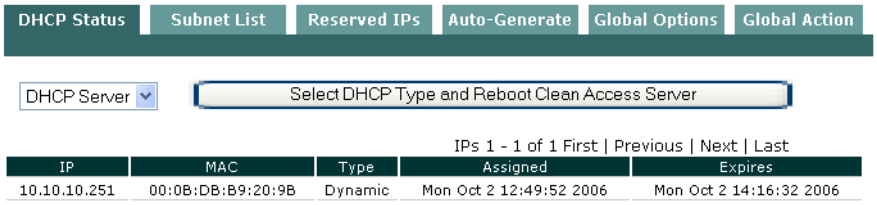
1. After committing an auto-generated list, the **Network > DHCP > DHCP Status** page appears and lists the newly-generated subnet. If the auto-generated subnet is restricted to a VLAN ID, the subnet is listed by that VLAN ID; otherwise, the **VLAN** column is blank if no VLAN is specified.

Figure 6-13 DHCP Status —VLANs



2. By clicking the **View MACs** icon (🔎) for the VLAN, you can see the MAC address, IP and type of client, as shown in Figure 6-14.

Figure 6-14 View MAC Address

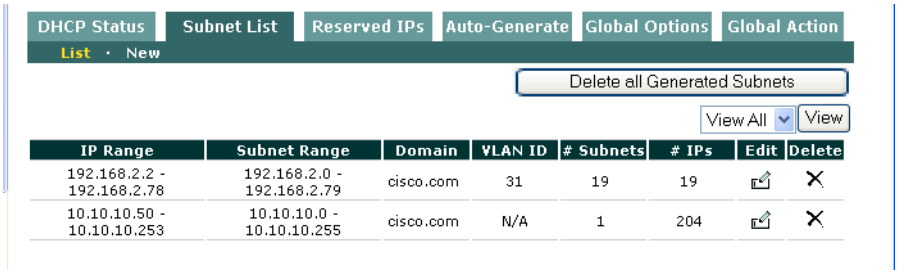


- For DHCP clients, the **Type** column lists "**Dynamic**" and the lease assignment and expiration times are shown.
- For reserved IP clients, the **Type** column lists "**Static**" and the lease time columns display N/A.

View or Delete Subnets from the Subnet List

1. You can view the list of subnets created or modify individual subnets from **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Subnet List > List**.

Figure 6-15 Subnet List—List

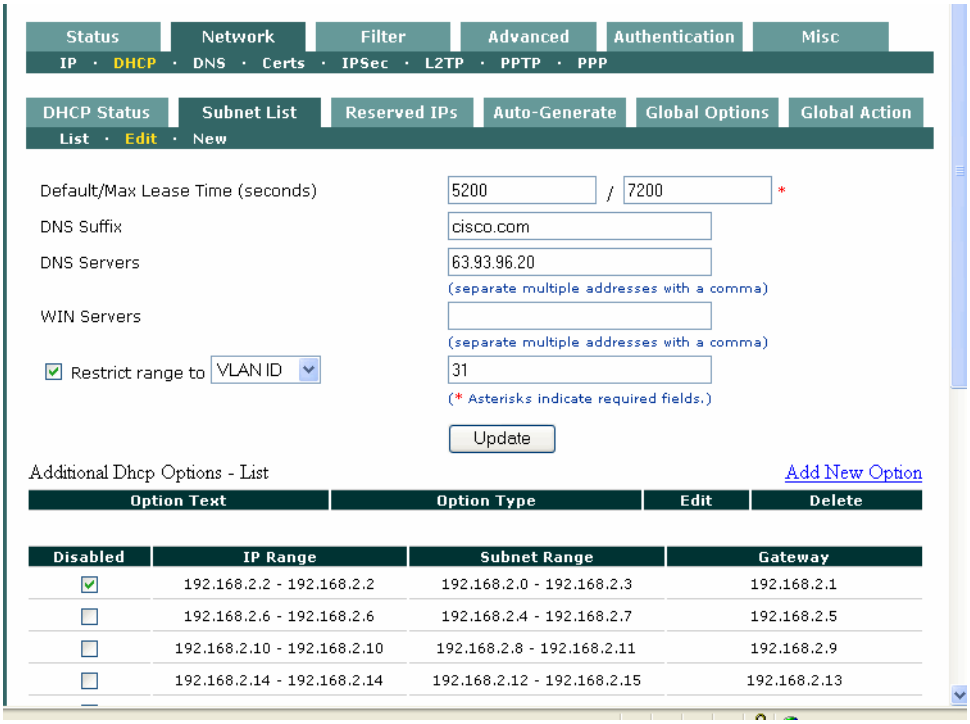


2. To view the subnets for a particular VLAN only, select the VLAN from the scroll menu next to the **View** button and click **View**.
3. To remove an individual subnet, click the **Delete** icon ( ) next to it.
4. To remove all auto-generated subnets, click the **Delete all Generated Subnets** button. Note that this deletes only auto-generated subnets; all manually entered subnets are retained.

Edit a Subnet

1. To edit a subnet, click the **Edit** button ( ) next to it in the **Subnet List** to bring up the **Edit Subnet List** form. The example below shows the **Edit** form for an auto-generated subnet. (The **Edit** form for a manually-generated subnet is similar to Figure 6-6 on page 6-8.)

Figure 6-16 Edit Subnet List



2. You can modify the lease time, DNS/WIN server information and VLAN ID restriction. Click **Update** to save the changes. To change the IP range, default gateway or subnet mask, the subnet must be deleted from **Subnet List** > **List** form and re-added with the modified parameters.
3. For auto-generated subnets, you can disable a particular subnet by clicking the **Disabled** checkbox next to it. This allows you to disable the IPs associated with a particular generated subnet so that the IPs are not leased out. This can be particular useful if you have one or two servers in the middle of a subnet range.

Reserving IP Addresses

By reserving an IP address, you can keep a permanent association between a particular IP address and device. A reserved device is identified by MAC address. Therefore, before starting, you need to know the MAC address of the device for which you want to reserve an IP address. The configuration for a reserved IP does not include a maximum or default lease time. The address is always available for the device, and in effect has an unlimited lease time. Table 6-3 lists several rules that apply to reserved IP addresses.

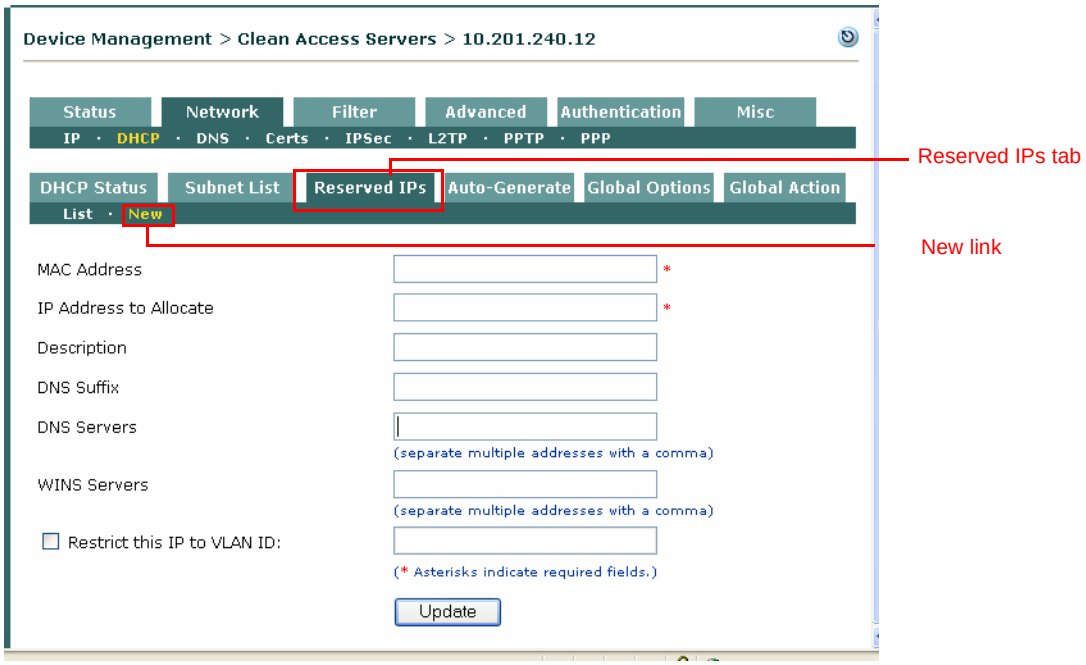
Table 6-3 Reserved IP Address Rules

A reserved address cannot be...	A reserved address must be...
• Within the address range of an IP pool. • A network or broadcast address. • Currently set as a default gateway for an existing IP address range.	• Within the address range of the Clean Access Server's managed network (as configured in **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**), or • Within the address range of the CAS's managed subnets (as configured in **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Managed Subnet**).

Add a Reserved IP Address

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Reserved IPs > New**.

Figure 6-17 Reserved IPs—New



2. In the **MAC Address** field, type the MAC address for the device for which you want to reserve an IP address, in hexadecimal MAC address format (e.g., 00:16:21:11:4D:67).

3. In the **IP Address to allocate** field, type the IP address that you want to reserve.
4. Enter an optional **Description**.
5. Provide values for the remaining fields:
   - **DNS Suffix** – The DNS suffix information to be passed to clients along with the address lease.
   - **DNS Servers** – The address of one or more DNS servers in the client's network. Multiple addresses should be separated by commas.
   - **WIN Servers** – The address of one or more WIN servers in the client's network. Multiple addresses should be separated by commas.
   - **Restrict this IP to VLAN ID** – If the client is associated with a particular VLAN, click this checkbox to specify the VLAN identifier in the **VLAN ID** field.
6. When finished, click **Update**.

The reserved IP now appears in under **Subnet List > List.** From there, it can be modified by clicking the **Edit** button () or removed by clicking **Delete** ().

User-Specified DHCP Options

The Global Options tab (Figure 6-18) allows advanced users to modify the DHCP configuration directly. DHCP options can be specified as follows:

- Root global options appear at the root level or top of the DHCP configuration file and apply to all DHCP subnet declarations. Root global options are inherited by everything in the file.
- Scoped global options are added to each subnet definition, but you can enable whether or not a subnet inherits the option. When DHCP options are enabled, an “Inherit Scoped Global Option” enable appears on the forms used to add or edit manually-created or automatically-generated subnets. Note that the “Inherit Scoped Global Option” checkbox appears only while customized DHCP options are enabled and only for subnets created after the options are enabled.
- Local options apply only to the subnet for which they are entered. Local DHCP options can be added to an individual subnet using the **Subnet List > Edit** form described in Add Local Scoped DHCP Option, page 6-22.

You can create DHCP option rules based on class restrictions to restrict access to DHCP subnets. You can create rules for:

- All clients on a specific VLAN
- Clients coming from a specific relay IP

You can create new options by selecting the options type or by creating a custom option to create an option that is not on the list, or of a different type.

Caution The DHCP configuration file should not be modified under most circumstances.

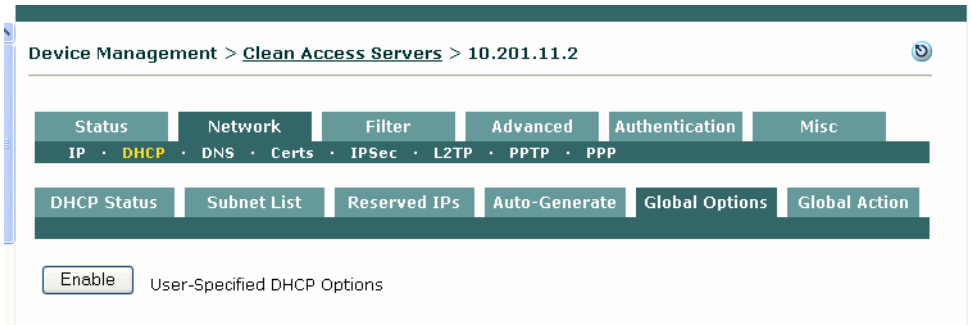
With release 4.1, a number of server directives are added to the DHCP global options configuration pages. A server directive instructs the DHCP server to behave differently, while a DHCP option refers to a specific piece of data to be returned by the DHCP server. For example, the "allow-bootp" server directive (disabled by default) instructs the DHCP server to allow older BOOTP clients to connect. See Table 6-4 “DHCP Server Directives” for additional details.

Note Most server directives can only be added as root global options. This is because their actions direct the behavior of the entire server and cannot be limited in scope or effect on a per-subnet basis.

Enable User-Specified DHCP Options

1. Go to the **Network > DHCP > Global Options** tab and click the **Enable** button (Figure 6-18).

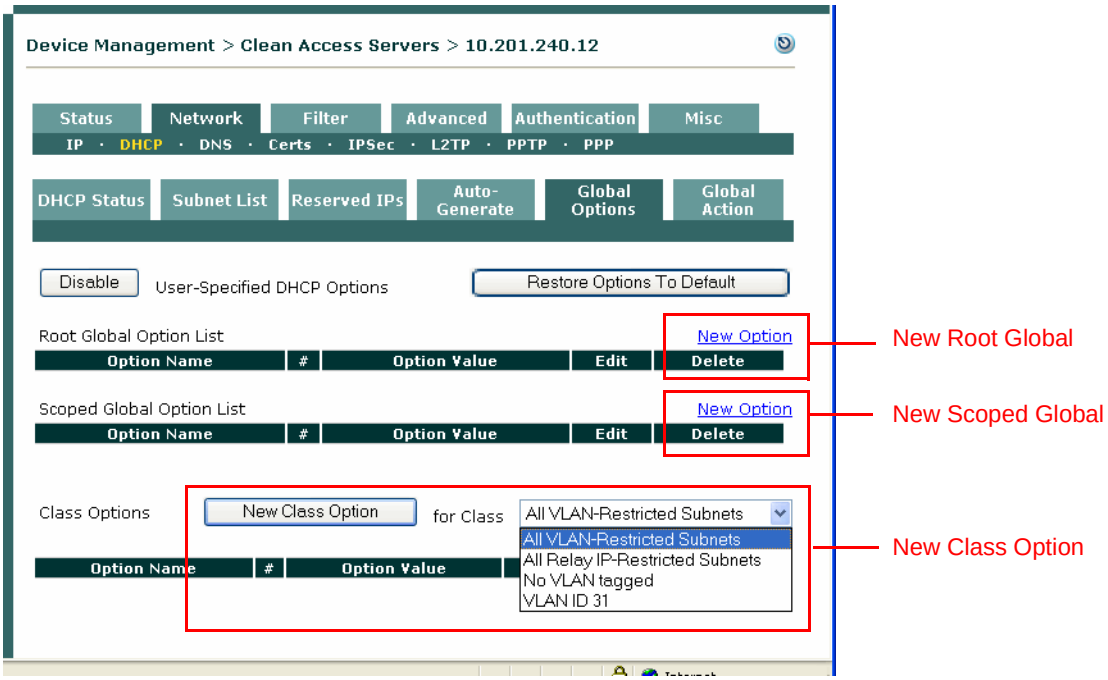
Figure 6-18 DHCP Global Options - Enable



2. With **Global Options** enabled on the CAS (Figure 6-19), choose one of the following option types to configure:
   - Root Global Option
   - Scoped Global Option
   - Class Option

   Once an option is added, it is displayed on this main page under the corresponding list name.

Figure 6-19 DHCP Global Options



Note When specifying DHCP Global Options (Root, Scoped or Class), you may select a particular DHCP option by entering its number in the **Option #** input box on the New/Edit form.

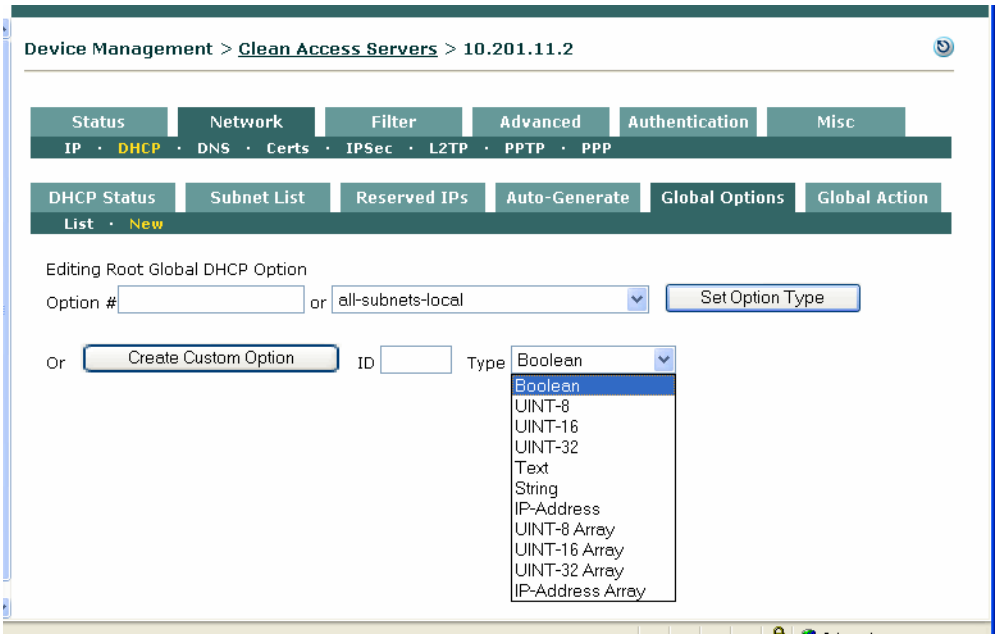
If the desired option number is not known, or if specifying a server directive which changes server behavior but has no corresponding DHCP option number, then select the name of the option or directive from the dropdown menu next to the **Set Option Type** button. In either case, click the **Set Option Type** button after the desired DHCP option type has been selected.

DHCP option numbers are specified in RFC 2132.

Add Root Global DHCP Option

3. Click the **New Option** link at the top right-hand corner of the **Root Global Option List** to open the Root Global DHCP Options form (Figure 6-20). This form allows you to enter text directly into the DHCP configuration file at the root level.

Figure 6-20 DHCP Global Options - New Root Global (Custom Option)

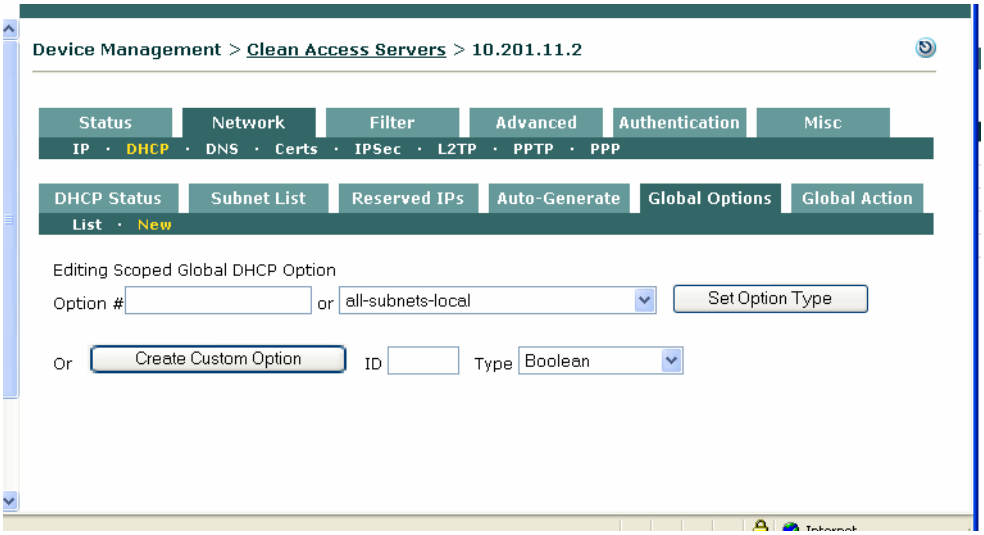


4. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.
5. If instead configuring a **Custom Option**, type the option number in the **ID** field, choose a data **Type** from the dropdown menu, and click **Create Custom Option**.

Add Scoped Global DHCP Option

6. From the **Global Options** main page (Figure 6-19), click the **New Option** link at the top right-hand corner of the **Scoped Global Option List** to open the Scoped Global DHCP Options form (Figure 6-20). This form allows you to enter text directly into the DHCP configuration file at the subnet scope level.

Figure 6-21 DHCP Global Options - New Scoped Global

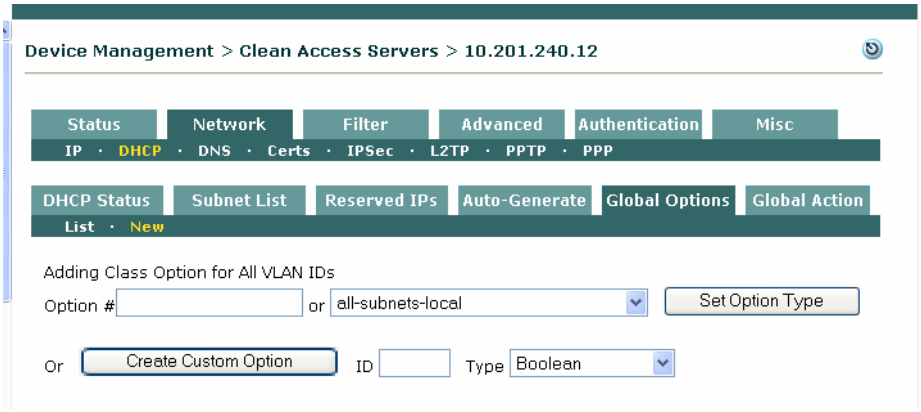


7. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.
8. If configuring a **Custom Option**, type the **ID** of the option, choose a data **Type** from the dropdown menu, and click **Create Custom Option**.

Add New Class Option

9. From the **Global Options** main page (Figure 6-19), choose one of the following **Class Types** from the dropdown menu to the right of the **Class Options** list:
   - **All VLAN-Restricted Subnets**—To apply the option to all subnets in the **Subnet List** (autogenerated or manually-created) that are restricted to a VLAN ID.
   - **All Relay IP-Restricted Subnets**—To apply the option to all subnets in the **Subnet List** (manually-created) that are restricted to a Relay IP.
   - **No VLAN tagged**—To apply the option to all subnets in the **Subnet List** that have no VLAN specified.
   - **VLAN ID <n>**—To apply the option to a specific subnet for VLAN ID (<n>) in the **Subnet List**.
10. Click the **New Class Option** button at the top right-hand corner of the **Class Options List** to open the **New Class Option** form (Figure 6-21).

Figure 22 DHCP Global Options - New Class Option For All VLAN IDs (VLAN Restricted Subnets)

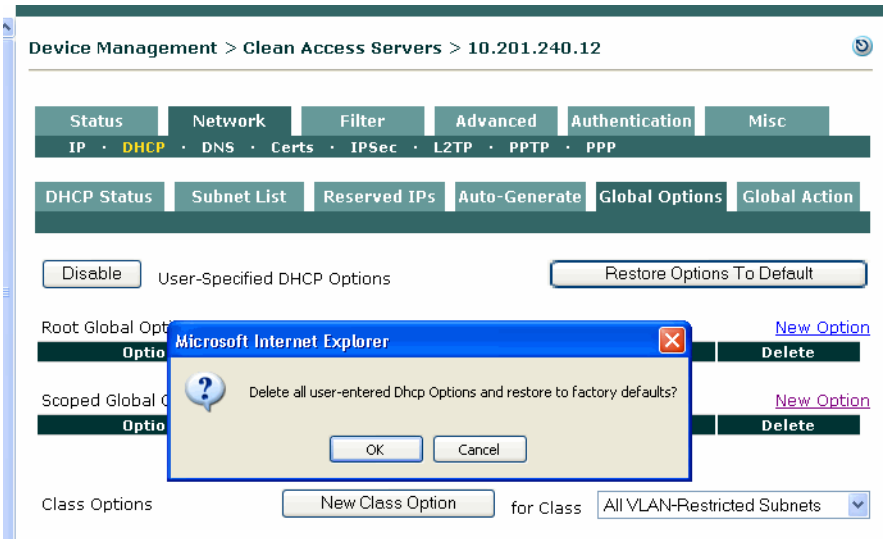


11. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.
12. If configuring a Custom Option, type the **ID** of the option, choose a **Type** from the dropdown menu, and click **Create Custom Option**.

Restore Options to Default

13. To restore factory defaults, click the **Restore Options To Default** button at the top-right side of the **Global Options > List** page (Figure 6-23).

Figure 6-23 Restore Global Options to Default



Disable DHPC Options

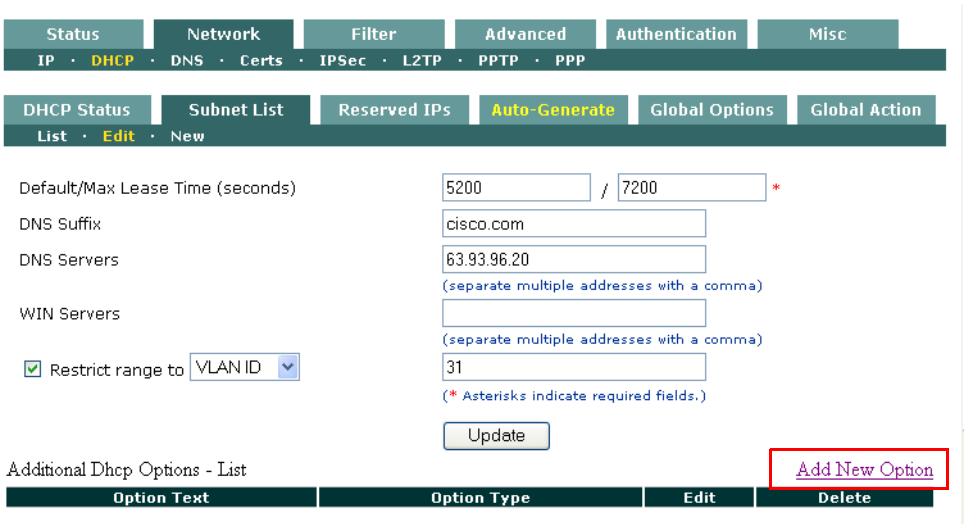
To disable admin-specified DHCP options, click the Disable button at the top-left side of he **Global Options > List** page (Figure 6-19 on page 6-19).

Add Local Scoped DHCP Option

1. Make sure DHCP options are enabled as described in Enable User-Specified DHCP Options, page 6-18.
2. Go to **Network > Subnet List > List** and click the **Edit** button () next to the subnet for which you want to add an option.
3. The **Edit** form appears.

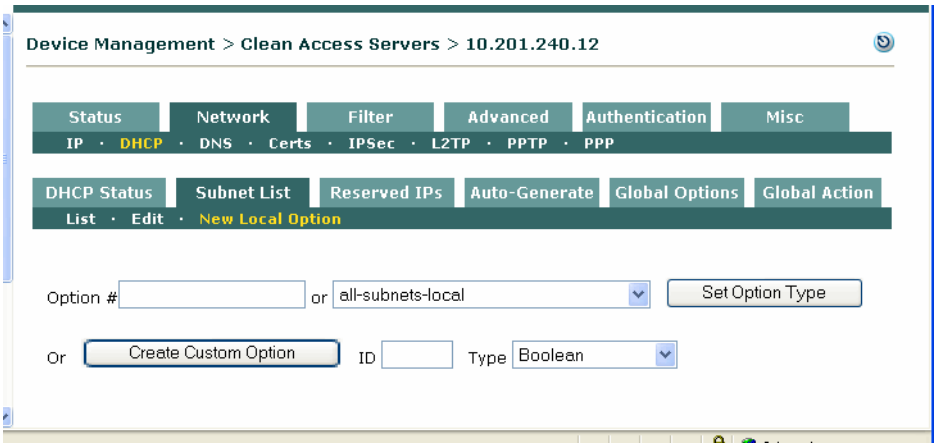
Figure 6-24 Edit Subnet List Form (Local Scoped DHCP Option

)



4. Click the **Add New Option** Link at the bottom of the form. The **New Local Option** form appears:

Figure 6-25 Add New Local Option



5. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.
6. If configuring a Custom Option, type the option number in the **ID** field, choose a data **Type** from the dropdown menu, and click **Create Custom Option**.

DHCP Server Directives

Table 6-4 DHCP Server Directives

Server Directive	Description
allow bootp	Allows booting by BOOTP devices. Disabled by default. Some older printers still in use require BOOTP. The BOOTP protocol does not specify a time limit for the lease assignment, although other server directives can invalidate BOOTP leases.
always-broadcast	Normal DHCP operation calls for the DHCP DISCOVER and OFFER packets to be broadcast if the DHCP client is unsure of where the DHCP server is located. In typical operation, the DHCP REQUEST and ACK, and all subsequent REQUESTS and ACKs between a known client and a known DHCP server are unicast. The "always-broadcast" server directive instructs the DHCP server to always respond to all DHCP packets with a broadcast packet.
always-reply-rfc1048	Some DHCP clients violate RFC 1048 when sending DHCP packets. The DHCP server responds by default to these clients with packets that also violate RFC 1048. A very small set of clients send a DHCP packet which violates RFC 1048, but do not accept as valid a return packet which violates RFC 1048. This server directive instructs the server to always respond with RFC-1048 compliant packets no matter what is received.
deny bootp	This is the default behavior of the server. This server directive instructs the server to reject BOOTP requests.

Table 6-4 DHCP Server Directives (continued)

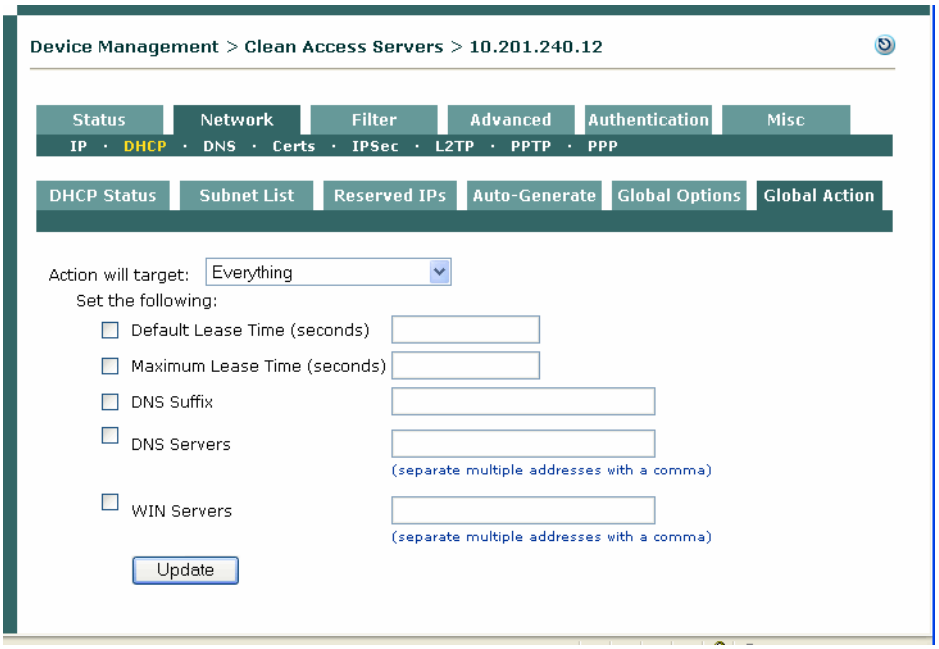
Server Directive	Description
dynamic-bootp-lease-length	Instructs the server to invalidate and make available for re-assignment IP leases assigned to BOOTP clients. Note that this does not guarantee that the BOOTP client will stop using the IP address. This server directive can be specified as a scoped global or local option.
filename	Instructs the DHCP server to fill out the filename portion of the DHCP packet. This is not an option, as it does not appear in the DHCP options list. This server directive can be specified as a scoped global or local option.
get-lease-hostname	Instructs the server to look up the domain name corresponding to the IP address of each address in the lease pool and use that address for the DHCP hostname.
next-server	Instructs the server to fill out the next-server field in all DHCP responses. This is typically used by devices which need additional configuration information, such as IP phones. This server directive can be specified as a scoped global or local option.
one-lease-per-client	Instructs the server to invalidate the first lease assigned to a DHCP client that has requested more than one. By default this is disabled, as some network devices require two or three addresses.
ping-check	Instructs the server to ping an IP address prior to assigning it. This is disabled by default, and has a significant negative impact on DHCP server performance.
server-identifier	Instructs the server to change its identifier. By default, the IP address of the untrusted network interface is used.
server-name	Instructs the server to change its name. By default, the hostname of the CAS is used. This server directive can be specified as a scoped global or local option.
use-lease-addr-for-default-route	Instructs the server to send a default route (gateway) equal to the assigned IP for all responses.

Global Action

The **Global Action** tab allows you to change fields on all DHCP elements of a particular CAS. For example, if you have 300 managed subnets and IP pools and you need to change the DNS server in all of them, you can achieve this using the **Global Action** form.

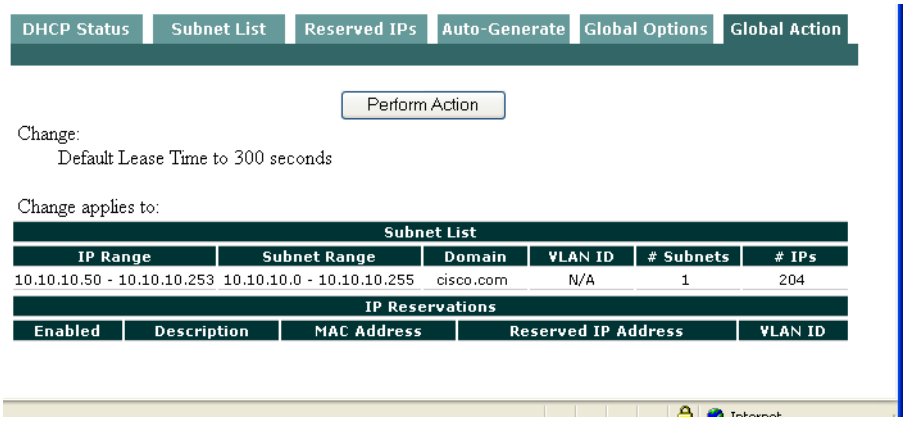
1. Go to the **Network > DHCP > Global Action** (Figure 6-26).

Figure 6-26 Global Action



2. In the **Action will target:** dropdown, choose one of the following options:
   - **Everything** (all of the options below combined)
   - **All Manual Subnets**
   - **All IP Reservations**
   - **All Auto-Generated Subnets**
   - **All by VLAN ID**
3. Click the checkbox for each applicable parameter, then type the value in the associated textbox.
   - **VLAN ID** (when **All by VLAN ID** is chosen)
   - **Default Lease Time (seconds)**
   - **Maximum Lease Time (seconds)**
   - **DNS Suffix**
   - **DNS Servers** (separate multiple addresses with a comma)
   - **WIN Servers** (separate multiple addresses with a comma)
4. Click **Update**.
5. Click **Perform Action** in the confirmation page that appears (Figure 6-27).

Figure 6-27 Example Global Action



IPSec/L2TP/PPTP/PPP on the CAS (Deprecated)

Warning **These features are deprecated in release 4.1(0) and will be removed in future releases.**

This chapter discusses how to configure the encryption mechanisms supported by the CAS.

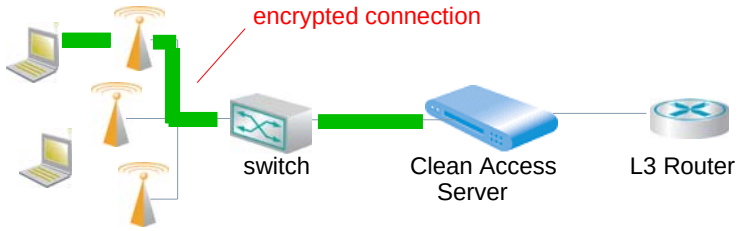
This chapter describes how to configure secure tunnels between users and the CAS. If you require support for a larger VPN base, Cisco NAC Appliance allows you to deploy a VPN concentrator in front of the Clean Access Server. In this case, see Chapter 8, “Integrating with Cisco VPN Concentrators” for details.

Overview

The Clean Access Server itself supports secure Virtual Private Network (VPN) connections between the Clean Access Server (CAS) and end user devices. The CAS supports VPN connections via PPTP, L2TP/IPSec or native IPSec clients. You can use Windows 2000, Windows XP, or other Pre-Shared Key VPN clients to use this feature. Note that each Clean Access Server supports the following number of concurrent VPN connections:

- IPSec — no limit is in place
- PPTP — 64 tunnels
- L2TP — 64 tunnels

Figure 7-1 Encrypted Connections



The Clean Access Server acts as an endpoint for the following encryption mechanisms:

- IPSec (IP Security)
- L2TP
- PPTP

You can use encryption whether the Clean Access Server is running in Real-IP/NAT Gateway mode or Virtual Gateway (bridge) mode.

User computers must have the appropriate client software. When configuring the client software, the user should set up the untrusted interface address of the Clean Access Server as the VPN gateway. For L2TP and PPTP, the user will need to provide the password for the PPP tunnel. For more information, see Configure PPP, page 7-9.

Note Devices allowed in the MAC filter list cannot establish VPN connections to the Clean Access Server (CAS). Only users logging in via web login or Clean Access agent can establish VPN connections to the CAS.

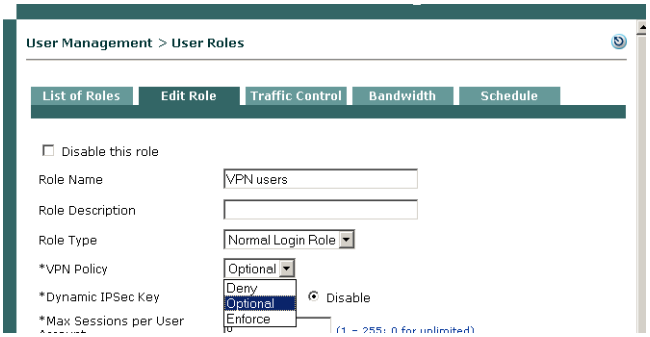
Enable VPN Policies

First, enable VPN policies for both the Clean Access Server and the user role. Then, perform the protocol-specific configuration described in the following sections.

1. Go to **Device Management > CCA Servers > List of Servers**, click the **Manage** button for the Clean Access Server, then go to **Network > IPSec**.

2. For the **VPN Policy for Clean Access Server** option, choose either **Optional** or **Enforce.** Note that the Clean Access Server supports the following number of concurrent VPN connections:
   - IPSec — no limit is placed
   - PPTP — 64 tunnels
   - L2TP — 64 tunnels

3. From **User Management > User Roles > List of Roles**, click the **Edit** icon next to the user role for which you want to enable encryption.



See "User Management: User Roles" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for additional details.

4. In the **Edit** form that appears, choose either **Optional** or **Enforce** for the **VPN Policy** field, according to what you chose for the Clean Access Server.
5. Click **Save Role**.

Configure IPSec Encryption

The IP Security Protocol (IPSec) is an encryption standard for securing traffic between two computers on a network. IPSec provides significantly better security for wireless users than the mechanism normally associated with wireless networks, WEP. For one thing, WEP uses a shared key, which all users in the network must use. With readily available tools, an intruder can figure out the key, given a large enough data sample. IPSec, on the other hand, uses unique, dynamic keys for data encryption between the client and server.

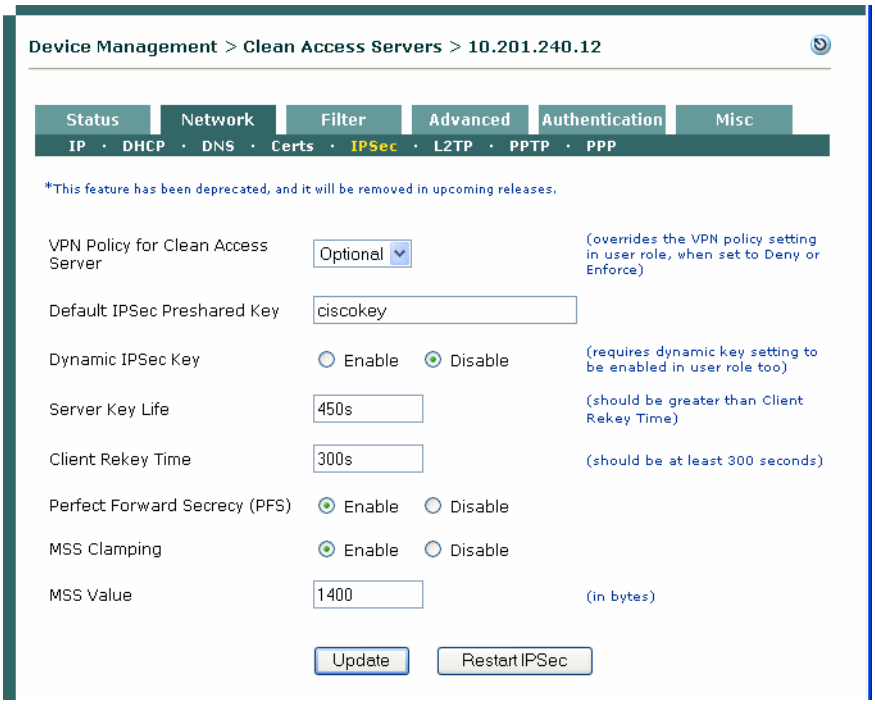
With the Clean Access Server, you can require users to use IPSec, make it optional, or deny use of IPSec on the network per user role.

To utilize IPSec encryption, users must have IPSec client software on their machines. Many operating systems include an IPSec client. Windows XP, for example, includes the client as a snap-in module.

To set up IPSec:

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP]> Network > IPSec**.

Figure 7-2 IPSec



2. For **VPN Policy for Clean Access Server**, choose either:
   - **Optional** – To make the use of IPSec connections to the Clean Access Server optional, at the client's discretion.
   - **Enforce** – To require the use of IPSec connections to the Clean Access Server.
3. Configure the following settings for the IPSec policy:
   - **Default IPSec Preshared Key** – Enter the key used to encrypt the data exchanged at the time of authentication negotiation.
   - **Dynamic IPSec Key** –
     The Dynamic IPSec Key feature must be enabled on both the Clean Access Server and user role. Click **Enable** to give each user is given a unique, one-time preshared key upon logging in. The user should use this key as the preshared key in their IPSec client to create the IPSec connection.

     Leave as **Disable** to have the user use the default preshared key (shared by all users) to create the IPSec connection. The key is given to users in the web logout page (Figure 7-3) or Clean Access Agent VPN Info dialog (Figure 7-4) after a successful login.

Figure 7-3 IPSec Key—Logout Page for Web Login Users

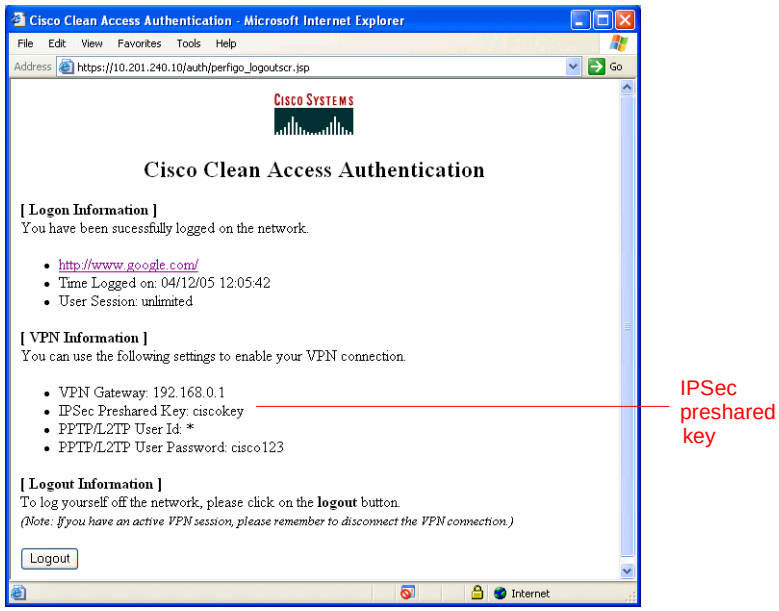
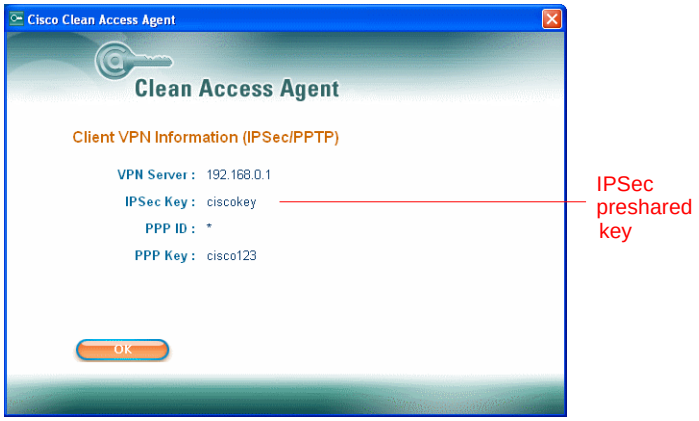


Figure 7-4 IPSec Key—Clean Access Agent Users (VPN Info)



- **Server Key Life** (default: 450 seconds) – How long the IPSec security association remains active. This should be greater than the Client Rekey Time.
- **Client Rekey Time** (default: 300 seconds) – This value is used by the IPSec client. It specifies how long the IPSec Client will propose that an IPSec SA be allowed to live before being regenerated. Typically, this value is shorter than the Server Key Life and at least 300 seconds.
- **Perfect Forward Secrecy (PFS)** – Enabling PFS (Perfect Forward Secrecy) ensures that the CAS utilizes completely new material when rekeying session keys. Otherwise, rekeys may be derived from material created at the point when the initial server key is created. Enabling PFS ensures that if one key is compromised, no other key is vulnerable due to the compromised key.

Note Enabling PFS may result in slower CAS performance. Use of the legacy IPSec Client enables PFS by default.

- **MSS Clamping** (default: 1400 bytes)– A restriction on the Maximum Segment Size (or packet size) of IPSec traffic. MSS Clamping replaces the traditional method of determining the maximum size of transmitted packets, dynamic MTU (maximum transfer unit) discovery. In MTU discovery, hosts negotiate the MTU size by ICMP at the time of data exchange. With MSS, the maximum packet size is predefined, so additional ICMP traffic is not needed.
- **MSS Value** – If MSS clamping is enabled, the maximum packet size, in bytes.

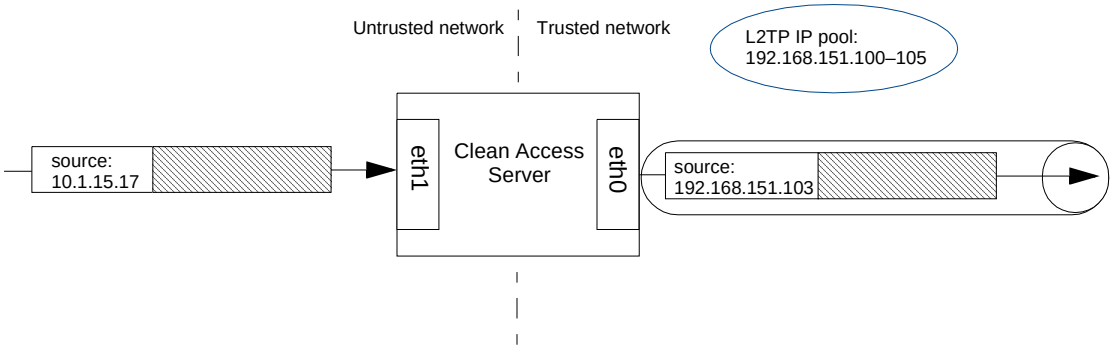
4. When finished, click **Restart IPSec** to restart the IPSec service with the new values.
5. Either allow or enforce the use of VPN by choosing the appropriate role policy in the role properties of the user (under **User Management** > **User Roles** > **Add** or **Edit**).

Configure L2TP Encryption

The Layer 2 Tunneling Protocol (L2TP) allows PPP frames to be tunneled through the network. L2TP and PPTP are alternatives to IPSec encryption. These formats are widely used due to the availability of client software supporting them.

Unlike IPSec, however, L2TP and PPTP require a dedicated IP address pool. The Clean Access Server uses the address pool to perform address translation of tunnelled traffic (Figure 7-5).

Figure 7-5 L2TP Address Translation



The address pool you use for both L2TP and PPTP pools depends on the Clean Access Server operating mode. Given a Clean Access Server with these interface addresses:

- eth0 (to trusted network): 192.168.151.55
- eth1 (to untrusted, managed network): 10.1.55.1

For Real-IP Gateway and Virtual Gateway, the IP pool must be a valid subnet (routable) on the eth0 side, such as 192.168.151.100–192.168.151.105.

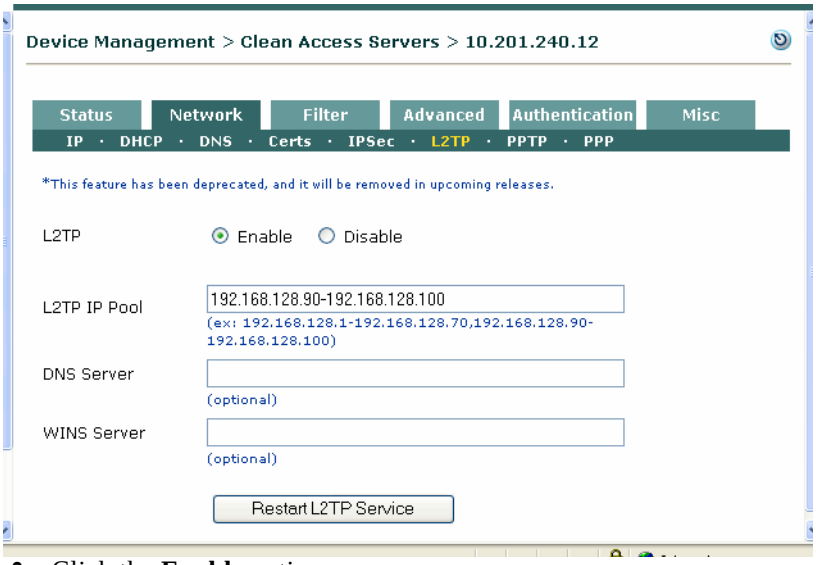
For NAT Gateway, the IP pool can be any private subnet, such as 10.1.70.20–10.1.70.200

Both L2TP and PPTP are used with PPP (Point-to-Point Protocol). Therefore, to set up L2TP or PPTP you will also need to configure PPP, as described below.

To set up L2TP:

1. Click the **L2TP** link in the **Network** tab to open the form.

Figure 7-6 L2TP



2. Click the **Enable** option.
3. In the **L2TP IP Pool** field, type the IP address range to be used for the point-to-point connections. Optionally, enter DNS and WIN Server addresses for the pool.
4. In the **PPP** form, enter the connection password (see Configure PPP, page 7-9) and click **Update**.
5. Click the **Restart L2TP Service** button.

Configure PPTP Encryption

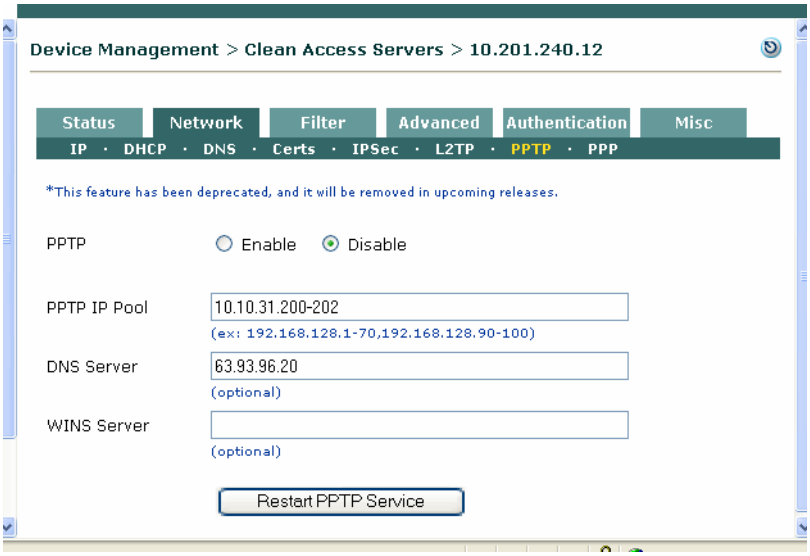
Like L2TP, the Point-to-Point Tunneling Protocol (PPTP), allows PPP frames to be tunneled through the network. The actual data is encrypted using a session key and the initial session key is different per user. The session key itself is changed periodically. If configuring PPTP, you must also Configure PPP, page 7-9.

Note The CAS in NAT mode does not support PPTP. For additional reference information on NAT/PPTP, refer to http://www.microsoft.com/technet/community/columns/cableguy/cg0103.mspx.

To set up PPTP:

1. In the **Network** tab, click **PPTP** on the submenu to open the PPTP form.

Figure 7-7 PPTP



2. Click the **Enable** option.
3. In **PPTP IP Pool**, type the IP address range to use for the point-to-point connections. For information on pool values, see Configure L2TP Encryption, page 7-6.
4. Optionally, type appropriate DNS Server and WIN Server addresses for the pool clients.
5. In the **PPP** form, enter the connection password (see Configure PPP, page 7-9) and click **Update**.
6. In the **PPTP** form, click the restart PPTP service button.

Configure PPP

Setting up L2TP and PPTP requires configuring PPP (Point-to-Point Protocol) The PPP form (opened by clicking the **PPP** link in the **Network** tab) lets you specify the password and user name used to authenticate parties in a point-to-point connection that uses L2TP or PPTP tunneling.

Figure 7-8 PPP

In most cases, the **User Name** value should be an asterisk, which means that any user name is accepted. The password should be the secret key used to authenticate the client participating in the point-to-point connection. By default, this is **cisco123**. Since the user is typically authenticated through the web login page prior to the establishment of the secure tunnel, you do not need to require unique login names/passwords for the encrypted connection.

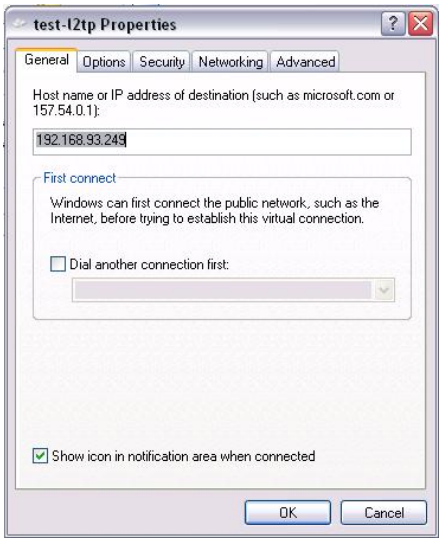
- After changing the values in the form, click the **Update** button to save your changes.
- Allow the use of encryption by setting user role VPN policies to **Enforce** or **Optional** (under **User Management > User Roles**)
- In the IPSec form (Figure 7-2), set the **VPN Policy for Clean Access Server** to **Enforce** or **Optional**.

Example Windows L2TP/IPSec Setup

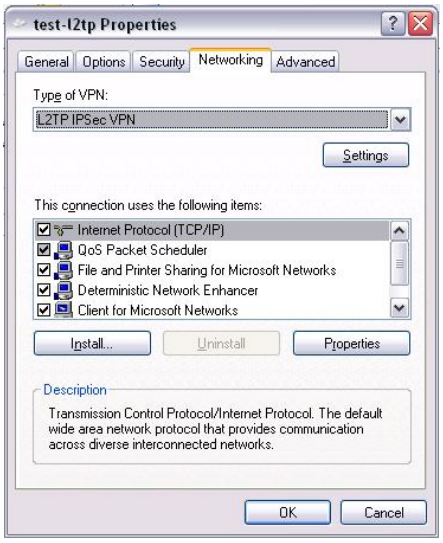
1. From the Start menu on a Windows XP system, right-click My Network Places.
2. Select Properties.
3. In the left window click “Create a new connection.”
4. Click Next in the New Connection Wizard that appears.
5. In the Network Connection Type dialog, choose the second option “Connect to the network at my workplace” and click Next.
6. In the Network Connection dialog, choose Virtual Private Network connection and click Next.
7. In the Connection Name dialog, type a new name for the connection (e.g. test-l2tp) and click Next.
8. In the VPN Server Selection dialog, type the Host name or IP address for the untrusted site (eth1).
9. You can add a shortcut to your desktop or just click Finish.

VPN Sign In

1. From the Network Connections window, right-click the new Virtual Private Network connection you just made (test-l2tp), and select Properties.
2. Click the General Tab. Enter the IP address of the Untrusted Interface as the Host name or IP address of destination.



3. Click the Networking Tab.
4. Change the Type of VPN from Automatic to L2TP/IPSEC VPN.



5. Click the Security tab.

6. Click the IPSec Settings button.
7. Enter the user name and the default password “ciscokey” and click OK.

8. Click OK.

Integrating with Cisco VPN Concentrators

This chapter describes the configuration required to integrate the Clean Access Server with Cisco VPN Concentrators. Topics include:

Overview

Cisco NAC Appliance enables administrators to deploy the Clean Access Server (CAS) in-band behind a VPN concentrator, or router, or multiple routers. Multi-hop Layer 3 in-band deployment is supported by allowing the Clean Access Manager (CAM) and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. Note that you can have a CAS supporting both L2 and L3 users. With layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before.

For users that are one or more L3 hops away, note the following considerations:

- User sessions are based on unique IP address rather than MAC address.
- If the user's IP address changes (for example, the user loses VPN connectivity), the client must go through the Clean Access certification process again.
- In order for clients to discover the CAS when they are one or more L3 hops away, the Clean Access Agent must be initially installed and downloaded via the CAS. This provides clients with the CAM information needed for subsequent logins when users are one or more L3 hops away from the CAS. Acquiring and installing the Agent by means other than direct download from the CAS (for example, Cisco Secure Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.
- The Certified List tracks both L2 and L3 VPN users by MAC address, and the Certified Devices Timer will apply to these users.
- All other user audit trails, such as network scanner and Clean Access Agent logs, are maintained for multi-hop L3 users.
- The Session Timer will work the same way for multi-hop L3 In-Band deployments and L2 (In-Band or Out-of-Band) deployments.

Note that when the Single Sign-On (SSO) feature is configured for multi-hop L3 VPN concentrator integration, if the user's session on the CAS times out but the user is still logged in on the VPN concentrator, the user session will be restored without providing a username/password.

- The Heartbeat Timer will not function in L3 deployments, and does not apply to Out-of-Band deployments.

  Note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

The topology and configuration required is fairly straightforward. Figure 8-1 illustrates a Cisco NAC Appliance network integrated with a VPN concentrator. Figure 8-2 illustrates the VPN concentrator configuration "before" and Figure 8-3 illustrates the configuration "after" integration with Cisco NAC Appliance when multiple accounting servers are being used. The Clean Access Server needs to be configured as the sole RADIUS accounting server for the VPN concentrator. If the VPN concentrator is already configured for one or more RADIUS accounting server(s), the configuration for these needs to be transferred from the concentrator to the CAS.

Note If using Split Tunneling on the VPN concentrator, make sure that the split tunnel allows access to the network being used for the Discovery Host. If the Discovery Host is the same as the CAM IP address, it should allow the CAM.

Single Sign-On (SSO)

In addition to being deployable with VPN concentrators, Cisco NAC Appliance provides the best user experience possible for Cisco VPN concentrator users through Single Sign-On (SSO). Users logging in through the VPN Client do not have to login again to Cisco NAC Appliance. Cisco NAC Appliance leverages the VPN login and any VPN user group/class attributes to map the user to a particular role.

This level of integration is achieved using RADIUS Accounting with the Clean Access Server acting as a RADIUS accounting proxy. Cisco NAC Appliance supports Single Sign-On (SSO) for the following:

- Cisco VPN Concentrators
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Airespace Wireless LAN Controllers
- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)

Note The "**Enable L3 support**" option must be checked on the CAS (under **Device Management** > **Clean Access Servers** > **Manage[CAS_IP]** > **Network** > **IP**) for the Clean Access Agent to work in VPN tunnel mode.

Note The Clean Access Server can acquire the client's IP address from either Calling_Station_ID or Framed_IP_address RADIUS attributes for SSO purposes. Cisco NAC Appliance RADIUS Accounting support for Single Sign-On (SSO) includes the Cisco Airespace Wireless LAN Controller. For SSO to work with Cisco NAC Appliance, the Cisco Airespace Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address attribute that the VPN concentrator uses). See also View Active VPN Clients, page 8-14.

See Configure Single Sign-On (SSO) on the CAS/CAM, page 8-9 for further specifics.

Figure 8-1 VPN Concentrator Integrated with Cisco NAC Appliance

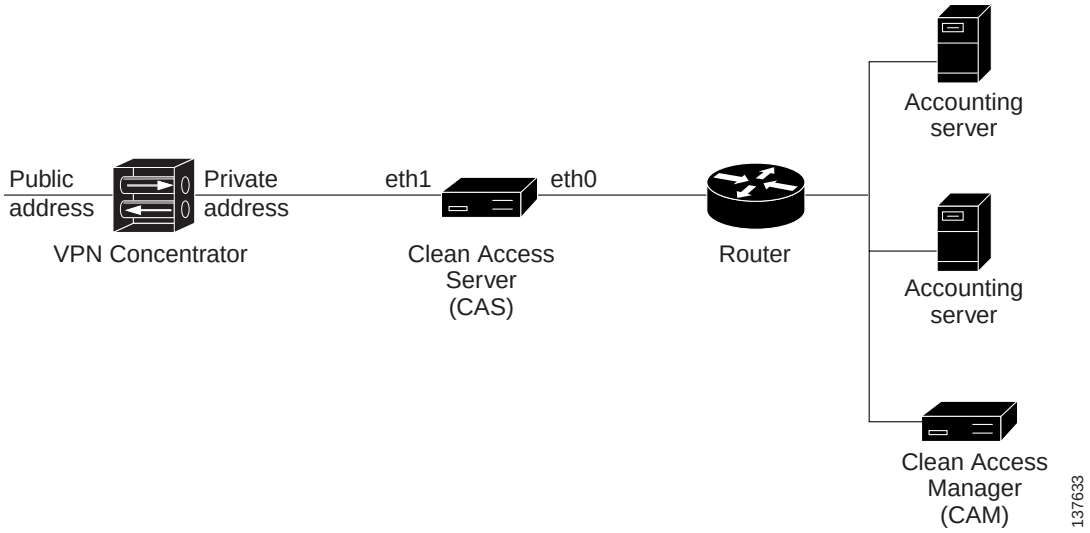


Figure 8-2 VPN Concentrator Before Clean Access Integration

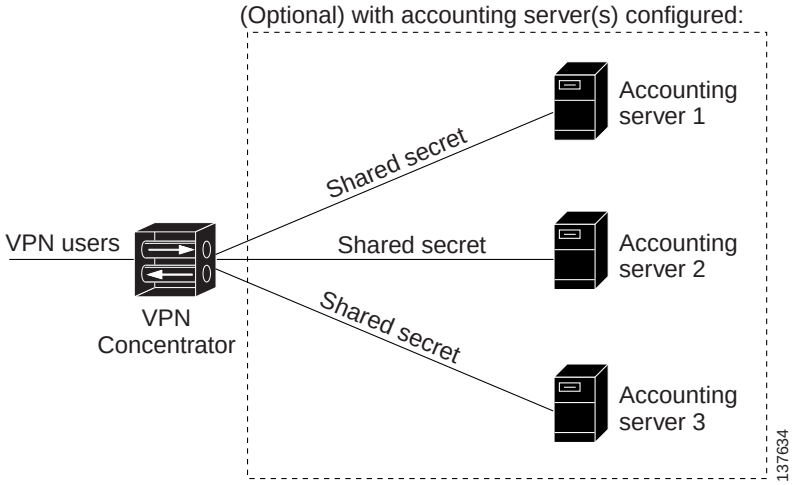
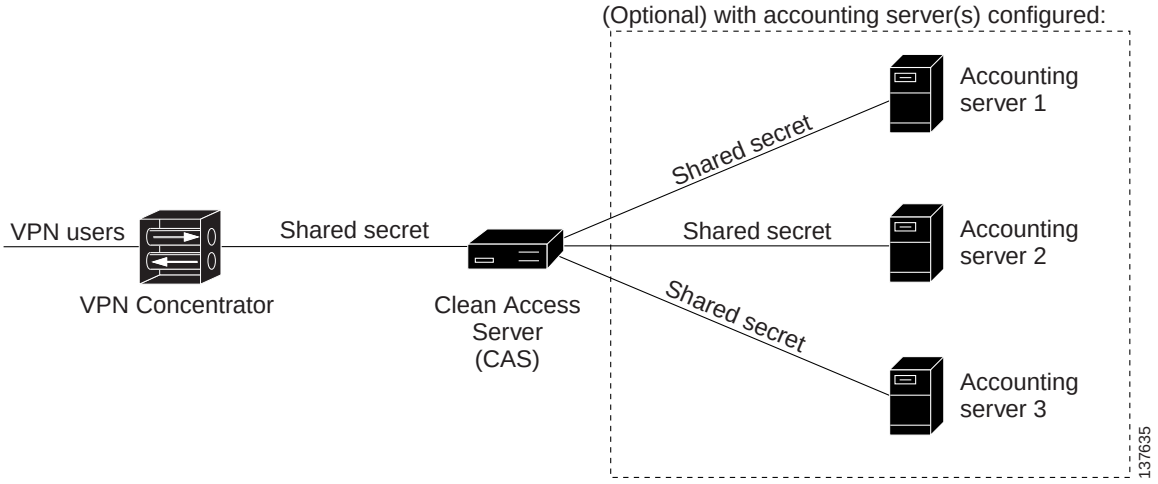


Figure 8-3 VPN Concentrator After Clean Access Integration



Configure Clean Access for VPN Concentrator Integration

The following steps are needed to configure Cisco NAC Appliance to work with a VPN concentrator.

Step 1 Add Default Login Page

Step 2 Configure User Roles and Clean Access Requirements for your VPN users.

Step 3 Enable L3 Support on the CAS

Step 4 Verify Discovery Host

Step 5 Add VPN Concentrator to Clean Access Server

Step 6 Make CAS the RADIUS Accounting Server for VPN Concentrator

Step 7 Add Accounting Servers to the CAS

Step 8 Map VPN Concentrator(s) to Accounting Server(s)

Step 9 Add VPN Concentrator as a Floating Device

Step 10 Configure Single Sign-On (SSO) on the CAS/CAM

Step 11 Create (Optional) Auth Server Mapping Rules

Step 12 Clean Access Agent L3 VPN Concentrator User Experience

Step 13 Test as Clean Access Agent with VPN Concentrator and SSO

Step 14 View Active VPN Clients (for troubleshooting)

Add Default Login Page

For both web login users and Clean Access Agent users, a login page must be added and present in the system in order for the user to authenticate via the Clean Access Agent. Go to **Administration > User Pages > Login Page > Add | Add** to quickly add the default user login page. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for complete details on login page configuration options.

Configure User Roles and Clean Access Requirements

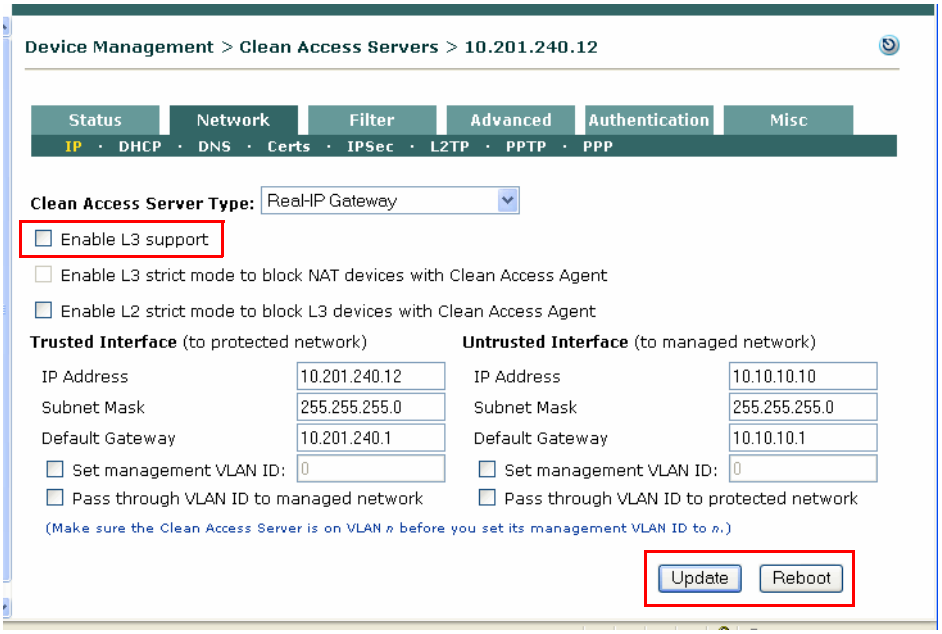
User roles must be configured along with Clean Access requirements to enforce the Clean Access process on VPN users. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for configuration details.

Enable L3 Support on the CAS

The "**Enable L3 support**" option must be checked on the **IP** form of the CAS for the Clean Access Agent to work in VPN tunnel mode.

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Network > IP**.

Figure 8-4 CAS Network Tab — Enable L3 Support



2. The **Clean Access Server Type**, **Trusted Interface**, and **Untrusted Interface** settings should already be correctly configured (from when the CAS was added).
3. Click the checkbox for **Enable L3 support**.
4. Click **Update**.
5. Click **Reboot**.

Note

- The enable/disable L3 feature is disabled by default, and ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.
- L3 and L2 strict options are mutually exclusive. Enabling one option will disable the other option.

See Enable L3 Support, page 5-13 for further details.

Verify Discovery Host

There must be a Discovery Host enabled in order for the Clean Access Agent to discover the CAS in VPN or L3 deployments. By default, the Discovery Host field is set to the IP address of the CAM. Because the VPN concentrator acts as a router between the user and the CAS, the Agent uses the Discovery Host to direct its UDP 8096 discovery packets to the network of the CAS. The CAS uses these packets to learn that a Clean Access Agent is active, and discards the packets before they ever reach the CAM. The Discovery Host field should be set in the CAM before the Agent is distributed and installed on client machines.

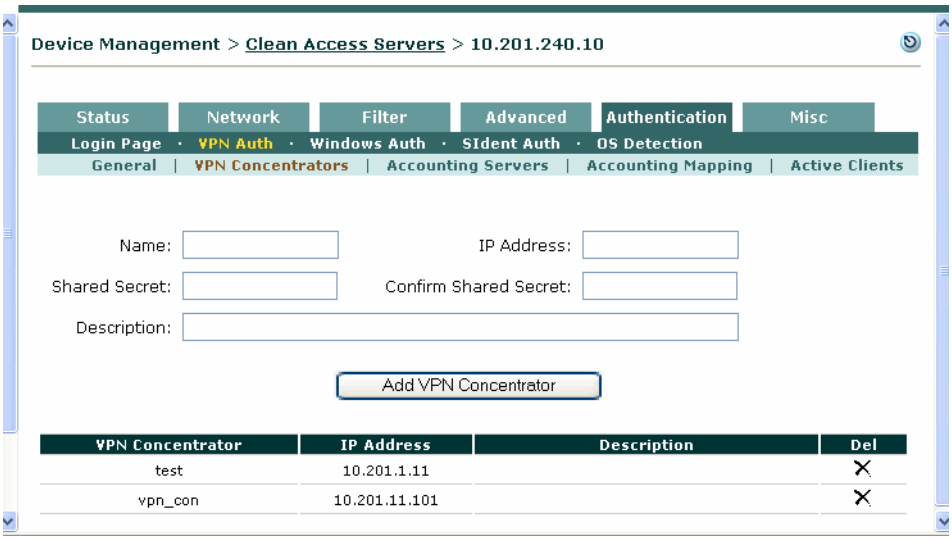
1. Go to **Device Management > Clean Access > Clean Access Agent > Distribution** .
2. Verify the IP address for the **Discovery Host** field is either the IP address of the CAM (default), or a trusted network IP address that requires traffic to be routed/forwarded via the CAS.
3. If changing the **Discovery Host**, click the **Update** button.

See VPN/L3 Access for Clean Access Agent, page 5-14, and the “ConfiguringAgent Distribution/Installation ” section of the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for additional information.

Add VPN Concentrator to Clean Access Server

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > VPN Concentrators**.

Figure 8-5 Add VPN Concentrator



2. Type a **Name** for the concentrator.
3. Type the Private **IP Address** of the concentrator.
4. Type a **Shared Secret** between the CAS and VPN concentrator. The same secret must be configured on the concentrator itself.
5. Retype the secret in the **Confirm Shared Secret** field.
6. Enter an optional **Description.**
7. Click **Add VPN Concentrator**.

Make CAS the RADIUS Accounting Server for VPN Concentrator

Make the CAS the RADIUS accounting server on the VPN concentrator (for example, on the VPN 3000 series, this is done under Configuration > System > Servers > Accounting). It is a good idea to record the settings for each accounting server to transfer to the CAS later. The CAS should be the only accounting server for the VPN concentrator, and the VPN concentrator should be configured with the trusted-side IP address of the CAS and have the same shared secret as the CAS.

For further details, refer to the appropriate product documentation, such as:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/tsd_products_support_series_home.html

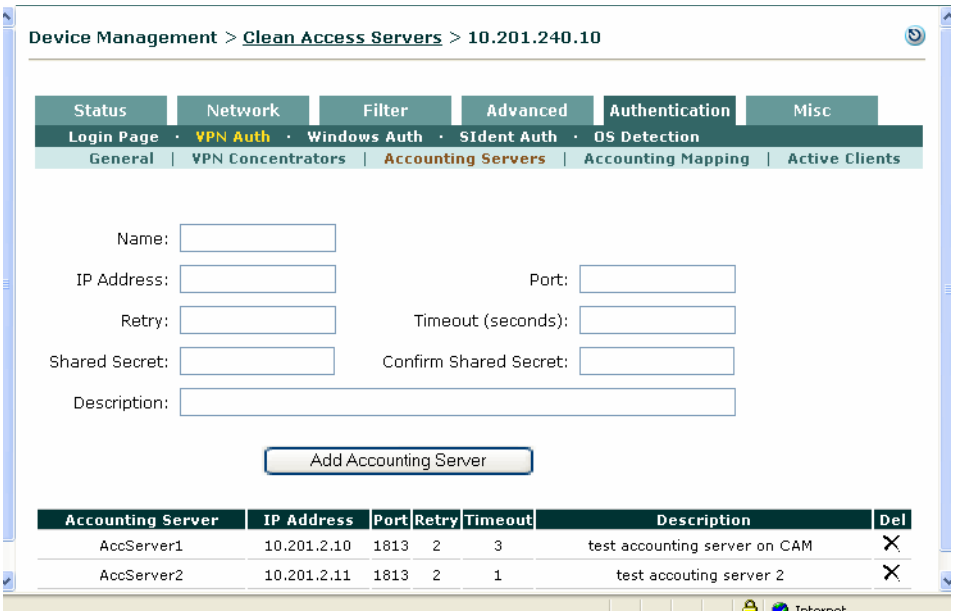
http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

Add Accounting Servers to the CAS

If the VPN concentrator is configured to work with an accounting server, the information for the accounting server(s) needs to be transferred to the CAS. The CAS maintains these associations instead.

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP]> Authentication > VPN Auth > Accounting Servers**.

Figure 8-6 Add Accounting Server(s)



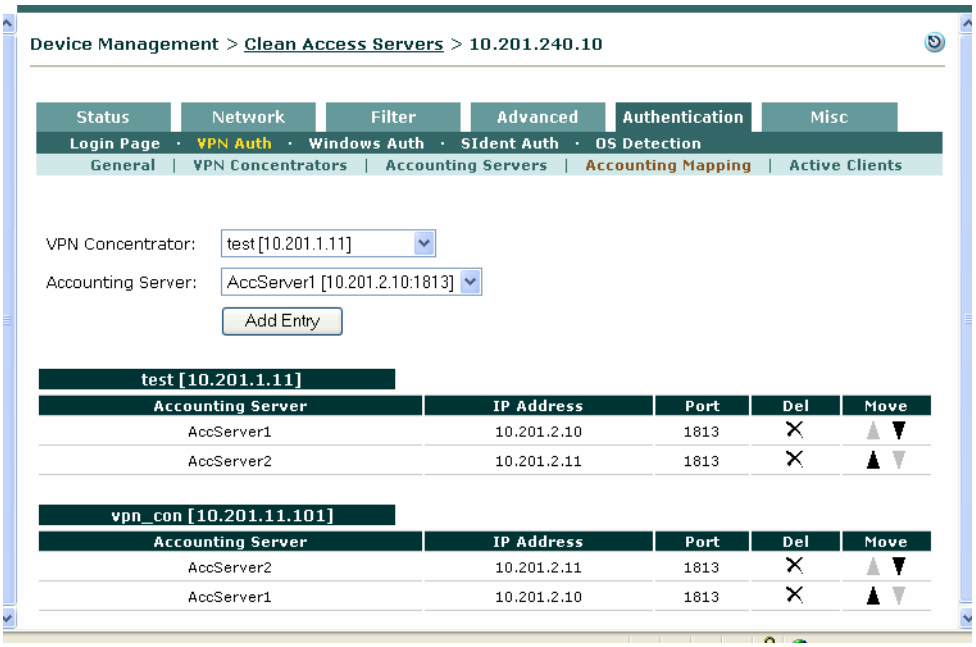
2. Type a **Name** for the accounting server.
3. Type the **IP Address** of the accounting server.
4. Type the **Port** of the accounting server (typically 1813)
5. Type the **Retry** number for the accounting server. This specifies the number of times to retry a request attempt if there is no response within the Timeout specified. For example, if the Retry is 2, and the Timeout is 3 (seconds), it will take 6 seconds for the CAS to send the request to the next accounting server on the list.
6. Type the **Timeout** of the accounting server (in seconds). This specifies how long the CAS should wait before retrying a request to the accounting server when there is no response.
7. Type a **Shared Secret** between the CAS and accounting server. You can transfer the settings from the VPN concentrator or create a new secret; however the same secret must be configured on the accounting server itself.
8. Retype the secret in the **Confirm Shared Secret** field.
9. Enter an optional **Description.**
10. Click **Add Accounting Server**.

Map VPN Concentrator(s) to Accounting Server(s)

If managing multiple VPN concentrators and multiple accounting servers, you can create mappings to associate the VPN concentrator(s) with sets of Accounting Servers. This allows the CAS to continue to the next server on the list in case an accounting server becomes unreachable.

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Accounting Mapping**.

Figure 8-7 Accounting Mapping



2. Choose a **VPN Concentrator** from the dropdown menu. The menu displays all VPN concentrators added to the CAS.
3. Choose an **Accounting Server** from the dropdown menu. The menu displays all accounting servers configured for the CAS.
4. Click the **Add Entry** button to add the mapping. The list below will display all the accounting servers associated per VPN concentrator by name, IP address, and port.

Add VPN Concentrator as a Floating Device

In general, if the Clean Access Server is not on the same subnet as clients, the CAS will not obtain client MAC information for IP addresses as clients log into the system. Where there is a VPN concentrator between users and the CAS (all Server Types), the CAS will see the MAC address of the VPN concentrator with each new client IP address because the VPN concentrator performs Proxy ARP for the client IP addresses. Unless the VPN concentrator is configured as a floating device, only the first user logging into Clean Access will be required to meet Clean Access requirements. Therefore, administrators must add the MAC address of the router/VPN concentrator to the Floating Device list under **Device Management > Clean Access > Certified Devices > Add Floating Device** (example entry: 00:16:21:11:4D:67 1 vpn_concentrator). See “Add Floating Devices” in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Configure Single Sign-On (SSO) on the CAS/CAM

Single Sign-On (SSO) allows the user to login only once via the VPN client before being directed through the Clean Access process. To perform SSO, Cisco NAC Appliance takes the RADIUS accounting information from the VPN concentrator/wireless controller for the user authentication and

uses it to map the user into a user role. This allows the user to go through the Clean Access process directly without having to also login on the Clean Access Server. SSO is configured on both the CAS and CAM as described below.

The most important attributes needed from RADIUS accounting packets are User_Name, Framed_IP_address, Calling_Station_ID. For a user to be qualified for SSO through the Clean Access Server, either the Framed_IP_address or Calling_Station_ID attribute (sent for the client's IP address) must be in the RADIUS accounting message.

Note RADIUS Accounting support for Single Sign-On (SSO) includes the Cisco Airespace Wireless LAN Controller. For SSO to work with Cisco NAC Appliance, the Cisco Airespace Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address attribute that the VPN concentrator uses).

Configure SSO on the CAS

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > General**.

Figure 8-8 General Settings (SSO / Logout / RADIUS Accounting Port)

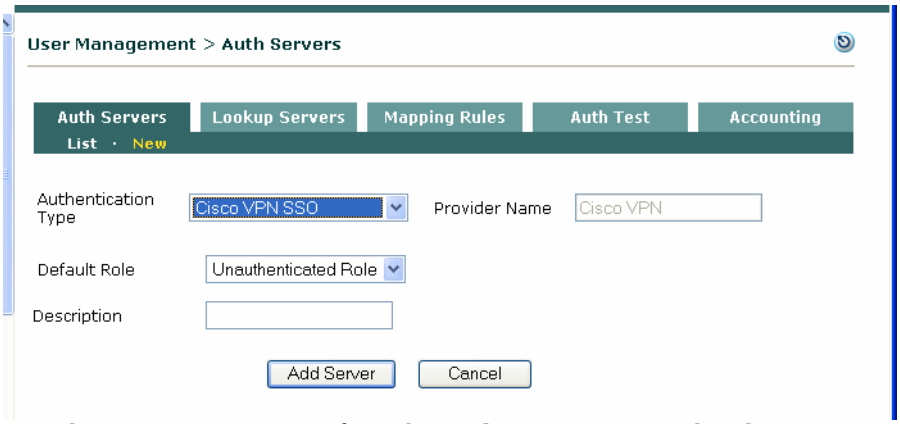
2. Click the checkboxes for **Single Sign-On** and **Auto-Logout** to enable these features for VPN users.
3. Leave the default port (1813) or configure a new one for **RADIUS Accounting Por**t.
4. Click **Update**.

Configure SSO on the CAM

To support SSO when configuring Cisco NAC Appliance VPN Concentrator integration, a Cisco VPN SSO authentication source must be added to the CAM.

1. Go to **User Management > Auth Servers > New**.

Figure 8-9 Add New Auth Server (in CAM)



2. Choose **Cisco VPN SSO** from the **Authentication Type** dropdown menu.
3. The **Provider Name** is set by default to **Cisco VPN**.
4. From the **Default Role** dropdown, choose the user role you want VPN client users to be assigned to for the Clean Access process.
5. Enter an optional **Description** to identify the VPN concentrator in the list of auth servers
6. Click **Add Server.**

The new Cisco VPN SSO auth server appears under **User Management > Auth Servers > List of Servers**.

- Click the **Edit** button ( ) next to the auth server to modify settings.
- Click the **Mapping** button ( ) next to the auth server to configure RADIUS attribute-based mapping rules for Cisco VPN SSO.

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for further details.

Create (Optional) Auth Server Mapping Rules

For the Cisco VPN SSO type, you can create mapping rules based on the RADIUS Auth Server attributes that are passed from the VPN Concentrator to map users into roles. The following RADIUS attributes can be used to configure Cisco VPN SSO mapping rules:

- Class
- Framed_IP_Address
- NAS_IP_Address
- NAS_Port
- NAS_Port_Type
- User_Name
- Tunnel_Client_Endpoint
- Service_Type
- Framed_Protocol
- Acct_Authentic

Mapping rules are configured in the CAM web admin console under **User Management > Auth Servers > Mapping Rules**. For complete configuration details, see "User Management: Configuring Auth Servers" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Clean Access Agent with VPN Concentrator and SSO

The Clean Access Agent supports multi-hop L3 deployment and VPN/L3 access from the Agent. The Agent will:

1. Check the client network for the Clean Access Server (L2 deployments), and if not found,
2. Attempt to discover the CAS by sending discovery packets to the CAM. This causes the discovery packets to go through the CAS even if the CAS is multiple hops away (multi-hop deployment) so that the CAS will intercept these packets and respond to the Agent.

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the Agent from the CAS. This can be done in two ways:

- From the Download Clean Access Agent web page (i.e. via web login)
- By client auto-upgrade to the 4.1.0.0 or above Agent. For this work, clients must have the 3.5.1 or above Agent already installed.

Either method allows the Agent to acquire the IP address of the CAM in order to send traffic to the CAM/CAS over the L3 network. Once installed in this way, the Agent can be used for both L3/VPN concentrator deployments or regular L2 deployments. See Enable L3 Support, page 5-13 for details

Note For VPN-concentrator SSO deployments, if the Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. Cisco Secure Downloads), the Agent will not be able to get the runtime IP information of the CAM and will not pop up automatically nor scan the client.

Note that:

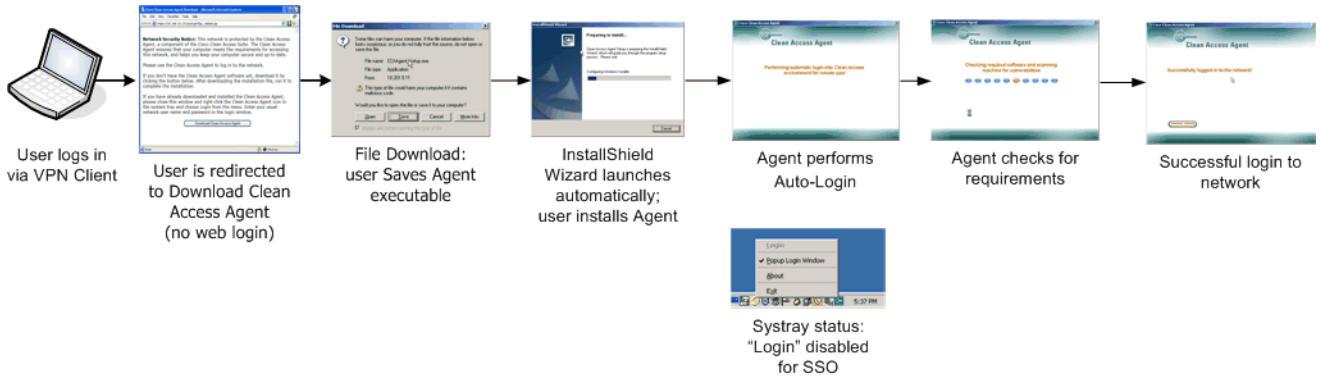
- Uninstalling the Agent while still on the VPN connection does not terminate the connection.
- If a 3.5.0 or prior version of the Agent is already installed, or if the Agent is installed through non-CAS means, such as Cisco Secure Downloads, you must perform web login to download the latest Agent setup files from the CAS directly and reinstall the Agent to get the L3 capability.

Clean Access Agent L3 VPN Concentrator User Experience

1. From the VPN Client, double-click the VPN connection entry for the VPN Concentrator configured for Cisco NAC Appliance.
2. Login as a user to the VPN Client | User Authentication dialog
3. Once logged in, open a browser and attempt to go to an intranet or extranet site.

Figure 8-10 illustrates the Clean Access process for a VPN user using the Clean Access Agent with Single Sign-On. Note that the initial download of the Clean Access Agent must be performed via the VPN connection.

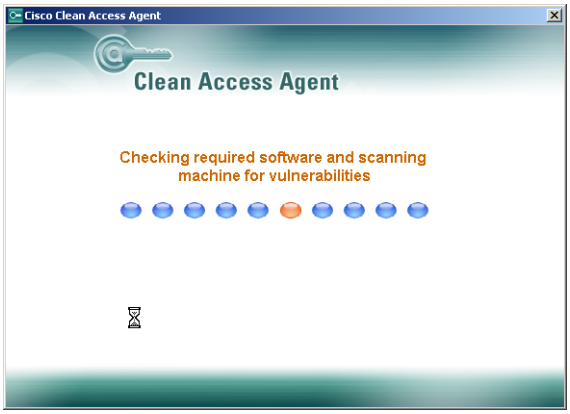
Figure 8-10 Clean Access Agent with SSO for VPN Users



With Single Sign-On, the Clean Access Agent performs automatic login and scanning as shown in Figure 8-11 and Figure 8-12.

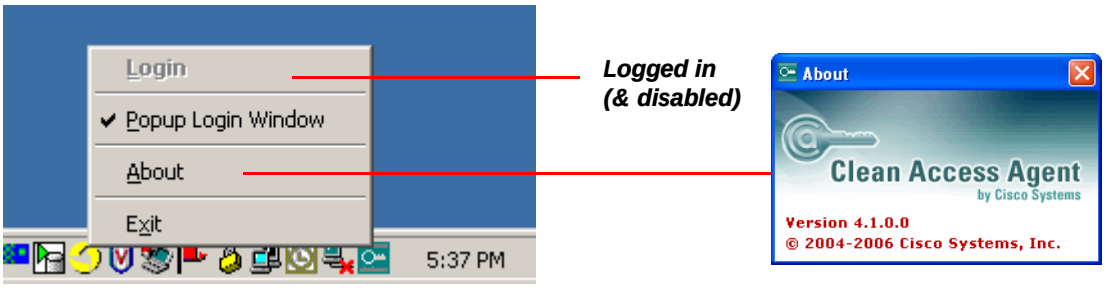
Figure 8-11 Agent Automatic Login (SSO)

Figure 8-12 Clean Access Agent Scanning



In addition, the “Login” option on the taskbar menu will be disabled for the Agent (Figure 8-13)

Figure 8-13 Systray Icon and Login Status



Note Web login always works in L2 or L3 mode, and L3 capability cannot be disabled.

View Active VPN Clients

The Active VPN Clients page lists IP addresses known to the CAS through VPN Single Sign-On (SSO) This page is intended for troubleshooting and is available in both the CAS management pages and CAS direct access console. The Active VPN Clients page shows a list of all users for which the CAS has received valid Radius accounting START packets.

Anytime the CAS receives a valid Radius Accounting START packet for a particular client machine, the CAS adds it to the Active VPN Clients list:

- If a client appears in this list, the client is able to perform SSO.
- If the client does not appear in this list, then most likely the START packet did not make it to the CAS or it was in an incorrect format.

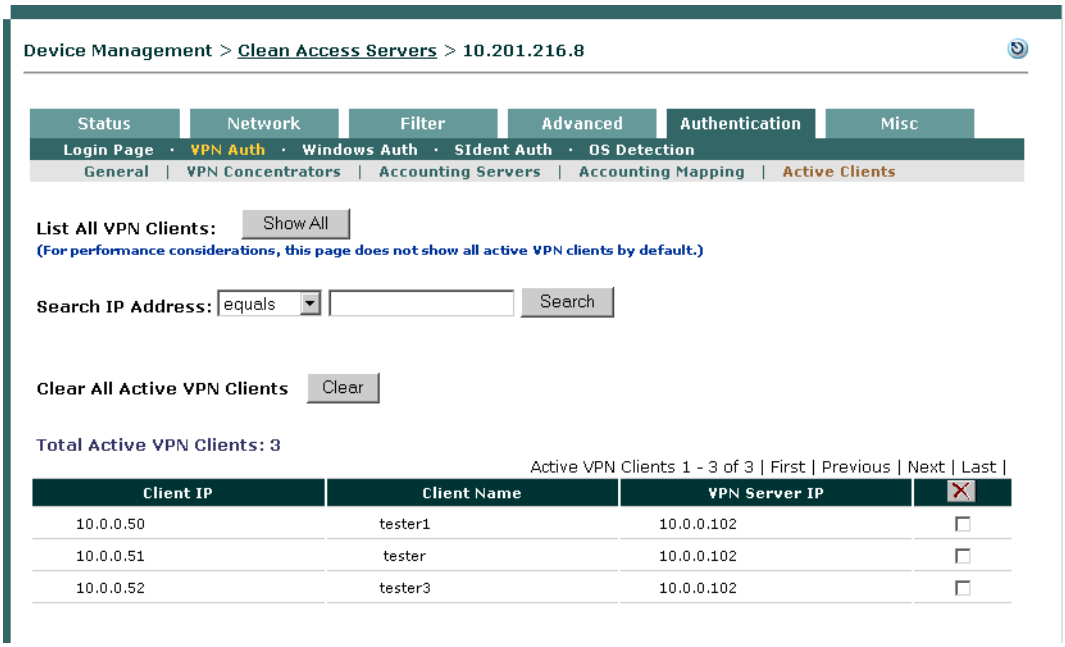
The key things the packet format must include are:

- Account-Status-type = 1 (indicating it is a START packet)
- Calling-station-Id (showing end machine's IP address)

To view active VPN clients:

1. Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Active Clients**

Figure 14 Active Clients (VPN Concentrator)



2. Click the **Show All** button to **List All VPN Clients** or perform a **Search**. The Active Clients page remains blank until you perform one of these two actions:
   a. Click **Show All** to display all current IP/user information from the system Single Sign-On (SSO) table.
   b. Alternatively, type an IP address in the **Search IP Address** text field, select an operator from the dropdown menu (**equals**, **starts with**, **ends with**, **contains**), and click the **Search** button to display results.
3. The table at the bottom of the page is populated with the following information. Entries are sorted by Client IP address.
   - **Total Active VPN Clients**—Displays the current number of active VPN clients in the SSO table.
   - **Client IP**—The client IP address received from the RADIUS accounting packet.
   - **Client Name**—The client name received from the RADIUS accounting packet.
   - **VPN Server IP**—The IP address of the Cisco VPN SSO auth server being used for Single Sign-On.

Note Clicking **Show All** or performing a new search refreshes the page with the latest SSO table information.

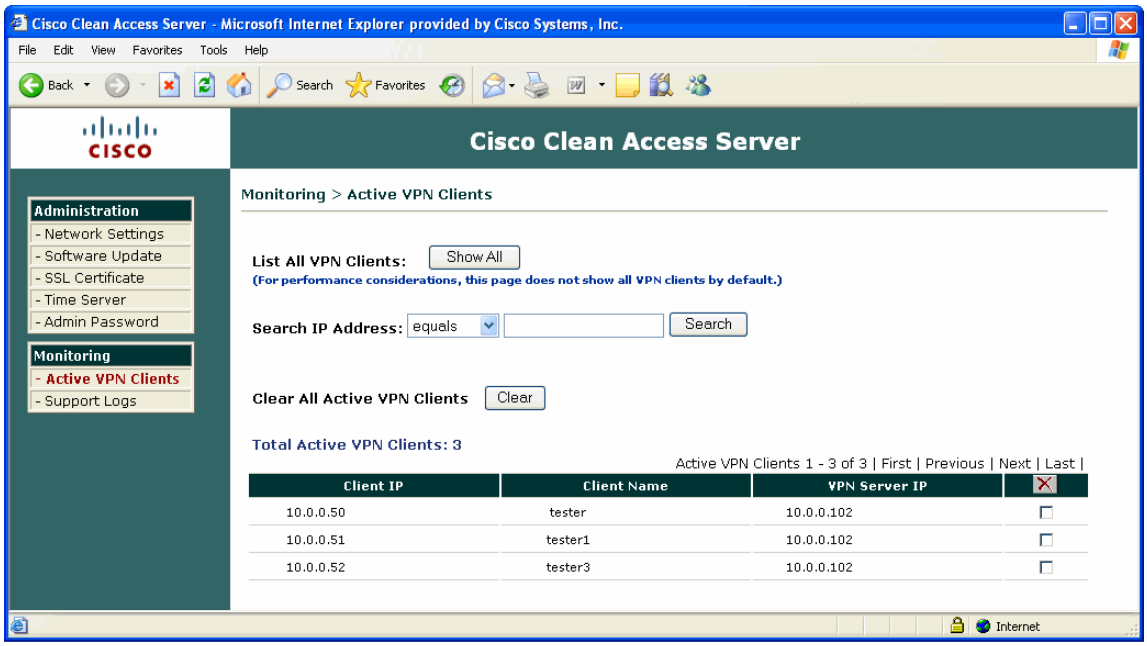
4. To remove entries from the Active Client page, either:
   a. Click the **Clear** button to **Clear All Active VPN Client** entries from the SSO table. For example, if VPN users lose their sessions due to a VPN server crash, the RADIUS accounting stop message will not be sent to the CAS, and those users will remain in the system SSO table until manually removed. Removing all entries from the Active VPN Clients page allows the system to restart from a fresh SSO table.

b. Click the checkbox for an individual entry and click the **Delete** button at the top of the column to remove that entry from the SSO table.

Note Clicking the **Clear** or **Delete** button only removes the user(s) from the system's current SSO client table; it does not remove the user(s) from the Online Users list.

Tip You can also view active VPN clients from the direct console of the CAS (https://<CAS_IP>/admin), from the **Monitoring > Active VPN Clients** page (Figure 8-15).

Figure 8-15 CAS Direct Access Console — Monitoring Active VPN Clients



Local Traffic Control Policies

This chapter describes how to set up traffic filtering rules in the Clean Access Server. Topics include:

Overview

Traffic control policies let you control what network resources can be accessed, and which users can access them. Traffic control policies are configured by user role, and must be configured for Clean Access Agent Temporary and quarantine roles.

Cisco NAC Appliance offers two types of traffic policies: IP-based policies, and host-based policies. IP-based policies are fine-grained and flexible and can stop traffic in any number of ways. IP-based policies are intended for any role and allow you to specify IP protocol numbers as well as source and destination port numbers. For example, you can create an IP-based policy to pass through IPSec traffic to a particular host while denying all other traffic.

Host-based policies are less flexible than IP-based policies, but have the advantage of allowing traffic policies to be specified by host name or domain name when a host has multiple or dynamic IP addresses. Host-based policies are intended to facilitate traffic policy configuration for Clean Access Agent Temporary and quarantine roles and should be used for cases where the IP address for a host is continuously changing or if a host name can resolve to multiple IPs.

Traffic control policies are directional. IP-based policies can allow or block traffic moving from the untrusted (managed) to the trusted network, or from the trusted to the untrusted network. Host-based policies allow traffic from the untrusted network to the specified host and trusted DNS server specified. When you create a new user role, it has the following default IP-based traffic control policies:

- All traffic from the untrusted network to the trusted network is blocked.
- All traffic from the trusted network to the untrusted network is allowed.

Since all traffic from the untrusted network is initially blocked, after creating a role you typically must create policies for permitting traffic as appropriate for the role.

Alternatively, a traffic control policy can block traffic to a particular machine or limit users to particular activities, such as email use or web browsing. Examples of policies are:

`deny access to the computer at 191.111.11.1`, or
`allow www communication from computers on subnet 191.111.5/24`

Finally, traffic control policies are hierarchical, and the order of the policy in the policy list affects how traffic is filtered. The first policy at the top of the list has the highest priority. The following examples illustrate how priorities work for Untrusted->Trusted traffic control policies.

Example 1:

- Priority 1: Deny Telnet
- Priority 2: Allow All

Result: Only Telnet traffic is blocked and all other traffic is permitted.

Example 2 (priorities reversed):

- Priority 1: Allow All
- Priority 2: Deny Telnet

Result: All traffic is allowed, and the second policy blocking Telnet traffic is ignored.

Example 3:

1. Allow TCP *.* 10.10.10.1/255.255.255.255
2. Block TCP *.* 10.10.10.0/255.255.255.0

Result: Allow TCP access to 10.10.10.1 while blocking TCP access to everything else in the subnet (10.10.10.*).

Local vs. Global Traffic Policies

Most traffic control policies are set globally for all Clean Access Servers using the Clean Access Manager global forms. By adding local traffic policies in individual Clean Access Servers, you can specialize filtering for the network managed by that CAS by extending policies defined globally.

This chapter describes the local traffic control policies configured on a CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**.

Note that global policies appear with yellow background while local policies appear with white background in the local list of traffic policies. To delete a policy, use the global or local form you used to create it.

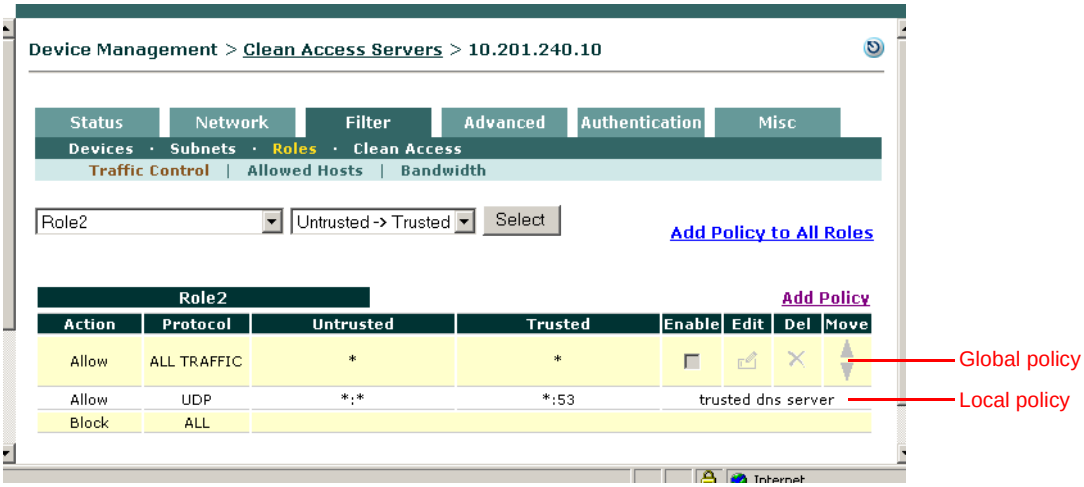
Global policies can only be accessed and modified from the **User Management > User Roles > Traffic Control** global forms. For details, see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Note A local traffic control policy for a CAS takes precedence over a global policy for all Clean Access Servers if the local policy has a higher priority.

View Local Traffic Control Policies

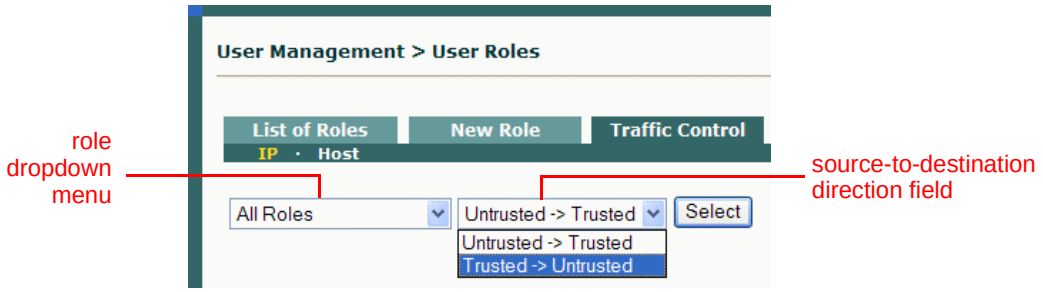
To view and configure local traffic control role policies, go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**. The policies appear by role in the **Traffic Control** form, as shown in Figure 9-1.

Figure 9-1 Local Traffic Control Policies



By default, the page lists the policies for traffic traveling from the untrusted network as the source to the trusted network as the destination. To view the policies for the opposite direction, with the trusted network as the source and the untrusted network as the destination, choose **Trusted->Untrusted** from the direction field and click **Select**.

Figure 9-2 Trusted -> Untrusted Direction Field



You can similarly display the policies for a single role by choosing the role from the role dropdown menu and clicking **Select**.

The priority of a policy corresponds to the order in which it appears in the list, the first item having the highest priority. You can change a policy's priority by clicking the corresponding up or down arrow in the **Move** column.

Add Local IP-Based Traffic Control Policies

Traffic control policies permit or block traffic to resources on the network and are created per role. Before creating a traffic control policy, make sure the role to which you want to assign the policy already exists. You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring IP-based traffic policies.

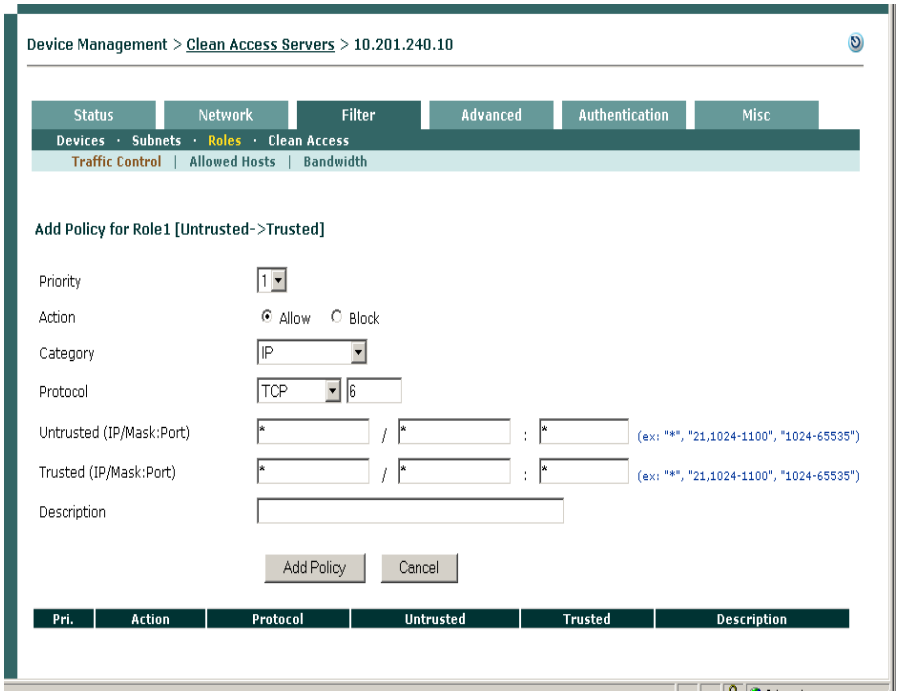
Add / Edit Local IP-Based Traffic Policy

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles**.
2. In the **Traffic Control** form, select the source-to-destination direction for which you want the policy to apply. Chose either **Trusted->Untrusted** or **Untrusted->Trusted**, and click **Select**.
3. For a new policy:
   - Click the **Add Policy** link next to the role for which you want to create the policy, or
   - Click **Add Policy to All Roles** to add the new policy to all the roles (except the Unauthenticated role) at once.

   To modify an existing policy:
   - Click **Edit** (✎) next to the policy you want to modify.

   Figure 9-3 shows the Add Policy form.

Figure 9-3 Add New Local IP Policy



Note The **Add Policy to All Roles** option adds the policy to all roles except the Unauthenticated role. Once added, traffic policies are modified individually and removed per role only.

4. Set the **Priority** of the policy from the **Priority** dropdown menu. The IP policy at the top of the list will have the highest priority in execution. By default, the form displays a priority lower than the last policy created (1 for the first policy, 2 for the second policy, and so on). The number of priorities in the list reflects the number of policies created for the role. The built-in **Block All** policy has the lowest priority of all policies by default.

Note To change the **Priority**, of a policy later, click the Up or Down arrows for the policy in the **Move** column of the IP policies list page.

5. Set the **Action** of the traffic policy as follows:
   - **Allow** (default)– Permit the traffic.
   - **Block** – Drop the traffic.
6. Set the **Category** of the traffic as follows:
   - **ALL TRAFFIC** (default) – The policy applies to all protocols and to all trusted and untrusted source and destination addresses.
   - **IP** — If selected, the **Protocol** field displays as described below.
   - **IP FRAGMENT** – By default, the Clean Access Server blocks IP fragment packets, since they can be used in denial of service attacks. To permit fragmented packets, define a role policy allowing them with this option.
7. The **Protocol** field appears if the **IP** Category is chosen, displaying the options listed below:
   - **CUSTOM:**—Select this option to specify a different protocol number than the protocols listed in the **Protocol** dropdown menu.
   - **TCP (6)** — For Transmission Control Protocol. TCP applications include HTTP, HTTPS, and Telnet.
   - **UDP (17)** — For User Datagram Protocol, generally used for broadcast messages.
   - **ICMP (1**) — For Internet Control Message Protocol.
   - **ESP (50)** — For Encapsulated Security Payload, an IPsec subprotocol used to encrypt IP packet data typically in order to create VPN tunnels
   - **AH (51)** — Authentication Header, an IPSec subprotocol used to compute a cryptographic checksum to guarantee the authenticity of the IP header and packet.
8. In the **Untrusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the untrusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application.
   If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.

Note You can specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring TCP/UDP ports. For example, you can specify port values such as: "*****" or "**21, 1024-1100**" or "**1024-65535**" to cover multiple ports in one policy. Refer to http://www.iana.org/assignments/port-numbers for details on TCP/UDP port numbers.

9. In the **Trusted (IP/Mask:Port)** field, specify the IP address and subnet mask of the trusted network to which the policy applies. An asterisk in the IP/Mask:Port fields means the policy applies for any address/application. If you chose TCP or UDP as the **Protocol**, also type the TCP/UDP port number for the application in the **Port** text field.

10. Optionally, type a description of the policy in the **Description** field.
11. Click **Add Policy** when finished. If modifying a policy, click the **Update Policy** button.

Note The traffic direction you select for viewing the list of policies (Untrusted -> Trusted or Trusted -> Untrusted) sets the source and destination when you open the **Add Policy** form:

- The first IP/Mask/Port entry listed is the source.
- The second IP/Mask/Port entry listed is the destination.

Add Local Host-Based Traffic Control Policies

Local host-based policies allow you to control user traffic to host sites for users in a role and for a particular Clean Access Server.

Default host policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after a Clean Access Agent **Update** or **Clean Update** is performed from the CAM.

You can configure custom DNS host-based policies for a role by host name or domain name when a host has multiple or dynamic IP addresses. Note that to use any host-based policy, you must first add a Trusted DNS Server for the user role.

Note

- After a software upgrade, new default host-based policies are disabled by default but enable/disable settings for existing host-based policies are preserved.
- After a Clean Update, all existing default host-based policies are removed and new default host-based policies are added with default disabled settings.

See “Clean Access Agent” in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details on the automatic **Updates** downloaded to the CAM under **Device Management > Clean Access > Updates**.

Enable Proxy Traffic

You can enable an individual CAS to parse host policies when user traffic passes through a specified proxy server.

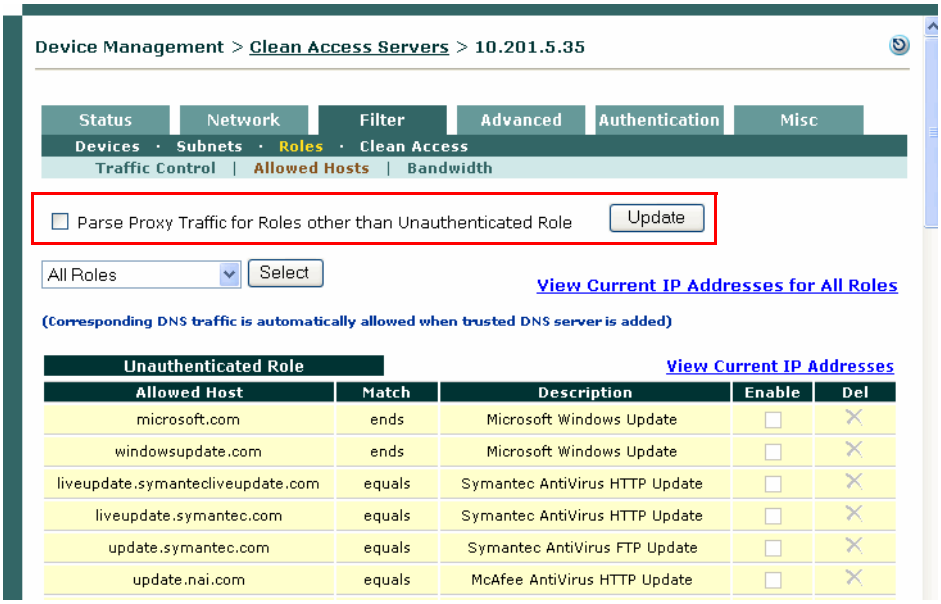
When the "**Parse Proxy Traffic for Roles other than Unauthenticated Role**" option is checked for an individual CAS, and a proxy server is specified on the CAS **Proxy** page, the CAS will check the payloads of GET, POST and CONNECT HTTP/HTTPS/FTP requests to make sure that the host is on the host policy list before allowing traffic to the proxy server. This allows users to access only the host sites enabled for a role (e.g. Temporary or quarantine users that need to meet requirements) when the specified proxy server is used. Note that the "parse proxy traffic" feature is enabled per CAS, and you must specify the Proxy server IP and port on the CAS **Proxy** page and enable the "**Parse Proxy Traffic for Roles other than Unauthenticated Role**" option for this feature to take effect.

Note For the Unauthenticated role, host policies do not work when a proxy server is specified, and the user is always redirected to the login page.

To enable host policies when traffic is going through proxy server specified on the CAS:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Proxy**
2. Specify the proxy IP/port as described in To Specify Proxy Server Settings on the CAS, page 5-41.
3. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** (Figure 9-4).

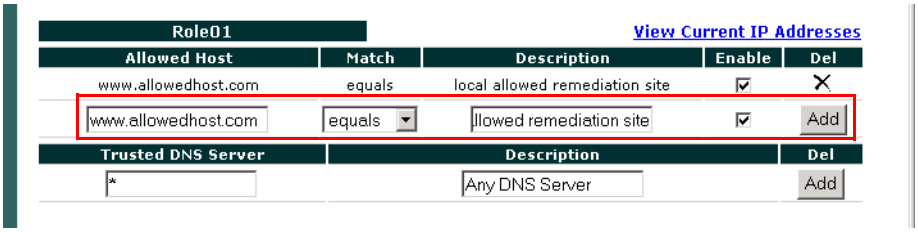
Figure 9-4 CAS—Allowed Hosts



4. Click the checkbox for "**Proxy Traffic for Roles other than Unauthenticated Role**." This option will apply to all roles other than the Unauthenticated role (not just Temporary/quarantine roles).
5. Click the **Update** button.

Add Local Allowed Host

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** and select the role for which to add a DNS host.

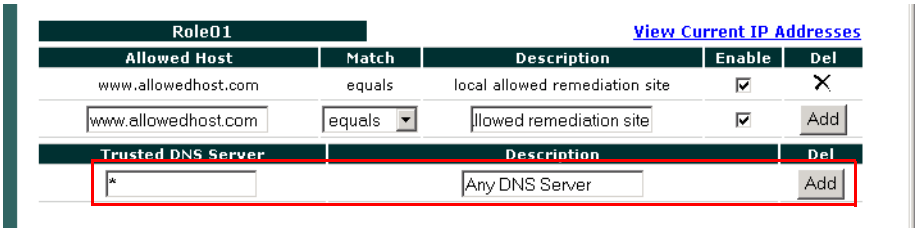


2. Type the hostname in the **Allowed Host** field (e.g. “allowedhost.com”).
3. In the **Match** dropdown menu, select an operator to match the host name: equals, ends, begins, or contains.
4. Type a description for the host in the **Description** field, such as “Allowed Host Update”
5. Click **Enable**.
6. Click **Add**.

Note You must add a Trusted DNS Server to the role to enable host-based traffic policies for the role.

Add Local Trusted DNS Server

1. Enter an IP address in the **Trusted DNS Server** field, or enter an asterisk “*” to specify any DNS server.



2. Type a description for the DNS server in the **Description** field.
3. Click **Add**.

Note When a trusted DNS server is added, an IP-based traffic policy allowing that server is automatically added for the role.

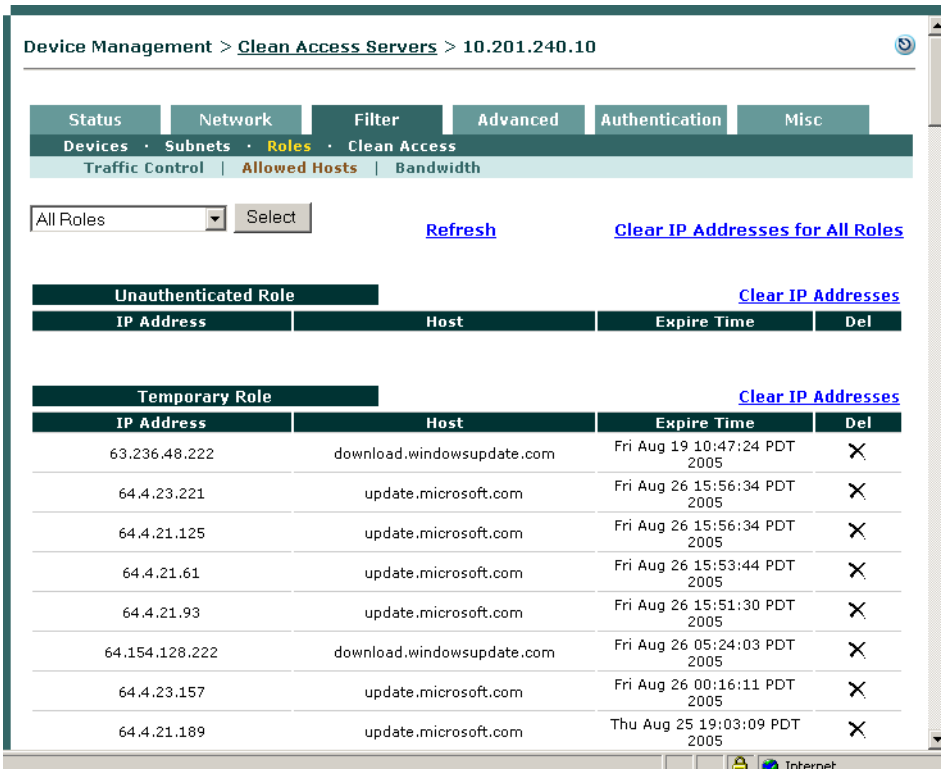
Note When you add a specific DNS server, then use this form later to add any (“*”) DNS server, the previously added server becomes a subset of the overall policy allowing all DNS servers, and will not be displayed. If you later delete the any (“*”) DNS server policy, the specific trusted DNS server you had previously allowed will be displayed again.

View IP Addresses Used by DNS Host

You can view the IP addresses used for the DNS host when clients connect to the host to update their systems.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts**
2. To view all IP addresses for DNS hosts accessed across all roles, click the **View Current IP addresses for All Roles** at the top of the page**.**

Figure 9-5 View Current IP Addresses for All Roles



Note You can view this list here from the CAS management pages, but modifying this list is done from the Clean Access Manager global filters forms. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

3. To view the IP addresses for DNS hosts accessed by clients in a specific role, click the **View Current IP addresses** link next to the desired role.
4. The IP address, Host name, and Expire time will display for each IP address accessed. Note that the Expire time is based on the DNS reply TTL. When the IP address for the DNS host reaches the Expire time, it becomes invalid.

Controlling Bandwidth Usage

Cisco NAC Appliance lets you control how much network bandwidth is available to users by role. You can independently configure bandwidth management using global forms in the CAM as needed for system user roles, or only on certain Clean Access Servers using local forms. However, the option must first be enabled on the CAS for this feature to work. You can also specify bandwidth constraints for each user within a role or for the entire role.

For example, for a CAM managing two CASes, you can specify all the roles and configure bandwidth management on some of the roles as needed (e.g. guest role, quarantine role, temporary role, etc.). If bandwidth is only important in the network segment where CAS1 is deployed and not on the network segment where CAS2 is deployed, you can then turn on bandwidth management on CAS1 but not CAS2.

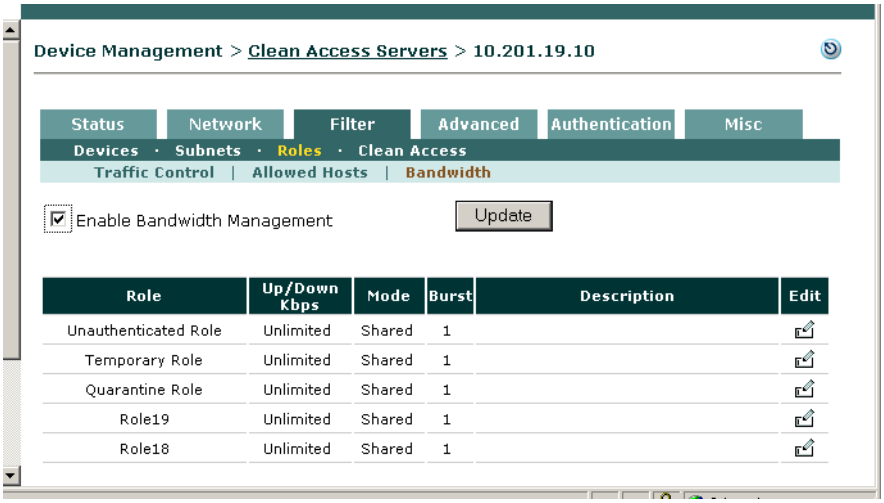
With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when downloading and reading pages), while users attempting to stream content or transfer large files are subject to the bandwidth constraint.

By default, roles have a bandwidth policy that is unlimited (specified as -1 for both upstream and downstream traffic).

To configure local bandwidth settings for a role:

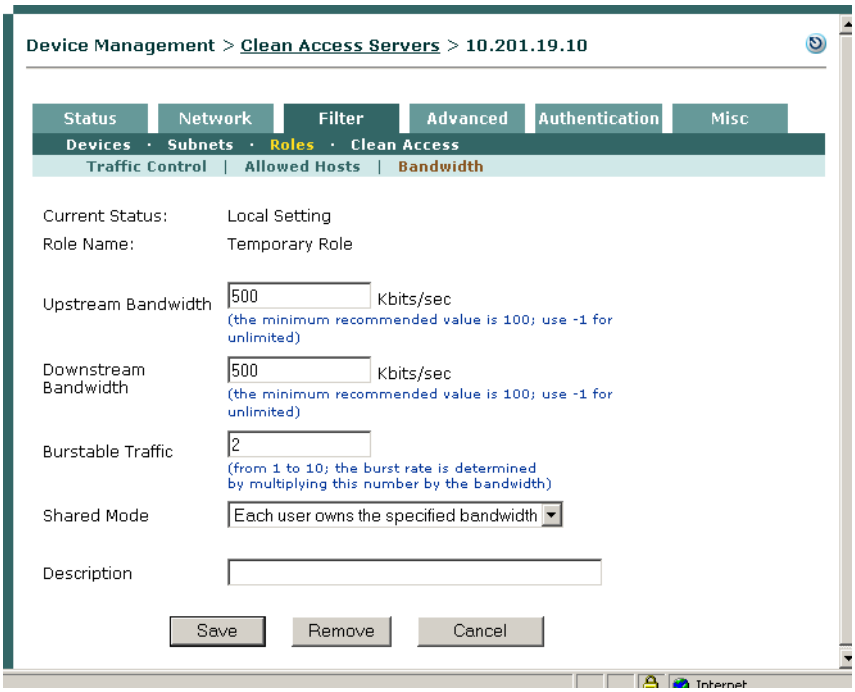
1. First, enable bandwidth management on the CAS by going to **Device Management > CCA Servers > Manage[CAS_IP] > Filter > Roles > Bandwidth**.
2. Select **Enable Bandwidth Management** and click **Update**.

Figure 9-6 Enable Bandwidth Management for the CAS



3. Click the **Edit** button ( ) next to the role for which you want to set bandwidth limitations. The **Role Bandwidth** form appears.

Figure 9-7 Local Bandwidth Form for User Role



4. The **Current Status** field lists either:
   - **Default Setting**: Local bandwidth management is not enabled (and settings from **User Management > User Roles > Bandwidth** are being used), or a local policy has not been set.
   - **Local Setting**: The configured local settings for this CAS apply for the selected role.
5. The **Role Name** fields lists the user role for which to configure local settings.
6. Set the maximum bandwidth in kilobits per second for upstream and downstream traffic in **Upstream Bandwidth** and **Downstream Bandwidth**. Upstream traffic moves from the untrusted (managed) to trusted side, while downstream traffic moves from the trusted to untrusted side.
7. Enter a **Burstable Traffic** level from 2 to 10 to allow brief (one second) deviations from the bandwidth limitation. A **Burstable Traffic** level of 1 has the effect of disabling bursting.

   The **Burstable Traffic** field is a traffic burst factor used to determine the “capacity” of the bucket. For example, if the bandwidth is 100 Kbps and the **Burstable Traffic** field is 2, then the capacity of the bucket will be 100Kb*2=200Kb. If a user does not send any packets for a while, the user would have at most 200Kb tokens in his bucket, and once the user needs to send packets, the user will be able to send out 200Kb packets right away. Thereafter, the user must wait for the tokens coming in at the rate of 100Kbps to send out additional packets. This can be thought of as way to specify that for an average rate of 100Kbps, the peak rate will be approximately 200Kbps. Hence, this feature is intended to facilitate bursty applications such as web browsing.
8. In the **Shared Mode** field, choose either:
   - **All users share the specified bandwidth** – The setting applies for all users in the role. In this case, the total available bandwidth is a set amount. In other words, if a user occupies 80 percent of the available bandwidth, only 20 percent of the bandwidth will be available for other users in the role.

- **Each user owns the specified bandwidth** – The setting applies to each user. The total amount of bandwidth in use may fluctuate as the number of online users in the role increases or decreases, but the bandwidth for each user is equal.

9. Optionally, type a **Description** of the bandwidth setting.
10. Click **Save** when finished.

The bandwidth setting is now applicable for the role and appears in the **Bandwidth** tab.

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for additional details on bandwidth management.

Local Authentication Settings

This chapter describes **Authentication** tab settings in the CAS management pages (other than **VPN Auth** settings which are described in Chapter 8, "Integrating with Cisco VPN Concentrators"). Topics include:

Overview

Most user-related configuration settings, such as roles, authentication sources, and local users, are configured for all Clean Access Servers in the global forms of the CAM web console. However, several aspects of user management can be configured locally for an individual CAS. These include:

- User presence scanning – Checks online users to see if their connections are still active. If not, the user session is terminated after a configurable period of time. This setting can be set globally or locally.
- Login pages – Prompts users accessing the network for their login credentials.
- Transparent Windows login – Allows single sign-on in Windows domains.

Local Heartbeat Timer

The heartbeat timer checks the connection status of online users by attempting to contact the client. If the client fails to respond, the user session can be timed out after a configurable amount of time. You can configure how long Cisco NAC Appliance waits to time out disconnected users, as well as how often it attempts to contact users. The actual connection check is performed by ARP message rather than by pinging. This allow the heartbeat check to function even if ICMP traffic is blocked.

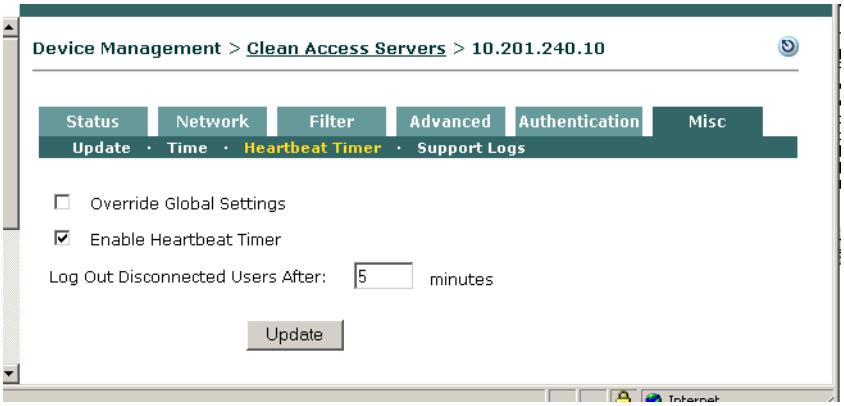
Note The CAS checks the connection of all users at once, regardless of when an individual user's session started.

The timer is configurable globally when accessed from **User Management > User Roles > Schedule > Heartbeat Timer**. By configuring a local setting in the Clean Access Server, you can override the global setting in the Clean Access Manager for that particular CAS.

To configure timeout properties based on connection status:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**.

Figure 10-1 Local Heartbeat Timer



2. Click the **Override Global Settings** checkbox.
3. Click the **Enable Heartbeat Timer** checkbox.
4. Specify a value for the **Log Out Disconnected Users After** field. After the system detects a disconnected user, this field sets the period of time after which the disconnected user is logged off the network.
5. Click **Update**.

For complete details on user session timeouts see Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

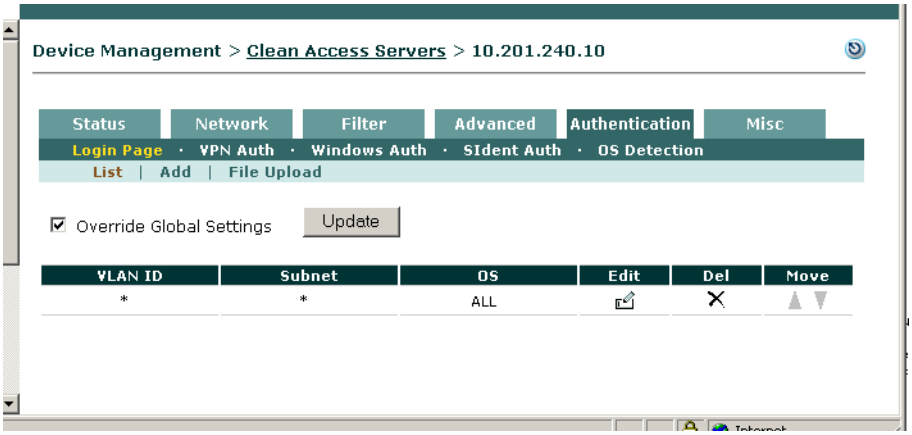
Local Login Page

A login page configured locally for a CAS takes precedence over the global login pages configured for all Clean Access Servers. If creating login pages local to a Clean Access Server, you can customize pages for particular VLANs, operating systems, and subnets.

Add Local Login Page

1. Go to the CAS management pages under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Authentication** > **Login Page**.
2. Select the **Override Global Settings** option and **Update**.

Figure 10-2 Override Global Login Page



3. Click the **Add** link that appears. Leave asterisks as default values for the **VLAN** and **Subnet** field to set the page for any VLAN/subnet or enter values to specify a VLAN/subnet. Likewise, leave the **Operating System** field as **ALL**, or specify an OS for which the login page will apply.
4. Click the **Add** button to add the page to the login page list.
5. In the login page list, click **Edit** next to the page to modify page contents and properties.
6. The **General** options page appears. Select a **Page Type**: **Frameless**, **Frame-based**, or **Small Screen (frameless)**.
7. Optionally enter a **Description** for the page.
8. Click **Update** to commit the changes made on the General page, then click **View** to see the login page with the updated changes.
9. Click the **Content** link. Specify the following content to appear on the login page:
   - **Image:** Use the dropdown menu to choose the logo to appear on the login page.
   - **Title:** Type the title of the login page.
   - **Username Label, Password Label, Login Label, Provider Label, Guest Label, Help Label, Root CA Label:** Use the checkboxes to specify the fields/buttons to appear on the login screen. Enter a label for each of the fields selected.
   - **Default Provider:** Use the dropdown menu to choose the default provider for the login page.

- **Available Providers:** The authentication sources you want to appear in the providers dropdown menu on the login page.
- **Instructions:** Type the instructions to be shown on the login page.
- **Root CA File:** The root CA certificate file to use, if the **Root CA Label** is enabled.
- **Help Contents:** Type help text to be presented to users on the login page. Note that only HTML content can be entered in this field (URLs cannot be referenced).

10. Click **Update** to commit the changes made on the Content page, then click **View** to see the login page with the updated changes.
11. Click the **Style** link. You can change the background (BG) and foreground (FG) colors and properties. Note that **Form** properties apply to the portion of the page containing the login fields.
12. Click **Update** to commit the changes made on the Style page, then click **View** to see the login page with the updated changes.
13. If frames are enabled in the **Login Page > General** settings, click the **Right Frame** link. You can enter either URL or HTML content for the right frame as described below:
    a. ***Enter URLs:*** (for a single webpage to appear in the right frame)

       For an external URL, use the format `http://www.webpage.com`.

       For a URL on the Clean Access Manager use the format:

       `https://<CAM_IP_address>/upload/file_name.htm`

       where `<CAM_IP_address>` is the domain name or IP listed on the certificate.

       If you enter an external URL or Clean Access Manager URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access to the external server or Clean Access Manager.

       For a URL on the local Clean Access Server use the format:

       `https://<CAS_eth0_IP_address>/auth/file_name.htm`

    b. ***Enter HTML:*** (to add a combination of resource files, such as logos and HTML links)

       Type HTML content directly into the **Right Frame Content** field.

       To reference any resource file you have already uploaded in the **File Upload** tab as part of the HTML content (including images, JavaScript files, and CSS files) use the following formats:

       To reference a link to an uploaded HTML file:

       ```
       <a href="file_name.html"> file_name.html </a>
       ```

       To reference an image file (such as a JPEG file) enter:

       ```
       <img src="file_name.jpg">
       ```

14. Click **Update** to commit the changes made on the Right Frame page, then click **View** to see the login page with the updated changes.

Enabling Web Client for Local Login Page

The web client option can be enabled for all deployments, but is required for L3 OOB.

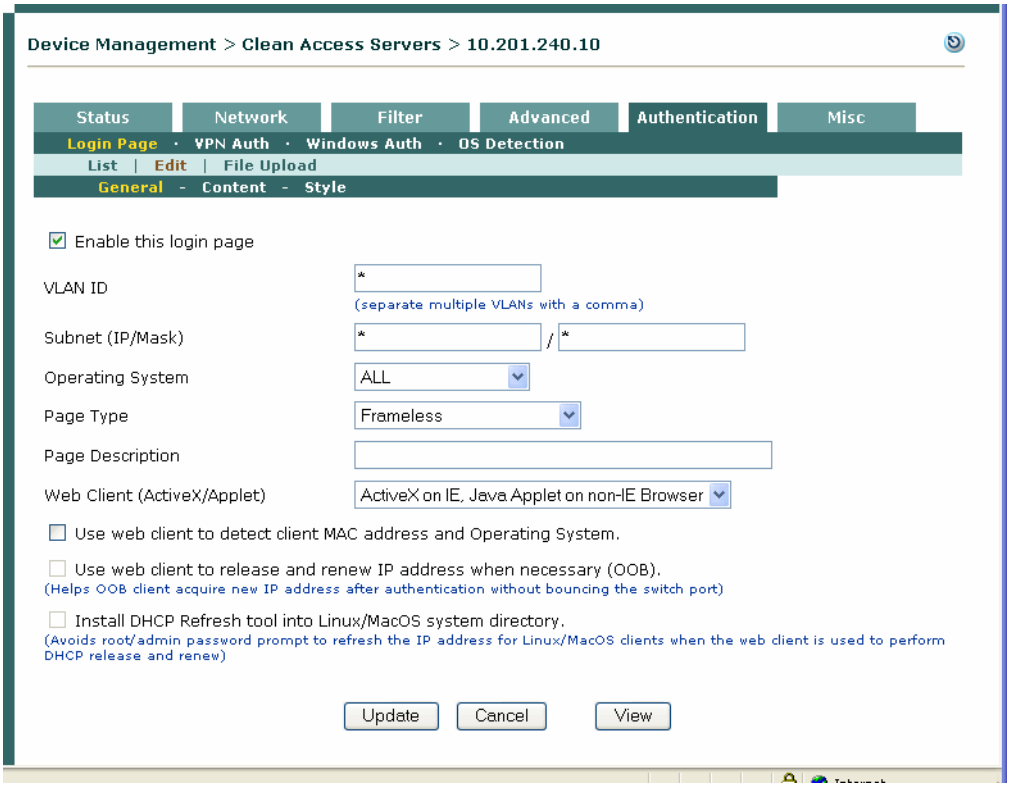
To set up the Cisco NAC Appliance for L3 out-of-band (OOB) deployment, you must enable the login page to distribute either an ActiveX control or Java Applet to web login users who are multiple L3 hops away from the CAS. The ActiveX control/Java Applet is downloaded when the user performs web login and is used to obtain the correct MAC address of the client. In OOB deployment, the CAM needs the correct client MAC address to control the port according to Certified List and/or device filter settings of the Port Profile.

With release 4.1, DHCP IP addresses can be refreshed for client machines using the 4.1.0.0+ Clean Access Agent, or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. This feature is intended to facilate NAC Appliance OOB deployment in VoIP environments.

Note For complete details, refer to "Configuring User Login Page and Guest Access " in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

1. Go to **Administration > User Pages > Login Page > Edit | General**

Figure 10-3 Enable ActiveX/Java Applet for L3 OOB



2. From the **Web Client (ActiveX/Applet)** dropdown menu, choose one of the following options. For "Preferred" options, the preferred option is loaded first, and if it fails, the other option is loaded. With Internet Explorer, Active X is preferred because it runs faster than the Java Applet.
   - **ActiveX Only**—Only runs Active X. If Active X fails, does not attempt to run Java Applet.

- **Java Applet Only**—Only runs Java Applet. If Java Applet fails, does not attempt to run Active X.
- **ActiveX Preferred**—Runs Active X first. If Active X fails, attempts to run Java Applet.
- **Java Applet Preferred**—Runs Java Applet first. If Java Applet fails, attempts to run Active X.
- **ActiveX on IE, Java Applet on non-IE Browser** (Default)—Runs Active X if Internet Explorer is detected, and runs Java Applet if another (non-IE) browser is detected. If Active X fails on IE, the CAS attempts to run a Java Applet. For non-IE browsers, only the Java Applet is run.

Two options need to be checked to use the ActiveX/Applet webclient to refresh the client's IP address:

3. Click the checkbox for "**Use web client to detect client MAC address and Operating System.**"
4. Click the checkbox for "**Use web client to release and renew IP address when necessary (OOB)**" to release/renew the IP address for the OOB client after authentication without bouncing the switch port.
5. When use of the web client is enabled for IP address release/renew, for Linux/Mac OS X clients, you can optionally click the checkbox for " **Install DHCP Refresh tool into Linux/MacOS system directory.**" This will install a DHCP refresh tool on the client to avoid the root/admin password prompt when IP address is refreshed.
6. Click **Update** to save settings.

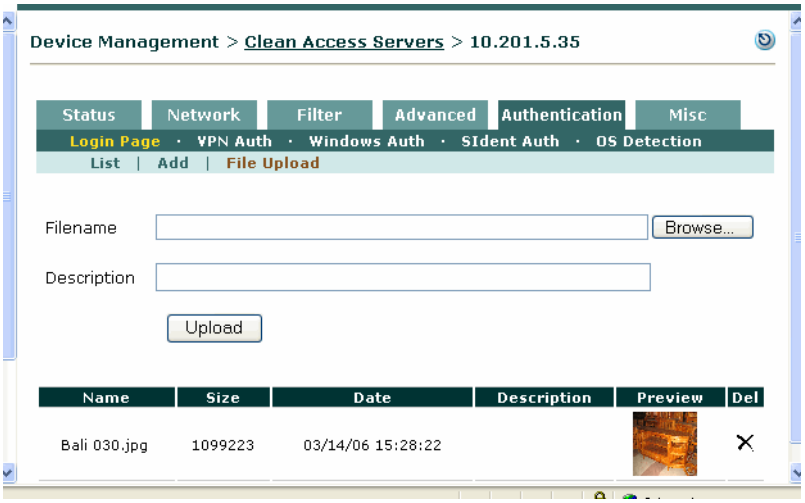
Note To use this feature. "Enable L3 support" must be enabled under **Device Management > CCA Servers > Manage[CAS_IP] > Network > IP**.

See Chapter 3, "Configuring Layer 3 Out-of-Band (L3 OOB)" and the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Local File Upload

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication** > **Login Page**.
2. Make sure the **Override Global Settings** option is enabled.
3. Click **File Upload**.

Figure 10-4 Upload Local File to CAS



4. Browse to a logo image file or other resource file on your workstation and select it in the **Filename** field.
5. Optionally enter text in the **Description** field.
6. Click **Upload**. The file should appear in the resources list.

Note

- Files uploaded to a specific Clean Access Server using **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Login Page > File Upload** are available to the Clean Access Manager and the local Clean Access Server only. On the Clean Access Server, uploaded files are located under `/perfigo/access/tomcat/webapps/auth`.
- Files uploaded to the CAM using **Administration > User Pages > File Upload** are available to the Clean Access Manager and all Clean Access Servers. These files are located under `/perfigo/control/tomcat/normal-webapps/upload` in the CAM.
- Files uploaded to the CAM prior to 3.6(2)+ are not removed and continue to be located under /perfigo/control/tomcat/normal-webapps/admin.

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for further details.

Enable Active Directory SSO Login

See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for complete information on configuring Active Directory Single Sign-On (SSO).

Enable Windows NetBIOS SSO Login

With Windows NetBIOS SSO login (formerly known as "Transparent Windows" login), users who are authenticated in their Windows domain can be automatically logged into the trusted network.

Note The feature has been deprecated. It is recommended to configure Active Directory SSO instead. Refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Implementing Windows NetBIOS SSO login involves several steps:

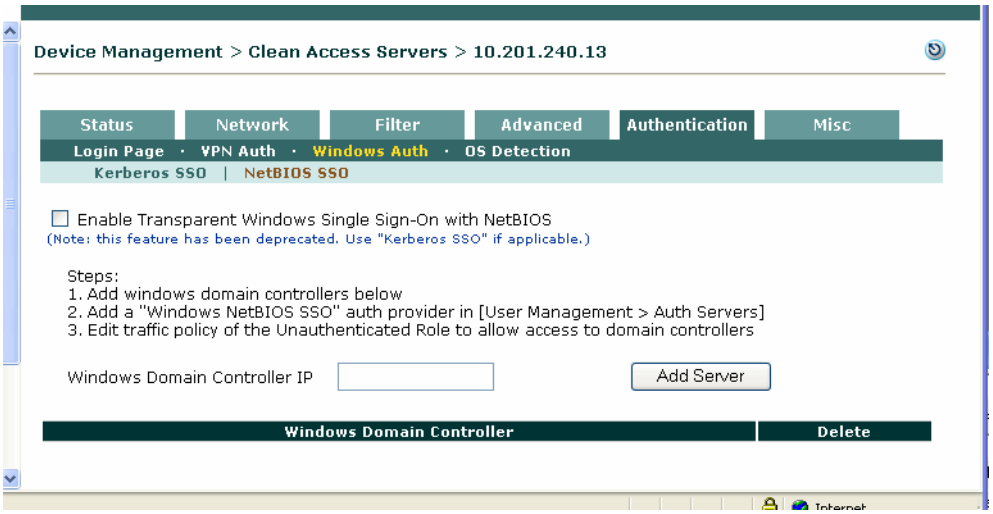
1. Add a Windows NetBIOS SSO authentication provider to the list of authentication servers in the CAM.
   (See Chapter 6, "User Management: Auth Servers" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.)
2. Modify the policy of the Unauthenticated role to allow users access to the domain controller.
   (See Chapter 8, "User Management: Traffic Control, Bandwidth, Schedule" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.)
3. Enable Windows NetBIOS SSO Login and specify the Windows domain controller in the CAS management pages (see steps below).

Note With Windows NetBIOS SSO, only authentication can be done— posture assessment, quarantining, remediation, do not apply. However, the user only needs to perform Ctrl-Alt-Dlt to login.

To configure the Windows domain controller:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication** > **Windows Auth > NetBIOS SSO** the CAS for which you want to enable transparent Windows login.

Figure 10-5 Enable Transparent Windows Login



2. Click the **Enable Transparent Windows Single Sign-On with NetBIOS** checkbox and then click **Update**.
3. Type the IP address of your Windows domain controller in the **Windows Domain Controller IP** field.
4. Click **Add Server**.

OS Detection

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. The platform information from JavaScript or the OS fingerprinting from the TCP/IP handshake can also be used to determine the client OS. This enhanced OS fingerprinting feature is intended to prevent users from changing identification of their client operating systems through manipulating HTTP information. Note that this is a "passive" detection technique (accomplished without Nessus) that only inspects the TCP handshake and is not impacted by the presence of a personal firewall.

Additionally, "**Current Version of OS Detection Fingerprint**" updates are downloaded via the **Device Management > Clean Access > Updates** interface. Updates to OS Detection Fingerprints (or signatures) are made as new operating systems become available for Windows machines. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for additional details.

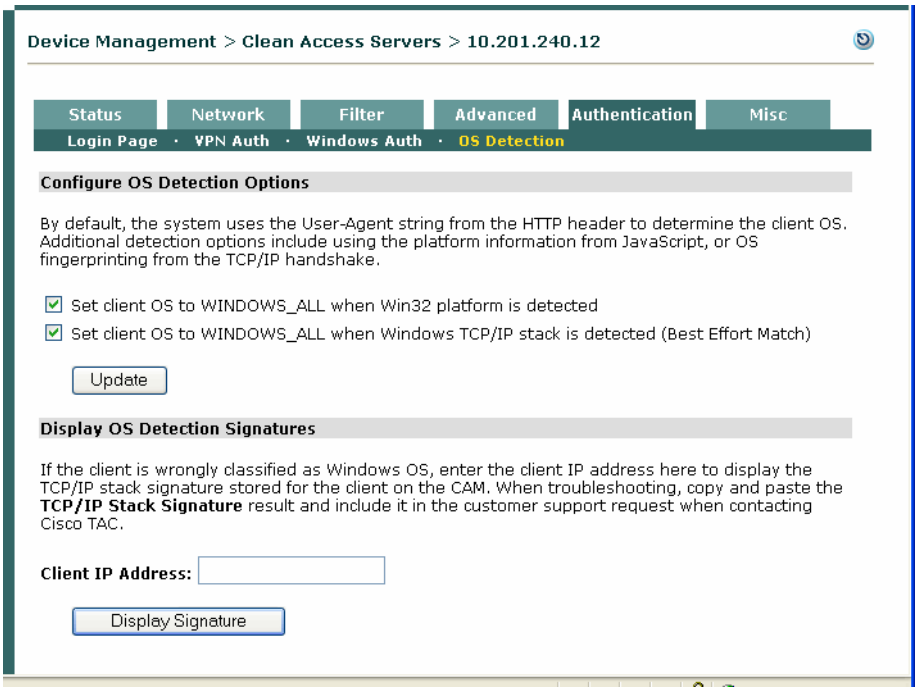
If the client is wrongly classified as Windows OS, you can submit the client IP address under **Display OS Detection Signatures** to display the TCP/IP stack signature stored for the client on the CAM. When troubleshooting, the **TCP/IP Stack Signature** result can copied/pasted for inclusion in the customer support request when contacting Cisco TAC.

Note The OS detection/fingerprinting feature uses both browser user-agent string and TCP/IP stack information to try to determine the OS of the client machine. While the detection routines will attempt to find the best match, it is possible that the OS may be detected incorrectly if the end-user modifies the TCP/IP stack on the client machine and changes the user-agent string on the browser. If there is concern regarding malicious users evading the OS fingerprinting/detection mechanisms, then administrators are advised to use network scanning in order to confirm the OS on the machine. If, for any reason, it is not possible or not desirable to use network scanning, then network administrators should consider pre-installing the Clean Access Agent on machines.

To Set OS Detection Settings:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection** in the CAS management pages of the web console.

Figure 10-6 OS Detection



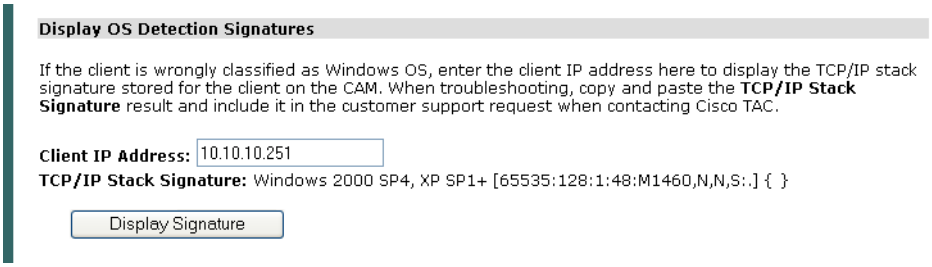
2. Click the checkbox for **Set client OS to WINDOWS_ALL when Win32 platform is detected** to add this as an additional detection option.
3. Click the checkbox for **Set client OS to WINDOWS_ALL when Windows TCP/IP stack is detected** (Best Effort Match) to add this as an additional detection option.
4. Click **Update**.

To Troubleshoot OS Detection Signatures:

When troubleshooting, the TCP/IP Stack Signature result can copied/pasted for inclusion in the customer support request when contacting Cisco TAC.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection**

Figure 10-7 Display TCP/IP Stack Signature



2. In the **Client IP Address** field, type the client IP address to be tested.
3. Click **Display Signature**. The OS signature result displays in the **TCP/IP Stack Signature** field.
4. Copy and paste the **TCP/IP Stack Signature** result to your support request when contacting Cisco TAC.

Local Clean Access Settings

This chapter describes local settings that can be configured at the CAS level for Clean Access implementation For complete information on Clean Access configuration in the CAM web console, see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*. Topics in this chapter include:

Overview

Most elements of Clean Access, such as login pages, Nessus scan plugin behavior, Clean Access Agent requirements, and Clean Access user roles, are configured at the global level for all CASes. However, certain tasks can also be performed at the local level for an individual CAS. These include the following.

- Clearing certified devices

  The Clean Access module on each Clean Access Server **automatically** adds devices to the Certified Devices list after the user authenticates and the device passes network scanning with no vulnerabilities found and/or meets Clean Access Agent requirements. Certified devices are considered clean until removed from the list. You can remove devices at a specified time or interval from the Certified Devices list in order to force them to repeat network scanning/Agent checking. Note that devices for Clean Access Agent users are always scanned for requirements at each login.

- Adding/clearing exempt devices

  An exempt device is one which is never subject to Clean Access requirements. You can specify a device as exempt to allow it to bypass Clean Access requirements, or you can clear an exempt device to force it to meet Clean Access requirements. Adding or clearing exempt devices is always done **manually**.

- Specifying floating devices

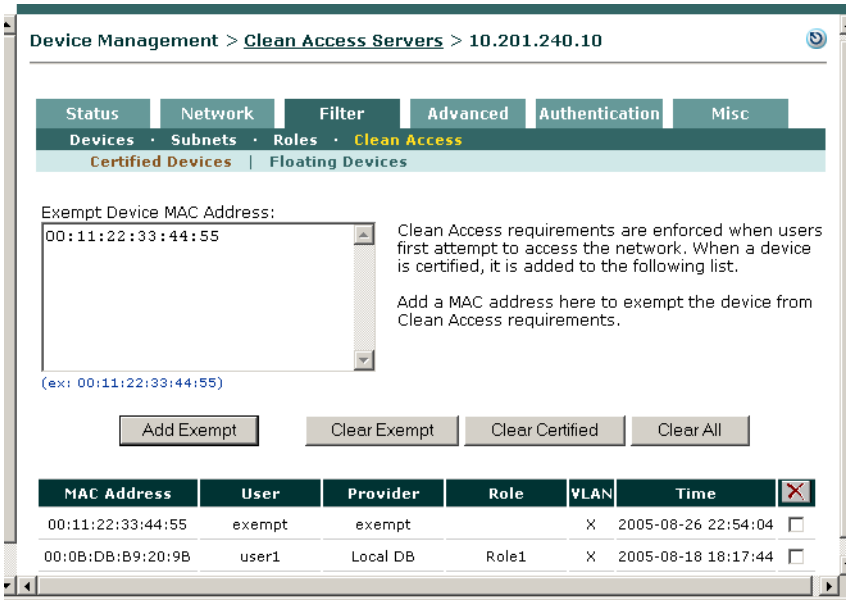
  A floating device requires Clean Access certification at every login and is certified only for the duration of a user session. Floating devices are always added manually.

Add Exempt Devices

Designating a device as exempt is the way a device can be **manually** added to the automatically-generated Certified Devices list. The CAS only adds a device to the Certified Devices list if the device has passed network scanning with no vulnerabilities found, or met Clean Access Agent system requirements, or both. Once added to the list, the device is considered clean and therefore exempt from having to go through certification while its MAC address remains on the Certified Devices list. Adding an exempt device in effect bypasses the automated Clean Access process to certify that the device you are adding to the list is clean.

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**.

Figure 11-1 Certified Devices (Local)



2. Type the MAC address of the exempt device in the text field. Use line breaks to separate multiple addresses.
3. Click **Add Exempt**.

Clear Exempt Devices

Clearing an exempt device means you are removing it from the Certified Devices list and forcing it to go through Clean Access certification. Because exempt devices are manually added to the list, they must also be manually removed. This also means that an exempt device on the Certified Devices list is protected from being automatically removed when the global Certified Devices Timer is used to clear the list at regularly scheduled intervals.

To manually clear exempt devices from the list:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see Figure 11-1).
2. Click **Clear Exempt**. All exempt devices for this Clean Access Server will be cleared from the list.

Clear Certified Devices

Devices are added to the Certified Devices list by the Clean Access Server and are considered clean until removed from the list.

If a certified device is moved from one CAS to another, it must go through Clean Access certification again for the new CAS unless it has been manually added as an exempt device at the global level for all CASes. This allows for the case where one CAS has more restrictive Clean Access requirements than another.

The CAM maintains the central Certified Devices list, which stores device information according to the certifying Clean Access Server. The CAM then publishes each Clean Access Server's certified devices to the appropriate CAS as well as any globally exempt devices to all Clean Access Servers.

Though devices can only be certified and added to the list per CAS, you can remove certified devices globally from all Clean Access Servers or locally from a particular CAS. Clearing certified devices means you want to force the devices to repeat the Clean Access scanning/requirement checking.

- Global level (auto) — You can clear the list at regular intervals using the Certified Devices Timer form (**Device Management > Clean Access > Certified Devices > Timer)**
- Global level (manual) — You can manually clear the Certified Device list using the global form **Device Management > Clean Access > Certified Devices**.
- Local level (manual) — You can manually clear certified devices for a specific Clean Access Server using the local form **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**

Note

- Clearing the Certified Device list either manually or automatically also logs the user off the network.
- Removing a user from **Monitoring > Online Users > View Online Users** does not remove the client from the Certified Devices list. This allows the user to log in again without forcing the client device to go through the Clean Access certification process when it is still considered clean.

To manually clear devices from the list for a specific Clean Access Server:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see Figure 11-1).
2. Click **Clear Exempt** to remove the devices that were added manually (using **Add Exempt**).
3. Click **Clear Certified** to remove the devices that were added to the list by meeting the Clean Access criteria.
4. Click **Clear All** to remove both types.
5. Remove individual users by selecting the checkbox next to the user's MAC address and clicking the **Kick Individual User** ( ) button.

Note Only certified devices for the particular CAS will appear in the local list. To view certified devices for all Clean Access Servers, go to **Device Management > Clean Access**.

Specify Floating Devices

A floating device is certified only for the duration of a user session. Once the user logs out, the next user of the device needs to be certified again. Floating devices are useful for shared equipment, such as kiosk computers or wireless cards loaned out by a library.

You can also specify devices that are never exempt from certification requirements by MAC address. This is useful for multi-user devices, such as dialup routers that channel multi-user traffic from the untrusted (managed) network. In such cases, the Clean Access Server will see only the MAC address of that device as the source address of traffic from the trusted network. If the device is not configured as a floating device, this means that after the first user is certified, additional users will be unintentionally exempt from certification. By configuring the router's MAC address as a floating device that is never certified, you can ensure that each user accessing the network through the device is individually assessed for vulnerabilities/requirements met.

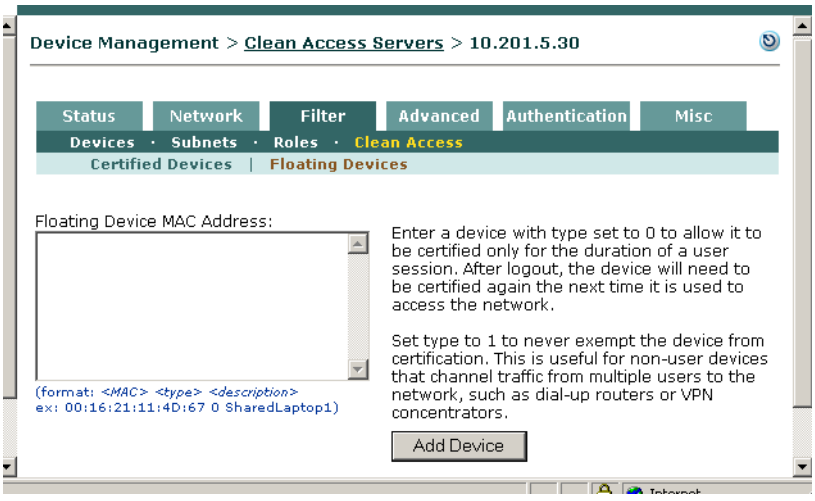
In this case, the users are distinguished by IP address. Note that users must have different IP addresses for this to work. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

See also Add VPN Concentrator as a Floating Device, page 8-9.

To specify a local floating device:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Floating Devices**.

Figure 11-2 Floating Devices (Local)



2. Specify a floating device by MAC address in the form:

   <MAC> <type> <description>

   Where:

   - *MAC* is the MAC address of the device (in standard hexadecimal MAC address format, e.g., `00:16:21:23:4D:00`).
   - *type* is either:

     0 - for session-scope certification, or

     1 - if the device should never be considered certified

– *description* is an optional description of the device.

Be sure to include spaces between each element and use line breaks to separate multiple entries. For example:

```
00:16:21:23:4D:00 0 LibCard1
00:16:34:21:4C:00 0 LibCard2
00:16:11:12:4A:00 1 Router1
```

3. Click **Add Device** to save the setting.

To remove a floating MAC address, click the **Delete** icon (✕) next to the address.

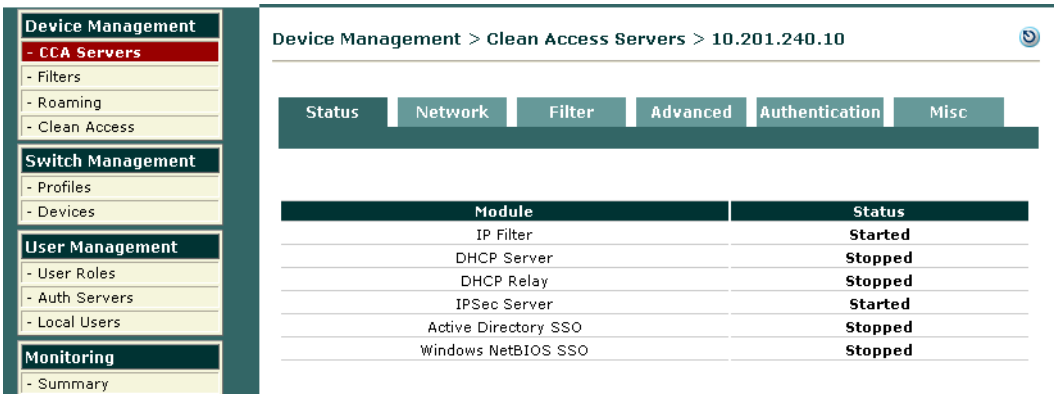
Administer the Clean Access Server

This chapter describes Clean Access Server (CAS) administration. Topics include:

Status Tab

The Status tab of the CAS management pages displays high-level status information on which modules are running in the Clean Access Server.

Figure 12-1 CAS Management Pages Status Tab



- **IP Filter**—An IP packet filter that analyzes packets to ensure that they come from valid, authenticated users.
- **DHCP Server**—The CAS's internal DHCP (Dynamic Host Configuration Protocol) server.
- **DHCP Relay**—The module that relays address requests and assignments between clients and an external DHCP server.
- **IPSec Server** — The module for establishing a secure, IP Security-based channel between the CAS and a client device. The module encrypts and decrypts data passed between the client and server.

- **Active Directory SSO**—The module that enables Active Directory Single Sign-On for authenticated Windows users.
- **Windows NetBIOS SSO**—The module that enables Windows NetBIOS login for authenticated Windows users.

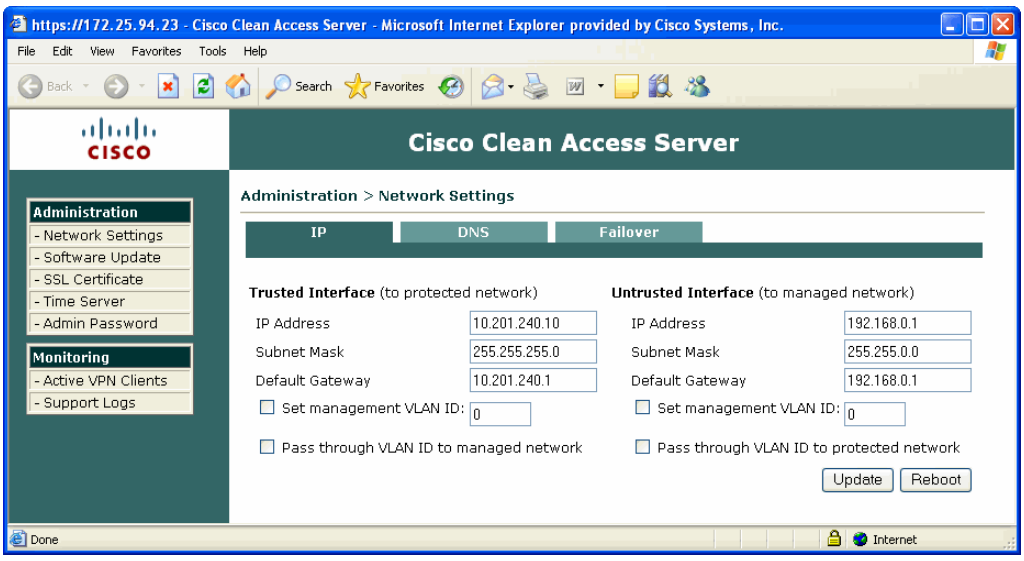
Clean Access Server Direct Access Web Console

The CAS management pages of the CAM web admin console (Figure 12-1) are the primary configuration interface for the Clean Access Server(s). However, each Clean Access Server has its own web admin console that allows configuration of certain limited Administration and Monitoring settings directly on the CAS (Figure 12-2). The CAS direct access web console is primarily used to download CAS support logs or r configure pairs of Clean Access Servers for High Availability. See Chapter 13, "Configuring High Availability (HA)" for details. If the CAS management pages become unavailable, you can also use the direct console interface for other functions such as managing SSL certificates for the CAS or performing system upgrade.

To access the Clean Access Server's direct access web admin console:

1. Open a web browser and type the IP address of the CAS's trusted (eth0) interface in the URL/address field: **https://<CAS_eth0_IP>/admin** (for example, `https://172.16.1.2/admin`)
2. Accept the temporary certificate and log in as user `admin` (default password is `cisco123`).

Figure 12-2 CAS Direct Access Web Admin Console



Note

- Make sure to precede the CAS IP address with "https://" and append it with "/admin"; otherwise you will see the redirect page for web login users.
- For security purposes, it is recommended to change the default password for the CAS web console.

Note that almost all of the settings in the CAS web console can be configured via the CAS management pages in the CAM web admin console, with the exception of the **Failover**, **DHCP Failover**, **Admin Password**, and **Support Logs.** The CAS direct access web console provides the following Administration pages for the local CAS:

- Network Settings (IP, DNS, Failover, DHCP Failover)
- Software Update
- SSL Certificates (Generate Temporary Certificate, Import Certificate, Export CSR/Private Key/Certificate)
- Time Server
- Admin Password

The **Monitoring** module of the CAS direct access console provides the following pages:

- Active VPN Clients
- Support Logs

Note For High Availability CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the standby CAS unit through its direct access web console. These settings include updating the SSL certificate, system time, time zone, DNS, or Service IP. See IP Form, page 5-9 and Modifying High Availability Settings, page 13-23 for details.

Manage CAS SSL Certificates

The elements of Cisco NAC Appliance communicate securely over Secure Socket Layer (SSL) connections. Cisco NAC Appliance uses SSL connections for the following:

- Between the CAM and the CAS
- Between the CAM and the browser accessing the CAM web admin console
- Between the CAS and end-users connecting to the CAS
- Between the CAS and the browser accessing the CAS direct access web console

During installation, the configuration utility script for both the CAM and CAS requires you to generate a temporary SSL certificate for the server being installed (CAM or CAS). A corresponding private key is also generated with the temporary certificate.

For a production deployment, you will typically want to replace the temporary certificate for the **Clean Access Server** with a CA-signed SSL certificate, since the CAS certificate is the one that is visible to the end user. Otherwise, if the Clean Access Server has a temporary certificate, users accessing the network will have to explicitly accept the certificate from the CAS each time they login.

Note Due to Java version dependencies on the system software, Cisco Clean Access only supports 1024- and 2048-bit key lengths for SSL certificates.

For the Clean Access Manager, it is not necessary to use a CA-signed certificate and you can continue to use a temporary certificate, if desired. For details on managing SSL certificates for the CAM, see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guid*e.

The following sections describes how to manage SSL certificates for the CAS:

- Generate Temporary Certificate, page 12-6
- Export CSR/Private Key/Certificate, page 12-7
- Verify Currently Installed Private Key and Certificates, page 12-8
- Import Signed Certificate, page 12-11
- View Certificate Files Uploaded for Import, page 12-13
- Troubleshooting Certificate Issues, page 12-13

Note You cannot use a CA-signed certificate that you bought for the Clean Access Manager on the Clean Access Server. You must buy a separate certificate for each Clean Access Server.

Web Console Pages for SSL Certificate Management

The actual CAM SSL certificate files are kept on the CAM machine, and the CAS SSL certificate files are kept on the CAS machine. After installation, the CAM and CAS certificates can be managed from the following web console pages (respectively):

Clean Access Manager Certificates:

- **Administration > CCA Manager > SSL Certificate**

Clean Access Server Certificates:

- CAS management pages: **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**, or
- CAS direct access console: **Administration > SSL Certificate**

Note You can use the CAS direct access console interface if the CAS management pages become unavailable. See Clean Access Server Direct Access Web Console, page 12-2 for further details.

The CAS management pages and CAS direct access console provide the same controls and allow you to perform the following SSL certificate-related operations:

- Generate a temporary certificate (and corresponding private key).
- Generate a PEM-encoded PKCS #10 Certificate Signing Request (CSR) based on the current temporary certificate.
- Import and export the private key. The Export Key feature is used to save a backup copy of the Private Key on which the CSR is based. When a CA-signed certificate is returned from the Certificate Authority and imported into the CAS, this Private Key must be used with it.

Note For High Availability CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the standby CAS unit through its direct access web console. These settings include updating the SSL certificate, system time/time zone, DNS, or Service IP. See Clean Access Server Direct Access Web Console, page 12-2 and Modifying High Availability Settings, page 13-23 for details.

Typical Steps for CAS New Installs

For new installations, the typical steps for managing the CAS certificate are as follows:

1. Synchronize time

   After CAM and CAS installation, make sure the time on the CAM and CAS is synchronized before regenerating the temporary certificate on which the Certificate Signing Request will be based. See the next section, Synchronize System Time, page 12-16, for details.

2. Check DNS settings for the CAS

   If planning to use the DNS name instead of the IP address of your servers for CA-signed certs, you will need to verify the CAS settings and regenerate a temporary certificate. See Regenerating Certificates for DNS Name Instead of IP, page 12-15 for details.

3. Generate Temporary Certificate, page 12-6

   A temporary certificate and private key are automatically generated during CAS installation. If changing time or DNS settings on the CAS, regenerate the temporary certificate and private key prior to creating the Certificate Signing Request.

4. Export (Backup) the private key to a local machine for safekeeping/backup.

   It is a good idea to always back up the private key corresponding to the current temporary certificate to a local hard drive for safekeeping **before** you generate and export the Certificate Signing Request. See Export CSR/Private Key/Certificate, page 12-7.

5. Export (save) the Certificate Signing Request (CSR) to a local machine.
   See Export CSR/Private Key/Certificate, page 12-7.

6. Send the CSR file to a Certification Authority (CA) authorized to issue trusted certificates.

7. After the CA signs and returns the certificate, import the CA-signed certificate to your server.

   When the CA-signed certificate is received from the CA, upload it as PEM-encoded file to the CAS temporary store. See Import Signed Certificate, page 12-11.

8. If necessary, upload any required intermediate CA certificate(s) as a single PEM-encoded file to the CAS temporary store.

9. Click **Verify and Install Uploaded Certificates** to verify the entire certificate chain and private key in the temporary store and install the verified certificates to the CAS.

10. Test as a client accessing the Clean Access Server.

Note Make sure the CA-signed certificate you are importing is the one with which you generated the CSR and that you have NOT subsequently generated another temporary certificate. Generating a new temporary certificate will create a new private-public key combination. In addition, always export and save the private key to a secure location when you are generating a CSR for signing (for safekeeping and to have the private key handy).

For additional details, see also Troubleshooting Certificate Issues, page 12-13.

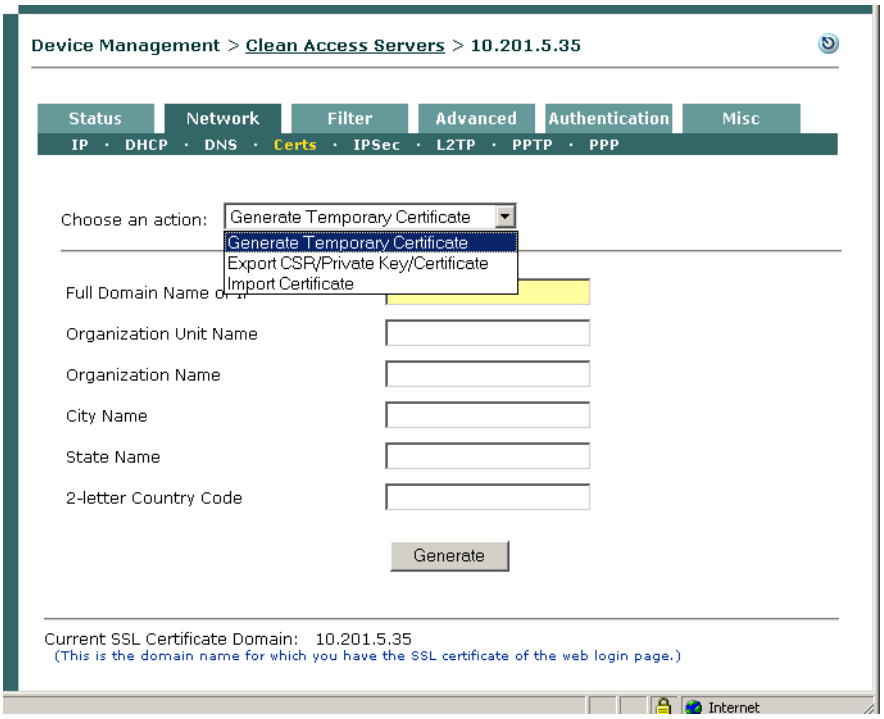
Generate Temporary Certificate

The following procedure describes how to generate a new temporary certificate for the CAS. Keep in mind that if the Clean Access Server has a temporary certificate, users accessing the network will have to explicitly accept the certificate from the CAS at each login. After generating a temporary certificate, you can generate a Certificate Signing Request (CSR) suitable for submission to a Certification Authority (CA). See also Regenerating Certificates for DNS Name Instead of IP, page 12-15 for additional details.

To generate a certificate:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**.
2. If not already selected, choose **Generate Temporary Certificate** from the **Choose an action** dropdown menu.

Figure 12-3 Certs—Generate Temporary Certificate



3. Type appropriate values for the form fields:
   - **Full Domain Name or IP** – The fully qualified domain name or IP address of the CAS for which the certificate is to apply. For example: `caserver.<your_domain_name>`
   - **Organization Unit Name** – The name of the unit within the organization, if applicable.
   - **Organization Name** – The legal name of the organization.
   - **City Name** – The city in which the organization is legally located.
   - **State Name** – The full name of the state in which the organization is legally located.
   - **2-letter Country Code** – The two-character, ISO-format country code, such as GB for Great Britain or US for the United States.
4. When finished, click **Generate**. This generates a new temporary certificate and new private key.

Note The **Current SSL Certificate Domain: <IP or domain name>** field at the bottom of each form displays the IP address or domain name of the current SSL certificate being used to access the web console page displayed. For example, if you are accessing the SSL Certificate management pages of a CAS, the domain name or IP address that is on the SSL certificate of that CAS will be shown. If accessing the SSL Certificate management pages of the CAM, the domain name/IP on the SSL certificate of the CAM will be shown.

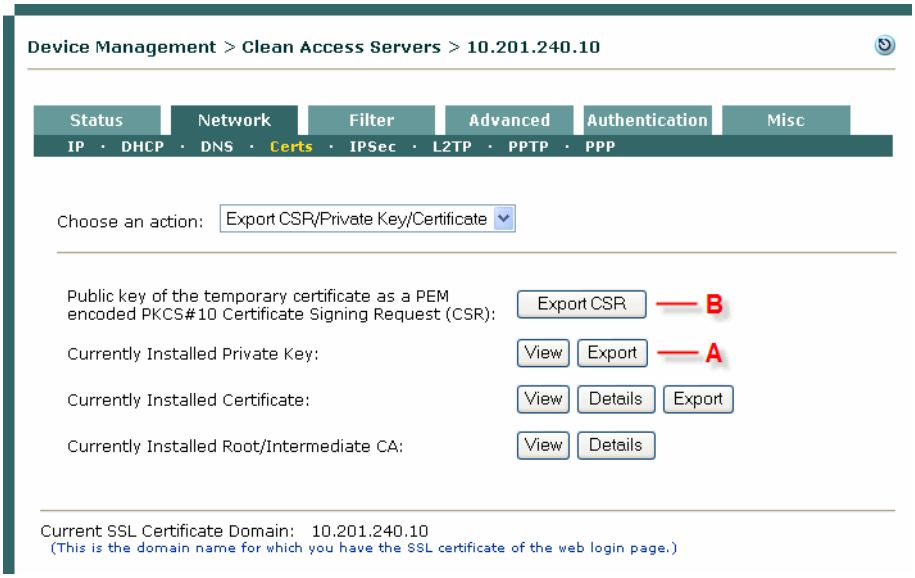
Export CSR/Private Key/Certificate

Exporting a CSR generates a PEM-encoded PKCS#10-formatted Certificate Signing Request suitable for submission to a certificate authority. The CSR will be based on the temporary certificate and private key currently in the keystore database.

To create a certificate request:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** (Figure 12-4).
2. Choose **Export CSR/Private Key/Certificate** from the **Choose an action** dropdown menu.

Figure 12-4 Certs —Export CSR/Private Key/Certificate



3. Create a backup of the private key used to generate the request by clicking the **Export** button for **Currently Installed Private Key** (A) in the Export CSR/Private Key/Certificate form. You are prompted to save or open the file (see Filenames for Exported Files, page 12-8). Save it to a secure location.

Note Cisco Clean Access only supports 1024- and 2048-bit key lengths for SSL certificates.

4. Click **Export CSR** (B). A certificate signing request file for the CAS is generated and made available for downloading (see Filenames for Exported Files, page 12-8).

Note This step will generate a certificate request based on the currently installed (temporary) certificate and private key pair. Make sure these are the ones for which you want to submit the CSR to the certificate authority.

5. **Save** the CSR file to your hard drive (or **Open** it immediately in a text editor if you are ready to fill out the certificate request form). Use the CSR file to request a certificate from a certificate authority. When you order a certificate, you may be asked to copy and paste the contents of the CSR file into a CSR field of the order form.
6. When you receive the CA-signed certificate back from the certification authority, you can import it into the Clean Access Server as described in Import Signed Certificate, page 12-11.
After the CA-signed cert is imported, the "currently installed certificate" is the CA-signed certificate. You can always optionally **Export** the **Currently Installed Certificate** if you need to access a backup of this certificate later.

Note The **Current SSL Certificate Domain: <IP or domain name>** field at the bottom of each form displays the IP address or domain name of the current SSL certificate being used to access the web console page displayed. For example, if you are accessing the SSL Certificate management pages of a CAS, the domain name or IP address that is on the SSL certificate of that CAS will be shown. If accessing the SSL Certificate management pages of the CAM, the domain name/IP on the SSL certificate of the CAM will be shown.

Filenames for Exported Files

File names for SSL Certificate files that can be exported from the CAS are as follows:

File Name [1]	Description
secsmart_csr.pem	CAS Certificate Signing Request (CSR)
secsmart_key.pem	CAS Currently Installed Private Key
secsmart_crt.cer [2]	CAS Currently Installed Certificate

1. For release 3.6.0.1 and below filename extensions are .csr instead of .pem.
2. For release 3.6(1) only, the filename is secsmart_crt.pem.

Verify Currently Installed Private Key and Certificates

You can verify the following files by viewing them under **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Export CSR/Private Key/Certificate** (Figure 12-4):

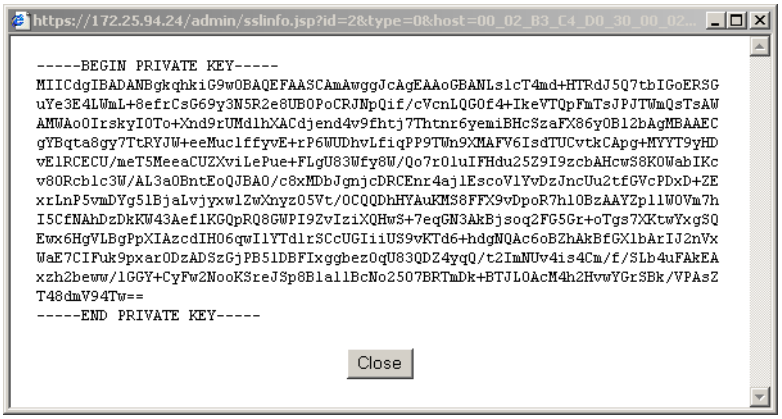
- Currently Installed Private Key
- Currently Installed Certificate
- Currently Installed Certificate Details
- Currently Installed Root/Intermediate CA Certificate
- Currently Installed Root/Intermediate CA Certificate Details

Note You must be currently logged into your web console session to view any certificate files.

On the CAS, if a particular file is not currently installed (for export) or not uploaded (for import), a dialog message "`Unable to read certificate from Clean Access Server`" will appear when you click the **View** or **Details** button. For example, if only a temporary certificate is present on the CAS, this message will appear if you click the View/Details buttons for "Root/Intermediate CA" or "Currently Installed Root/Intermediate CA" on the Import and Export forms, respectively.

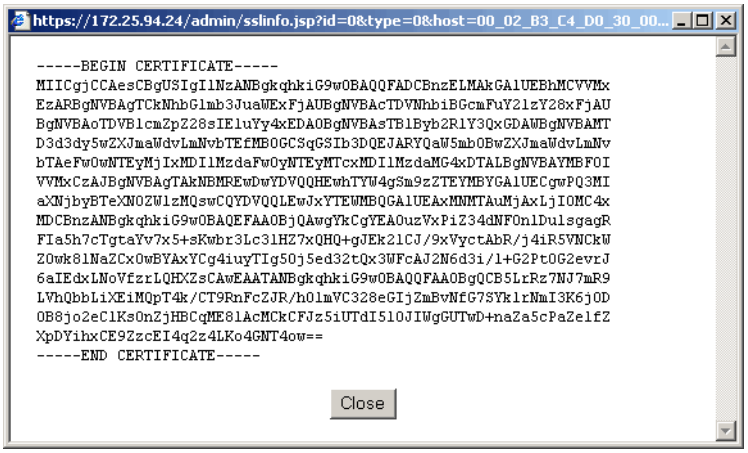
Clicking **View** for "**Currently Installed Private Key**" brings up the dialog shown in Figure 12-5 (BEGIN PRIVATE KEY/END PRIVATE KEY).

Figure 12-5 View Currently Installed Private Key



Clicking **View** for "**Currently Installed Certificate**" brings up the dialog shown in Figure 12-6 (BEGIN CERTIFICATE / END CERTIFICATE).

Figure 12-6 View Currently Installed Certificate



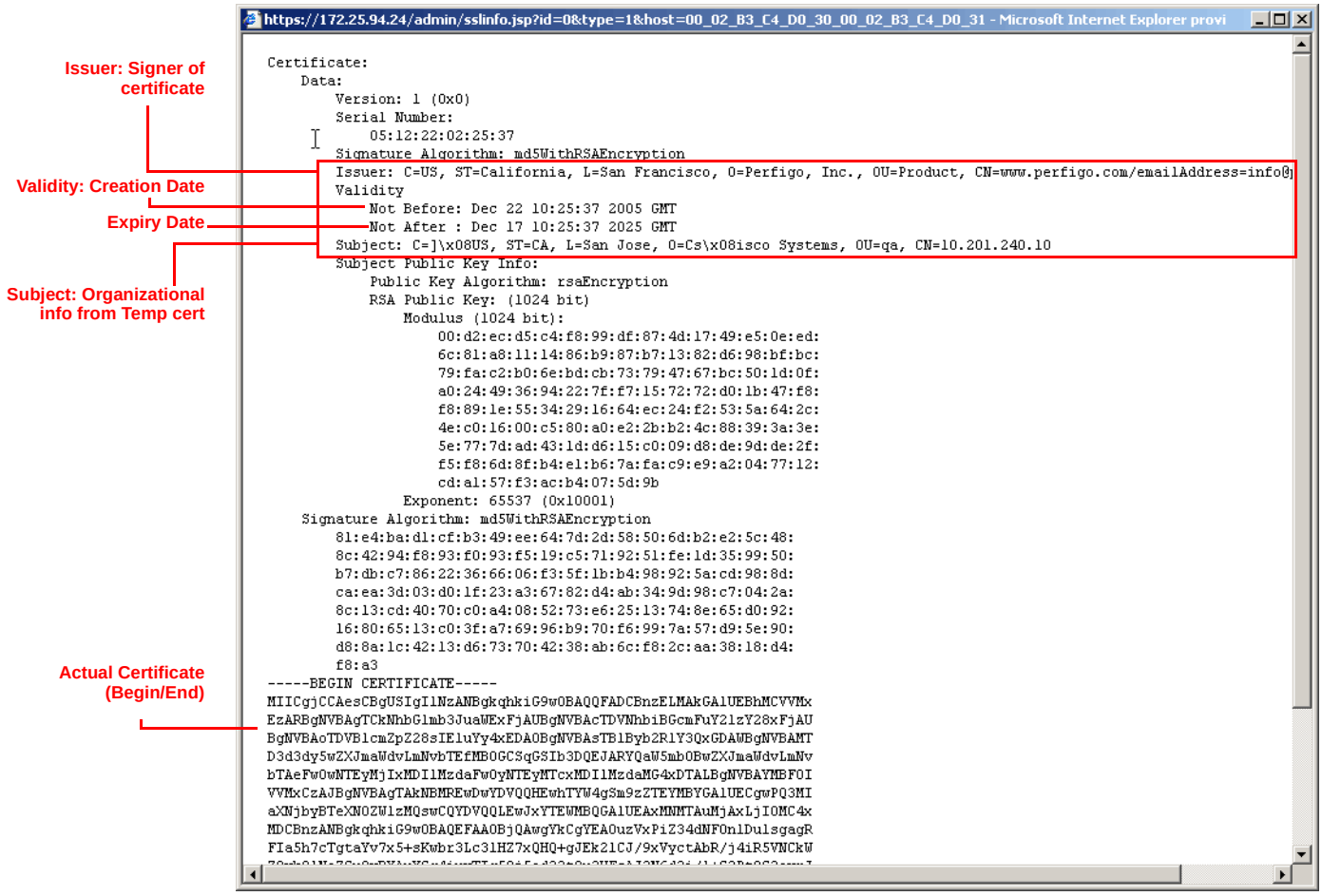
Clicking **Details** for "**Currently Installed Certificate**" brings up the dialog shown in Figure 12-7 ("Certificate:"). The **Currently Installed Certificate Details** form provides an easy way to verify whether you have a temporary or CA-signed certificate. The most important fields to check are:

- **Issuer** —Who signed the current certificate. The temporary certificate generated during installation will have the Issuer information shown in Figure 12-7.
- **Validity**—The creation date ("Not Before:") and expiry date ("Not After":) of the certificate.

Note The time set on the CAS must fall within the creation date/expiry date range set on the SSL certificate of the CAM. The time set on the user machine must fall within the creation date/expiry date range set on the SSL certificate of the CAS.

- **Subject**—The server and organizational information you entered when you generated the temporary certificate.
- **Begin Certificate/End Certificate**—The actual certificate is displayed in this section. It is identical to the information shown when you click **View** "Currently Installed Certificate".

Figure 12-7 View Currently Installed Certificate Details (Example Temporary Certificate)



Clicking **View** or **Details** for "**Currently Installed Root/Intermediate CA Certificate**" will bring up similar dialogs for the root or intermediate certificates you have installed on your CAS.

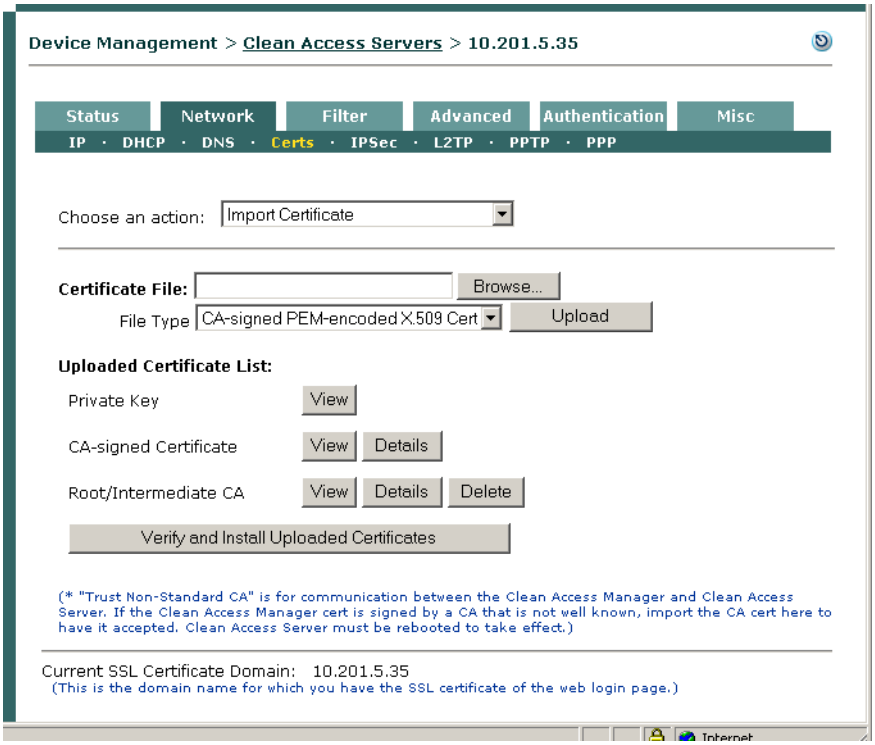
Import Signed Certificate

If you have received a CA-signed PEM-encoded X.509 certificate for the Clean Access Server, you can import it into the Clean Access Server as described here. Before starting, make sure that the root and CA-signed certificate files are in an accessible file directory location. If using a certificate authority for which intermediate CA certificates are necessary, make sure these files are also present and accessible.

To import a CA-signed certificate:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs** (Figure 12-8).
2. Choose **Import Certificate** from the **Choose an action** dropdown menu.

Figure 12-8 Certs —Import Certificate



3. Click the **Browse** button next to the **Certificate File** field and locate the certificate file on your directory system.

Note Make sure there are no spaces in the filename when importing files (you can use underscores).

4. Select the **File Type** from the dropdown menu:
   - **CA-signed PEM-encoded X.509 Cert** — Select this option to upload the PEM-encoded CA-signed certificate.
   - **Root/Intermediate CA** — Select this option to upload the PEM-encoded intermediate CA certificate or root certificate. To install chained certificates (i.e. multiple intermediate CA files):

     a. If the certificate chain is using a different file format (e.g. .p7b), you must convert the chain to PEM format first.

b. Copy and paste the root and intermediate certificate information into a single file, then upload that as the Intermediate CA PEM-encoded file to the CAS.

Note Only one Intermediate CA file can be uploaded to the CAS, and it must be in PEM format.

- **Private Key** — Select this option if you need to upload the Private Key for the CAS (from backup). Typically, you only need to do this if the current Private Key does not match the Private Key used to create the original CSR on which the CA-Signed certificate is based.
- **Trust Non-Standard CA** — On the CAS, select this option if uploading a certificate needed for communication between the CAM and CAS that is signed by a non-standard organization. For example, you may have a non-standard certificate for the CAM that is signed by your institution (e.g. university), but a CA-signed certificate from VeriSign for your CAS. If the Clean Access Manager certificate is signed by a CA that is not well known, import the CA cert using the **Trust Non-Standard CA** option to have it accepted. The Clean Access Server must be rebooted for this to take effect.

5. Click **Upload** to upload the certificate file to the temporary store on the Clean Access Server.
6. Click **Verify and Install Uploaded Certificates** to verify the entire certificate chain and private key in the temporary store and install the verified certificate files to the correct locations in the CAS. If any files are missing, errors will be displayed indicating which files need to be uploaded. For example, if an intermediate CA certificate is required for the certificate authority you are using, upload it to the CAS temporary store in order for the certificate chain to be verified and installed on the CAS.

Note Neither the CAM nor CAS will install an unverifiable certificate chain. You must have delimiters (Begin/End Certificate) for multiple certificates in one file, but you do not need to upload certificate files in any particular sequence because they are verified in the temporary store first before being installed.

7. If you try to upload a root/intermediate CA certificate for the CAS that is already in the list, you may see an error message “this intermediate CA is not necessary” after you click the **Verify and Install Uploaded Certificates** button. You must **Delete** the uploaded **Root/Intermediate CA** in order to remove any duplicate files.

Note The **Current SSL Certificate Domain: <IP or domain name>** field at the bottom of each form displays the IP address or domain name of the current SSL certificate being used to access the web console page displayed. For example, if you are accessing the SSL Certificate management pages of a CAS, the domain name or IP address that is on the SSL certificate of that CAS will be shown. If accessing the SSL Certificate management pages of the CAM, the domain name/IP on the SSL certificate of the CAM will be shown.

View Certificate Files Uploaded for Import

You can verify certificate files you have uploaded to the temporary store for import into the CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Import Certificate** (Figure 12-4), as follows:

- Uploaded Private Key
- Uploaded CA-Signed Certificate
- Uploaded CA-Signed Certificate Details
- Uploaded Root/Intermediate CA Certificate
- Uploaded Root/Intermediate CA Certificate Details

Note You must be currently logged into your web console session to view any certificate files.

On the CAS, if a particular file is not currently installed (for export) or not uploaded (for import), a dialog message "`Unable to read certificate from Clean Access Server`" will appear when you click the **View** or **Details** button. For example, if only a temporary certificate is present on the CAS, the message will appear if you click the View/Details buttons for "Root/Intermediate CA" or "Currently Installed Root/Intermediate CA" on the Import and Export forms, respectively.

Troubleshooting Certificate Issues

Issues can arise during Cisco NAC Appliance certificate management, particularly if there are mismatched SSL certificates somewhere along the certificate chain. Common problems on SSL certificates can be time-oriented (if the clocks are not synchronized on the CAM and CAS, authentication fails), IP-oriented (certificates are created for the wrong interface) or information-oriented (wrong or mistyped certificate information is imported). This section describes the following:

- CAS Cannot Establish Secure Connection to CAM
- Private Key in Clean Access Server Does Not Match the CA-Signed Certificate
- Regenerating Certificates for DNS Name Instead of IP
- Certificate-Related Files

CAS Cannot Establish Secure Connection to CAM

If clients attempting login get the following error message, "Clean Access Server could not establish a secure connection to the Clean Access Manager at <IPaddress or domain> (see Figure 12-9), this commonly indicates one of the following issues:

- The time difference between the CAM and CAS is greater than 5 minutes.
- Invalid IP address
- Invalid domain name
- CAM is unreachable

The time set on the CAM and the CAS must be 5 minutes apart or less. To resolve this issue:

1. Set the time on the CAM and CAS correctly first (see Synchronize System Time, page 12-16)

2. Regenerate the certificate on the CAS using the correct IP address or domain.
3. Reboot the CAS.
4. Regenerate the certificate on the CAM using the correct IP address or domain.
5. Reboot the CAM.

Figure 12-9 Troubleshooting: "CAS Cannot Establish Secure Connection to CAM"

Note If you check `nslookup` and `date` from the CAS, and both the DNS and TIME settings on the CAS are correct, this can indicate that the cacerts file on the CAS is corrupted. In this case it is recommended to back up the existing cacerts file from /usr/java/j2sdk1.4/lib/security/cacerts, then override it with the file from /perfigo/common/conf/cacerts, then perform "service perfigo restart" on the CAS.

Note If the error message on the client is "Clean Access Server is not properly configured, please report to your administrator," this typically is not a certificate issue but indicates that a default user login page has not been added to the CAM. See "Add Default Login Page" in the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

Private Key in Clean Access Server Does Not Match the CA-Signed Certificate

This issue can arise if a new temporary certificate is generated but a CA-signed certificate is returned for the CSR (certificate signing request) generated from a previous temporary certificate and private key pair.

For example, an administrator generates a CSR, backs up the private key, and then sends the CSR to a CA authority, such as VeriSign.

Subsequently, another administrator regenerates a temporary certificate after the CSR has been sent. When the CA-signed certificate is returned from the CA authority, the private key on which the CA-certificate is based no longer matches the one in the Clean Access Server.

To resolve this issue, re-import the old private key and then install the CA-signed certificate.

Regenerating Certificates for DNS Name Instead of IP

If planning to regenerate certificates based on the DNS name instead of the IP address of your servers:

- Make sure the CA-signed certificate you are importing is the one with which you generated the CSR and that you have NOT subsequently generated another temporary certificate. Generating a new temporary certificate will create a new private-public key combination. In addition, always export and save the private key when you are generating a CSR for signing (to have the private key handy).
- When importing certain CA-signed certificates, the system may warn you that you need to import the root certificate (the CA's root certificate) used to sign the CA-signed certificate, or the intermediate root certificate may need to be imported.
- Make sure there is a DNS entry in the DNS server.
- Make sure the DNS address in your Clean Access Server is correct (see Configure DNS Servers on the Network, page 5-17).
- For High-Availability (failover) configurations, use the DNS name for the Service IP (virtual DNS)
- It is recommended to reboot when you generate a new certificate or import a CA-signed certificate.
- When using a DNS-based certificate, if it is not CA-signed, the user will simply be prompted to accept the certificate.

Certificate-Related Files

For troubleshooting purposes, Table 12-1 lists certificate-related files on the Clean Access Server. For example, if the admin console becomes unreachable due to a mismatch of the CA-certificate/private key combination, these files may need to be modified directly in the file system of the Clean Access Server.

Table 12-1 Clean Access Server Certificate-Related Files

File	Description
/root/.tomcat.key	Private key
/root/.tomcat.crt	Certificate
/root/.tomcat.csr	Certificate Signing Request
/root/.chain.crt	Intermediate certificate
/perfigo/common/conf/perfigo-ca-bundle.crt	The root CA bundle

Synchronize System Time

For logging purposes and other time-sensitive tasks (such as SSL certificate generation), the time on the Clean Access Manager and Clean Access Servers needs to be correctly synchronized. The **Time** form lets you set the time on the Clean Access Server and modify the time zone setting for the CAS operating system.

After CAM and CAS installation, you should synchronize the time on the CAM and CAS before regenerating a temporary certificate on which a Certificate Signing Request (CSR) will be based. The easiest way to ensure this is to automatically synchronize time with the time server (**Sync Current Time** button)

Note The time set on the CAS must fall within the creation date/expiry date range set on the CAM's SSL certificate. The time set on the user machine must fall within the creation date /expiry date range set on the CAS's SSL certificate.

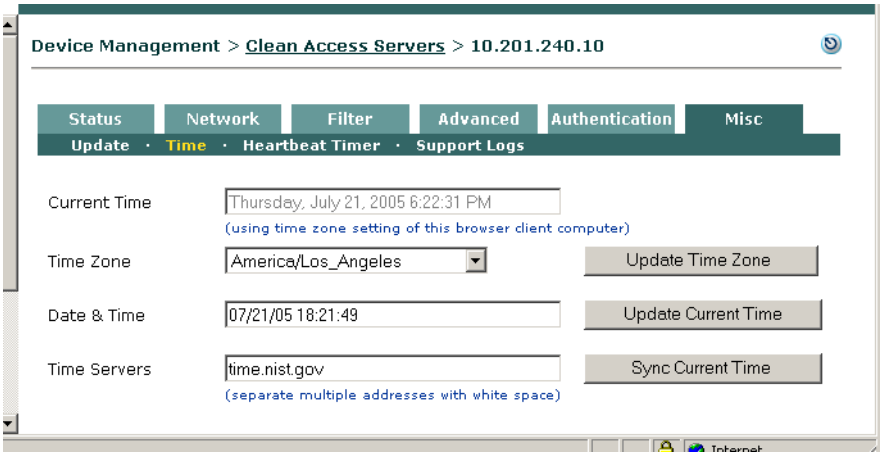
Note For High Availability CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the standby CAS unit through its direct access web console. These settings include updating the SSL certificate, system time/time zone, DNS, or Service IP. See Clean Access Server Direct Access Web Console, page 12-2 and Modifying High Availability Settings, page 13-23 for details.

The time can be modified on the CAM under **Administration > CCA Manager > System Time**. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

To view the current time:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time**.
2. The system time for the Clean Access Server appears in the **Current Time** field.

Figure 12-10 Time Form



There are two ways to adjust the system time —manually, by typing in the new time, or automatically, by synchronizing from an external time server.

To manually modify the system time:

1. In the **Time** form of the **Misc** tab, either:
2. Type the time in the **Date & Time** field and click **Update Current Time**. The time should be in the form: `mm/dd/yy hh:ss PM/AM`
3. Or, click the **Sync Current Time** button to have the time updated by the time servers listed in the **Time Servers** field.

To automatically synchronize with the time server:

The default time server is the server managed by the National Institute of Standards and Technology (NIST), at **time.nist.gov**. To specify another time server:

1. In the **Time** form of the **Misc** tab type the URL of the server in the **Time Servers** field. The server should provide the time in NIST-standard format. Use a space to separate multiple servers.
2. Click **Update Current Time**.

If more than one time server is listed, the CAS tries to contact the first server in the list when synchronizing. If available, the time is updated from that server. If it is not available, the CAS tries the next one, and so on, until a server is reached.

The CAS will then automatically synchronize time with the configured NTP server at periodic intervals.

To change the time zone of the server system time:

1. In the **Time** form of the **Misc** tab, choose the new time zone from the **Time Zone** dropdown menu.
2. Click **Update Time Zone**.

Support Logs and Loglevel Settings

The **Support Logs** page on the Clean Access Server is intended to facilitate TAC support of customer issues. The **Support Logs** page allows administrators to combine a variety of system logs (such as information on open files, open handles, and packages) into one tarball that can be sent to TAC to be included in the support case. Administrators should download these support logs when sending their customer support request.

The **Support Logs** pages on the CAM web console and CAS direct access web console (Figure 12-11)provide web page controls to configure the level of log detail recorded for troubleshooting purposes in /perfigo/logs. These web controls are intended as convenient alternative to using the CLI `loglevel` command and parameters in order to gather system information when troubleshooting.

For normal operation, the log level should always remain at the default setting (severe). The log level is only changed temporarily for a specific troubleshooting time period —typically at the request of the customer support/TAC engineer. In most cases, the setting is switched from “Severe” to “All” for a specific interval, then reset to “Severe” after data is collected. Note that once you reboot the CAM/CAS, or perform the `service perfigo restart` command, the log level will return to the default setting (Severe).

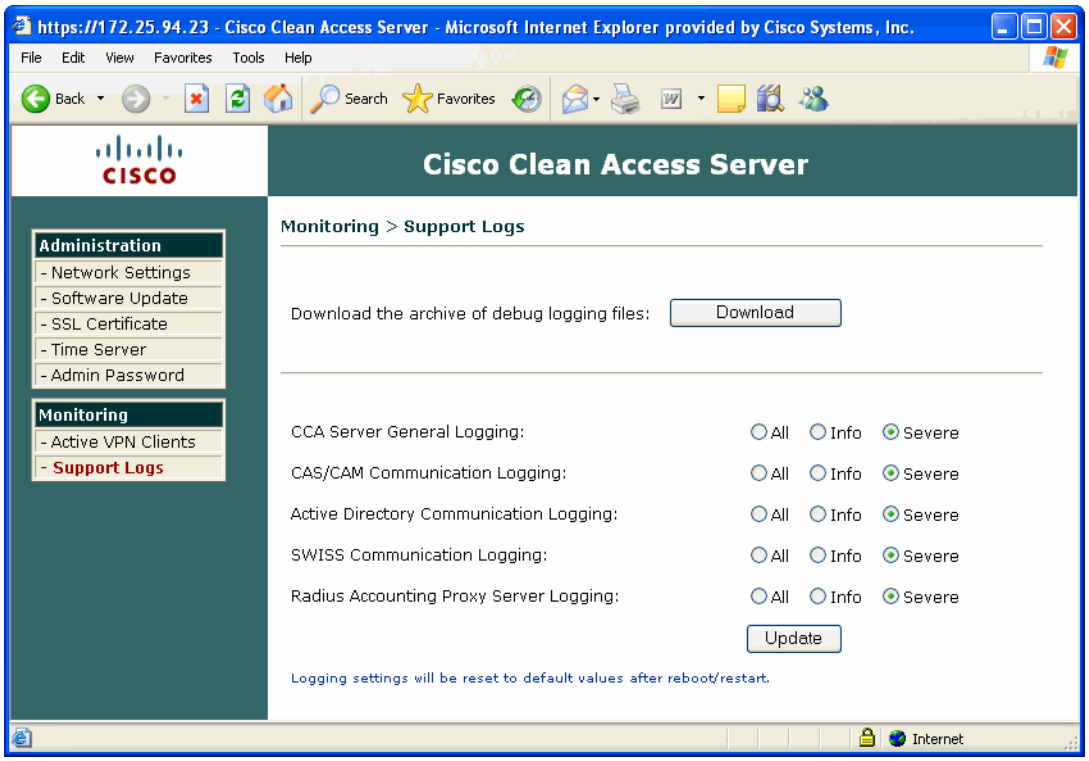
Caution Do not leave the log level set at “All” or “Info” indefinitely, as this will cause the log file to grow very quickly.

To Download CAS Support Logs:

Note To optimize memory usage, CAS support logs page are only available from the CAS direct access console under "Monitoring." (They are not available from the CAS management pages.)

1. Open the CAS direct access console from a browser using **https://<CAS_eth0_IP>/admin** as the URL/Address.
2. Go to **Monitoring > Support Logs** (Figure 12-11)

Figure 12-11 CAS Support Logs



3. Click the **Download** button to download the **cas_logs.<cas-ip-address>.tar.gz** file to your local computer.
4. Send this .tar.gz file with your customer support request.

Note To retrieve the compressed support logs file for the Clean Access Manager, go to **Administration > CCA Manager > Support Logs**. See the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide* for details.

To Change the Loglevel for CAS Logs:

1. Open the CAS direct access console (**https://<CAS_eth0_IP>/admin**).
2. Go to **Monitoring > Support Logs.**
3. Choose the CAS log category to change:

- **CCA Server General Logging**: This category contains general logging events for this CAS not contained in the other three categories listed below. For example a user that logs in (needs to post request to the CAM) will be logged here.
- **CAS/CAM Communication Logging**: This category contains the majority of relevant logs: CAM/CAS configuration or communication errors specific to this CAS. For example, if the CAM's attempt to publish information to this CAS fails, the event will be logged here.
- **SWISS Communication Logging**: This category contains log events related to SWISS (proprietary communication protocol) packets sent between this CAS and the Clean Access Agent.
- **Radius Accounting Proxy Server Logging**: This category contains RADIUS accounting log events related to Single Sign-On (SSO) for this CAS when integrated with a Cisco VPN Server.

4. Click the loglevel setting for the category of log:
   - **All**: This is the lowest loglevel, with all events and details recorded.
   - **Info**: Provides more details than the Severe loglevel. For example, if a user logs in successfully an Info message is logged.
   - **Severe**: This is the default level of logging for the system. A log event is written to /perfigo/logs only if the system encounters a severe error, such as:

     - CAM cannot connect to CAS

     - CAM and CAS cannot communicate

Note To discover the CAS, the Clean Access Agent sends SWISS (proprietary CAS-Agent communication protocol) packets on UDP port 8905 for L2 users and on port 8906 for L3 users. The CAS always listens on UDP port 8905 and 8906 and accepts traffic on port 8905 by default. The CAS will drop traffic on UDP port 8906 unless L3 support is enabled.The Agent performs SWISS discovery every 5 seconds.

CHAPTER 13

Configuring High Availability (HA)

This chapter describes how to set up two Clean Access Servers in high availability (HA) mode.By deploying Clean Access Servers in high-availability mode, you can ensure that important user authentication and connection tasks continue in the event of an unexpected shutdown. Topics include:

Overview

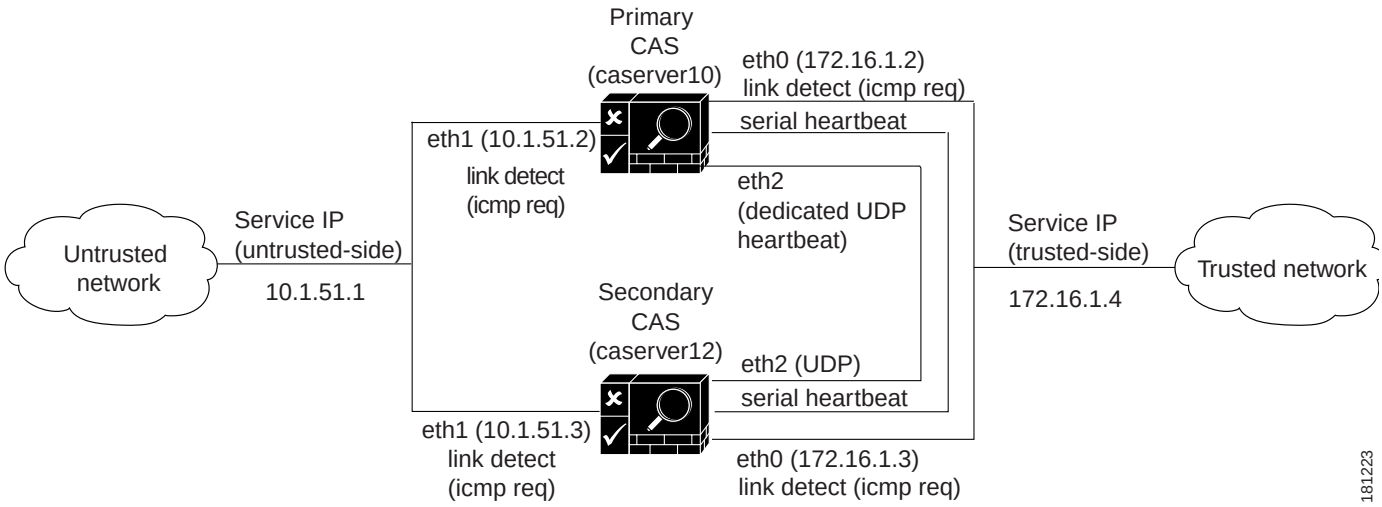
The following key points provide a high-level summary of HA-CAS operation:

- The Clean Access Server high-availability mode is an Active/Passive two-server configuration in which a standby CAS machine acts as a backup to an active CAS machine.
- The active CAS performs all tasks for the system. Since most of the CAS configuration is stored on the CAM, when CAS failover occurs, the CAM pushes the configuration to the newly-active CAS.
- The standby CAS does not forward any packets between its interfaces.
- The standby CAS monitors the health of the active CAS via heartbeat interface (serial and/or UDP). Heartbeat packets can be sent on the serial interface, dedicated eth2 interface, or eth0 interface (if an eth2 interface is not available).
- The primary and secondary CAS machines exchange UDP heartbeat packets every 2 seconds. If the heartbeat timer expires, stateful failover occurs.

- In addition to heartbeat-based failover, the CAS also provides link-based failover based on eth0 or eth1 link failure. The CAS sends ICMP ping packets to an external IP address via the eth0 and/or eth1 interface. Failover will occur if only one CAS can ping the external addresses. Note that the status of these ping packets is communicated between the CASes via the heartbeat interface; therefore heartbeat connection is still required if using link-based failover.
- Both Clean Access Servers share a virtual Service IP for the eth0 trusted interface and eth1 untrusted interface. The Service IP should be used for SSL certificates.

Figure 13-1 illustrates the basic connections in an example HA-CAS configuration.

Figure 13-1 Clean Access Server Example High-Availability Configuration



Note "Primary/Secondary" denotes the server mode when it is configured for HA. "Active/Standby" denotes the runtime status of the server.

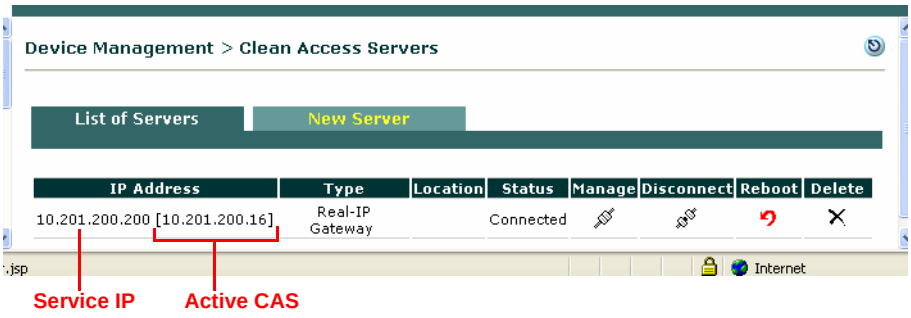
When first configuring the HA peers, you must specify an HA-Primary CAS and HA-Secondary CAS. Initially, the HA-Primary is the active CAS, and the HA-Secondary is the standby (passive) CAS. If a failover event occurs, such as the active CAS shuts down or stops responding to the peer's heartbeat signal, the standby assumes the role of the active CAS.

When the CAS starts up again, it checks to see if its peer is active. If the peer is active, the starting CAS becomes the standby. If the peer is not active, then the starting CAS assumes the active role.

Typically, Clean Access Servers are configured as an HA pair at the same time, but you can add a new Clean Access Server to an existing standalone CAS to create a high-availability pair. In order for the pair to appear to the network and to the Clean Access Manager as one entity, you must specify a **Service IP address** for the trusted interface (eth0) and a Service IP address for untrusted interface (eth1) of the pair.

Use the Service IP of the CASes to add the CAS to the CAM. Figure 13-2 shows how the active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair in the **List of Servers** in the CAM web console. In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate.

Figure 13-2 Active CAS in an HA-Pair



Note If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA. After HA configuration is complete on both CASes, the Service IP is then entered in the **New Server** form to add the HA-CAS pair to the CAM.

Note For extra security, it is recommended to connect the serial ports of each Clean Access Server (using "null modem cable") for heartbeat exchange.

Failover Events

- If both UDP heartbeat and serial heartbeat interfaces are configured, then both must fail for the standby system to take over. See Physical Connection, page 13-4 for additional details.
- If the CAS is unable to communicate with the CAM via heartbeat:
  - Users that are already connected will not be affected.
  - New users will not be able to log in.
- You can configure link-based failover. Two IP addresses that are external to the CAS are configured for link-detect: one on the trusted network, the other on the untrusted network.
  - The active and standby CAS will send ICMP ping packets via eth0 to the IP address on the trusted network.
  - The active and standby CAS will send ICMP ping packets via eth1 to the IP address on the untrusted network.

  The status of these ping packets is communicated between the CASs via the heartbeat signal:
  - If the active and standby CAS can ping both external IPs, no failover occurs
  - If the active and standby CAS cannot ping either of the external IPs, no failover occurs
  - If the active CAS cannot ping either of the external IPs, but the standby CAS can ping them, failover occurs

Choosing External IPs for Link-Based Failover

- Keep in mind that when the CAS initiates traffic, it will always send packets out of its untrusted (eth1) interface except for packets destined to its default gateway. Therefore, when choosing an external IP on trusted network for CAS to ping via the eth0 interface, choose any IP belonging to a subnet other than the CAS subnet.
- When choosing an external IP on the untrusted network for CAS to ping via the eth1 interface:

- This IP has to exist on the CAS management subnet
- It cannot be the default gateway of the CAS
- The CAS will send these ping packets out of the eth1 interface
- Verify whether **Set Management VLAN ID** is enabled for the eth1 interface. If this option is not enabled, CAS will send traffic out untagged on the eth1 interface. The switch will determine whether these packets should be received on its native VLAN. Therefore, on the untrusted interface, ensure that the native VLAN is being forwarded.
- The external IP address will be in the CAS management subnet, but on the untrusted side, the traffic will be going out from the CAS in the native VLAN; hence ensure the native VLAN is being forwarded towards the external IP device.

Refer to c. Configure HA-Primary Mode and Update, page 13-9 and c. Configure HA-Secondary Mode and Update, page 13-14 for additional configuration details.

CAS High Availability Requirements

This section describes addition planning considerations when implementing high availability:

Physical Connection

Cisco recommends the use of a **dedicated** connection for failover heartbeat on Clean Access Server high-availability pairs. You can use:

- A serial null-modem cable, or
- A dedicated Ethernet NIC card, configured as the eth2 interface of the CAS, or
- UDP heartbeat over eth0 **and** a serial null-modem cable.

It is recommended to configure a third NIC card as the eth2 interface of CAS. If your server only has two network interfaces, you can purchase one of the following NIC cards for this purpose:

- PWLA8492MT = Intel PRO/1000 MT Dual Port Server Adapter (copper)
- PWLA8492MF = Intel PRO/1000 MF (dual SX fiber LC connectors)

Note For serial cable connection for HA (either HA-CAM or HA-CAS), the serial cable must be a “null modem” cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

If a third network interface (e.g. eth2) is available, it can be used for UDP heartbeat instead of eth0. In this case, the eth2 interfaces on the two machines are connected using a crossover cable. If installing an additional Ethernet interface, configure the IP address for the interface (see Configuring Additional NIC Cards, page 4-19 for details).

If a dedicated Ethernet interface (e.g. eth2) is not available on the server machine, eth0 is supported for the Heartbeat UDP interface, in conjunction with serial heartbeat. See Selecting and Configuring the Heartbeat UDP Interface, page 13-7.

Serial heartbeat connection generally requires the server machine to have at least two serial ports: one port (ttyS0) is used for the serial heartbeat connection and the other is used to access to the server for configuration tasks. For details, see Serial Port High-Availability Connection, page 13-7.

Note Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete. See Connect the Clean Access Servers and Complete the Configuration, page 13-18.

Switch Interfaces for OOB Deployment

For Out-of-Band deployments, ensure that Port Security is not enabled on the switch interfaces to which the CAS and CAM are connected. This can interfere with CAS HA and DHCP delivery.

Service IP Addresses

In addition to the IP addresses for the trusted and untrusted interfaces for each individual CAS, you will need to provide two Service IP addresses for the trusted and untrusted interfaces of the CAS pair (see Figure 13-1 on page 13-2 for an example configuration). A **Service IP address** is the common IP address that the external network uses to address the pair.

In addition, either the trusted or untrusted interface Service IP address should be used to generate the SSL certificate. If a CAS was previously configured and added to the CAM as a standalone CAS, it must be deleted prior to configuring it for HA.

After HA configuration is complete on both CASes, use the Service IP in the **New Server** form to add the HA-CAS pair to the CAM. Note that the HA-CAS pair is automatically added as the same Server Type (for example, Out-of-Band Virtual Gateway).

Host Names

For heartbeat, each CAS needs to have a unique hostname (or node name). For HA CAS pairs, this host name will be provided to the peer, and must be resolved via DNS or added to the peer's /etc/hosts file.

DHCP Synchronization

If the Clean Access Servers operate as DHCP Servers (not in DHCP Relay or DHCP Passthrough mode) additional configuration steps must be taken to enable the Clean Access Servers to keep their DHCP-related information synchronized. DHCP information, such as information regarding active leases and lease times, is exchanged by SSH tunnel, which you configure as described in Configure DHCP Failover, page 13-20.

SSL Certificates

As in standalone mode, in HA mode the Clean Access Servers can use either a temporary, self-signed certificate or a CA (Certificate Authority)-signed certificate. A temporary certificate is useful for testing or development. A production deployment should have a CA-signed certificate. Considerations in either case are:

1. Both the temporary or CA-signed certificates can use either the Service IP address (for either the trusted interface or untrusted interface) or a domain name as the certificate domain name.
2. If creating a certificate using a domain name, then the domain name must map to the Service IP in DNS. If you are not using a domain name in the certificate, then the DNS mapping is not necessary.
3. For a temporary certificate, generate the temporary certificate on one of the Clean Access Servers, and transfer it from that CAS to the other CAS.
4. For a CA-signed certificate, you will need to import the CA-signed certificate into each of the Clean Access Servers in the pair.

Note The CA-signed certificate must be either based on the Service IP or a hostname/domain name resolvable to the Service IP through DNS.

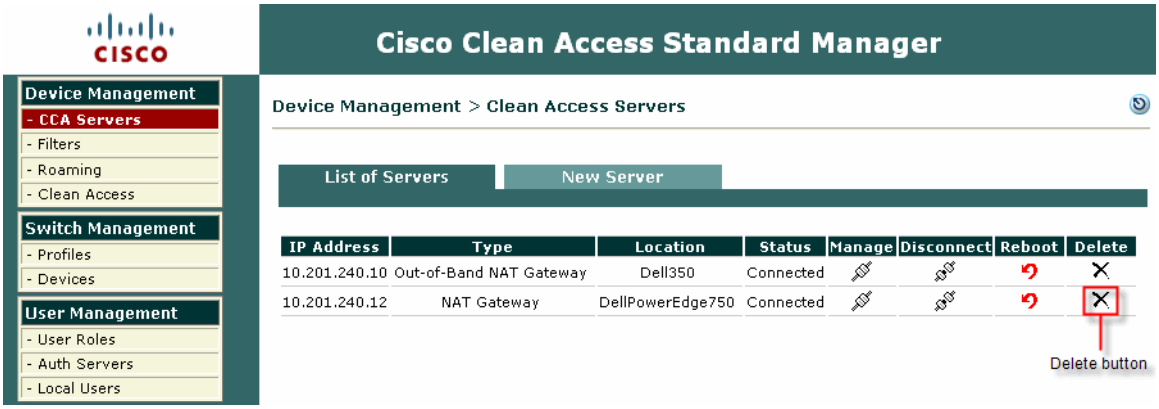
Note The Clean Access Server maintains session information during failover. For example, if user A is logged into the system in role B, when failover occurs, user A will still be logged in and have access specified by role B. If the CAS is the DHCP server and a user has a particular IP address prior to failover, DHCP failover on the CAS will ensure that the user is given the same IP address when the IP address is renewed. See Configure DHCP Failover, page 13-20.

Note For HA CAS pairs, any CAS network setting changes performed on an HA-Primary CAS through the CAS management pages or CAS direct access web console must also be repeated on the HA-Secondary CAS unit through its direct access web console. These settings include updating the SSL certificate, system time, time zone, DNS, or Service IP. See Clean Access Server Direct Access Web Console, page 12-2 and Modifying High Availability Settings, page 13-23 for details.

Before Starting

1. Before starting, make sure that both Clean Access Servers are installed and accessible over the network. See Perform the Initial Configuration, page 4-9.
2. If the Clean Access Servers have already been added to the management domain of a CAM, they should be removed. Use the **Delete** button in the **List of Servers** tab to remove the CASes.

Figure 13-3 List of Servers



Note Cisco NAC Appliance 4.1(x) web consoles support Internet Explorer 6.0 and 7.0 browsers.

Selecting and Configuring the Heartbeat UDP Interface

The Heartbeat UDP interface, if specified, is used to send UDP heartbeat traffic related to high availability. The interface used depends on the interfaces available on the server machine and the load level expected. This interface can use either a dedicated interface such as eth2 or the trusted interface eth0, if a dedicated interface is not available.

On some servers, an additional NIC card can be installed to provide an interface dedicated to UDP heartbeat (e.g. eth2). In this case, configure the IP address for the new interface as described in Configuring Additional NIC Cards, page 4-19. When a dedicated interface is used, the dedicated interfaces on both machines should be connected using a crossover cable.

Servers running a CAS typically use both available interfaces (eth0 and eth1), with eth0 configured as the trusted network interface. The eth0 trusted network interface can be shared in most deployments. When eth0 is used as the heartbeat interface, it is recommended to additionally configure serial heartbeat connection.

Note If using eth0 as the UDP heartbeat interface, make sure that the management interfaces on the CAS are in their own VLAN, not on a VLAN with other user traffic. This is a general best practice that allows you to segment and protect management traffic when running the failover heartbeat over the same physical interface.

Serial Port High-Availability Connection

If each machine running the CAS software has two serial ports, use one of the ports for the serial cable connection.

By default, the first serial connector detected on the server is configured for console input/output (to facilitate installation and other types of administrative access).

When high-availability mode is selected, the serial console login (ttyS0) is automatically disabled to free the serial port for HA mode. To re-enable ttyS0 as the console login, deselect the **Disable Serial Login** checkbox on the **Failover** tab after clicking **Update** and before clicking **Reboot**. For details, see steps c. Configure HA-Primary Mode and Update, page 13-9 and c. Configure HA-Secondary Mode and Update, page 13-14.

Note The serial console login and HA serial heartbeat cannot be located on the same serial port.

Configure High Availability

The following sections describe how to set up high availability in four general procedures:

- Step 1: Configure the Primary Clean Access Server, page 13-8
- Step 2: Configure the HA-Secondary Clean Access Server, page 13-14
- Step 3: Connect the Clean Access Servers and Complete the Configuration, page 13-18
- Step 4: Failing Over an HA-CAS Pair, page 13-19
- Step 5: Configure DHCP Failover, page 13-20
  If configuring high availability for Clean Access Servers that operate as DHCP servers (not in DHCP relay or passthrough mode), you also need to configure the SSH tunnel between them.

Note "Primary/Secondary" denotes the server mode when it is configured for HA.
"Active/Standby" denotes the runtime status of the server.

Configure the Primary Clean Access Server

The general sequence to configure the primary CAS is as follows:

a. Access the Primary CAS Directly
b. Configure the Host Information for the Primary
c. Configure HA-Primary Mode and Update
d. Configure the SSL Certificate
e. Reboot the Primary Server
f. Add the CAS to the CAM Using the Service IP

These steps are detailed in the following sections.

When done, continue to Configure the HA-Secondary Clean Access Server, page 13-14.

a. Access the Primary CAS Directly

Each Clean Access Server has its own web admin console that allows configuration of certain limited Administration settings directly on the CAS. The CAS direct access web console must be used to configure CAS pairs for HA.

To access the primary Clean Access Server's direct access web admin console:

1. Open a web browser and type the IP address of the trusted (eth0) interface of the CAS in the URL/address field, as follows: **https://<PrimaryCAS_eth0_IP>/admin** (for example, `https://172.16.1.2/admin`)
2. Accept the temporary certificate and log in as user `admin` (default password is `cisco123`).

Note
- In order to copy and paste values to/from configuration forms, it is recommended to keep both web consoles open for each CAS (primary and secondary). See also a. Access the HA-Secondary CAS Directly, page 13-14.
- To ensure security, it is recommended to change the default password of the CAS.

b. Configure the Host Information for the Primary

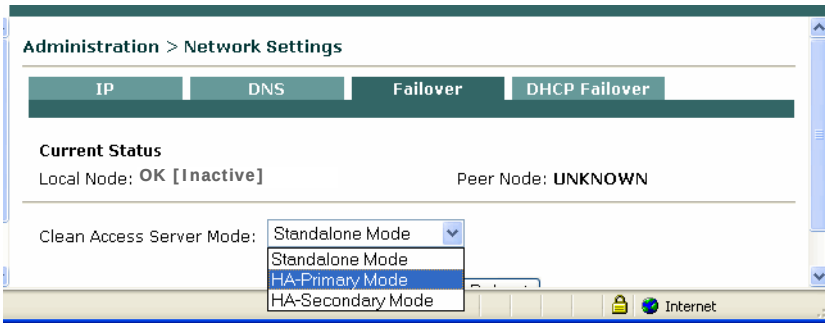
3. Click the **Network Settings** link, then the **DNS** tab.
4. In the **Host Name** field, type the host name for the primary CAS (for example, caserver10). Make sure there is a domain in the **Host Domain** field, such as cisco.com. If necessary, add one and click **Update**.

Figure 13-4 DNS Tab

c. Configure HA-Primary Mode and Update

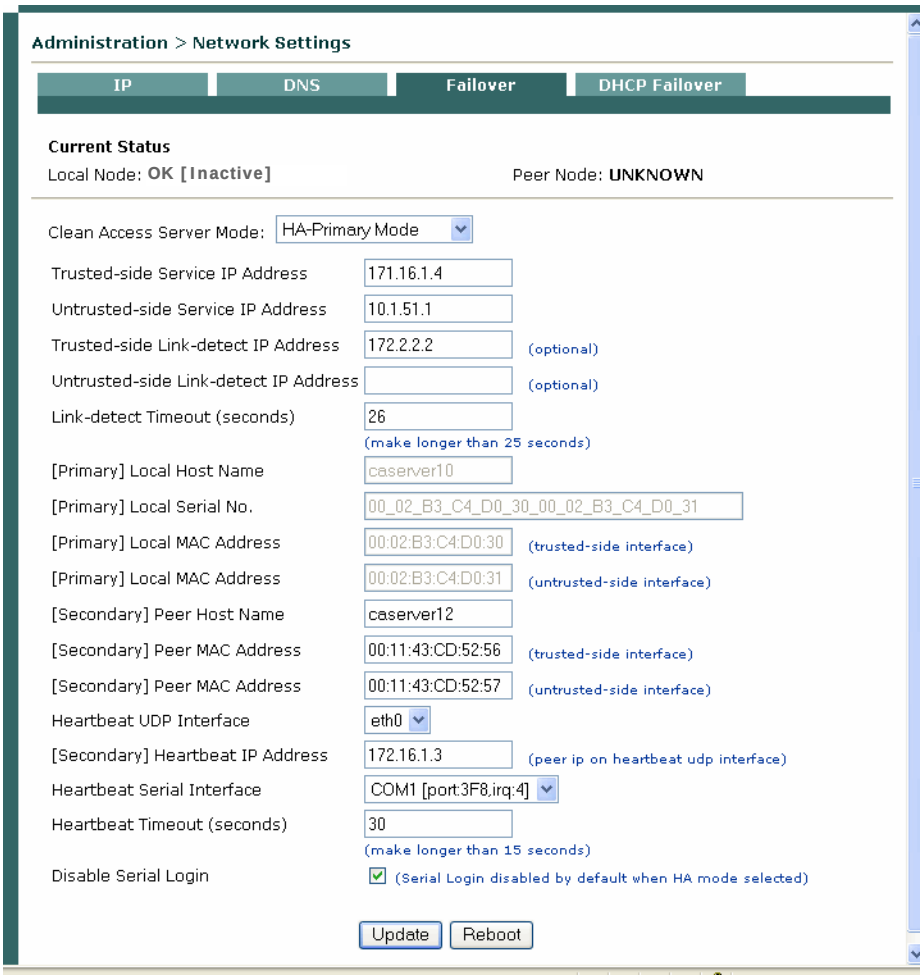
5. Click the **Failover** tab and choose **HA-Primary Mode** from the **Clean Access Server Mode** dropdown menu.

Figure 13-5 Failover —Choose Mode



6. In the **HA-Primary Mode** form that opens, type values for the following fields.

Figure 13-6 Failover —HA-Primary Mode



- **Trusted-side Service IP Address**: The common IP address by which the pair is addressed from the trusted network (172.16.1.4 in the example in Figure 13-1 on page 13-2).
- **Untrusted-side Service IP Address**: The common address for the pair on the untrusted (managed) network (10.1.51.1 in the sample).
- **Trusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS will attempt to ping this address on its trusted interface (eth0). Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.
- **Untrusted-side Link-detect IP Address (Optional):** When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this address on its untrusted interface (eth1). You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.
- **Link-detect Timeout (seconds) (Optional):** This configures the length of time the CAS will attempt to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Enter a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note In addition to Heartbeat Serial/UDP configuration, you can optionally configure the CAS to respond to link failures on the trusted and/or untrusted sides as failover events. The CAS will attempt to ping the trusted and/or untrusted link-detect addresses specified, then count the number of nodes it can reach:
0-for no addresses
1-for either trusted/untrusted
2-for both trusted/untrusted
If the Standby CAS can reach more nodes than the Active CAS, the Standby CAS will take over and become the Active CAS. If both CASes can ping the same number of addresses (all addresses or only one address), no failover event occurs, since neither CAS has the advantage. To enable link-detect, enter at least one link-detect IP address on each CAS and a link-detect timeout. See also Choosing External IPs for Link-Based Failover, page 13-3 for further details.

Note The CAS performs Heartbeat connection and (optionally) Link-detect according to the same interval, approximately every 1-2 seconds.

- **[Primary] Local Host Name**: Filled in by default for the HA-Primary CAS, as configured under **Administration > Network Settings > DNS | Host Name** (caserver10 in the sample).
- **[Primary] Local Serial No**: Filled in by default for the HA-Primary CAS. The local serial number identifies this CAS to the Clean Access Manager (and is composed of eth0/eth1 MAC addresses). In an HA-CAS pair, the serial number of the Primary CAS is the key used to associate all the configuration information specific to this CAS in the CAM database.
- **[Primary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Primary CAS.
- **[Primary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Primary CAS.

Note

- You may want to copy and paste the **[Primary] Local Host Name**, **[Primary] Local Serial No**, and **[Primary] Local MAC Address (trusted/untrusted)** values into a text file. These values are necessary later when configuring the HA-Secondary CAS.
- To enter the HA-Secondary CAS information into the form for the HA-Primary CAS, copy and paste the corresponding fields from the HA-Secondary CAS web console.

- **[Secondary] Peer Host Name**: The host name for the HA-Secondary CAS peer (caserver12 in the sample). You will need to specify this value again as the **Host Name** value in the peer machine's **DNS** tab.
- **[Secondary] Peer MAC Address (trusted-side interface)**: This is the peer MAC address from the trusted (eth0) side of the HA-Secondary CAS.
- **[Secondary] Peer MAC Address (untrusted-side interface)**: This is the peer MAC address from the untrusted (eth1) side of the HA-Secondary CAS.
- **Heartbeat UDP Interface:** Options are N/A, eth0, eth2, eth3, eth4. If a dedicated Ethernet connection is not available, it is recommended to use eth0 for the Heartbeat UDP interface in conjunction with serial heartbeat when configuring a Clean Access Server in HA mode.

- **[Secondary] Heartbeat IP Address**: The IP address of the trusted interface (eth0) of the HA-Secondary CAS (in the sample, 172.16.1.3).
- **Heartbeat Serial Interface:** Select the COM port for the serial connection. It is recommended to use both serial and UDP connections for the Heartbeat interface.

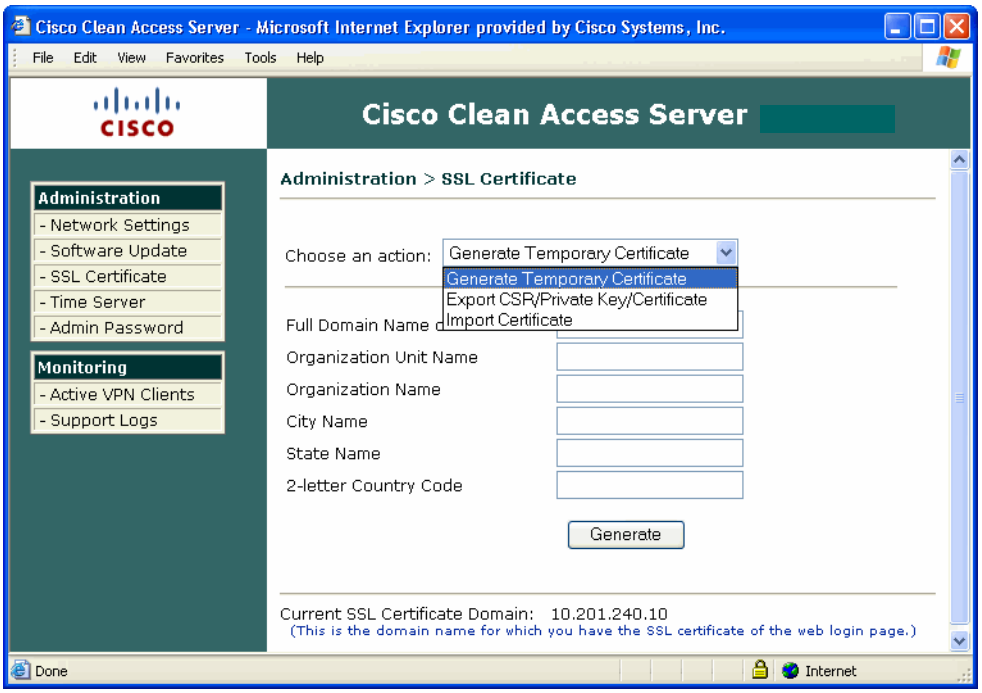
Note Do not connect the serial cable before starting HA (failover) configuration. The serial cable must be connected after the configuration is complete.

- **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.
- **Disable Serial Login**: Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), deselect the **Disable Serial Login** checkbox at this stage (after **Update** and before **Reboot**).
- **Update**: Click to update the HA configuration information for the CAS without rebooting it.
- **Reboot:** This is used to reboot the CAS at the end of HA-Primary CAS configuration. (Do **not** click Reboot at this point.)

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Primary CAS. Click the **SSL Certificate** link from the **Administration** menu. The **Generate Temporary Certificate** form appears.

Figure 13-7 Generate Temporary Certificate



8. In the **SSL Certificate** page, perform one of the following procedures, depending on whether you intend to use a temporary, self-signed certificate or a CA-signed certificate:

If using a temporary certificate for the HA pair:

a. Complete the **Generate Temporary Certificate** form and click **Generate**. The certificate must be associated with the Service IP addresses of the HA pair.

b. When finished generating the temporary certificate, select **Export CSR/Private Key/Certificate** from the **Choose an action** dropdown menu.

c. Click the **Export** button for **Currently Installed Private Key** to export the SSL private key. Save the key file to disk. You must import this key file later when configuring the HA-Secondary CAS.

d. Click the **Export** button for **Currently Installed Certificate** to export the current temporary certificate. Save the certificate file to disk. You will have to import this file into the HA-Secondary CAS later.

If using a CA-signed certificate for the HA pair:

a. Choose **Import Certificate** from the **Choose an action** menu

b. Use the **Browse** button next to the **Certificate File** field and navigate to the certificate file.

c. Choose **CA-signed PEM-encoded X.509 Cert** from the **File Type** dropdown menu:

d. Click **Upload** to import the certificate. Note that you will need to import the same certificate later to the HA-Secondary CAS.

e. Click **Verify and Install Uploaded Certificates**.

f. Choose **Export CSR/Private Key/Certificate** from the **Choose an action** list.

g. Click the **Export Private Key** button. You must import this key later when configuring the HA-Secondary CAS.

See Manage CAS SSL Certificates, page 12-3 for additional details.

Note The CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

e. Reboot the Primary Server

9. **Reboot** the Clean Access Server from either the CAS direct access interface (**Network Settings** > **Failover** > **Reboot** button) or from the CAM web console (**Administration** > **CCA Manager** > **Network & Failover** > **Reboot** button).

f. Add the CAS to the CAM Using the Service IP

10. In the CAM web console, go to **Device Management** > **CCA Servers** > **New Server**, and add the CAS to the CAM using the Service IP for the pair (172.16.1.4) as the **Server IP** address.

11. Configure any other settings desired, such as DHCP settings, to control the runtime behavior of the CAS.

12. Test the configuration by trying to log into the untrusted (managed) network from a computer connected to the untrusted interface of the Clean Access Server. Proceed to the next step only if you can successfully access the network.

Configure the HA-Secondary Clean Access Server

The general sequence to configure the HA-Secondary CAS is as follows:

a. Access the HA-Secondary CAS Directly

1. Access the web console for the HA-Secondary CAS by opening a web browser and typing the IP address of the trusted (eth0) interface of the HA-Secondary CAS in the URL/address field, as follows: **https://<StandbyCAS_eth0_IP>/admin** (for example, `https://172.16.1.3/admin`)
2. Log in as user `admin` (default password is `cisco123`). (It is recommended that you change the default password for the CAS to ensure the security of your network environment.)

Note

- In order to copy and paste values to/from configuration forms, it is recommended to keep both web consoles open for each CAS (primary and secondary). See also a. Access the Primary CAS Directly, page 13-8.
- To ensure security, it is recommended to change the default password of the CAS.

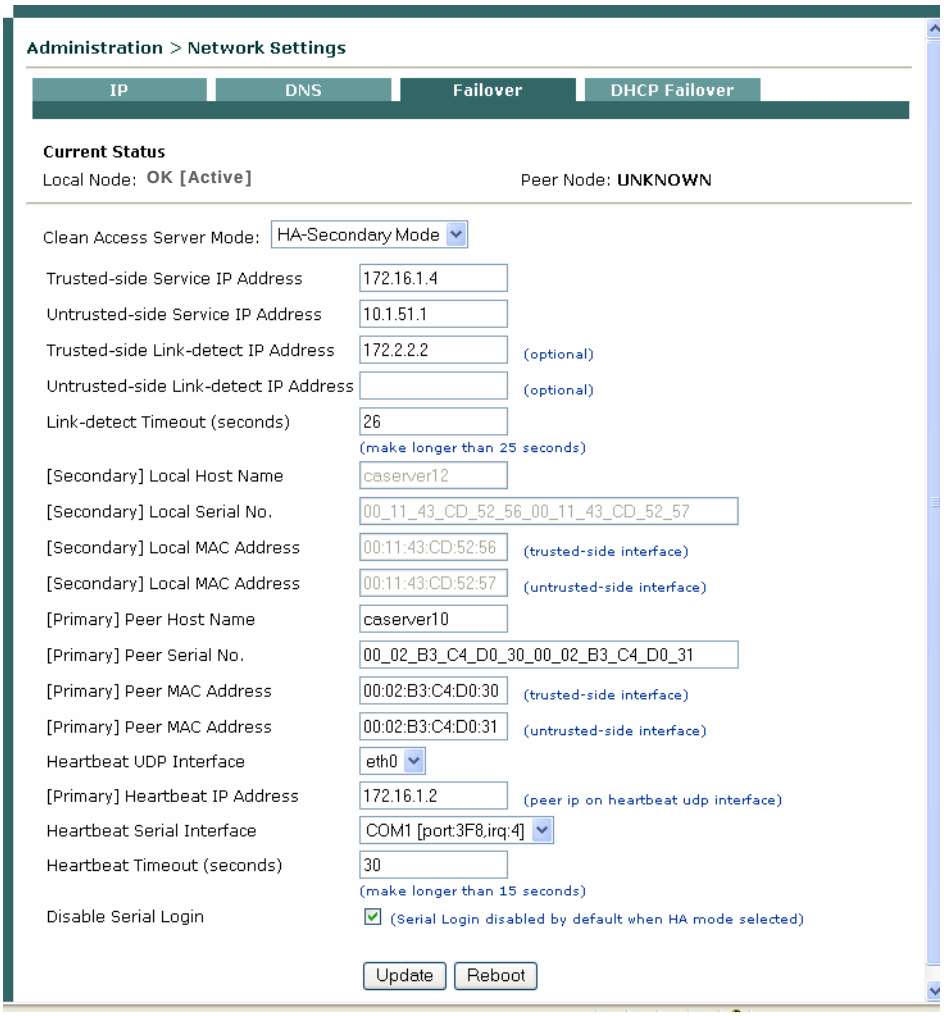
b. Configure the Host Information for the HA-Secondary

3. In the **Network Settings** page, open the **DNS** tab.
4. Change the host name to the unique host name for the secondary CAS, such as `caserver12`. You must have the same domain name specified in this tab as you did for the primary Clean Access Server (see b. Configure the Host Information for the Primary, page 13-9).

c. Configure HA-Secondary Mode and Update

5. Click the **Failover Setting** tab and select **HA-Secondary Mode** from the **Choose Clean Access Server Mode** dropdown menu.

Figure 13-8 Failover —HA-Secondary Mode



6. In the HA-Secondary form, complete the following fields:
   - **Trusted-side Service IP Address**: The IP address by which the pair is addressed from the *trusted* network. Use the same value as for the primary CAS (172.16.1.4 in the example in Figure 13-1 on page 13-2).
   - **Untrusted-side Service IP Address**: The IP address by which the pair is addressed from the *untrusted* (managed) network. Use the same value as for the primary CAS (10.1.51.1 in the example).
   - **Trusted-side Link-detect IP Address (Optional)**: When an IP address (e.g. for an upstream router) is optionally entered in this field, the CAS will attempt to ping this address on its trusted interface (eth0). Typically, the same trusted-side link-detect address is entered on both the HA-Primary and HA-Secondary CAS, but you can specify different addresses for each CAS if your network topology is different.
   - **Untrusted-side Link-detect IP Address (Optional):** When an IP address (e.g. for a downstream switch) is optionally entered in this field, the CAS will attempt to ping this address on its untrusted interface (eth1). You can enter the same or different untrusted-side link-detect addresses on both the HA-Primary and HA-Secondary CAS.

– **Link-detect Timeout (seconds) (Optional):** This configures the length of time the CAS will attempt to ping the Trusted-side and/or Untrusted-side Link-detect IP address(es). Enter a time of at least 26 seconds. If the CAS cannot ping the node for the period of time specified, the node is not pingable.

Note See Choosing External IPs for Link-Based Failover, page 13-3 for additional details.

– **[Secondary] Local Host Name**: Filled in by default for the HA-Secondary CAS (caserver12 in the sample).

– **[Secondary] Local Serial No**: Filled in by default for the HA-Secondary CAS.

– **[Secondary] Local MAC Address (trusted-side interface)**: Filled in by default; the MAC address of the eth0 interface for the HA-Secondary CAS.

– **[Secondary] Local MAC Address (untrusted-side interface)**: Filled in by default; the MAC address of the eth1 interface for the HA-Secondary CAS.

Note

- You may want to copy and paste the **[Secondary] Local Host Name**, **[Secondary] Local Serial No**. and **[Secondary] Local MAC Address (trusted/untrusted)** values into a text file. These values are needed to configure the HA-Primary CAS.
- To enter the HA-Primary CAS information into the form for the HA-Secondary CAS, copy and paste the corresponding fields from the web console of the HA-Primary CAS.

– **[Primary] Peer Host Name**: The host name of the HA-Primary CAS, as specified in the **Host Name** field in the primary's **DNS** tab (caserver10 in the sample).

– **[Primary] Peer Serial No**: The serial number of the HA-Primary CAS. When the HA-Secondary CAS becomes Active, it must use the serial number of the HA-Primary CAS to identify itself to the CAM in order to access the CAS configuration information.

– **[Primary] Peer MAC Address (trusted-side interface)**: The peer MAC address from the trusted side (eth0) of the HA-Primary CAS.

– **[Primary] Peer MAC Address (untrusted-side interface)**: The peer MAC address from the untrusted side (eth1) of the HA-Primary CAS.

– **Heartbeat UDP Interface:** Options are N/A, eth0, eth2, eth3, eth4. If a dedicated Ethernet connection is not available, it is recommended to use eth0 for the Heartbeat UDP interface when configuring a Clean Access Server in HA mode.

– **[Primary] Heartbeat IP Address**: The IP address of the trusted-side interface (eth0) of the HA-Primary CAS (in the sample, 172.16.1.2)

– **Heartbeat Serial Interface:** Select the COM port for the serial connection. It is recommended to use both serial and UDP connections for the Heartbeat interface.

– **Heartbeat Timeout (seconds):** Choose a value greater than 15 seconds.

– **Disable Serial Login**: Serial login is disabled by default when HA mode is selected. To re-enable the serial console (ttyS0), deselect the **Disable Serial Login** checkbox at this stage (after **Update** and before **Reboot**).

– **Update**: Click to update the HA configuration information for the CAS without rebooting it.

d. Configure the SSL Certificate

7. Now configure the SSL certificate for the HA-Secondary CAS. Click the **SSL Certificate** link. In the **SSL Certificate** page, perform one of the following procedures:

If using a temporary certificate for the HA pair:

a. Select **Import Certificate** from the **Choose an action** menu.

b. Use the **Browse** button next to the **Certificate File** field to find the private key associated with temporary certificate file that you previously exported from the primary CAS.

c. Choose **Private Key** as the File Type.

d. Click **Upload** to upload the private key.

e. With **Import Certificate** selected from the **Choose an action:** menu, browse to the temporary certificate associated with the private key.

f. Choose **CA-signed PEM-encoded X.509 Cert** as the File Type.

g. Click **Upload** to upload the temporary certificate.

h. Click **Verify and Install Uploaded Certificates**.

If using a CA-signed certificate for the HA pair:

a. Select **Import Certificate** from the **Choose an action** menu.

b. Use the **Browse** button next to the **Certificate File** field to select the private key file you exported from the primary CAS.

c. Choose **Private Key** as the File Type.

d. Click **Upload** to upload the private key.

e. With **Import Certificate** selected from the **Choose an action:** menu, browse to the same CA-signed certificate file you imported into the primary Clean Access Server.

f. Choose **CA-signed PEM-encoded X.509 Cert** as the File Type.

g. Click **Upload** to upload the CA-signed certificate.

h. Click **Verify and Install Uploaded Certificates**.

Note In some cases, you will be required to import a CA-Root certificate and/or an Intermediate Root certificate. If so, choose the **Root/Intermediate Certificate** file type when importing the file(s). See Manage CAS SSL Certificates, page 12-3 for additional details.

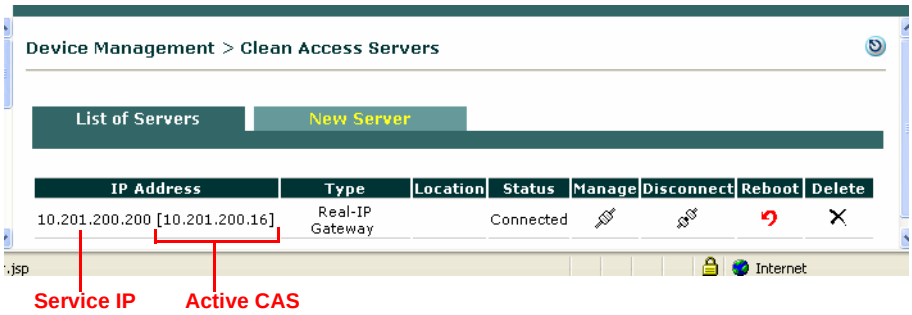
e. Reboot the HA-Secondary Server

8. From the CAS direct access interface (**Network Settings > Failover**), click the **Reboot** button to reboot the Clean Access Server.

Connect the Clean Access Servers and Complete the Configuration

1. Shut down the HA-Primary CAS machine and connect the `caserver10` and `caserver12` machines using a serial null modem cable (connecting available serial ports) and/or a crossover cable (connecting Ethernet ports if using a third Ethernet interface such as eth2 for failover).
2. Open the Clean Access Manager administration console.
3. Go to **Device Management > CCA Servers > List of Servers.** The Active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 13-9. Since the HA-Primary CAS is turned off, the IP address of the HA-Secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.

Figure 13-9 Active CAS in an HA-Pair



4. Click the **Manage** button for the pair. The management pages of the HA-Secondary CAS (now the Active CAS) should appear.
5. Configure the DHCP Server settings so that they match the DHCP settings of the HA-Primary CAS. If the HA-CAS pair operates as a DHCP server, follow the steps in Configure DHCP Failover, page 13-20 to allow the peer Clean Access Servers to keep DHCP information in synchronization
6. From a client computer connected to the Clean Access Server's untrusted interface, test the configuration by trying to log on to the untrusted (managed) network as an authorized user. If successful, remain logged on and proceed to the next step.

Failing Over an HA-CAS Pair

Note For a DHCP Server HA-CAS pair, perform the steps in Configure DHCP Failover, page 13-20 first.

To test your HA system, use the following steps:

1. Turn on the HA-Primary CAS machine. Make sure that the CAS is fully started and functioning before proceeding.
2. From the client computer, log off the user's session and try to log onto the untrusted (managed) network again as the user.
3. The HA-Secondary CAS should still be active and providing services for the user.
4. Shut down the HA-Secondary CAS machine.

Note Cisco recommends "shutdown" or "reboot" on the machine to test failover, or, if a CLI command is preferred, `service perfigo stop` and `service perfigo start`. For a Virtual Gateway CAS, use `service perfigo maintenance` instead to bring the CAS to maintenance mode and allow network connectivity to the management VLAN. See Using the Command Line Interface (CLI), page 4-17 for details.

5. After about 15 seconds, you should be able to continue browsing, with the HA-Primary CAS becoming the Active server and providing the service.
6. Turn on the HA-Secondary CAS machine (the standby server).
7. Check the event log on the Clean Access Manager. It should correctly indicate the status of the Clean Access Servers (e.g "`caserver10 is dead. caserver12 is up`").
8. Testing of the high availability configuration is now complete.

Configure DHCP Failover

High-availability peer Clean Access Servers (CASes) that operate in DHCP server mode exchange information regarding their DHCP activities, such as active leases and lease times, by secure SSH connection (tunnel). If configuring high availability for Clean Access Servers that will operate as DHCP servers (not in DHCP relay or passthrough mode), you need to configure DHCP failover. Keys for the server and for the account accessing the server are required for both the HA-Primary and HA-Secondary Clean Access Servers. As a result, a total of four keys must be exchanged. The interface described below is provided to facilitate the generation and exchange of the security keys necessary to transfer DHCP failover information between the primary and secondary Clean Access Servers.

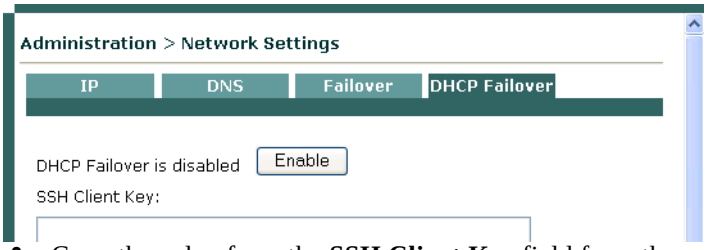
Note After the DHCP server and CAS failover have been configured, both primary and secondary Clean Access Servers must be failed over in order to create the /var/state/dhcp directory on each server. The /var/state/dhcp directory must exist on both servers for DHCP failover to function correctly. See Connect the Clean Access Servers and Complete the Configuration, page 13-18 and Failing Over an HA-CAS Pair, page 13-19.

To Configure DHCP Failover

To start, open the admin console of the primary CAS and the secondary CAS (`https://<ServerIP>/admin`). You will have two browsers open during this process.

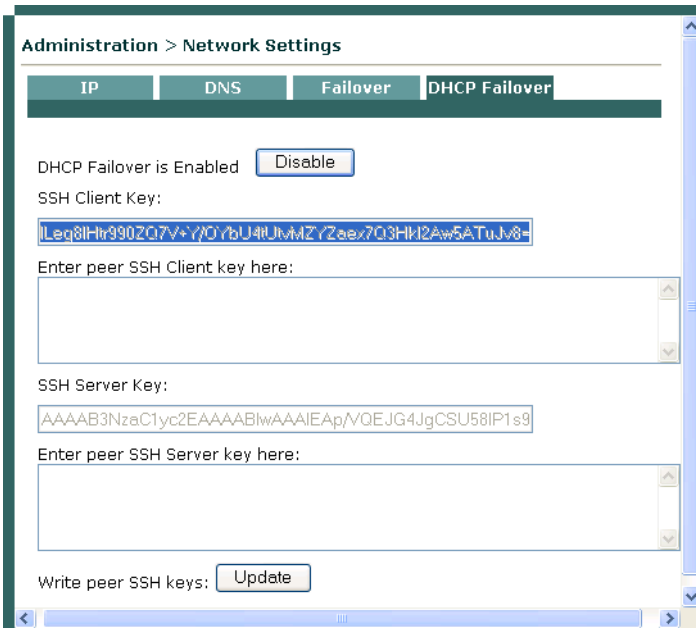
1. Go to the admin console of the primary CAS and click the **DHCP Failover** tab.
2. Click the **Enable** button to enable DHCP failover on the primary CAS (notice that this button toggles to **Disable** afterwards).

Figure 13-10 Enable DHCP Failover



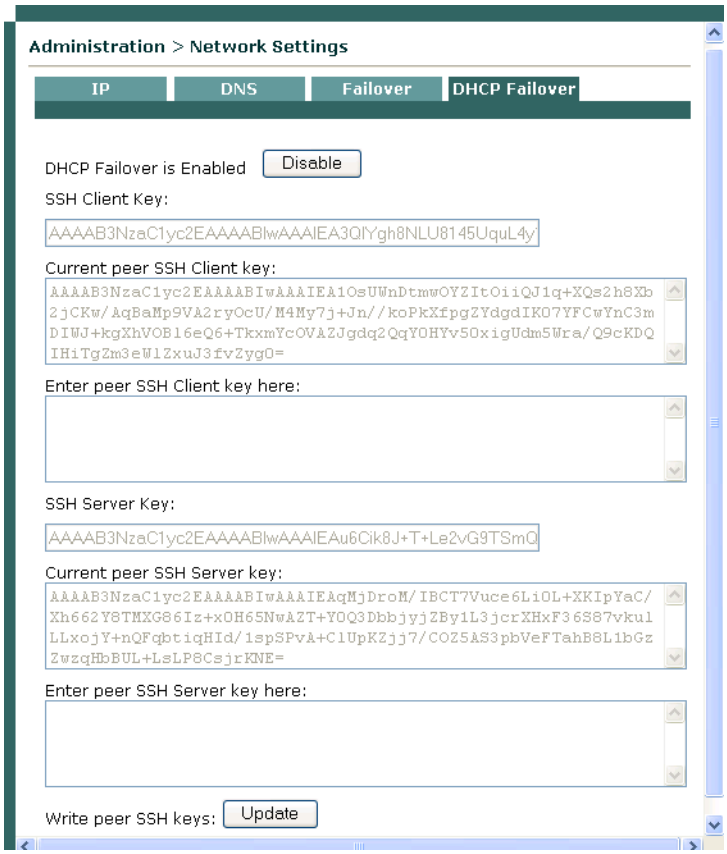
3. Copy the value from the **SSH Client Key** field from the primary CAS.

Figure 13-11 DHCP Failover — Primary CAS



4. Go to the admin console of the secondary CAS and click the **DHCP Failover** tab.
5. Click the **Enable** button to enable DHCP failover on the secondary CAS.
6. Paste the SSH Client Key you copied from the primary CAS into the field **Enter peer SSH Client key here**:
7. While still in the admin console of the secondary CAS, copy the value from the **SSH Client Key** field.
8. Now go back to the admin console of the primary CAS and paste the SSH Client Key of the secondary CAS into the **Enter peer SSH Client key here:** field.
9. While still in the admin console of the primary CAS, copy the value from the **SSH Server Key** field.
10. Now go to the admin console of the secondary CAS and paste the SSH Server Key of the primary CAS into the **Enter peer SSH Server key here:** field.
11. While in the admin console of the secondary CAS, copy the value from the **SSH Server key** field.
12. Click the **Update** button to write the peer SSH keys to the secondary CAS.
13. Go to the admin console of the primary CAS and paste the SSH Server Key from the secondary CAS into the **Enter peer SSH Server key here:** field.
14. Click the **Update** button to write the peer SSH keys to the primary CAS. DHCP failover configuration is now complete.

Figure 13-12 DHCP Failover — Configuration Complete



Modifying High Availability Settings

The following instructions describe how to change settings for an existing high-availability Clean Access Server pair. Changing the Service IP, the subnet mask, or the default gateway for a high-availability pair requires updating the Clean Access Manager and rebooting the Clean Access Server.

Additionally, if the Service IP address is changed and the SSL certificate for the Clean Access Server is based on the Service IP, a new certificate must be generated and imported to each Clean Access Server in the high-availability pair. If the SSL certificate is based on the host name of the Clean Access Server, generating a new certificate is not necessary. However, make sure to change the IP address for that host name in your DNS server.

The general sequence of steps is as follows:

1. Update the Clean Access Server settings in the Clean Access Manager first (but do not reboot).
2. Update the HA settings in the direct access web console for the primary CAS and reboot the primary CAS.
3. While the primary CAS reboots, wait for the secondary CAS to become active in the CAM's List of Servers.
4. Repeat steps 1-3 for the secondary CAS and reboot the secondary CAS.
5. While the secondary CAS reboots, the primary CAS becomes active in the Clean Access Manager and displays the new settings.

To Change IP Settings for an HA-CAS

1. From the CAM web admin console, go to **Device Management** > **CCA Servers**
2. Click the **Manage** button for the Clean Access Server.
3. Click the **Network** tab.
4. Change the **IP Address**, **Subnet Mask**, or **Default Gateway** settings for the trusted/untrusted interfaces as desired.
5. Click the **Update** button only.

Caution Do not click the **Reboot** button at this stage.

6. If the SSL certificate for the CAS was based on the previous IP address, you will need to generate a new SSL certificate based on the new IP address configured. This can be done under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Network** > **Certs**. See Manage CAS SSL Certificates, page 12-3 for details.
7. If the SSL certificate was based on the host name of your Clean Access Server, you do not need to generate a new certificate. However, make sure to change the IP address for that host name in your DNS server.
8. Next, open the direct access web admin console for the **primary** Clean Access Server as follows:

   `https://<Primary_CAS_eth0_IPaddress>/admin`

9. The IP form for the primary CAS will reflect the changes you made in the CAM web console under **Device Management** > **CCA Servers** > **Manage [CAS_IP]** > **Network** > **IP**.
10. In Clean Access Server direct access console, click the **Network** > **Failover** tab.

11. Change the following as needed:
    - Trusted-side Service IP Address
    - Untrusted-side Service IP Address
    - [Secondary] Peer Host Name
    - [Secondary] Peer MAC Address (trusted-side interface)
    - [Secondary] Peer MAC Address (untrusted-side interface)
    - [Secondary] Heartbeat IP Address
12. Click the **Update** button, then the **Reboot** button.
13. Next, from to the Clean Access Manager web admin console, go to **Device Management** > **CCA Servers** and wait for the secondary Clean Access Server to become active. (Note that this can take up to a few minutes.) The active CAS of a high-availability pair is displayed in brackets next to the Service IP for the pair, as shown in Figure 13-1 on page 13-2. The IP address of the secondary CAS should appear in brackets in the **List of Servers** with a status of Connected.
14. Once the IP address of the secondary CAS appears in brackets in the **List of Servers**, and the CAS has a status of Connected, repeat steps 1-11 for the secondary CAS.
15. Once changes are made and the secondary CAS is rebooted, the primary CAS will appear as the active server on the List of Servers and displays all the new IP information.

Upgrading an Existing Failover Pair

For instructions on upgrading an existing failover pair to a new CCA release, see "Upgrading High Availability Pairs" in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(0)* at http://www.cisco.com/en/US/products/ps6128/prod_release_note09186a008070866a.html.

Useful CLI Commands for HA

The following are useful directories to know about for HA on the CAS:

- /etc/ha.d/perfigo.conf
- /etc/ha.d/ha.cf

How to Verify Primary/Secondary Configuration Status on the HA CAS

The /etc/ha.d/perfigo.conf file shows a variety of configuration information for an HA-CAS, including hostname (cas1), peer hostname (cas2), HA mode (Primary), heartbeat interface (UDP/serial), and link-detect interface information:

```
[root@cas1 ha.d]# more perfigo.conf
#linux-ha
#Mon Aug 28 18:50:15 PDT 2006
WIRELESS_SERVICEIP=10.10.20.4
PING_DEAD=25
HOSTNAME=cas1
HA_DEAD=15
PEERGUSSK=
PEERMAC=00\:16\:35\:BF\:FE\:67
PEERHOSTNAME=cas2
TRUSTED_PINGNODE=10.10.40.100
```

```
UNTRUSTED_PINGNODE=10.10.20.100
HAMODE=PRIMARY
PEERMAC0=00\:16\:35\:BF\:FE\:66
PEERHOSTIP=10.10.50.2
HA_FAILBACK=off
HA_UDP=eth2
WIRED_SERVICEIP=10.10.20.4
HA_SERIAL=ttyS0
```

The /etc/ha.d/ha.cf file shows additional information about the heartbeat and link-based connections:

```
[root@cas1 ha.d]# more ha.cf
# Generated by make-hacf-ss.pl
udpport         694
ucast           eth2 10.10.50.2
baud            19200
serial          /dev/ttyS0
keepalive       2
deadtime        15
deadping        25
auto_failback   off
apiauth         default uid=root
respawn         hacluster /usr/lib64/heartbeat/ipfail
ping            10.10.20.100
ping            10.10.40.100

log_badpack     false
warntime        10
debug           0
debugfile       /var/log/ha-debug
logfile         /var/log/ha-log
watchdog        /dev/watchdog
node            cas1
node            cas2
```

How to Verify Active/Standby Runtime Status on the HA CAS

The following example shows how to use the CLI to determine the runtime status (active or standby) of each CAS in the HA pair. You can generally find the fostate.sh command from the /store directory of your last upgrade, for example, **`/store/cca_upgrade-4.x.x`**.

1. Cd to `/store/cca_upgrade-4.x.x`, and run the fostate.sh script on the first CAS:

```
[root@cas1 cca_upgrade-4.x.x]# ./fostate.sh
My node is active, peer node is standby
[root@cas1 cca_upgrade-4.x.x]#
```

   This CAS is the active CAS in the HA-pair.

2. Run the fostate.sh script on the second CAS:

```
[root@cas2 cca_upgrade-4.x.x]# ./fostate.sh
My node is standby, peer node is active
[root@cas2 cca_upgrade-4.x.x]#
```

   This CAS is the standby CAS in the HA-pair.

Adding High Availability Cisco NAC Appliance To Your Network

The following diagrams illustrate how HA-CAMs and HA-CASs can be added to an example core-distribution-access network (with Catalyst 6500s in the distribution and access layers).

Figure 13-13 shows a network topology without Cisco NAC Appliance, where the core and distribution layers are running HSRP (Hot Standby Router Protocol), and the access switches are dual-homed to the distribution switches.

Figure 13-13 Example Core-Distribution-Access Network Before Cisco NAC Appliance

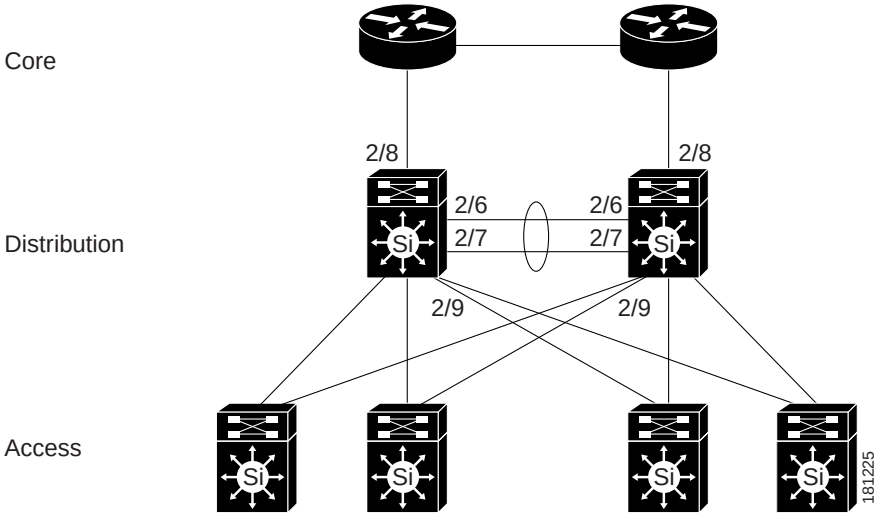


Figure 13-14 shows how HA-CAMs can be added to the core-distribution-access network. In this example, the HA heartbeat connection is configured over both serial and eth1 interfaces.

Figure 13-14 Adding HA CAMs to Network

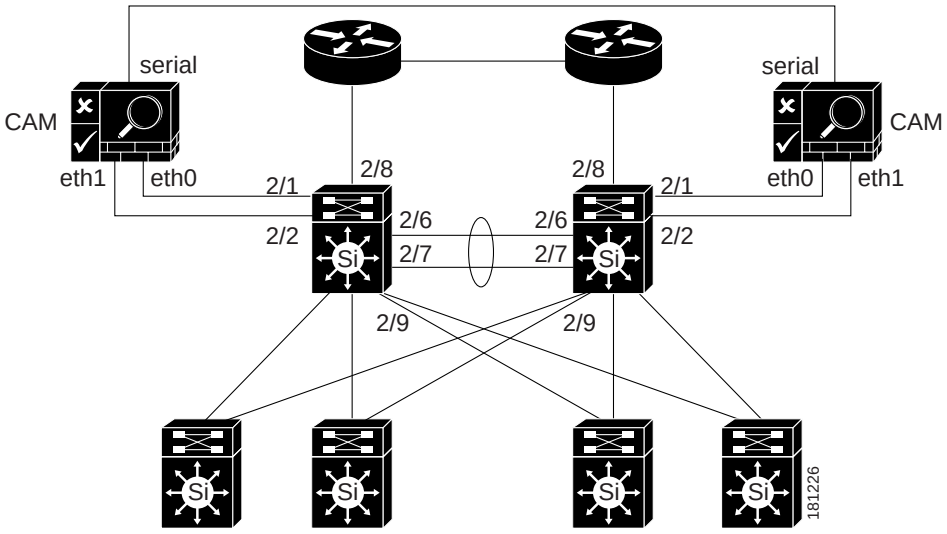
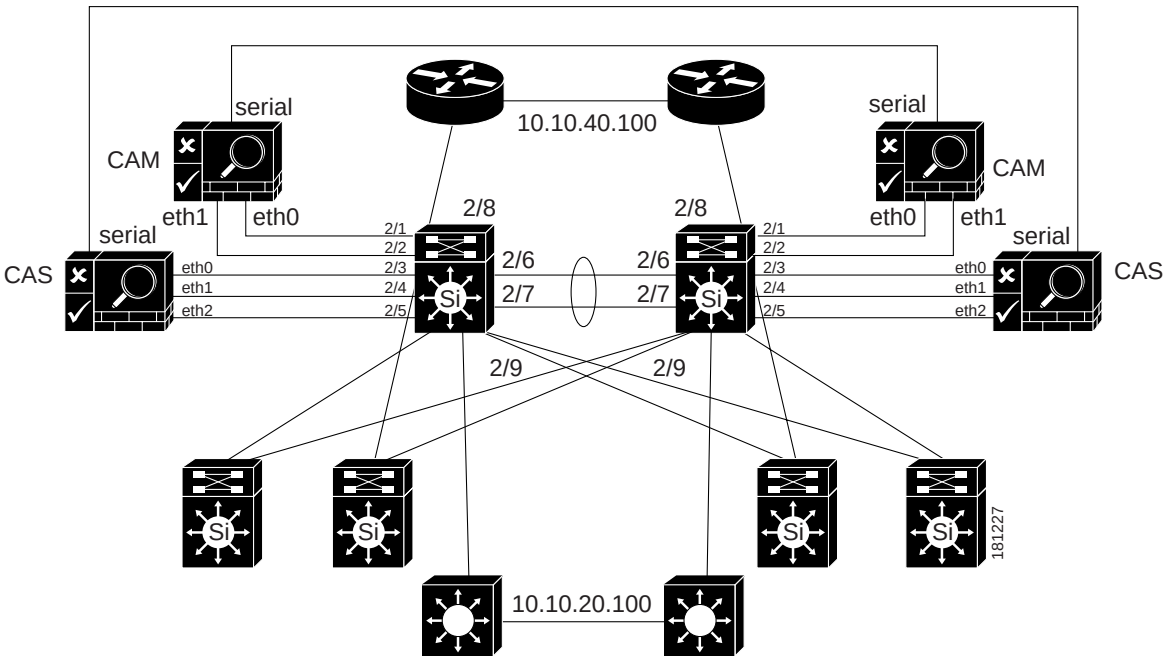


Figure 13-15 shows how HA-CASs can be added to the core-distribution-access network. In this example, the CAS is configured as an L2 OOB Virtual Gateway in Central Deployment. The HA heartbeat connection is configured over both a serial interface and a dedicated eth2 interface. Link-failure based failover connection can also be configured over the eth0 and/or eth1 interfaces.

Figure 13-15 Adding HA CAS to Network



T

U

V

W