Cisco NAC Appliance - Clean Access Server Configuration Guide

Release 4.8(1)
January 2011

Americas 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: 408 527-0883

Text Part Number: OL-19939-01

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco NAC Appliance - Clean Access Server Configuration Guide

CONTENTS

About This Guide xi

Audience xi

Purpose xi

Document Organization xii

Document Conventions xii

New Features in this Release xiii

Product Documentation xiii

Documentation Updates xv

Obtaining Documentation and Submitting a Service Request xv

xv

CHAPTER 1 Introduction 1-1

What Is Cisco NAC Appliance? 1-1

Cisco NAC Appliance Components 1-2

Clean Access Manager (CAM) 1-4

Clean Access Server (CAS) 1-4

Cisco NAC Appliance Agents 1-5

Cisco NAC Appliance Updates 1-5

Clean Access Server Features 1-5

CAS Management Pages Summary 1-6

Global vs. Local Administration Settings 1-7

Priority of Settings 1-8

CHAPTER 2 Planning Your Deployment 2-1

Overview 2-1

Clean Access Server Operating Modes 2-1

Real-IP Gateway 2-2

Virtual Gateway 2-2

Central Versus Edge Deployment 2-4

Routed Central Deployment (L2) 2-4

Multi-Hop L3 Deployment 2-6

Bridged Central Deployment 2-6

Edge Deployment 2-7

CAS Operating Mode Summary 2-8

CHAPTER 3 Configuring Layer 3 Out-of-Band (L3 OOB) 3-1

Overview 3-1

Layer 3 Out-of-Band Deployment Use Cases 3-3

Layer 2 vs Layer 3 Out-of-Band Implementation 3-3

Layer 3 Out-of-Band L3 OOB Details 3-3

Layer 3 OOB: Configuration 3-4

Layer 3 OOB: Configuration 3-4

Layer 3 OOB: Important Configuration Notes 3-5

Layer 3 OOB: Networking 3-7

CHAPTER 4 Configuring the CAS Managed Network 4-1

Overview 4-1

Add the CAS to the CAM 4-1

Add New Server 4-2

IP Addressing Considerations 4-3

Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments) 4-4

List of Clean Access Servers 4-5

Configure Clean Access Server-to-Clean Access Manager Authorization 4-6

Summary of Steps to Configure Clean Access Server-to-Clean Access Manager Authorization 4-6

Enable Authorization and Specify the Authorized Clean Access Manager 4-7

Troubleshooting when Adding the Clean Access Server 4-8

Configure Network Settings for the CAS 4-10

Navigating the CAS Management Pages 4-10

IP Form 4-11

Change Clean Access Server Type 4-13

Switching Between NAT and Real-IP Gateway Modes 4-14

Switching Between Virtual Gateway and NAT/ Real-IP Gateway Modes 4-14

Enable Network Access (L3, L3 Strict or L2 Strict) 4-15

Enable L3 Support 4-15

Enable L3 Strict Mode 4-17

Enable L2 Strict Mode 4-17

Connecting to the CAS Using the SWISS Protocol 4-19

What is the SWISS Protocol? 4-19

Discovery Host 4-21

VPN SSO Considerations 4-22

Overcoming Network Latency Issues That Can Delay Discovery 4-22

Using Layer 3 SWISS Packet Delay to Conserve Bandwidth 4-22
Supporting Multiple Active NICs on the Client Machine 4-23
Configuring DHCP 4-24
Configure DNS Servers on the Network 4-24
Configuring Managed Subnets or Static Routes 4-25
Overview 4-25
Configure Managed Subnets for L2 Deployments 4-27
Adding Managed Subnets 4-28
Configure Static Routes for L3 Deployments 4-29
Configuring Static Routes for Layer 2 Deployments 4-30
Add Static Route 4-30
Configure ARP Entries 4-31
Add ARP Entry 4-31
Understanding VLAN Settings 4-32
Enable Subnet-Based VLAN Retag in Virtual Gateway Mode 4-33
VLAN Mapping in Virtual Gateway Modes 4-34
Native VLAN, Management VLAN, Dummy VLAN 4-34
VLAN Mapping for In-Band 4-35
VLAN Mapping for Out-of-Band 4-35
Switch Configuration for Out-of-Band Virtual Gateway Mode 4-35
Configure VLAN Mapping 4-36
Local Device and Subnet Filtering 4-38
Configure Local Device Access Filter Policies 4-39
View Active L2 Device Filter Policies 4-42
Configure Subnet Access Filter Policies 4-43
CAS Fallback Policy 4-44
Configuring CAS Fallback 4-45
Configure Proxy Server Settings on the CAS 4-47

CHAPTER 5 Configuring DHCP 5-1
Overview 5-1
Enable the DHCP Module 5-2
Configure DHCP Relay or DHCP Server Mode 5-2
DHCP Status Options 5-4
Configuring IP Ranges (IP Address Pools) 5-5
Auto-Generated versus Manually Created Subnets 5-6
Subnetting Rules 5-6
Create IP Pools Manually 5-8

Auto-Generating IP Pools and Subnets 5-10
Add Managed Subnet 5-11
Create Auto-Generated Subnet 5-11
Working with Subnets 5-15
View Users by MAC Address/VLAN 5-15
View or Delete Subnets from the Subnet List 5-15
Edit a Subnet 5-16
Configuring a Real-IP CAS as DHCP Server for L3 Clients 5-18
Reserving IP Addresses 5-22
Add a Reserved IP Address 5-22
User-Specified DHCP Options 5-23
Global Action 5-30

CHAPTER 6 Integrating with Cisco VPN Concentrators 6-1
Overview 6-1
Single Sign-On (SSO) 6-2
Configure Cisco NAC Appliance for VPN Concentrator Integration 6-4
Add Default Login Page 6-5
Configure User Roles and Requirements 6-5
Enable L3 Support on the CAS 6-5
Verifying the Discovery Host 6-6
Adding/Editing VPN Concentrator Entries 6-6
Make CAS the RADIUS Accounting Server for VPN Concentrator 6-7
Adding/Editing Accounting Server Entries 6-8
Mapping VPN Concentrator(s) to Accounting Server(s) 6-9
Add VPN Concentrator as a Floating Device 6-10
Configure Single Sign-On (SSO) on the CAS/CAM 6-10
Configure SSO on the CAS 6-10
Configure SSO on the CAM 6-12
Configure VPN SSO in a FIPS 140-2 Compliant Deployment 6-13
Import a Trusted CA 6-13
Set up Identity certificate 6-14
Create a Site-to-Site VPN to CAS 6-15
Create (Optional) Auth Server Mapping Rules 6-17
Cisco NAC Appliance Agent with VPN Concentrator and SSO 6-18
Cisco NAC Appliance Agent Layer 3 VPN Concentrator User Experience 6-18
View Active VPN Clients 6-19

CHAPTER 7 Local Traffic Control Policies 7-1

Overview 7-1

Local vs. Global Traffic Policies 7-2

View Local Traffic Control Policies 7-3

Add Local IP-Based Traffic Control Policies 7-4

Add / Edit Local IP-Based Traffic Policy 7-4

Add Local Host-Based Traffic Control Policies 7-6

Enable Proxy Traffic 7-6

Add Local Allowed Host 7-8

Add Local Trusted DNS Server 7-9

View IP Addresses Used by DNS Host 7-9

Add Layer 2 Ethernet Traffic Control Policies 7-10

Enable Layer 2 Ethernet Traffic Control 7-11

Add Layer 2 Ethernet Traffic Control 7-12

Controlling Bandwidth Usage 7-14

CHAPTER 8 Configuring Active Directory Single Sign-On (AD SSO) 8-1

Overview 8-1

Cisco NAC Appliance Agent/AD Server Compatibility for AD SSO 8-2

Windows SSO Process (Kerberos Ticket Exchange) 8-2

CAS Communication with AD Server 8-4

AD SSO Configuration Step Summary 8-5

Configuration Prerequisites 8-5

Configuration Step Summary 8-6

Add Active Directory SSO Auth Server 8-6

Configure Traffic Policies for Unauthenticated Role 8-7

TCP/UDP Ports Supporting AD SSO Implementation 8-8

Add Policy for AD Server 8-9

Configure AD SSO on the CAS 8-11

Configuring a CAS User on the AD Server for AD SSO 8-14

Create the CAS User 8-14

Install and Run KTPass 8-18

Install the Correct Version of ktpass.exe to Support Your AD SSO Deployment 8-18

Run the ktpass.exe Command 8-22

Configure AD SSO Without KTPass 8-26

Configure AD SSO in a Windows 7 Client Environment 8-34

Enable Additional Algorithms on Existing AD Servers 8-35

Manually Enable DES on Individual Windows 7 Client Machines 8-36

Configure Active Directory for FIPS 140-2 Compliant AD SSO 8-36
Prerequisites 8-36
Configuring Your Windows Environment for FIPS 140-2 Compliance 8-37
Configure the User Profile 8-37
Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos) 8-40
Confirm Active AD SSO Service 8-41
Enable GPO Updates 8-41
Enabling a Login Script (Optional) 8-43
Introducing a Delay to Allow Script Use 8-44
Using Network-Based Scripts in Out-of-Band Mode with IP Address Changes 8-45
Reference Script 8-45
Delay Script with Delete Command 8-45
Add LDAP Lookup Server for Active Directory SSO (Optional) 8-46
Configure an LDAP Lookup Server 8-47
Cross-Forest Group Mapping using LDAP Lookup 8-47
Troubleshooting 8-48
General 8-48
KTPass Command 8-48
Cannot Start AD SSO Service on CAS 8-48
AD SSO Service Starts, But Client Not Performing SSO 8-49
Kerbtray 8-49
CAS Log Files 8-50
“Integrity check on decrypted field failed” Error 8-50

CHAPTER 9 Local Authentication Settings 9-1
Overview 9-1
Local Heartbeat Timer 9-1
Local Login Page 9-3
Add Local Login Page 9-3
Enabling Web Client for Local Login Page 9-4
Local File Upload 9-6
Enable Active Directory SSO Login 9-7
Enable Windows NetBIOS SSO Login 9-8
OS Detection 9-9

CHAPTER 10 Local Certified and Floating Devices 10-1
Overview 10-1
Add Exempt Devices 10-2

Clear Exempt Devices 10-3
Clear Certified Devices 10-3
Specify Floating Devices 10-4

CHAPTER 11 Administering CAS Certificates, Time, and Support Logs 11-1
Status Tab 11-1
Clean Access Server Direct Access Web Console 11-2
Manage CAS SSL Certificates 11-6
SSL Certificate Overview 11-6
Web Console Pages for SSL Certificate Management 11-7
CA-Signed Certificates 11-8
Intermediary Certificates 11-9
Certificates for High Availability (HA) Pairs 11-9
Regenerating Certificates for DNS Name Instead of IP 11-9
Typical SSL Certificate Setup on the CAS 11-10
Phase 1: Establish SSL Communication Between the CAS and CAM 11-10
Phase 2: Set Up Your CAS and CAM For Production Deployment 11-10
Phase 3: Adding a New CAM or CAS to an Existing Production Deployment 11-11
Generate Temporary Certificate 11-12
Generate and Export a Certification Request (Non-FIPS CAS Only) 11-14
Manage Signed Certificate/Private Key 11-16
Import Signed Certificate/Private Key 11-16
Export Certificate and/or Private Key 11-18
Manage Trusted Certificate Authorities 11-19
Import/Export Trusted Certificate Authorities 11-20
View Current Private Key/Certificate and Certificate Authority Information 11-21
SSL Requirements for Mac OS X/CAS Communication 11-23
CAS Temporary Certificate Requirements for SSL Connection to Mac OS X Agent 11-23
Installing the Root Certificate for Mac OS 10.4.x 11-23
Installing the Root Certificate for Mac OS 10.5 11-24
Enable the Root User on Mac OS X 11-27
Obtaining the Root Certificate from the CAS 11-28
Troubleshooting Certificate Issues 11-31
HA Active-Active Situation Due to Expired SSL Certificates 11-31
CAS Cannot Establish Secure Connection to CAM 11-32
Private Key in Clean Access Server Does Not Match the CA-Signed Certificate 11-32
Certificate-Related Files 11-32
System Upgrade 11-33
Synchronize System Time 11-35

Support Logs and LogLevel Settings 11-37

Downloading CAS Support Logs 11-38

Change the LogLevel Setting through CLI 11-40

APPENDIX A Open Source License Acknowledgements A-1

Notices A-1

OpenSSL/Open SSL Project A-1

License Issues A-1

A-3

INDEX

About This Guide

Revised January 31, 2011, OL-19939-01

This preface includes the following sections:

- Audience
- Purpose
- Document Organization
- Document Conventions
- New Features in this Release
- Product Documentation
- Documentation Updates
- Obtaining Documentation and Submitting a Service Request

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 Agent end-user client software. Use this document along with the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* and *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* to install, configure, and administer your Cisco NAC Appliance deployment.

Purpose

The *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)* describes how to configure the Clean Access Server to implement the Cisco NAC Appliance 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, configure your deployment to work with AD SSO, and perform CAS-specific (local) configuration tasks.

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

Document Organization

Table 1 Document Organization

Chapter	Description
Chapter 1, “Introduction”	Provides a high-level overview of the Cisco NAC Appliance solution
Chapter 2, “Planning Your Deployment”	Discusses planning considerations for deploying the software
Chapter 3, “Configuring Layer 3 Out-of-Band (L3 OOB)”	Provides a general overview of the configuration needed for Layer 3 Out-of-Band deployment
Chapter 4, “Configuring the CAS Managed Network”	Describes how to set up the Clean Access Server’s managed domain
Chapter 5, “Configuring DHCP”	Describes how to configure each of the DHCP modes of the Clean Access Server
Chapter 6, “Integrating with Cisco VPN Concentrators”	Describes the configuration required to integrate the Clean Access Server with Cisco VPN Concentrators
Chapter 7, “Local Traffic Control Policies”	Describes how to set up traffic filtering rules in the Clean Access Server
Chapter 8, “Configuring Active Directory Single Sign-On (AD SSO)”	Describes how to configure Active Directory (AD) Single Sign-On (SSO) for the Cisco NAC Appliance
Chapter 9, “Local Authentication Settings”	Describes Authentication tab settings in the Clean Access Server management pages
Chapter 10, “Local Certified and Floating Devices”	Describes local settings that can be configured at the Clean Access Server level for Clean Access implementation
Chapter 11, “Administering CAS Certificates, Time, and Support Logs”	Describes Clean Access Server (CAS) administration
Appendix A, “Open Source License Acknowledgements”	Contains Open Source License information for Cisco products

Document Conventions

Table 2 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

Table 2 Document Conventions

Item	Convention
Indicates web administrator console modules, menus, tabs, links and submenu links.	**Boldface** font
Indicates a menu item to be selected.	**Administration > User Pages**

New Features in this Release

For a brief summary of the new features and enhancements available in this release refer to Documentation Updates and the "New and Changed Information" section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

Product Documentation

This section 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 in Weblink in Browser."

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Appliance Service Contract/Licensing Support	• Obtaining and installing product licenses • Information on service contracts, ordering and RMA
Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later	• Agent System Requirements, Agent/Server Version Compatibility, Agent/OS/Browser Support Matrix, Agent/AD Server Compatibility for AD SSO, and Agent Localized Language Template Support
Switch Support for Cisco NAC Appliance	• Which switches and NMEs support OOB deployment • Known issues/troubleshooting for switches and WLCs
Getting Started with Cisco NAC Network Modules in Cisco Access Routers	• Installing or upgrading the Clean Access Server (CAS) software on the Cisco NAC network module (NME-NAC-K9)
Connecting Cisco Network Admission Control Network Modules	• Connecting Cisco NAC network module (NME-NAC-K9) in an Integrated Services Router

Table 3 Cisco NAC Appliance Document Set

Document Title	Refer to This Document For Information On:
Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide	• Provides instructions to upgrade your existing Cisco NAC-3310, NAC-3350, and NAC-3390 with a field-replaceable FIPS card necessary to introduce FIPS compliance in your network
Release Notes for Cisco NAC Appliance, Version 4.8(1)	Details on the latest 4.7 release, including: • New features and enhancements • Fixed caveats • Upgrade instructions • Supported AV/AS product charts • CAM/CAS/Agent compatibility and version information
Cisco NAC Appliance Hardware Installation Guide, Release 4.8	Details on CAM/CAS installation topics: • Hardware specifications on the various CAM/CAS platforms • How to install the Clean Access Manager and Clean Access Server Platforms • How to install Cisco NAC Appliance software on the CASM/CAS • How to configure CAM and CAS pairs for High Availability
Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)	Complete CAM details, including: • 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 CASs in the deployment)
Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)	CAS-specific details, including: • 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.

Documentation Updates

Table 4 Updates to Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.8(1)

Date	Description
1/31/11	Release 4.8(1)
10/5/10	Removed “Windows 2000 OS” support
7/26/10	Release 4.8

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What’s New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Introduction

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

- What Is Cisco NAC Appliance?, page 1-1
- Cisco NAC Appliance Components, page 1-2
- Clean Access Server Features, page 1-5
- CAS Management Pages Summary, page 1-6
- Global vs. Local Administration Settings, page 1-7

What Is Cisco NAC Appliance?

The Cisco Network Admission Control (NAC) Appliance (formerly 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 client posture assessment and remediation. 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 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).
- Cisco NAC Appliance compliance policies—Allows you to configure client posture assessment and remediation via use of Cisco NAC Appliance Agents 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 network only during posture assessment and remediation while bypassing it after certification.
- 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.

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

Cisco NAC Appliance Components

Cisco NAC Appliance is a network-centric integrated solution administered from the Clean Access Manager web console and enforced through the Clean Access Server and (optionally) the 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 Cisco NAC Appliance deployment. The secure web console of the Clean Access Manager is the single point of management for up to 20 Clean Access Servers in a deployment (or 40 CASs if installing a SuperCAM). For Out-of-Band (OOB) deployment, the web admin console allows you to control switches and VLAN assignment of user ports through the use of SNMP.

  Note The CAM web admin console supports Internet Explorer 6.0 or above only, and requires high encryption (64-bit or 128-bit). High encryption is also required for client browsers for web login and 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 Cisco NAC Appliance system requirements.

  You can install a CAS as either a stand-alone appliance (like the Cisco NAC-3300 series) or as a network module (Cisco NME-NAC-K9) in a Cisco ISR chassis and deploy it In-Band (always inline with user traffic) or Out-of-Band (inline with user traffic only during authentication/posture assessment). The CAS can also be deployed in Layer 2 mode (users are L2-adjacent to CAS) or Layer 3 mode (users are multiple L3 hops away from the CAS).

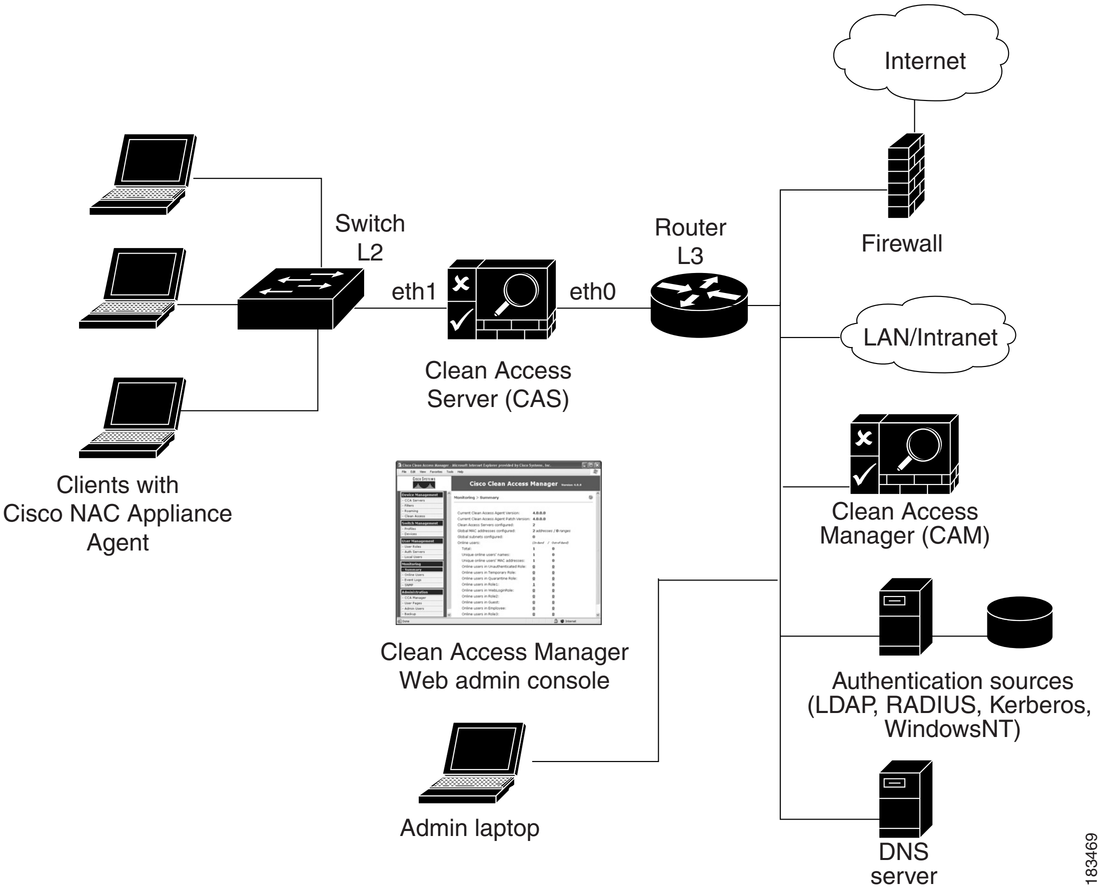
You can also deploy several CASs of varying size/capacity to fit the needs of varying network segments. You can install Cisco NAC-3300 series appliances in your company headquarters core, for example to handle thousands of users and simultaneously install one or more Cisco NAC network modules in ISR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

- **Cisco NAC Appliance Agents**—Optional read-only persistent or temporal Agents that reside on client machines. Cisco NAC Appliance Agent check applications, files, services, or registry keys to ensure that client machines meet your specified network and software requirements prior to gaining access to the network.

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

- **Cisco NAC Appliance 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 AV vendors and AS vendors.

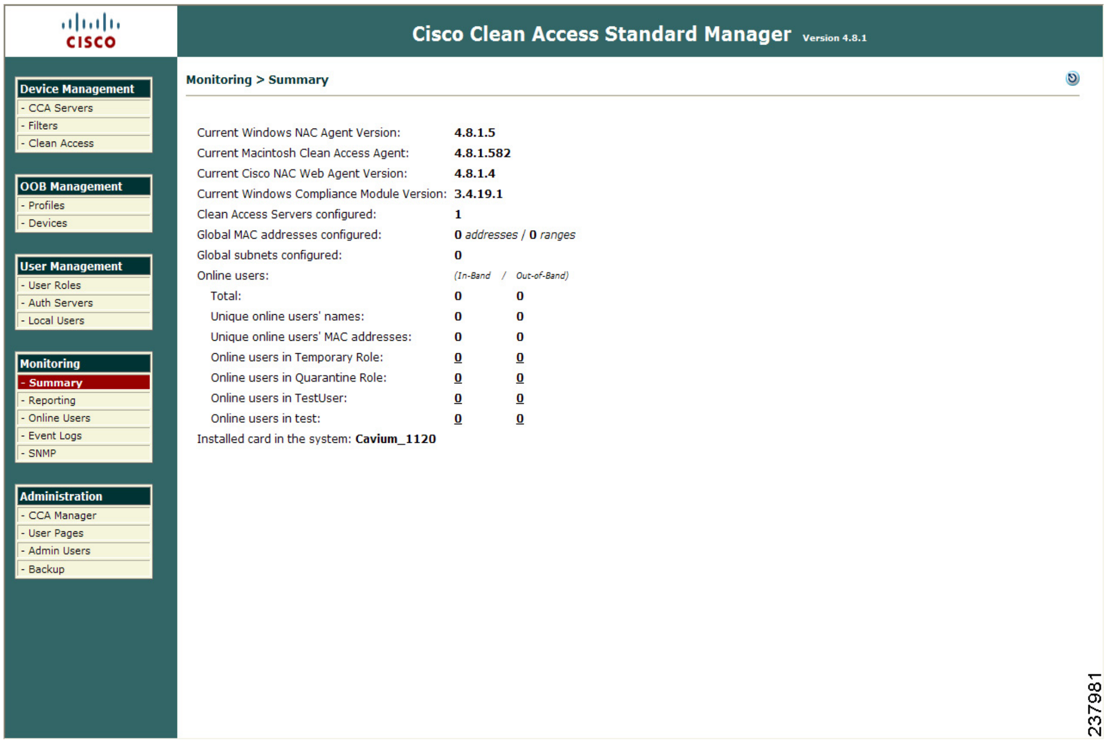
Figure 1-1 Cisco NAC Appliance Deployment (L2 In-Band Example)



Clean Access Manager (CAM)

The Clean Access Manager (CAM) is the administration server and database which centralizes configuration and monitoring of all Clean Access Servers, users, and policies in a Cisco NAC Appliance deployment. You can use it to manage up to 20 Clean Access Servers. The web admin console for the Clean Access Manager is a secure, browser-based management interface (Figure 1-2). See "Admin Console Summary" in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for a brief introduction to the modules of the web console. For out-of-band (OOB) deployment, the web admin console provides the **OOB Management** module to add and control switches in the Clean Access Manager's domain and configure switch ports.

Figure 1-2 CAM Web Admin Console



Cisco Clean Access Standard Manager Version 4.8.1

Monitoring > Summary

Current Windows NAC Agent Version:	4.8.1.5	
Current Macintosh Clean Access Agent:	4.8.1.582	
Current Cisco NAC Web Agent Version:	4.8.1.4	
Current Windows Compliance Module Version:	3.4.19.1	
Clean Access Servers configured:	1	
Global MAC addresses configured:	0 *addresses* / 0 *ranges*	
Global subnets configured:	0	
Online users:	*(In-Band* /	*Out-of-Band)*
Total:	0	0
Unique online users' names:	0	0
Unique online users' MAC addresses:	0	0
Online users in Temporary Role:	0	0
Online users in Quarantine Role:	0	0
Online users in TestUser:	0	0
Online users in test:	0	0
Installed card in the system: **Cavium_1120**		

Clean Access Server (CAS)

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

- IB Virtual Gateway (L2 transparent bridge mode)
- IB Real-IP Gateway
- OOB Virtual Gateway
- OOB Real-IP Gateway

The *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* describes the global configuration and administration of Clean Access Servers and Cisco NAC Appliance deployment using the Clean Access Manager web admin console.

Cisco NAC Appliance Agents

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

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

The Cisco NAC Appliance Agent types available in Cisco NAC Appliance are:

- Cisco NAC Agent (persistent Agent for Windows client machines)
- Windows Clean Access Agent (persistent Agent for Windows client machines available prior to release 4.6(1) with which release 4.7 is backward compatible)
- Mac OS X Clean Access Agent (persistent Agent for Macintosh client machines)
- Cisco NAC Web Agent (temporal Agent for Windows client machines)

For more information on the Agent types available in Cisco NAC Appliance, see the "Cisco NAC Appliance Agents" chapter in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Cisco NAC Appliance Updates

Regular updates of pre-packaged policies/rules can be used to check the up-to-date status of operating systems, antivirus/antispyware software, and other client software. Cisco NAC Appliance provides built-in support for major AV and AS vendors. For more information, see the "Retrieving Cisco NAC Appliance Updates" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

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
- Cisco NAC Appliance 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.

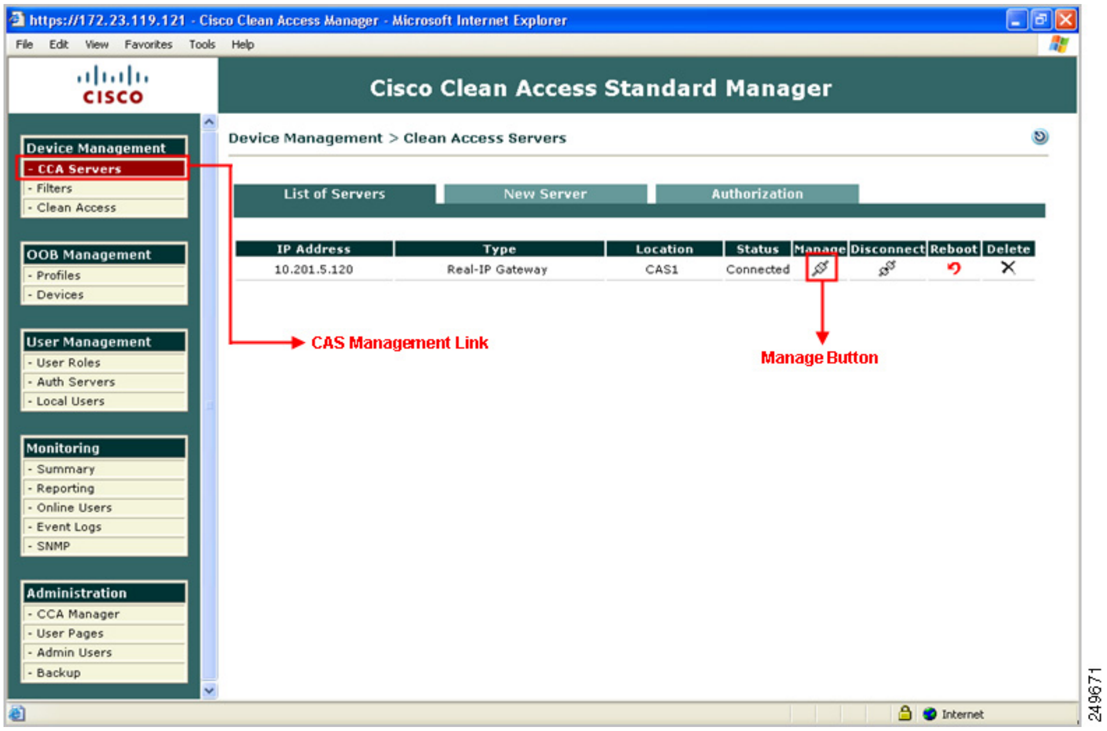
Note Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability.

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 4-1. 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.

Figure 1-3 Device Management > CCA Servers > List of Servers



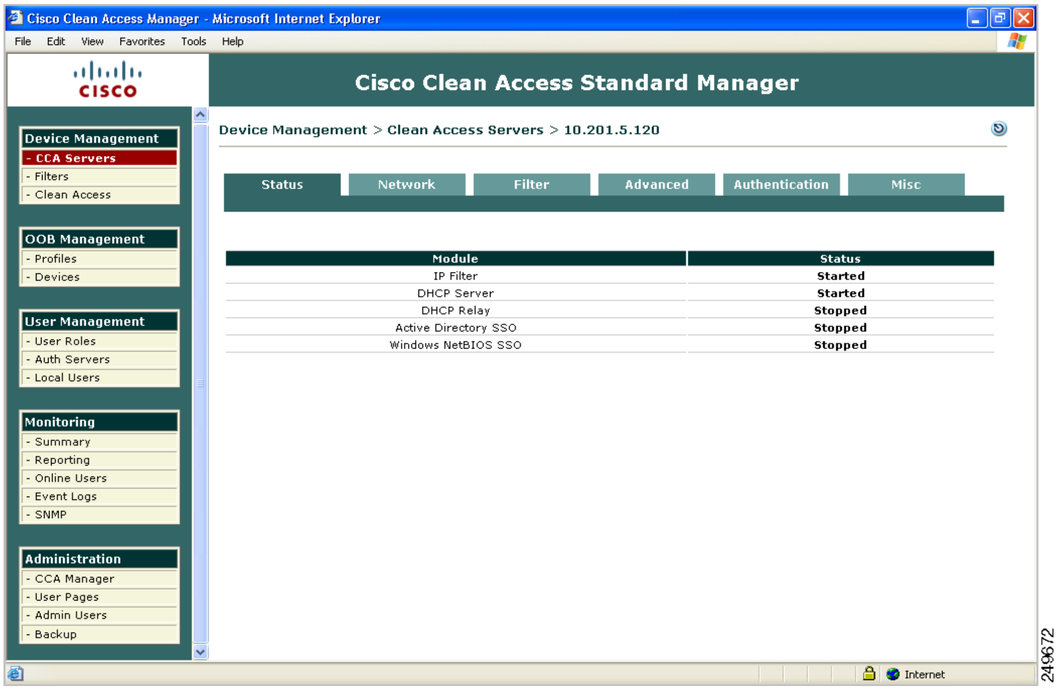
IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.5.120	Real-IP Gateway	CAS1	Connected				✕

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

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

3. The CAS management pages are shown in Figure 1-4. The **Status** tab of appears by default.

Figure 1-4 CAS Management Pages



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

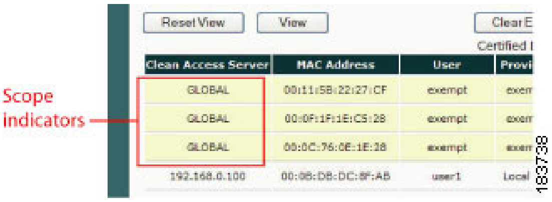
Global vs. Local Administration Settings

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

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

The global or local scope of a setting is indicated in the **Clean Access Server** column in the web admin console, as shown in Figure 1-5.

Figure 1-5 Scope of Settings



Scope Indicators

Clean Access Server	MAC Address	User	Provi
GLOBAL	00:11:5B:22:27:CF	exempt	exem
GLOBAL	00:0F:1F:1E:C5:28	exempt	exem
GLOBAL	00:0C:76:0E:1E:28	exempt	exem
192.168.0.100	00:0B:DB:DC:8F:AB	user1	Local

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

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

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

Priority of Settings

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

- For device filter policies affecting a *range* of MAC addresses and traffic control policies, the priority of the policy (higher or lower in **Device Management > Filters > Devices > Order**) determines which global or local policy to enforce. Any device filter policy for an individual MAC address takes precedence over a filter policy (either global or local) for a range of addresses that includes the individual MAC address.
- For subnet filter policies where one subnet filter specifies a subset of an address range in a broader subnet filter, the CAM determines the priority of the filter based on the size of the subnet address range. The smaller the subnet (like a /30 or /28 subnet mask), the higher the priority in the subnet filter hierarchy.
- Some features must be enabled on the CAS first (via the CAS management pages) before being configured in the CAM, for example:
  - Layer 3 support for the Agent (for multi-hop Layer 3 deployments)
  - Bandwidth Management
  - Use of VPN policy between CAS and users in user role
- Cisco NAC Appliance requirements and network scanning plugins are configured globally from the CAM and apply to all CASs.

CHAPTER 2

Planning Your Deployment

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

- Overview, page 2-1
- Clean Access Server Operating Modes, page 2-1
- Central Versus Edge Deployment, page 2-4

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 posture assessment, filtering and other services.
- **IB Real-IP Gateway**—Operates as the default gateway 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).

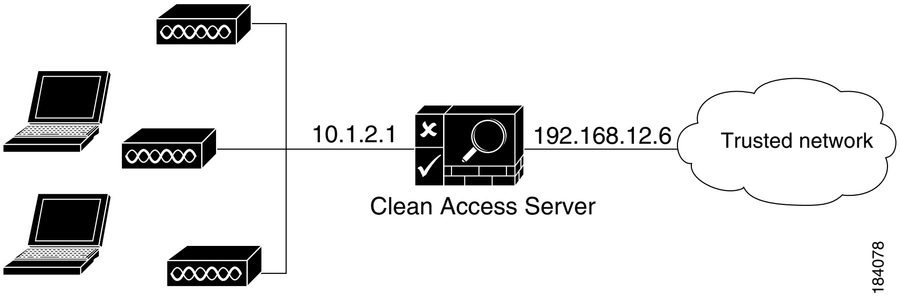
The Clean Access Manager can control both in-band and out-of-band CASs in its domain. However, the Clean Access Server itself must be *either* in-band or out-of-band.

For more information on OOB configuration in the CAM, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1).* 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 4-25.

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 4-25 and Chapter 5, "Configuring DHCP".

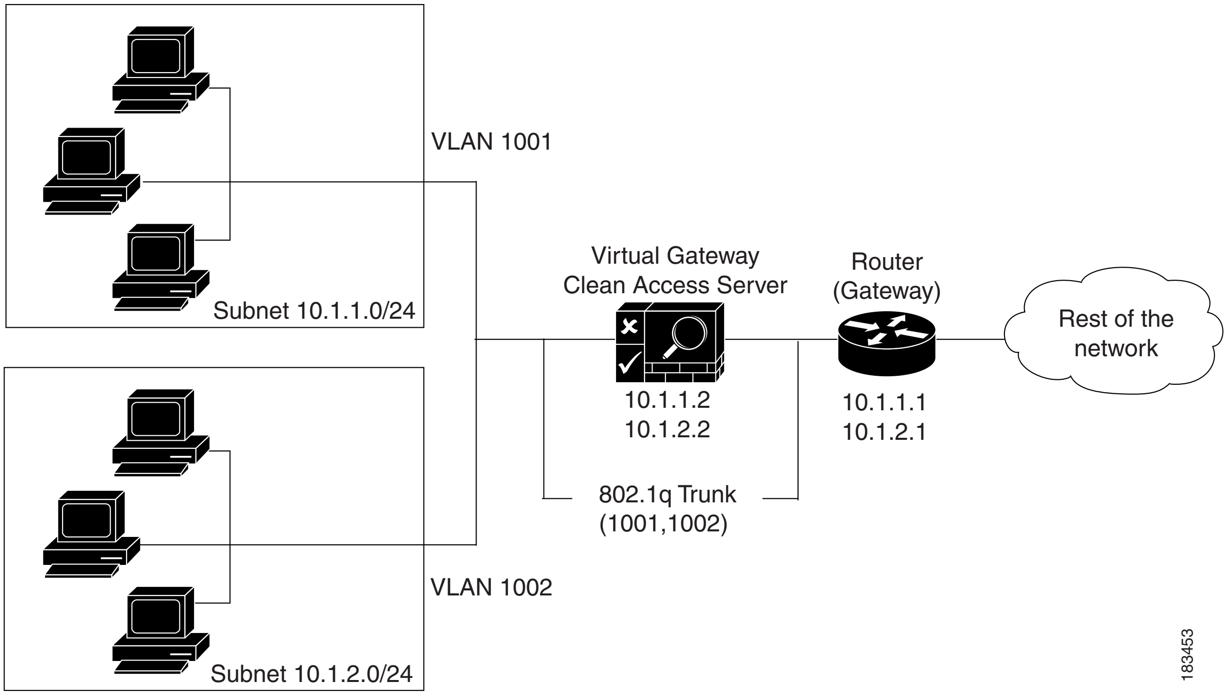
Virtual Gateway

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), Cisco recommends connecting 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, page 4-36.

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:

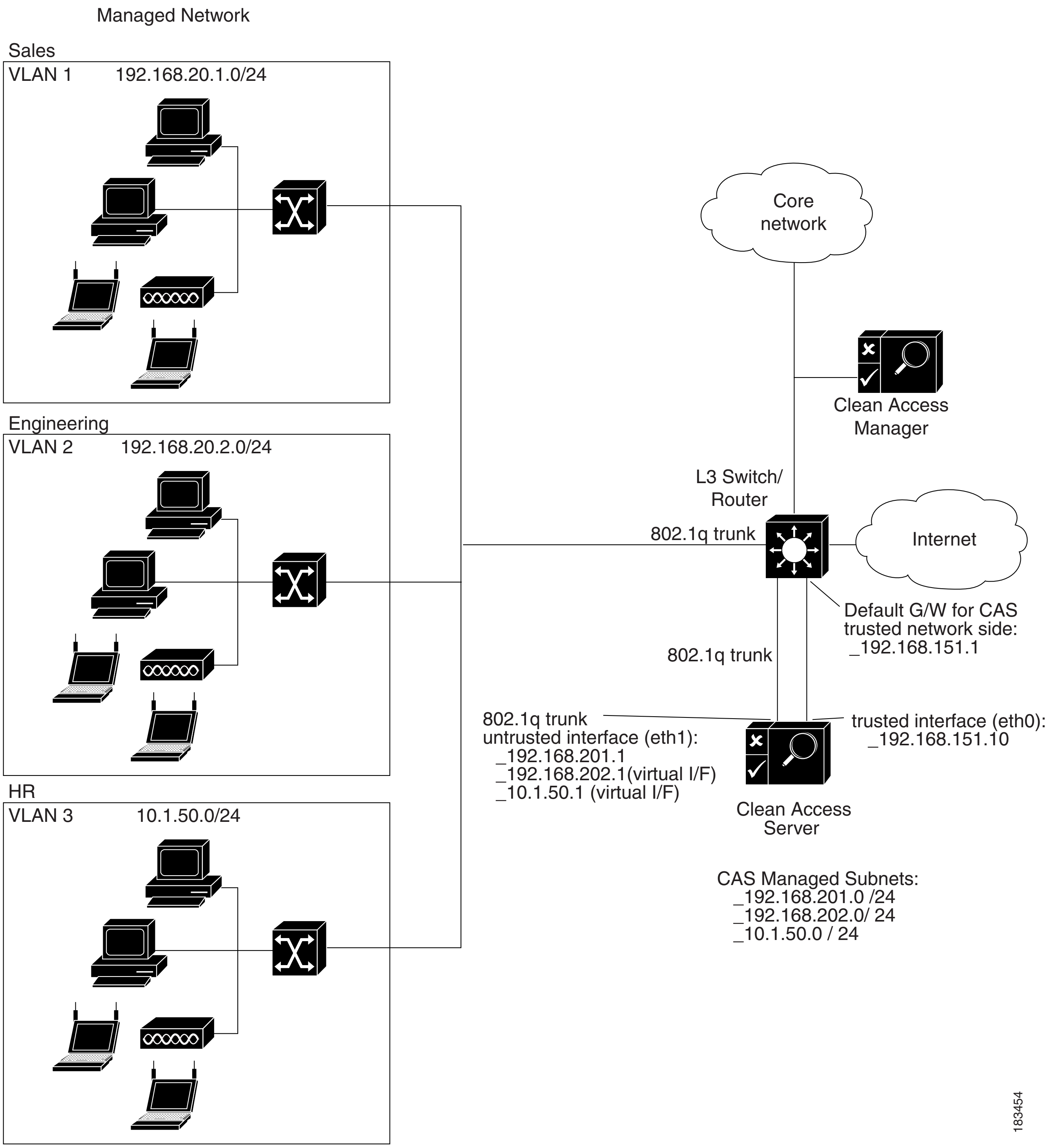
1. Turn off routing on your existing Layer 3 switch or router for the subnets that you wish to manage through the CAS.
2. Configure the untrusted interface of the CAS to be the gateway for the managed subnets.
3. Configure the default gateway of the CAS's trusted interface to be the L3 switch or the 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.

Note Agent communication with the CAS requires a Maximum Transmission Unit (MTU) of 1500 bytes. In routed or tunneled environments (like VPN, GRE, Metro Ethernet etc.), all hops must allow 1500 byte packets or support Path MTU Discovery (PMTU-D).

If there appears to be an issue with Agent communication in such environments yet basic IP connectivity has been verified, evaluate the MTU end-to-end. Please contact your Cisco WAN support representative for specific options to address this requirement.

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


Managed Network
Sales
VLAN 1 192.168.20.1.0/24
Engineering
VLAN 2 192.168.20.2.0/24
HR
VLAN 3 10.1.50.0/24
Core network
Clean Access Manager
L3 Switch/ Router
802.1q trunk
Internet
Default G/W for CAS trusted network side: _192.168.151.1
802.1q trunk
802.1q trunk untrusted interface (eth1): _192.168.201.1 _192.168.202.1(virtual I/F) _10.1.50.1 (virtual I/F)
trusted interface (eth0): _192.168.151.10
Clean Access Server
CAS Managed Subnets: _192.168.201.0 /24 _192.168.202.0/ 24 _10.1.50.0 / 24
183454

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 CASs 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:

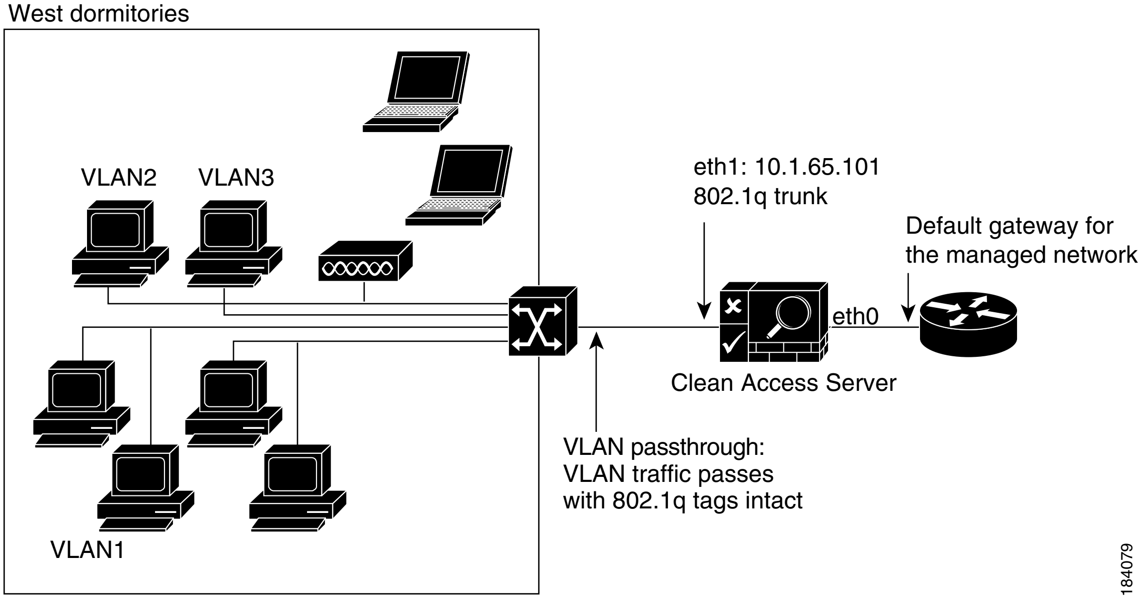
1. Enable L3 on the CAS by going to **Device Management > CCA Servers > Manage [CAS_IP] > Network** and clicking the checkbox for **Enable L3 support for Clean Access Agent**.
2. Managed subnets should be configured for user subnets that are Layer 2 adjacent to the CAS. For user subnets that are one 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. Ensure the IP address in the **Discovery Host** field under **Device Management > Clean Access > Clean Access Agent > Installation** is the correct address for your network.
4. If enabling the L3 multi-hop feature for VPN concentrator integration, perform all the configuration described in Chapter 6, “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, Cisco recommends deploying 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.

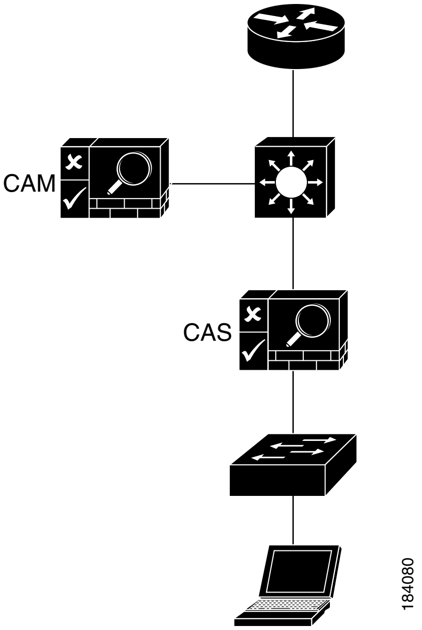
Figure 2-4 Bridged Central Deployment in a VLAN-Enabled Network



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.
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.
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 4.1.1.0+ Agent or ActiveX/ Java Applet downloaded from web login page.

CHAPTER 3

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 Configuration Guide, Release 4.8(1).*

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—Agent or ActiveX/Java Applet

The MAC detection mechanism of the Agent automatically acquires the client MAC address in L3 OOB deployments.

Users performing web login will download and execute either an ActiveX 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.

Agent Login for L3 OOB Users

Cisco NAC Appliance enables multi-hop L3 support for out-of-band (wired) deployments, enabling 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.

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

Users performing web login will download and execute either an ActiveX 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

- Complete ActiveX/Java Applet and Browser Compatibility information is available in *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.
- Java applets are supported for major browsers including Safari 1.2+, Mozilla (Camino, Opera), and Internet Explorer on Windows XP, Mac OS X, 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 X Clients:** On Apple Mac OS X, 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 X 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 ActiveX 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 ActiveX 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 2 vs Layer 3 Out-of-Band 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 Agent

The Agent will inform CAS of the device MAC address.

Without the Agent (using Web Login)

- Web-login page will download ActiveX 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 the Agent

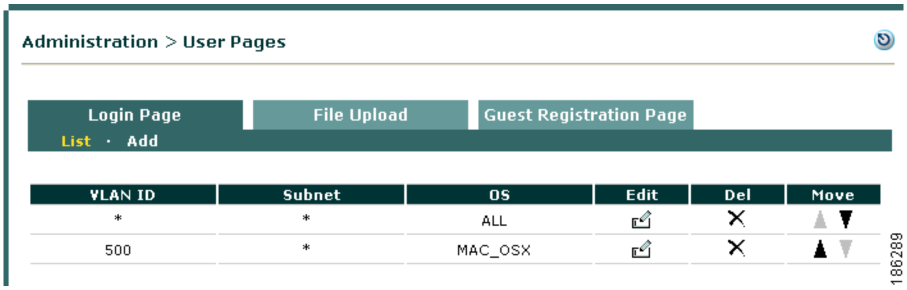
- Agent informs CAS of MAC address
- No additional configuration is needed

Without the Agent (using Web Login)

Configure the Login Page

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

Figure 3-1 Administration User Page



Administration > User Pages

VLAN ID	Subnet	OS	Edit	Del	Move
*	*	ALL	✎	✕	▼
500	*	MAC_OSX	✎	✕	▲

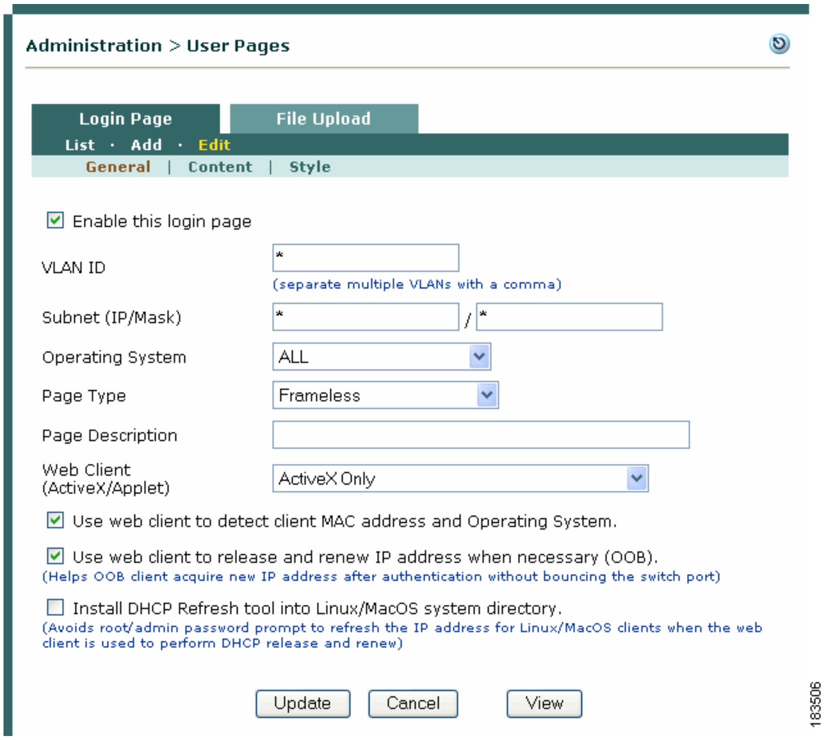
Layer 3 OOB: Configuration

- On Login Page, there is a checkbox and a “Use ActiveX or Java Applet to detect client MAC address when Clean Access Server cannot detect the MAC address” dropdown menu 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
- Java Applet supported on most browsers

Note DHCP IP addresses can be refreshed for client machines using the 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 Configuration Guide, Release 4.8(1)* for further details.

For detailed information on Access to Authentication VLAN change detection, refer to the “Configuring Access to Authentication VLAN Change Detection” section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Figure 3-2 Administration User Page Edit



☑ Enable this login page

VLAN ID: *
(separate multiple VLANs with a comma)

Subnet (IP/Mask): * / *

Operating System: ALL

Page Type: Frameless

Page Description:

Web Client (ActiveX/Applet): ActiveX Only

☑ Use web client to detect client MAC address and Operating System.

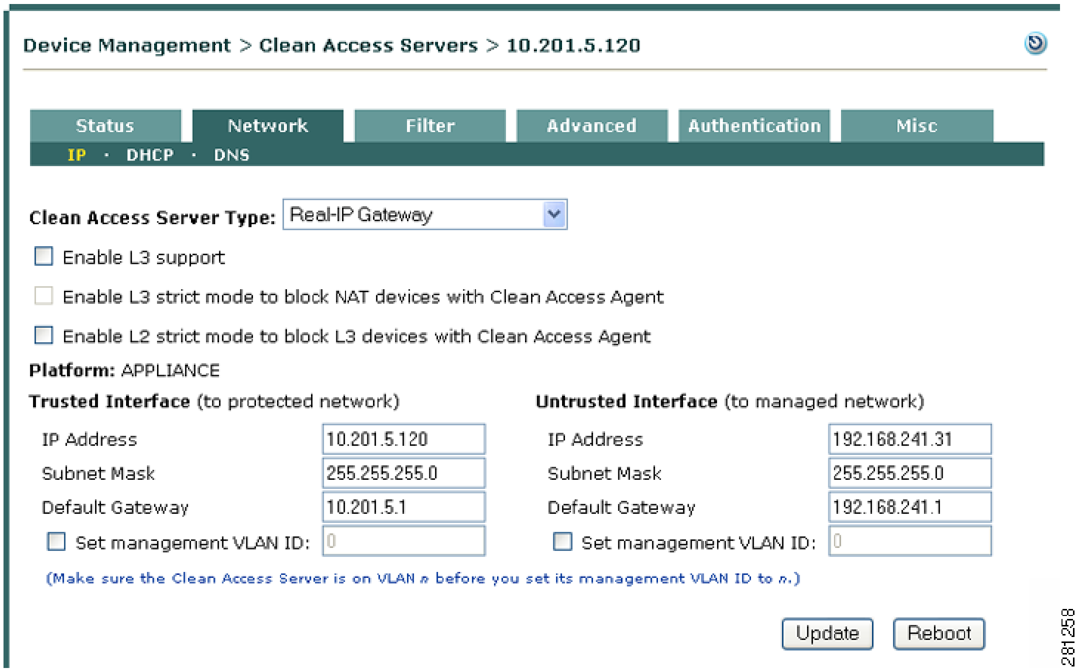
☑ Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

☐ Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

Layer 3 OOB: Important Configuration Notes

- If a Managed Subnet is configured, Cisco NAC Appliance does 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**.

Figure 3-3 Enabling L3 Support



Device Management > Clean Access Servers > 10.201.5.120

Clean Access Server Type: Real-IP Gateway

□ Enable L3 support

□ Enable L3 strict mode to block NAT devices with Clean Access Agent

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

Platform: APPLIANCE

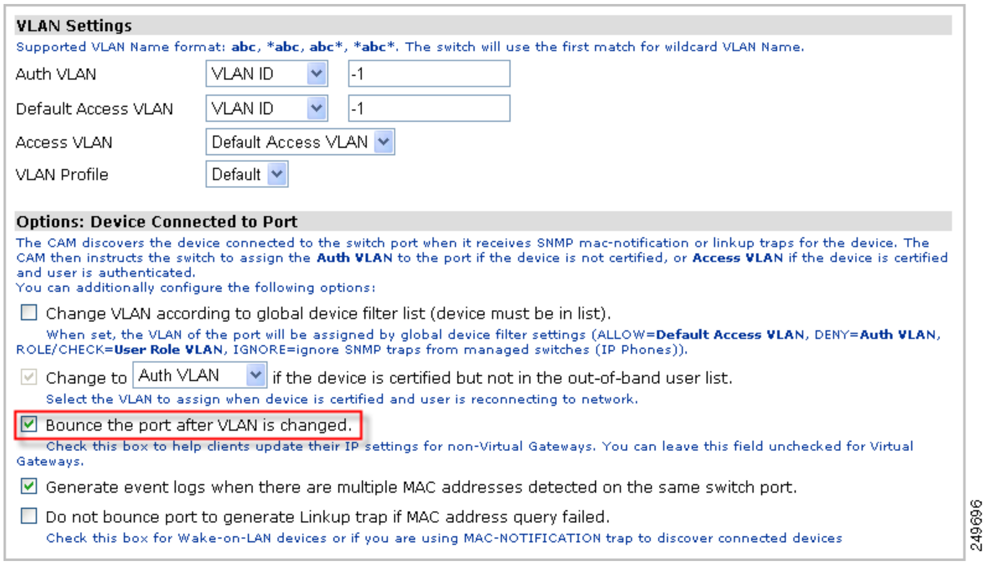
Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

- Client machines should be able to execute either ActiveX or Java Applet.
- When the CAM changes the VLAN on the switch port from the Authentication 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.

    or
  - If using a version 4.1.2.0 or later Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses, the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled. If you use this method, be sure to follow the guidelines and warnings detailed in the “DHCP Release/Renew with Agent/ActiveX/Java Applet,” “Configuring Access to Authentication VLAN Change Detection,” and “Advanced Settings” sections of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Figure 3-4 VLAN Setting Changes to Bounce a Port



VLAN Settings

Supported VLAN Name format: **abc**, ***abc**, **abc***, ***abc***. The switch will use the first match for wildcard VLAN Name.

Auth VLAN	VLAN ID	-1
Default Access VLAN	VLAN ID	-1
Access VLAN	Default Access VLAN	
VLAN Profile	Default	

Options: Device Connected to Port

The CAM discovers the device connected to the switch port when it receives SNMP mac-notification or linkup traps for the device. The CAM then instructs the switch to assign the **Auth VLAN** to the port if the device is not certified, or **Access VLAN** if the device is certified and user is authenticated.
You can additionally configure the following options:

☐ Change VLAN according to global device filter list (device must be in list).
When set, the VLAN of the port will be assigned by global device filter settings (ALLOW=**Default Access VLAN**, DENY=**Auth VLAN**, ROLE/CHECK=**User Role VLAN**, IGNORE=ignore SNMP traps from managed switches (IP Phones)).

☑ Change to Auth VLAN if the device is certified but not in the out-of-band user list.
Select the VLAN to assign when device is certified and user is reconnecting to network.

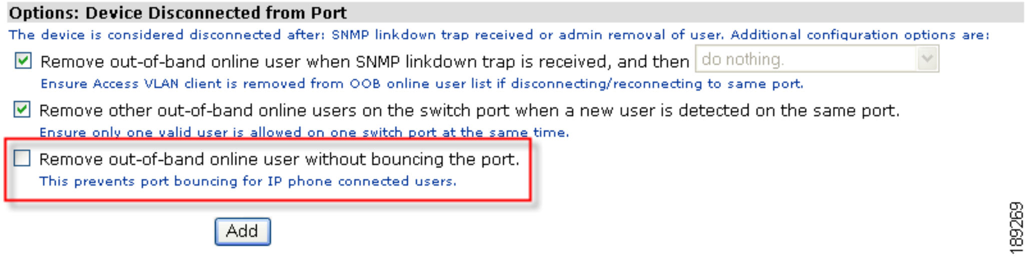
☑ Bounce the port after VLAN is changed.
Check this box to help clients update their IP settings for non-Virtual Gateways. You can leave this field unchecked for Virtual Gateways.

☑ Generate event logs when there are multiple MAC addresses detected on the same switch port.

☐ Do not bounce port to generate Linkup trap if MAC address query failed.
Check this box for Wake-on-LAN devices or if you are using MAC-NOTIFICATION trap to discover connected devices

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

Figure 3-5 Unchecked OOB Selection



Options: Device Disconnected from Port

The device is considered disconnected after: SNMP linkdown trap received or admin removal of user. Additional configuration options are:

☑ Remove out-of-band online user when SNMP linkdown trap is received, and then do nothing.
Ensure Access VLAN client is removed from OOB online user list if disconnecting/reconnecting to same port.

☑ Remove other out-of-band online users on the switch port when a new user is detected on the same port.
Ensure only one valid user is allowed on one switch port at the same time.

☐ Remove out-of-band online user without bouncing the port.
This prevents port bouncing for IP phone connected users.

Layer 3 OOB: Networking

- Cisco recommends adding an ACL on your network access switch(es) to prevent SWISS packets from traversing the access VLAN. This simultaneously cuts down on unnecessary packets on the access network, and can help prevent authentication looping on the client machine when SWISS packets make it back to the CAS.

Note Web login redirection could fail or the Agent may not pop up in a Layer 3 OOB Real-IP deployment using ACLs. For Layer 3 OOB deployments where Access Control Lists are used to allow or block client machine discovery packets, the CAS certificate and Discovery Host should be the same untrusted interface IP address or hostname. In addition, the SWISS discovery mechanism for Layer 3 OOB requires that an ACL configured on the network authentication switch allows TCP/UDP port 8905 traffic for the Authentication VLAN to the CAS untrusted interface, while blocking TCP/UDP port 8905 traffic on the Access VLAN to the CAS untrusted interface. (These ACLs are not necessary if your Layer 3 OOB deployment employs Policy Based Routing.)

- 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.
- The following failure scenarios might cause the Cisco NAC Agent to appear following successful user authentication when the client machine roams between CASs in Layer 3 (both In-Band and Out-of-Band) and Layer 2 /Layer 3 Out-of-Band environments. Erroneous Agent login dialogs could also appear if users roam from the Cisco NAC Appliance network in Layer 3 mode to a non-NAC network:
  - ARP poisoning
  - Temporary loss of network connection between the client machine and the CAS
  - Access to untrusted interface IP address on the CAS from non-NAC network segments on NAC-enabled client machines

  Cisco offers the following recommendations to prevent this situation:
  - Ensure all trusted networks (post-authentication) can reach the CAS untrusted interface IP address through the CAS trusted interface only
  - Block discovery packets from all non-NAC networks to the CAS untrusted interface IP address (discovery packets that arrive on the trusted interface of the CAS are blocked by default)

Note These scenarios are not specific to OOB logoff feature and represent general Cisco NAC Agent behavior for some Out-of-Band topologies.

CHAPTER 4

Configuring the CAS Managed Network

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

- Overview, page 4-1
- Add the CAS to the CAM, page 4-1
- Configure Network Settings for the CAS, page 4-10
- Connecting to the CAS Using the SWISS Protocol, page 4-19
- Configuring DHCP, page 4-24
- Configure DNS Servers on the Network, page 4-24
- Configuring Managed Subnets or Static Routes, page 4-25
- Configure ARP Entries, page 4-31
- Understanding VLAN Settings, page 4-32
- VLAN Mapping in Virtual Gateway Modes, page 4-34
- Local Device and Subnet Filtering, page 4-38
- CAS Fallback Policy, page 4-44
- Configure Proxy Server Settings on the CAS, page 4-47

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:

- Add New Server, page 4-2
- IP Addressing Considerations, page 4-3
- Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments), page 4-4

- List of Clean Access Servers, page 4-5
- Configure Clean Access Server-to-Clean Access Manager Authorization, page 4-6
- Troubleshooting when Adding the Clean Access Server, page 4-8

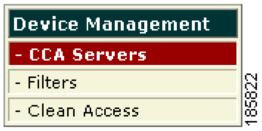
The Clean Access Server gets almost all of its runtime parameters from the Clean Access Manager, and cannot operate unless it is added to the domain of a Clean Access Manager. Once it is added to the CAM, the CAS can be configured and monitored through the admin console.

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.

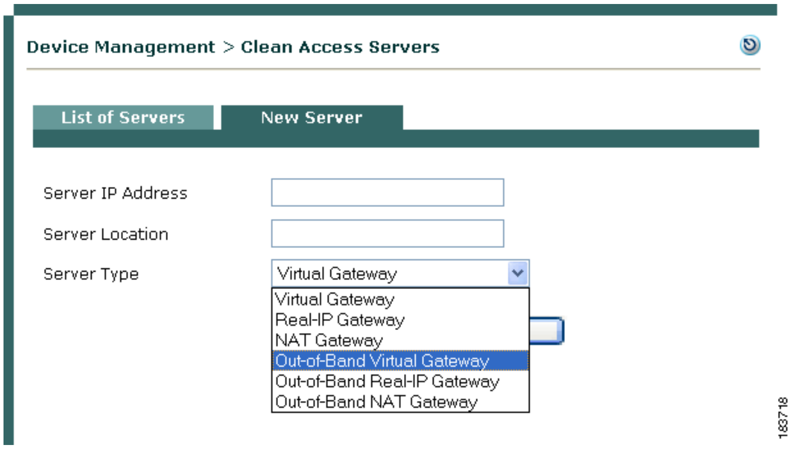
For Virtual Gateway with VLAN mapping (In-Band or OOB), the untrusted interface (eth1) of the CAS should not be connected to the switch until VLAN mapping has been configured correctly under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > VLAN Mapping**. See Additional Notes for Virtual Gateway with VLAN Mapping (L2 Deployments), page 4-4 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 4-1 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 4-4.

   - **Real-IP Gateway**—CAS operates as a gateway for the untrusted network

6. The Out-of-Band Server Types appear in the dropdown menu when you apply an OOB-enabled license to a Cisco NAC Appliance deployment. For OOB, the CAS operates as a Virtual or Real-IP Gateway while client traffic is In-Band (in the Cisco NAC Appliance network) during authentication and certification. Once clients are authenticated and certified, they are considered "out-of-band" (no longer passing through the Cisco NAC Appliance 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).

   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 Configuration Guide, Release 4.8(1).*

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 (IB 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 Mode:

- 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.

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, page 4-36 for detailed steps.
4. If the CAM is down and the CAS is performing VLAN mapping in "fail open" state, do not reboot the CAS because the VLAN mapping capability will be lost until the CAM comes back online.

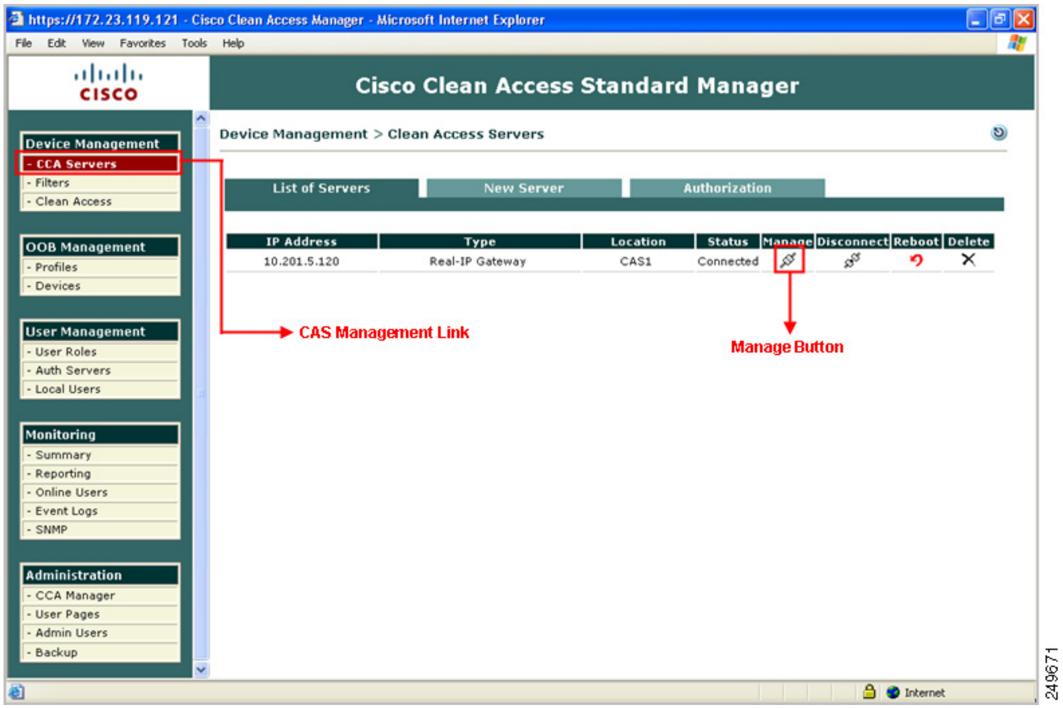
Caution To avoid switch errors, make sure to correctly set VLAN Mapping in the CAS before connecting the eth1 interface of the CAS. Failure to do so could cause spanning tree loops and shut down the switch.

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 4-2 List of Servers



IP Address	Type	Location	Status	Manage	Disconnect	Reboot	Delete
10.201.5.120	Real-IP Gateway	CAS1	Connected			↺	✕

CAS Management Link

Manage Button

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.

Configure Clean Access Server-to-Clean Access Manager Authorization

When you add Clean Access Servers to the CAM, you can also choose to enable mutual Authorization between the appliances to enhance network security.

Using the CAM Authorization web console page, administrators can enter the Distinguished Names (DNs) of one or more CASs to ensure secure communications between the CAM and CAS(s). Once you enable the Authorization feature and add one or more CASs to the Authorized CCA Servers list, the CAM does not accept communications from CASs that do not appear in the list. Therefore, when you choose to employ and enable this feature in your network, you must add *all* of your managed CASs to the Authorized CCA Servers list to ensure you maintain CAM-CAS connection for all of the CASs in your network.

Likewise, you must also enable this feature and specify a CAM DN on all of the CASs in your network to establish two-way authorization between the CAMs/CASs.

Note Administrators should expect a few minutes of downtime when updating Trusted CAs on the CAS, as updating certificate information restarts services. This is due to the fact that the CAM/CAS use mutual authentication to communicate back and forth and although you are no longer required to reboot the CAS when you change the certificate or import new Trusted CAs, the CAM-to-CAS connections are still "reset" to ensure network security. Therefore, Cisco recommends performing this type of action during periods of very low Cisco NAC Appliance network traffic.

If you have deployed your CAMs/CASs in an HA environment, you can enable authorization for both the HA-Primary and HA-Secondary machines in the HA pair by specifying the DN of only the HA-Primary appliance. For example, if the CAM manages a CAS HA pair, you only need to list the HA-Primary CAS on the CAM's Authorization page. Likewise, if you are enabling this feature on a CAS managed by a CAM HA pair, you only need to list the HA-Primary CAM on the CAS's Authorization page.)

Summary of Steps to Configure Clean Access Server-to-Clean Access Manager Authorization

1. Configure CAS Authorization on the CAM web console under **Device Management > Clean Access Servers > Authorization** (see Enable Authorization and Specify the Authorized Clean Access Manager, page 4-7).
2. Configure CAM Authorization on the CAS web console under **Administration > Authorization** (see the "Enable Authorization and Specify Authorized Clean Access Servers" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*).
3. Before deploying in a production environment, obtain trusted CA-signed certificates for CAM and CAS and import them to CAM/CAS under **Administration > SSL > Trusted Certificate Authorities** (for CAM), and **Administration > SSL > Trusted Certificate Authorities** (for CAS).

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

4. If you are upgrading your Cisco NAC Appliance release, clean up Trusted Certificate Authorities on the CAM under **Administration > CCA Manager > SSL > Trusted Certificate Authorities**, and on the CAS under **Administration > SSL > Trusted Certificate Authorities** (see Manage Trusted Certificate Authorities, page 11-19 and the “View and Remove Trusted Certificate Authorities” section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*, respectively).

Note If you use the Authorization feature in a CAS HA-pair, follow the guidelines in “Backing Up and Restoring CAM/CAS Authorization Settings” in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* to ensure you are able to exactly duplicate your Authorization settings from one CAS to its high availability counterpart.

Enable Authorization and Specify the Authorized Clean Access Manager

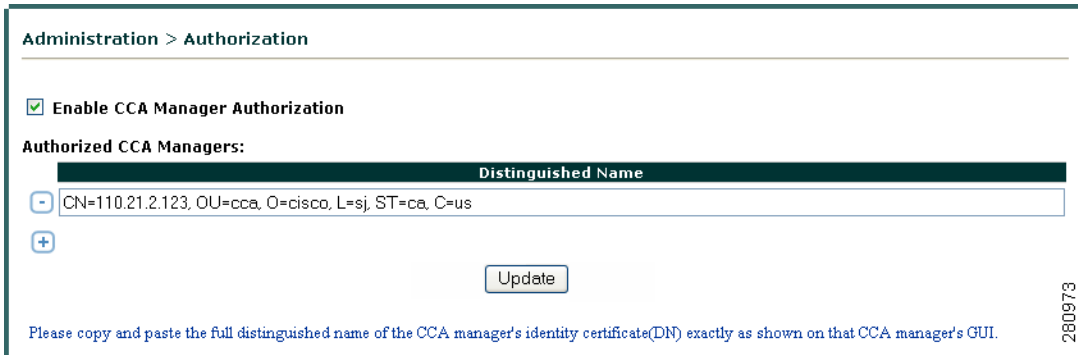
To enable authorization and specify the CAM authorized to communicate with your CAS:

Step 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_address*>**/admin**). For example:

```
https://172.16.1.2/admin
```

Step 2 Go to **Administration > Authorization** (Figure 4-3).

Figure 4-3 Administration > Authorization



Administration > Authorization

☑ Enable CCA Manager Authorization

Authorized CCA Managers:

	Distinguished Name
-	CN=110.21.2.123, OU=cca, O=cisco, L=sj, ST=ca, C=us
+	

Update

Please copy and paste the full distinguished name of the CCA manager's identity certificate(DN) exactly as shown on that CCA manager's GUI.

Step 3 Click the **Enable CCA Server Authorization** to turn on the Cisco NAC Appliance authorization feature.

Warning **Do not click the Enable CCA Server Authorization option without also entering one or more full distinguished names of CAMs you want to authorize to communicate securely with the CAS. If you enable this feature and have not specified any CAM distinguished names, you will not be able to communicate with any of the CAMs in your network.**

Step 4 Click the plus icon “+” and enter the full distinguished name of the CAM you want to authorize to communicate securely with the CAS. For example, enter a text string like “CN=110.21.2.123, OU=cca, O=cisco, L=sj, ST=ca, C=us” in the Distinguished Name field.

Note Distinguished names require exact syntax. Therefore, Cisco recommends copying the CAM DN from the "CCA Manager Certificate" entry in the certificate information table in the **Administration > CCA Manager > SSL > X509 Certificate** CAM web console page and pasting it into the CAS's Authorization page to ensure you specify the exact name for the CAM on the CAS.

Step 5 Click **Update** to ensure the CAM you have added is authorized to communicate back-and-forth with the CAS.

When you click **Update**, the CAS restarts services between the CAS and CAM in the Authorized CCA Manager list, which may cause brief network interruptions to users logged into the Cisco NAC Appliance system.

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 the "CAS CLI Commands" section in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* 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 SSL certificates. For details, see Typical SSL Certificate Setup on the CAS, page 11-10 and Troubleshooting Certificate Issues, page 11-31 in this guide, and the corresponding sections of the CAS guide.
4. 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 the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* and *Cisco NAC Appliance Service Contract/Licensing Support* for more details.
5. 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`
6. If the CAS is a Virtual Gateway, make sure the CAM and CAS are on different subnets (or VLANs).
7. If the CAS is a Virtual Gateway, and both ports of the CAS are connected to the same switch:
   a. Physically disconnect 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.

8. Check the CAM Event Log (under **Monitoring > Event Logs**). This can help pinpoint license and other issues.

9. Make sure there are no firewall rules blocking RMI ports (see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details):

10. Perform `service perfigo restart` on both the CAM and CAS.

11. Perform `service perfigo reboot` on both CAM and CAS.

12. Contact TAC. See Obtaining Documentation and Submitting a Service Request, page xv.

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 Configuration Guide, Release 4.8(1).*

Configure Network Settings for the CAS

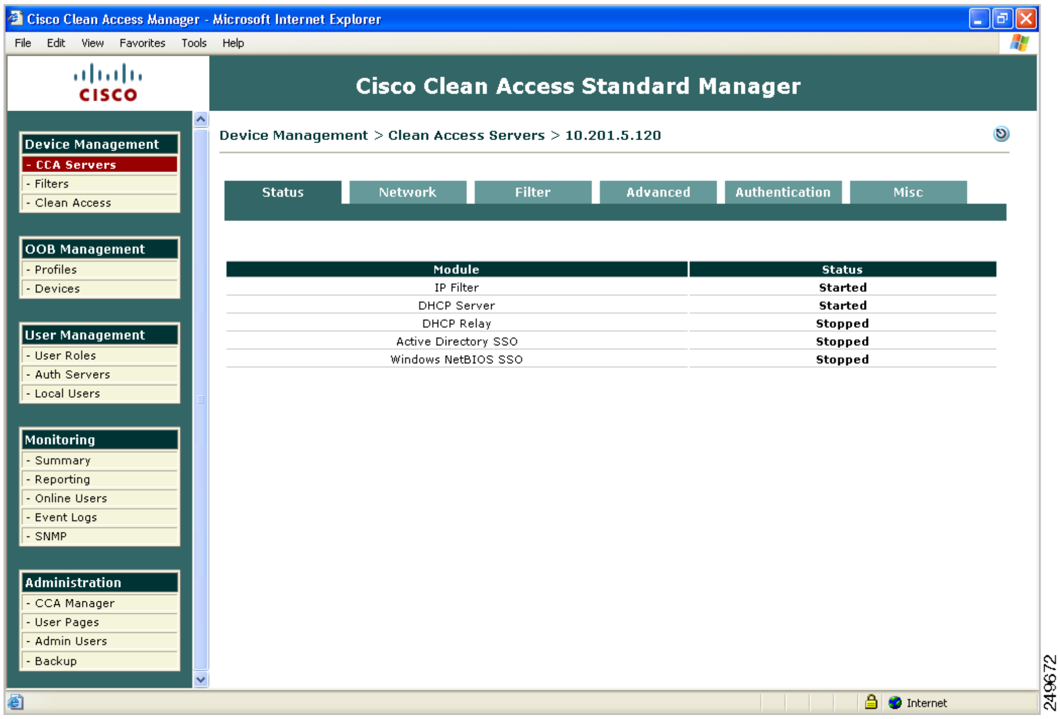
This section describes the following:

- Navigating the CAS Management Pages, page 4-10
- IP Form, page 4-11
- Change Clean Access Server Type, page 4-13
- Enable L3 Support, page 4-15

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 4-4.

Figure 4-4 Clean Access Servers Management Pages



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

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.

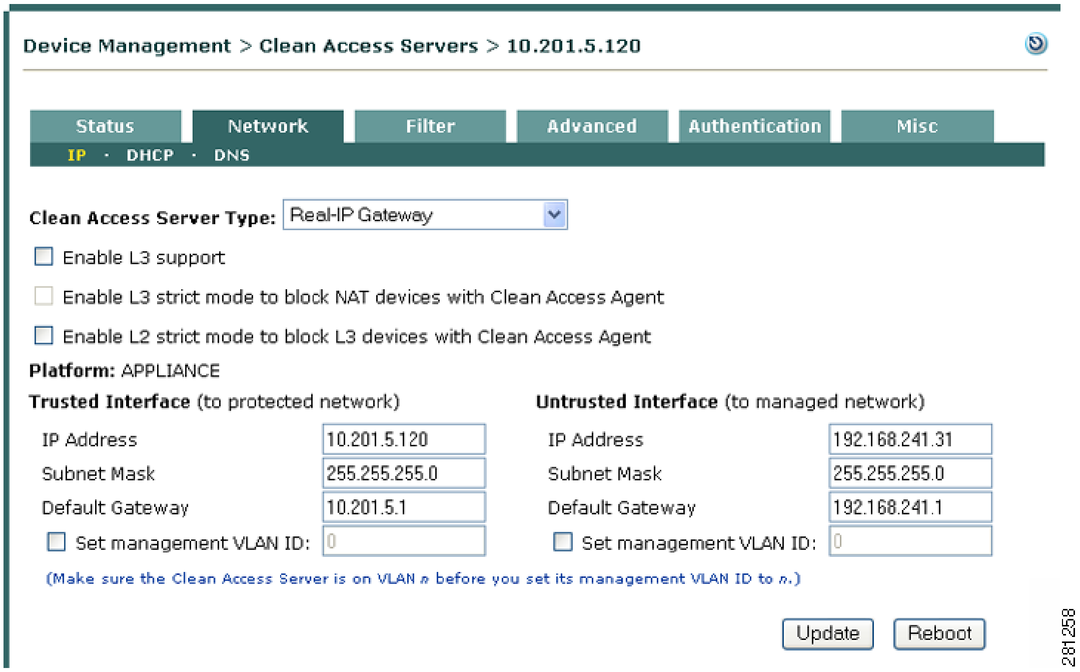
Within each tab, click the submenu links to access individual configuration forms.

IP Form

The **IP** form in the **Network** tab (Figure 4-5) 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 4-5 CAS Network IP Settings



Clean Access Server Type: Real-IP Gateway

□ Enable L3 support

□ Enable L3 strict mode to block NAT devices with Clean Access Agent

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

Platform: APPLIANCE

Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

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 4-1. See Change Clean Access Server Type, page 4-13 for additional details.
  - In-Band: Virtual Gateway or Real-IP Gateway
  - OOB: Out-of-Band Virtual Gateway or Out-of-Band Real-IP Gateway
- **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 and 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 4-15 for details.

- **Enable L3 strict mode to block NAT devices with NAC 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 Agent and blocks all L3 Agent users with NAT devices between those users and the CAS. See Enable L3 Strict Mode, page 4-17 for details.
- **Enable L2 strict mode to block L3 devices with NAC Agent**—When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the 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, page 4-17 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 disables the other.
- 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.

- **Platform**—The platform type for the CAS. This setting reads "APPLIANCE" if the CAS is a standard Clean Access Server appliance, or "NME-NAC" if the CAS is a Cisco NAC network module installed in a Cisco ISR router chassis.

  For more information on the Cisco NAC network module, see the Cisco NAC network module information included in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* and *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

  For detailed installation and configuration information, see *Getting Started with NAC Network Modules in Cisco Access Routers* and *Installing Cisco Network Modules in Cisco Access Routers*.

  Note You can also determine the CAS platform type using the CAS `service perfigo platform` CLI command. See the "CAS CLI Commands" section in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for more information.

- **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 4-34 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 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 11-2 and the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* 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 11-6.

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:

- 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, etc.)
- Ensure the CAS eth1 interface IP address and all assignable DHCP addresses (if used) are routable
- If you have two CASs configured in an HA deployment, after you make necessary configuration changes, be sure to reboot the HA-Primary CAS, *then* reboot the HA-Secondary CAS

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

To switch between Virtual and Real-IP 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 the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8*). 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 gateway clients get a new IP address after successful authentication and certification.

Note If using a version 4.1.2.0 or later Agent, ActiveX Control, or Java Applet to refresh client DHCP IP addresses, the **Bounce the switch port after VLAN is changed** option in the Port profile can be left disabled. If you use this method, be sure to follow the guidelines and warnings detailed in the "DHCP Release/Renew with Agent/ActiveX/Java Applet," "Configuring Access to Authentication VLAN Change Detection," and "Advanced Settings" sections of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

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

By default, Cisco NAC Appliance supports In-Band web login and 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 Agent clients from connecting to the Clean Access Server through NAT devices.

For L2 discovery, the Agent sends SWISS 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 Gateway) or as a bridge before the default gateway (Virtual Gateway), the CAS will respond and the Agent will attempt to authenticate the CAS before launching a login session.

Note This function does not apply to the Cisco NAC Web Agent.

If the CAS does not respond via L2 discovery, the Agent performs 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 **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. The Agent then attempts to authenticate the CAS before launching a login session

Note To discover the CAS, the 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, Cisco recommends using the Enable L2 strict mode to block L3 devices with the 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 4-5 on page 4-11).
2. Click **Update**.
3. Click **Reboot**.

Note For 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 Agent and Web Login users:

1. Go **Device Management > CCA Servers > Manage [CAS_IP] > Network** and uncheck the option for "**Enable L3 support**" (see Figure 4-5 on page 4-11).
2. Click **Update**.
3. Click **Reboot**.

VPN/L3 Access for Agents

The Clean Access Manager, Clean Access Server, and Agent support multi-hop L3 deployment. The Agent:

1. Checks the client network for the Clean Access Server (L2 deployments), and if not found,
2. Attempts 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 through the Agent download page after web login or through auto-upgrade. Either method allows the Agent to acquire the IP address of the Discovery Host (by default, 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 L3/VPN concentrator deployments or regular L2 deployments. If using the or Cisco NAC Web Agent, clients must launch the Agent via the Launch Cisco NAC Web Agent page after web login.

Acquiring and installing the Agent on the client by means other than direct download from the CAS will not provide the necessary Discovery 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 the following ways:
  - Agent Download web page (i.e., via web login)
  - Auto-Upgrade to Agent version 4.6.2.113 or later
  - "Launch Cisco NAC Web Agent" web page
- You can enable SSO by integrating Cisco NAC Appliance with Cisco VPN Concentrators and/or Cisco Adaptive Security Appliances (ASAs).

Note

- Uninstalling the Agent while still on the VPN connection does not terminate the connection.
- For VPN SSO deployments, if the Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. the Cisco Software Download Site), 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.
- 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 Software Download Site), 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

Administrators with L3 deployments can optionally restrict L3 Agent clients from connecting to the Clean Access Server through NAT devices using the **Enable L3 strict mode to block NAT devices with NAC 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 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 NAC 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 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 NAC Agent**—When this option is enabled, the CAS verifies the source MAC address of user packets against the MAC address sent by the 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

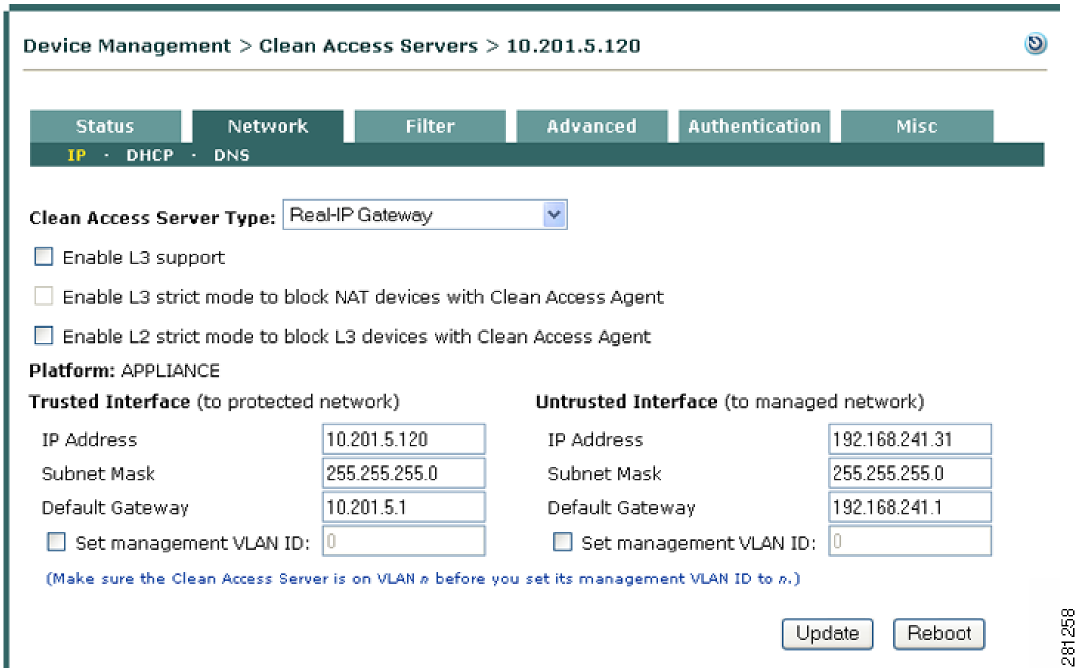
Administrators can optionally restrict Agent users to be connected to the Clean Access Server directly as their only gateway using the **Enable L2 strict mode to block L3 devices with NAC Agent** option.

When this feature is enabled, the 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 an Agent

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

Figure 4-6 CAS Network Tab



Device Management > Clean Access Servers > 10.201.5.120

Clean Access Server Type: Real-IP Gateway

☐ Enable L3 support

☐ Enable L3 strict mode to block NAT devices with Clean Access Agent

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

Platform: APPLIANCE

Trusted Interface (to protected network)		Untrusted Interface (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
☐ Set management VLAN ID:	0	☐ Set management VLAN ID:	0

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

2. Click the checkbox for **Enable L2 strict mode to block L3 devices with NAC 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 disables the other.

See the "Cisco NAC Appliance Agents" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for additional information.

Connecting to the CAS Using the SWISS Protocol

This section describes the SWISS proprietary session initiation protocol the Agent uses to discover and initiate client machine connection to the CAS. This section contains the following topics:

- What is the SWISS Protocol?
- Discovery Host
- VPN SSO Considerations
- Overcoming Network Latency Issues That Can Delay Discovery
- Using Layer 3 SWISS Packet Delay to Conserve Bandwidth
- Supporting Multiple Active NICs on the Client Machine

What is the SWISS Protocol?

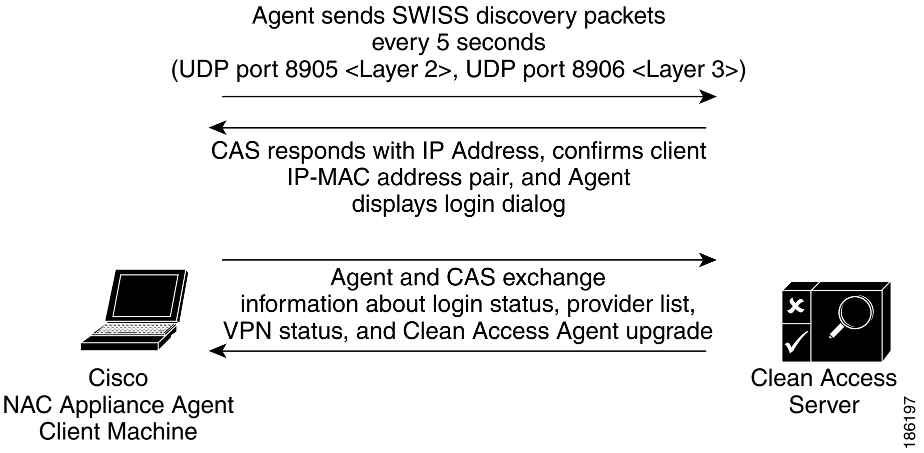
The Agent connects to the CAS by sending SWISS unicast discovery packets out on UDP ports 8905 (Layer 2) and 8906 (Layer 3) until a CAS responds and initiates a user login session. The UDP 8905 packets are directed to the client machine's default gateway and the UDP 8906 packets are directed to the IP address configured in the CAMs **Discovery Host** field (**Device Management > Clean Access > Clean Access Agent > Installation**).

To enhance network security and adhere to FIPS 140-2 compliance, Cisco NAC Appliance encapsulates SWISS communications between client machines and CASs, including Discovery Packet transmission/acknowledgement, authentication, and posture assessment results using the HTTPS protocol. The SWISS mechanism also features an enhanced handler that uses 3DES encryption for SWISS protocol functions.

Note SWISS protocol interaction only applies between the CAS and the Windows and Macintosh Agents. The Cisco NAC Web Agent does not connect to the CAS using the SWISS protocol.

Figure 4-7 outlines the basic Agent discovery and login session initiation process.

Figure 4-7 Agent and CAS Interaction Using the SWISS Protocol


Agent sends SWISS discovery packets every 5 seconds (UDP port 8905 <Layer 2>, UDP port 8906 <Layer 3>)
CAS responds with IP Address, confirms client IP-MAC address pair, and Agent displays login dialog
Agent and CAS exchange information about login status, provider list, VPN status, and Clean Access Agent upgrade
Cisco NAC Appliance Agent Client Machine
Clean Access Server
186197

1. After the user connects to the network and the client machine receives an IP address (via network DHCP server or the CAS itself, depending on your system configuration), the Agent starts sending UDP discovery packets on both ports 8905 and 8906.
2. The CAS intercepts SWISS discovery packets and responds to the Agent with the CAS certificate and instructs the Agent to initiate a user login session on the client machine.
3. The Agent and CAS engage in a SWISS protocol request-response exchange to determine:
   - Authenticity of the CAS prompting login from the Agent
   - User login status (including client IP-MAC address pair for Cisco NAC Appliance release 4.1(3) and later)
   - Authentication provider list
   - VPN connection status
   - Agent upgrade version, availability, and messaging
   - SSO status (Windows Agents only)
   - VPN SSO delay interval (if required)

Layer 2 Discovery Packets

If the user is "Layer 2 adjacent" to the CAS, the UDP discovery packets sent out on port 8905 are directed to the client machine's default gateway IP address and arrive at the CAS before they reach the default gateway device. That way, the CAS is able to respond to the client machine's search for the Cisco NAC Appliance network and Agent displays the user login dialog on the client machine. (Once it intercepts the UDP discovery packets, the CAS does not forward the packets on to the client machine's default gateway.)

Layer 3 Discovery Packets

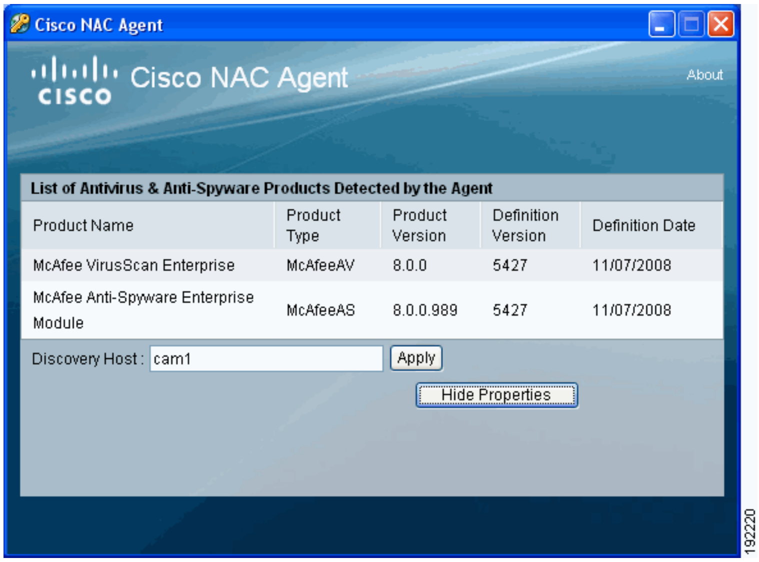
If the user is one or more Layer 3 hops away from the CAS, the Agent must establish a connection with the CAS using discovery packets sent out over UDP port 8906. Although the Layer 3 discovery packets are directed to the Discovery Host address on the CAM, which is most likely (but not always) the CAM's eth0 interface, these packets must traverse (pass from the untrusted to the trusted side of) the CAS in order to reach the CAM. That way, the CAS is able to intercept and respond to the client machine's search for the Cisco NAC Appliance network and the Agent displays the user login dialog on the client machine.

Note In a Layer 3 Out-of-Band deployment, Cisco recommends adding an ACL on your network access switch(es) to prevent SWISS packets from traversing the access VLAN. This simultaneously cuts down on unnecessary packets on the access network, and can help prevent authentication looping on the client machine when SWISS packets make it back to the CAS.

Discovery Host

The Discovery Host address on the CAM can be any IP address on the trusted side of the Cisco NAC Appliance network. By default, the Discovery Host address is the CAM eth0 IP address, since CAM only exists on the trusted side of the network and has exist for the Cisco NAC Appliance system to work at all. You can display the destination Discovery Host IP address the Agent uses to address Layer 3 discovery packets by right clicking on the Agent icon on the client taskbar and selecting **Properties** to bring up the Agent Properties and Information dialog (Figure 4-8).

Figure 4-8 Discovery Host Address in Agent Properties Dialog



List of Antivirus & Anti-Spyware Products Detected by the Agent

Product Name	Product Type	Product Version	Definition Version	Definition Date
McAfee VirusScan Enterprise	McAfeeAV	8.0.0	5427	11/07/2008
McAfee Anti-Spyware Enterprise Module	McAfeeAS	8.0.0.989	5427	11/07/2008

Discovery Host : cam1

In order for the Agent to discover the CAS and initiate a user login session, the Discovery Host must match the address assignment on the CAM. When users install and launch the Agent on the client machine, the Discovery Host setting automatically corresponds to the Discovery Host IP address configured on the CAM. The Discovery Host must be configured on the Agent installer in order for the Agent to discover the Cisco NAC Appliance network. If the Discovery Host is missing when the Agent is downloaded and installed on the client machine, the Agent does not know which destination IP address to use for the UDP discovery packets and will not be able to appropriately direct SWISS discovery packets.

New Agent downloads and upgrades automatically use the most recent Discovery Host address assignment. You must ensure that previously-installed Agents get updated if the Discovery Host IP address changes on the CAM. You can accomplish this in one of the following ways:

Cisco NAC Agent on Windows Client Machines

- Change the DiscoveryHost parameter in the Agent configuration XML file (**NACAgentCFG.xml**) and upload it to the CAM so users will automatically get the new XML file at their next login, or make the Agent update mandatory so that when users download the Agent update, the client machines are automatically updated to direct queries to the new Discovery Host address.

Note For details on using the Discovery Host parameter in Windows and Macintosh versions of the Clean Access Agent, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

VPN SSO Considerations

If users are connected to the network through an existing VPN connection and the Agent automatically sends SWISS discovery packets out searching for a CAS through which the user can log in, the CAS uses the SWISS packet request-response mechanism to tell the Agent not to display the user login dialog on the client machine. In addition, some VPN concentrators do not send out user session information immediately, so the CAS builds a "delay" into the user login session initiation process whenever VPN SSO has been configured on the Cisco NAC Appliance system. That way, the user is not required to enter their credentials more than once to log into the network for their session.

Overcoming Network Latency Issues That Can Delay Discovery

When the client machine sends out a SWISS discovery packet, it waits a full second for a CAS discovery response packet to return before trying to send a subsequent packet 5 seconds later. If the CAS responds, but network latency issues prevent the response packet from reaching the client machine in time, the client continues to check for a CAS through which it can connect to the network. To address this potential situation, administrators can set an additional "SwissTimeout" period on the client machine to allow a little extra time for the CAS discovery response packet to reach the client machine. To help ensure client machines are able to discover and authenticate with a Clean Access Server in a network featuring this sort of inherent latency, you can specify a value for the setting in the **NACAgentCFG.xml** Agent configuration file to affect the behavior of client machines where the Cisco NAC Agent is installed. For more details, see the "Cisco NAC Agent XML Configuration File Settings" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Note For details on configuring this feature for Windows and Macintosh versions of the Clean Access Agent, refer to the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)* and *Release Notes for Cisco NAC Appliance, Version 4.5(1)*.

Using Layer 3 SWISS Packet Delay to Conserve Bandwidth

In an effort to cut down on discovery packet transmission on the network, the Agent is designed to begin increasing the interval for Layer 3 discovery packet transmission when the Agent is unable to locate a CAS on the network. Instead of perpetually sending discovery packets every 5 seconds (as is the case for all Layer 2 discovery packets sent out on UDP port 8905), the Layer 3 discovery packets sent out on UDP port 8906 decrease in frequency with each subsequent transmission until the interval between discovery packets reaches 30 minutes. After that, the Agent stops searching for a CAS until a network connection event (like unplugging the Ethernet cable from the interface and plugging it back in again) "wakes up" port 8906 and restarts the discovery process.

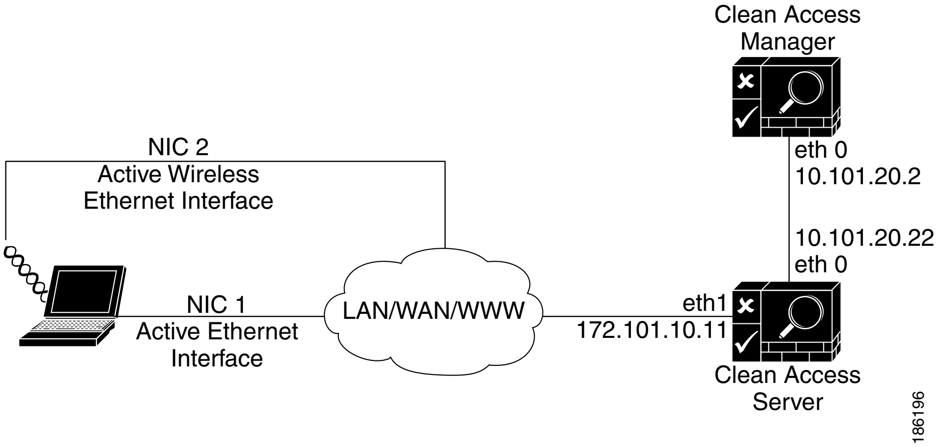
Supporting Multiple Active NICs on the Client Machine

The Cisco NAC Appliance system supports Agent client machines with more than one active NIC pointing to the same (untrusted side) eth1 interface on a CAS. Historically, this particular scenario could lead to a problem where, even after a user had already logged into the network via the Agent, another user login dialog would repeatedly appear and ask the user to enter their credentials again. This situation occurred because the CAS would receive SWISS discovery packets from over the additional active interface(s) and the CAS would not determine that the request from the additional IP address-MAC address pair(s) did not originate from the same client machine on which there was already an active Agent session. To address this potential problem, when responding to a Agent query for user login, the CAS includes a "valid" IP address-MAC address pair in the return SWISS packet(s) essentially saying, "You can establish a connection to the Cisco NAC Appliance network on the client machine interface <*MAC address*> with IP Address *A.B.C.D*. All other requests from this client will be ignored while this session remains active."

Note If you use the Access to Authentication VLAN change detection feature on a client machine with more than one active NIC, all active NICs on the client use the feature. By design, the NIC with the lowest metric always takes precedence for routing purposes, and you can determine the metric using the `route print` command from a command prompt. For more detailed information on the VLAN change detection feature, see "Configuring Access to Authentication VLAN Change Detection" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Figure 4-9 illustrates a common scenario where the CAS behavior helps avoid a potential problem. If the user logs in to the network via an Agent session using NIC1 (the client machine's active Ethernet interface), the CAS responds back that it will allow login requests from the NIC1 interface with the associated IP address. If the CAS then receives SWISS discovery packets originating from NIC2 (the client machine's Wireless Ethernet connection that points to the same eth1 interface on the CAS), the CAS does *not* initiate another Agent login session because the IP address-MAC address pair for NIC2 does not match the pair the CAS allowed when the session was established using NIC1.

Figure 4-9 Multiple Active Interfaces Pointing to the Same CAS eth1 IP Address



Configuring DHCP

You can configure the CAS to be a DHCP server when the CAS is in Real-IP Gateway mode, if a DHCP server does not already exist on your network. For complete details, see Chapter 5, “Configuring DHCP.”

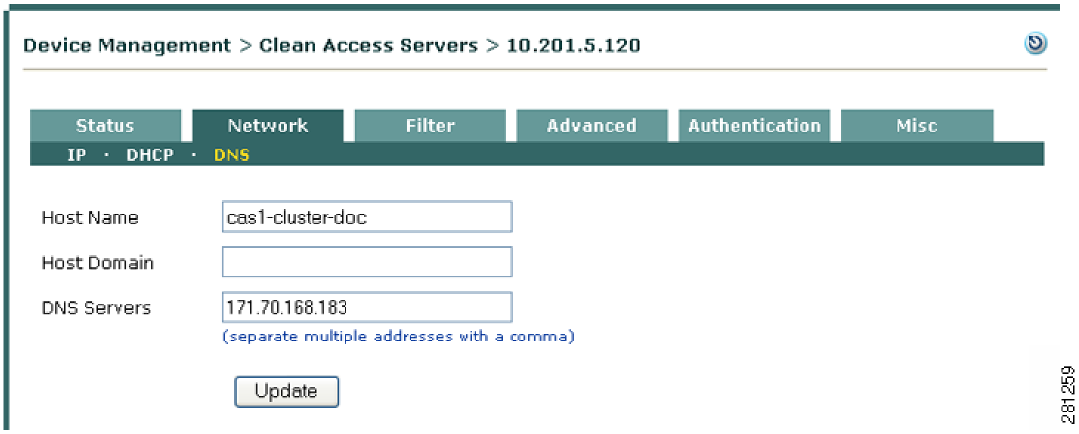
Configure DNS Servers on the Network

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 4-10 DNS Form



Host Name: cas1-cluster-doc

Host Domain:

DNS Servers: 171.70.168.183

(separate multiple addresses with a comma)

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 11-2 and the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details.

Configuring Managed Subnets or Static Routes

This section describes the following:

- Overview, page 4-25
- Configure Managed Subnets for L2 Deployments, page 4-27
- Configure Static Routes for L3 Deployments, page 4-29

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. You must configure the untrusted (authentication) VLAN in the **VLAN ID** field of the Managed Subnet.

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 4-29 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 4-1 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 5-5 for details.

Table 4-1 Guidelines for Adding Managed Subnets vs. Static Routes

Layer 2—In-Band or Out-of-Band (CAS has L2 proximity to users)	Layer 3 (Multi-Hop) —In-Band Only (e.g. CAS is behind VPN Concentrator or Router or L3 Switch)	
For Real-IP Gateways:	For Real-IP Gateways:	
	If the router below the CAS performs proxy ARP:	If the router below the CAS does NOT perform proxy ARP:

Table 4-1 Guidelines for Adding Managed Subnets vs. Static Routes

Layer 2—In-Band or Out-of-Band (CAS has L2 proximity to users)	**Layer 3 (Multi-Hop) —In-Band Only (e.g. CAS is behind VPN Concentrator or Router or L3 Switch)**	

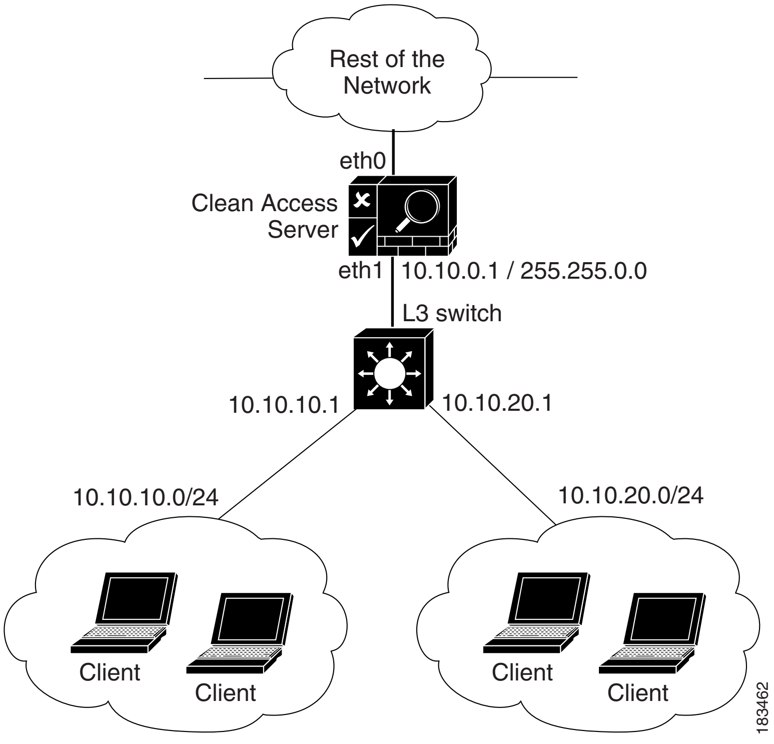
Add a managed subnet under **Advanced > Managed Subnet** to assign the gateway IP address of the subnet to the CAS.
For example, to configure the CAS to be the gateway (10.10.10.1) for VLAN 10 /subnet 10.10.10.0, specify the following managed subnet:
IP Address: 10.10.10.1
Subnet Mask: 255.255.255.0
VLAN ID: 10
	Always add a managed subnet under **Advanced > Managed Subnet**	1. Always add static routes for the subnets on the untrusted side under **Advanced > Static Routes**. For example:
		`Network     Mask    Interface   Gateway`
		`10.10.10.0  /24     eth1        10.10.10.1`
		`10.10.20.0  /24     eth1        10.10.20.1`
		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:
		`10.10.10.0 255.255.255.255 eth1`
		See Figure 4-11 on page 4-27.

For Virtual Gateways:	**For Virtual Gateways:**	
	If the router below the CAS performs proxy ARP:	**If the router below the CAS does NOT perform proxy ARP:**

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.
	Always add a managed subnet under **Advanced > Managed Subnet**	1. Add static route for the subnets on the untrusted side under **Advanced > Static Routes**. For example:
		`Network     Mask    Interface   Gateway`
		`10.10.10.0  /24     eth1        10.10.10.1`
		Note When deploying the CAS in L3 VGW mode, the gateway is not optional and you must specify the gateway for the static route.

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 4-11 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 untrusted (authentication) 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_eth0_IP_address>** 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)

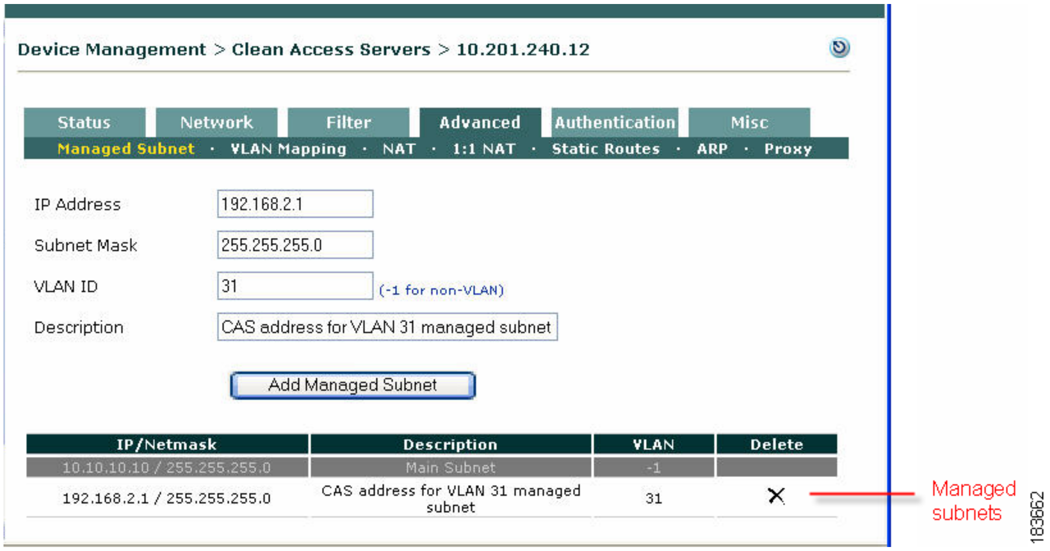
- Subnet Mask: 255.255.255.0

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 4-12 Managed Subnet



Device Management > Clean Access Servers > 10.201.240.12

Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

VLAN ID: 31 (-1 for non-VLAN)

Description: CAS address for VLAN 31 managed subnet

IP/Netmask	Description	VLAN	Delete
10.10.10.10 / 255.255.255.0	Main Subnet	-1	
192.168.2.1 / 255.255.255.0	CAS address for VLAN 31 managed subnet	31	✕

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 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 4-1 on page 4-25, "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 untrusted (authentication) 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.
6. Reboot. A reboot is needed after adding a managed 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 4-31. 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 4-15) lets you set up routing rules in the Clean Access Server. Static Routes have the form:

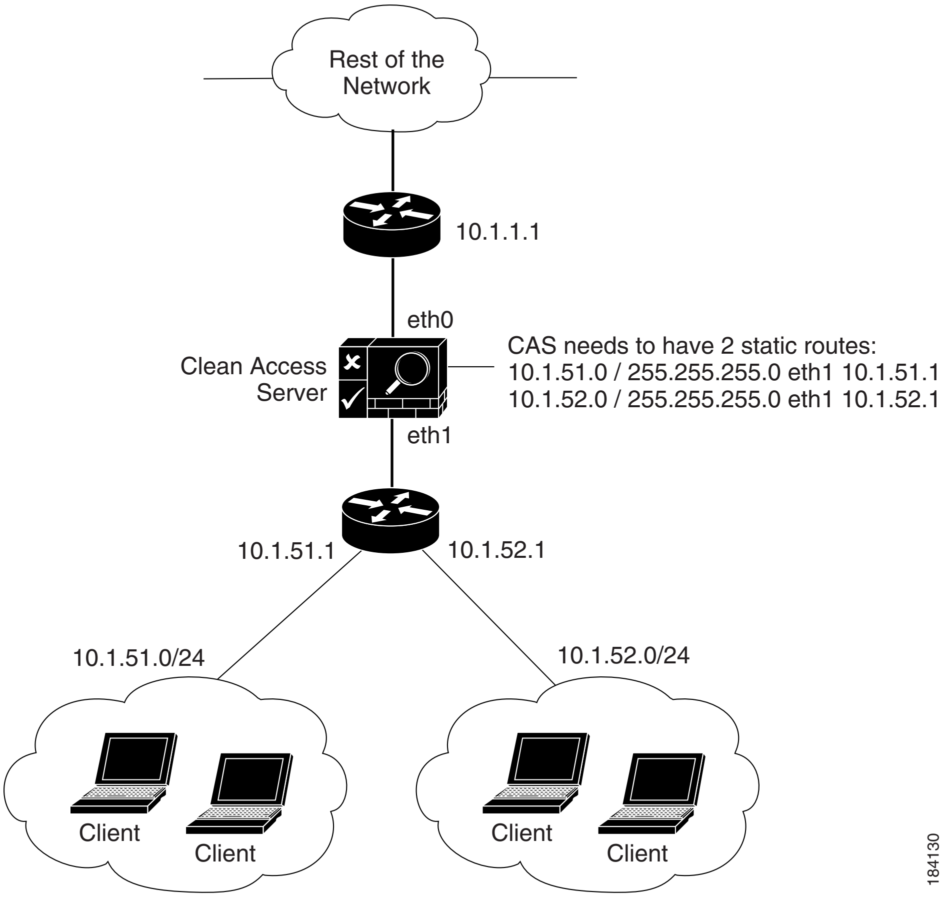
Network / subnet mask / send packets to interface (trusted or untrusted) / Gateway IP address (optional)

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 4-13 illustrates a Layer 3 deployment scenario that requires a static route.

Figure 4-13 Static Route Example (Layer 3)

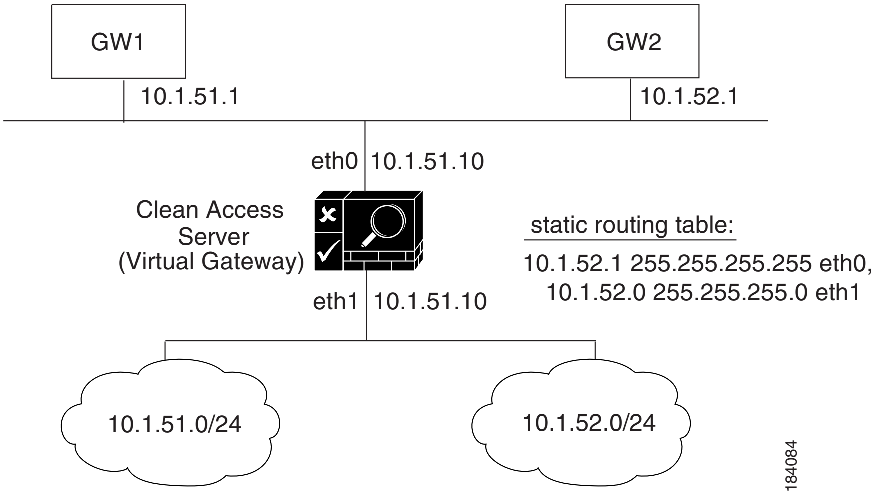


CAS needs to have 2 static routes:
10.1.51.0 / 255.255.255.0 eth1 10.1.51.1
10.1.52.0 / 255.255.255.0 eth1 10.1.52.1

Configuring Static Routes for Layer 2 Deployments

Figure 4-14 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).

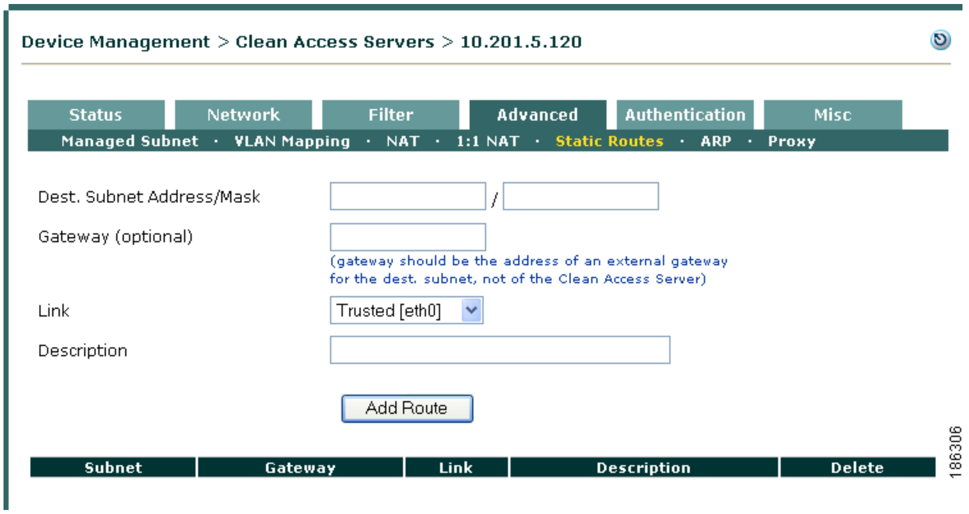
Figure 4-14 Static Route Example (Layer 2)



Add Static Route

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

Figure 4-15 Static Routes


Device Management > Clean Access Servers > 10.201.5.120
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add Route
186306

Dest. Subnet Address/Mask	/
Gateway (optional)	(gateway should be the address of an external gateway for the dest. subnet, not of the Clean Access Server)
Link	Trusted [eth0]
Description	

Subnet	Gateway	Link	Description	Delete

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 4-14).

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:

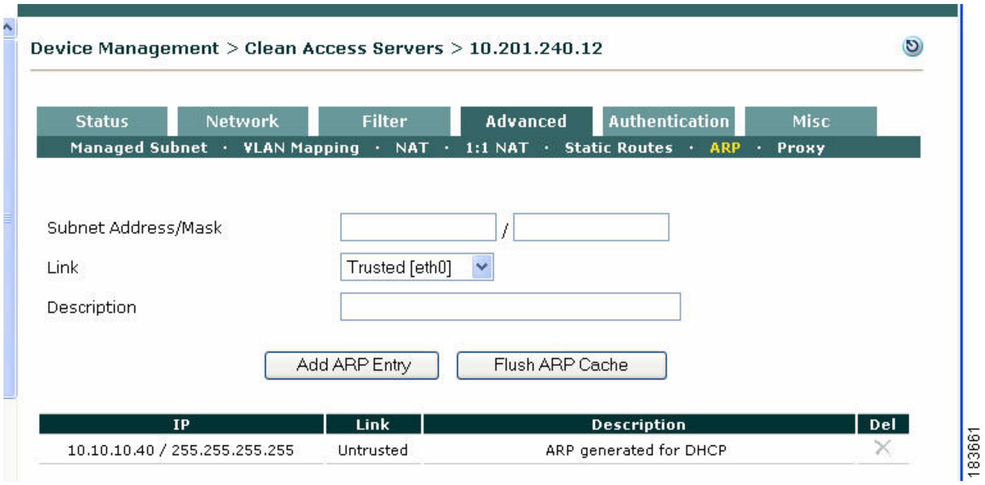
- The untrusted network specified for the Clean Access Server in the **IP** form.
- Any managed subnets you added (see Configuring Managed Subnets or Static Routes, page 4-25).
- Auto-generated subnets created during DHCP configuration. These entries are identified by the description "ARP Generated for DHCP." (see Figure 5-12 on page 5-14)

Add ARP Entry

Use the following steps to manually create an ARP entry.

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

Figure 4-16 Create ARP Entry


Device Management > Clean Access Servers > 10.201.240.12
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add ARP Entry
Flush ARP Cache
183661

Subnet Address/Mask	/
Link	Trusted [eth0]
Description	

IP	Link	Description	Del
10.10.10.40 / 255.255.255.255	Untrusted	ARP generated for DHCP	×

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, 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 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 the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8*.

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.

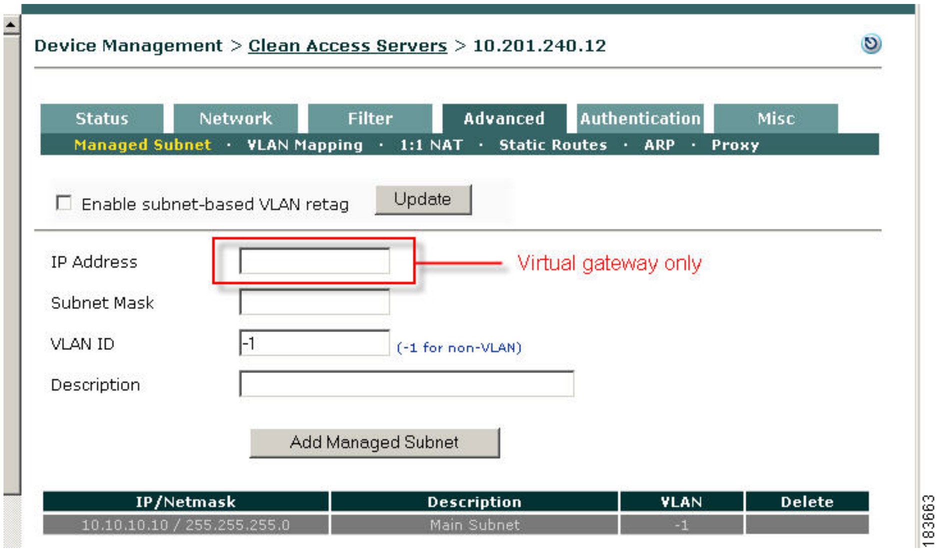
In addition, once VLAN tagging is configured, traffic from users on a particular VLAN ID and authenticated by an external authentication source can be mapped to a specific user role (under **User Management> Auth Servers > Mapping Rules**). Role mapping rules can use the user's VLAN ID as one of the attributes when assigning a user to a role. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* 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 4-27. Traffic originating from the untrusted interface of the CAS is tagged according to the VLAN ID set for the managed subnet.

For CASs 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 4-17.

Figure 4-17 Enable Subnet-Based VLAN Retag for Virtual Gateway



Device Management > Clean Access Servers > 10.201.240.12

☐ Enable subnet-based VLAN retag

IP Address
Subnet Mask
VLAN ID -1 (-1 for non-VLAN)
Description

IP/Netmask	Description	VLAN	Delete
10.10.10.10 / 255.255.255.0	Main Subnet	-1	

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 Configuration Guide, Release 4.8(1)* 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

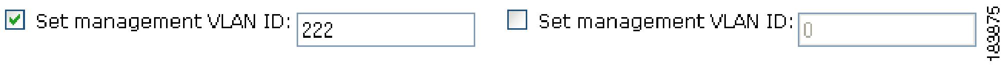
Example switch configuration on the switch interfaces connecting to eth1 of the CAS:

- 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)

Figure 4-18 Setting the Management VLAN ID



☑ Set management VLAN ID: 222

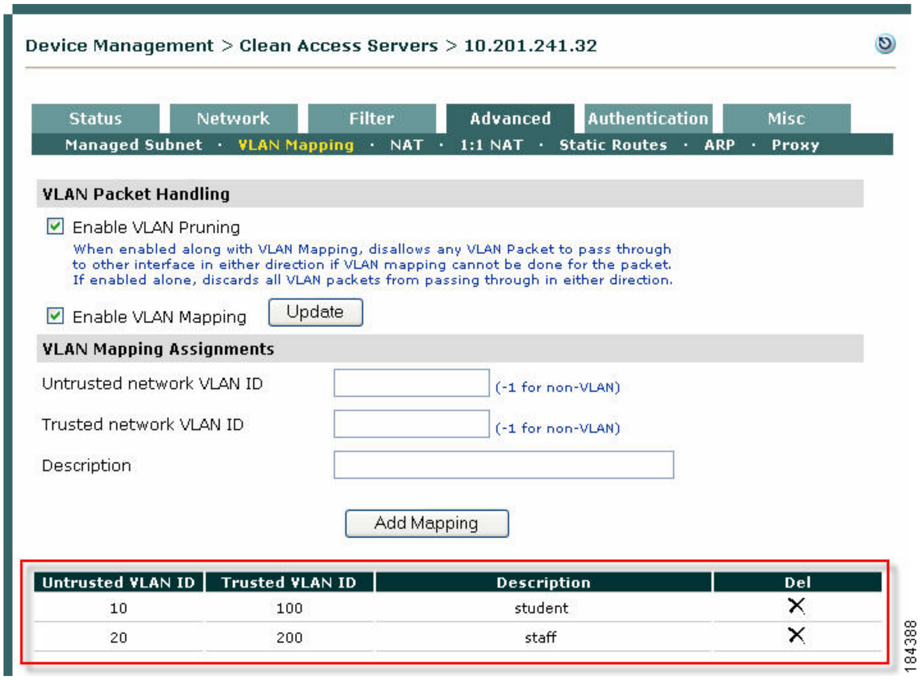
□ Set management VLAN ID: 0

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

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

Figure 4-19 Enable VLAN Mapping


Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Update
Add Mapping
184388

Device Management > Clean Access Servers > 10.201.241.32

VLAN Packet Handling

☑ Enable VLAN Pruning

When enabled along with VLAN Mapping, disallows any VLAN Packet to pass through to other interface in either direction if VLAN mapping cannot be done for the packet. If enabled alone, discards all VLAN packets from passing through in either direction.

☑ Enable VLAN Mapping

VLAN Mapping Assignments

Untrusted network VLAN ID (-1 for non-VLAN)

Trusted network VLAN ID (-1 for non-VLAN)

Description

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
10	100	student	✕
20	200	staff	✕

4. Click the checkbox for **Enable VLAN Pruning** if you want to block any unmapped VLAN packets passing across CAS interfaces in both directions (from Untrusted -> Trusted and from Trusted -> Untrusted).

Note VLAN Pruning is enabled by default.

The following table briefly describes the net effect on VLAN traffic when VLAN pruning and VLAN mapping are enabled and disabled:

VLAN Pruning	VLAN Mapping	Result
ON	ON	Discard all unmapped VLAN packets
ON	OFF	Discard all VLAN packets regardless of mapping
OFF	ON	Potential Layer 2 UDP broadcast storm due to VLAN packet loop
OFF	OFF	Potential Layer 2 UDP broadcast storm due to VLAN packet loop

Warning **If the Enable VLAN Pruning option is enabled alone, the CAS discards *all* VLAN packets passing through in either direction.**

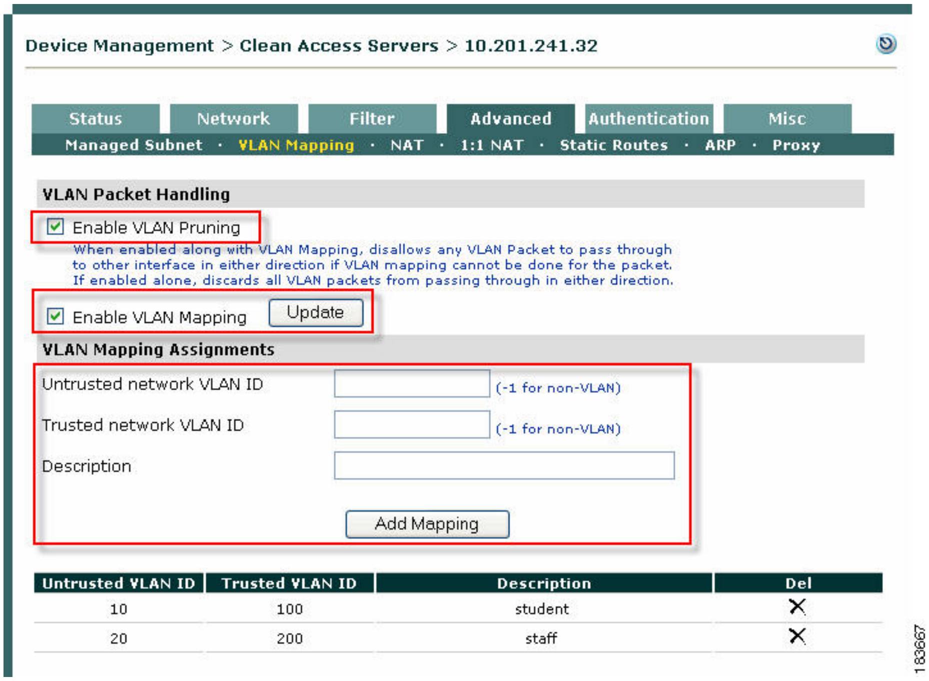
5. Click the checkbox for **Enable VLAN Mapping** and click **Update**.
6. Enter the Auth VLAN ID for the **Untrusted network VLAN ID** field.
7. Enter the Access VLAN ID for the **Trusted network VLAN ID** field.
8. Type an optional **Description** (such as **Users on edge switch**).

9. Click **Add Mapping**.

To Verify VLAN Mapping

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 4-20 Verify VLAN Mapping


Device Management > Clean Access Servers > 10.201.241.32
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Update
Add Mapping
183667

VLAN Packet Handling

☑ Enable VLAN Pruning

When enabled along with VLAN Mapping, disallows any VLAN Packet to pass through to other interface in either direction if VLAN mapping cannot be done for the packet. If enabled alone, discards all VLAN packets from passing through in either direction.

☑ Enable VLAN Mapping

VLAN Mapping Assignments

Untrusted network VLAN ID (-1 for non-VLAN)

Trusted network VLAN ID (-1 for non-VLAN)

Description

Untrusted VLAN ID	Trusted VLAN ID	Description	Del
10	100	student	✕
20	200	staff	✕

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 typically override global settings.

A 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).

A 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. Cisco strongly recommends you do not configure any local (CAS-specific) device filters when deployed in an Out-of-Band environment. See "Global Device and Subnet Filtering" in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details.

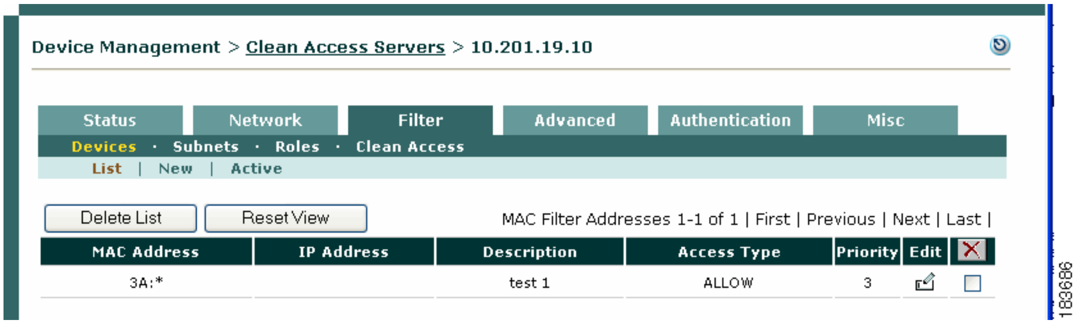
Note Device filter settings and/or subnet filter settings take precedence over the CAS Fallback Policy. While in CAS fallback mode, CAS device filter settings determine behavior based on the client MAC address. If device filter settings do not apply (for example, if the CAS is a Layer 3 gateway and cannot determine the client MAC address), the CAS also looks for applicable subnet filter settings before applying the CAS Fallback Policy. See CAS Fallback Policy, page 4-44 for details.

Configure Local Device Access Filter Policies

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

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

Figure 4-21 Local Device Filters List


Device Management > Clean Access Servers > 10.201.19.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
List | New | Active
Delete List
Reset View
183686

MAC Filter Addresses 1-1 of 1 | First | Previous | Next | Last |

MAC Address	IP Address	Description	Access Type	Priority	Edit	☒
3A:*		test 1	ALLOW	3		□

Step 2 Click **New**. The New local filter form appears as shown in Figure 4-22.

Step 3 In the **Devices** 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.

Step 4 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

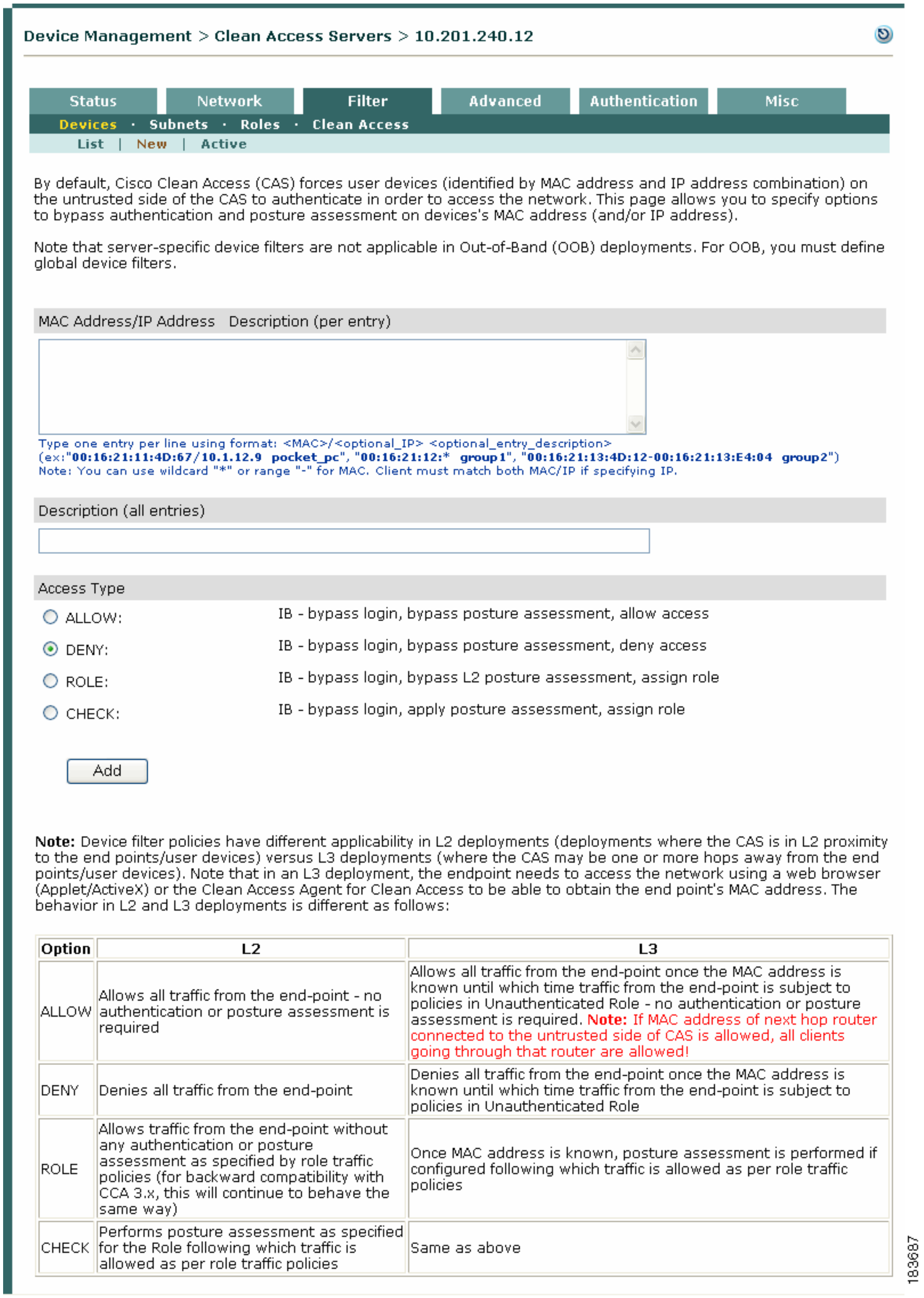
Step 5 If using **CHECK** or **ROLE**, choose a role from the **User Role** dropdown menu.

Step 6 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 4-22 New Local Filter


Device Management > Clean Access Servers > 10.201.240.12
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
List | New | Active

By default, Cisco Clean Access (CAS) forces user devices (identified by MAC address and IP address combination) on the untrusted side of the CAS to authenticate in order to access the network. This page allows you to specify options to bypass authentication and posture assessment on devices's MAC address (and/or IP address).

Note that server-specific device filters are not applicable in Out-of-Band (OOB) deployments. For OOB, you must define global device filters.

MAC Address/IP Address Description (per entry)

Type one entry per line using format: <MAC>/<optional_IP> <optional_entry_description>
(ex:"**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**")
Note: You can use wildcard "*" or range "-" for MAC. Client must match both MAC/IP if specifying IP.

Description (all entries)

Access Type

○ 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

Note: Device filter policies have different applicability in L2 deployments (deployments where the CAS is in L2 proximity to the end points/user devices) versus L3 deployments (where the CAS may be one or more hops away from the end points/user devices). Note that in an L3 deployment, the endpoint needs to access the network using a web browser (Applet/ActiveX) or the Clean Access Agent for Clean Access to be able to obtain the end point's MAC address. The behavior in L2 and L3 deployments is different as follows:

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 Layer 2 devices in filter policies for a particular Clean Access Server:

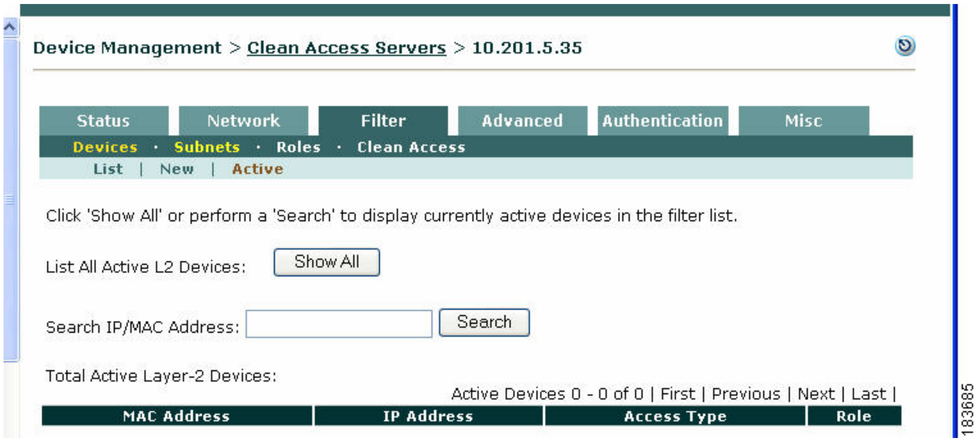
Step 1 Go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Filter > Devices > Active**.

Step 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.

Step 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.

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 4-23 Active



Device Management > Clean Access Servers > 10.201.5.35

Click 'Show All' or perform a 'Search' to display currently active devices in the filter list.

List All Active L2 Devices: Show All

Search IP/MAC Address: Search

Total Active Layer-2 Devices:

Active Devices 0 - 0 of 0 | First | Previous | Next | Last |

MAC Address	IP Address	Access Type	Role

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

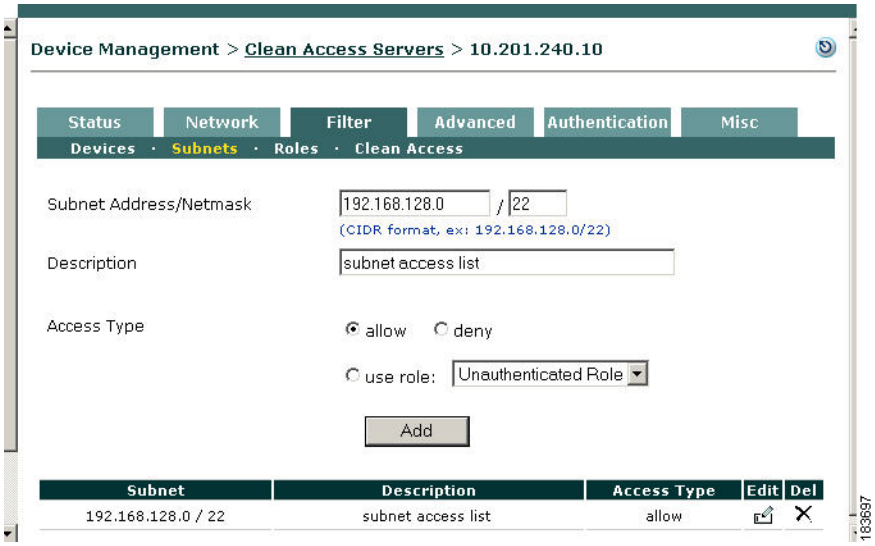
Configure Subnet Access Filter Policies

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 4-24 Local Subnet Filter


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Add
183697

Subnet Address/Netmask	192.168.128.0 / 22 (CIDR format, ex: 192.168.128.0/22)
Description	subnet access list
Access Type	● allow ○ deny ○ use role: Unauthenticated Role

Subnet	Description	Access Type	Edit	Del
192.168.128.0 / 22	subnet access list	allow	✎	✕

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 from 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).

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, Cisco recommends deploying a CAS high availability (HA) failover bundle. See the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details.

The CAS checks the status of the CAM periodically, according to the Detect Interval specified. If the CAM is unreachable a predetermined percentage of the time over the course of the specified Detect Timeout period, the CAS sets the traffic policy of every user role to "Allow All, "Block All" or "Ignore" based on the specified Fallback Policy. You can specify the **Detect Interval**, **Detect Timeout**, and **Fail Percentage** threshold values as described below.

Device filter settings and/or subnet filter settings take precedence over the CAS Fallback Policy. While in CAS fallback mode, CAS device filter settings determine behavior based on the client MAC address. If device filter settings do not apply (for example, if the CAS is a Layer 3 gateway and cannot determine the client MAC address), the CAS also looks for applicable subnet filter settings before applying the CAS Fallback Policy.

Note If the CAS enters Fallback mode and the **Enable Heartbeat Timer** option is enabled in the **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer** web console page, user sessions are still terminated and cleared from the Online Users List and Certified Devices List after the specified time period has passed. For more information, see Local Heartbeat Timer, page 9-1.

During CAS fallback recovery (where the CAS is reconnecting to the CAM), a login dialog appears to users accessing the Cisco NAC Appliance network via the CAS, but they are unable to authenticate and login for approximately 2 minutes. (Until CAS fallback recovery completes, users see a "Failed to add user to the list" error message when attempting to log in.)

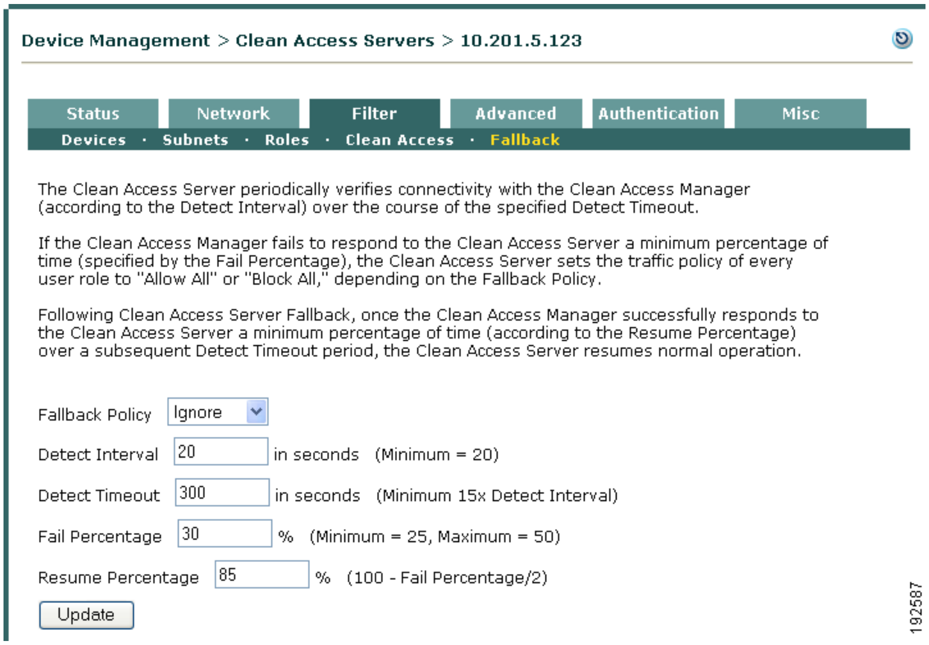
Note You can use the **failSafeStatus** script in the CAS CLI to determine whether or not the CAS is currently operating normally or in Fallback state. To run the script, log into the CAS CLI as root and type `failSafeStatus` from the **/perfigo/access/bin/** directory.

Note Starting from release 4.5(1), when a standby CAS in an HA pair assumes the role of an active CAS that is performing DHCP address management and has gone into Fallback state, the new active CAS also assumes DHCP functions in addition to user login.

Configuring CAS Fallback

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

Figure 4-25 CAS Fallback


Device Management > Clean Access Servers > 10.201.5.123

The Clean Access Server periodically verifies connectivity with the Clean Access Manager (according to the Detect Interval) over the course of the specified Detect Timeout.

If the Clean Access Manager fails to respond to the Clean Access Server a minimum percentage of time (specified by the Fail Percentage), the Clean Access Server sets the traffic policy of every user role to "Allow All" or "Block All," depending on the Fallback Policy.

Following Clean Access Server Fallback, once the Clean Access Manager successfully responds to the Clean Access Server a minimum percentage of time (according to the Resume Percentage) over a subsequent Detect Timeout period, the Clean Access Server resumes normal operation.

Fallback Policy: Ignore

Detect Interval: 20 in seconds (Minimum = 20)

Detect Timeout: 300 in seconds (Minimum 15x Detect Interval)

Fail Percentage: 30 % (Minimum = 25, Maximum = 50)

Resume Percentage: 85 % (100 - Fail Percentage/2)

Step 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.

Step 3 Specify a **Detect Interval** (default is 20 seconds). The **Detect Interval** specifies how often the CAS polls the CAM to verify whether it is still reachable on the network. The minimum **Detect Interval** must be 20 seconds.

Step 4 Specify a **Detect Timeout** (default is 300 seconds). The **Detect Timeout** specifies the duration of time the CAS continues to poll the CAM before determining whether or not it is reachable. If the **Fail Percentage** of verification polls fail (see Table 4-2), the CAS declares the CAM unreachable and triggers the CAS Fallback Policy. The **Detect Timeout** value must be at least 15 times the **Detect Interval** (default is 300 seconds), but Cisco recommends setting the **Detect Timeout** to 30 times the **Detect Interval** value (e.g. Detect Timeout of 600 seconds for a Detect Interval of 20 seconds).

Note Default values for the **Detect Interval** and **Detect Timeout** settings apply to new installations of Cisco NAC Appliance release 4.5(1) and later. If you upgrade from a previous Cisco NAC Appliance release, your original **Detect Interval** and **Detect Timeout** values are preserved, and you may have to specify new settings to maintain expected CAS Fallback behavior.

Step 5 Specify a **Fail Percentage**. The **Fail Percentage** specifies the percentage of CAS polling events allowed to fail over the course of the **Detect Timeout** before the CAS declares the CAM unreachable and triggers the Fallback Policy. To help ensure network stability and minimize CAS Failover events, the **Fail Percentage** setting must be at least 25%, but cannot be more than 50%.

To determine the number of CAS events/polls to monitor over the course of the **Detect Timeout**, simply divide the **Detect Timeout** by the **Detect Interval**. Once you know the number of verification polls the CAS performs, apply the Fail Percentage to determine how many poll events must fail during the **Detect Timeout** to trigger CAS Fallback.

For example, if the CAS performs 15 verification polls over the course of the **Detect Timeout** period, and the CAS is configured to Fallback when 30% of the CAS-to-CAM verification polls fail (that is, you have specified a **Fail Percentage** value of 30), then CAS Fallback will occur when 5 or more verification polls to the CAM fail—30% of 15 polls is 4.5 polls (rounded up to 5). (See Table 4-2 for more examples.)

Note For CAS Fallback calculations, always round fractions up to the next integer value.

Step 6 The **Resume Percentage** value is automatically populated depending on the specified **Fail Percentage** value. The **Resume Percentage** indicates the percentage of successful responses from the CAM required to bring the CAS back into normal operation after a CAS Fallback event.

Following a CAS Fallback event, the CAS continues monitoring connection with the CAM according to the specified Fallback parameters and resumes normal operation when the CAM responds to a minimum percentage of periodic connection verification polls over the course of the **Detect Timeout**. The function determining the **Resume Percentage** value is a 100% success rate minus one half of the **Fail Percentage**. Therefore, if the specified **Fail Percentage** is 30%, the CAS resumes normal operation when the CAM responds to 85% (100% minus one half of 30%, or 15%) of the polls during the **Detect Timeout** period.

Step 7 Click **Update**.

Table 4-2 provides some sample CAS Fallback settings with Fallback Policy results in a Cisco NAC Appliance system where CAS Fallback has been enabled. Values in bold are user specified.

Table 4-2 Sample CAS Fallback Settings and Results

Detect Interval (specify)	Detect Timeout (specify)	Number of CAS Polls over Detect Timeout (Detect Timeout/ Detect Interval)	Fail Percentage 25%-50% (specify)	Number of Failed Polls to Trigger CAS Fallback (CAS Polls x Fail Percentage)	Resume Percentage (100 - Fail Percentage/2)	Number of Successful Polls over Detect Timeout for CAS to Resume Operation (CAS Polls x Resume Percentage)
20 sec	**300 sec**	15	**30%**	5 (4.5 rounded up)	85%	13 (12.75 rounded up)
20 sec	**600 sec**	30	**30%**	9	85%	26 (25.5 rounded up)
20 sec	**400 sec**	20	**25%**	5	88% (87.5% rounded up)	18 (17.5 rounded up)
30 sec	**600 sec**	20	**30%**	6	85%	17

Configure Proxy Server Settings on the CAS

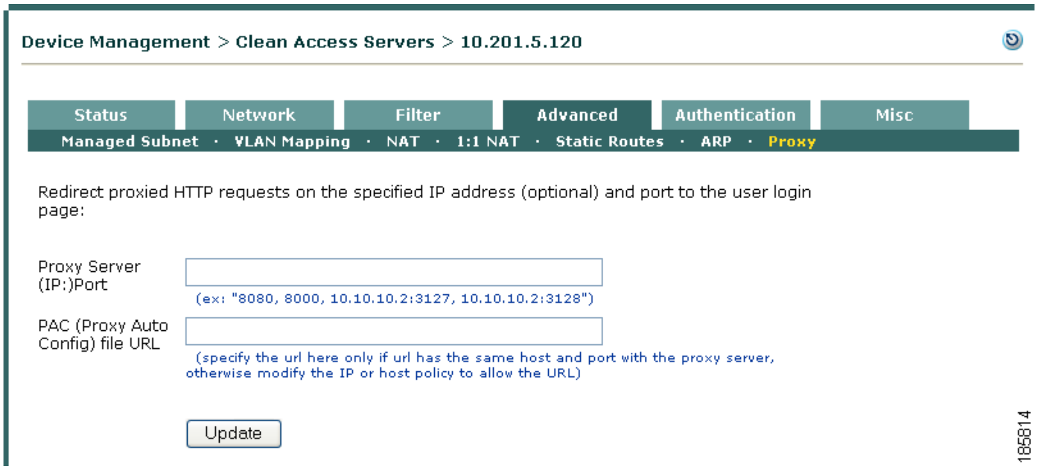
By default, the Clean Access Server redirects client traffic on ports 80 and 443 to the login page. If users on your untrusted network are required to use a proxy server and/or different ports, you can configure the CAS with corresponding proxy server information in order to appropriately redirect HTTP/HTTPS 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).
- The URL for a preconfigured Proxy PAC file—This is a file the CAS should use to redirect the user session. The URL you specify must have the same IP address and port as the Proxy server to successfully enable session redirection. If the URL has a different IP address or port from the Proxy settings, you must configure an IP or host policy for the user session, instead.

To Specify Proxy Server Settings on the CAS:

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

Figure 4-26 Proxy Settings for Client Traffic


Device Management > Clean Access Servers > 10.201.5.120
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Update
185814

Redirect proxied HTTP requests on the specified IP address (optional) and port to the user login page:

Proxy Server (IP:)Port
(ex: "8080, 8000, 10.10.10.2:3127, 10.10.10.2:3128")

PAC (Proxy Auto Config) file URL
(specify the url here only if url has the same host and port with the proxy server, otherwise modify the IP or host policy to allow the URL)

Step 2 Specify the proxy source:

- Enter the Proxy IP address in the **Proxy Server (IP:)Port**. 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.

- Enter the URL for a preconfigured Proxy PAC file the CAS should use to redirect the user session.

Note The URL you specify must have the same IP address and port as the Proxy server to successfully enable session redirection. If the URL has a different IP address or port from the Proxy settings, you must configure an IP or host policy for the user session, instead.

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

CHAPTER 5

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 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 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, page 5-1
- Enable the DHCP Module, page 5-2
- Configuring IP Ranges (IP Address Pools), page 5-5
- Reserving IP Addresses, page 5-22
- User-Specified DHCP Options, page 5-23
- Global Action, page 5-30

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 Gateway CAS forwards messages from clients to another DHCP server.
- **DHCP Server**—In this mode, a Real-IP Gateway CAS acts as the DHCP server and allocates client IP addresses for the managed (untrusted) network.

When a Real-IP 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.

Table 5-1 Recommended DHCP limits

Parameter	Limit
DHCP IP lease recommended limit of pool size	5000
Default/Min-Max lease time	0-2147483647 seconds
Recommended lease time	1800-7200 seconds

Note In case of pool size, a warning message is displayed if the limit exceeds.

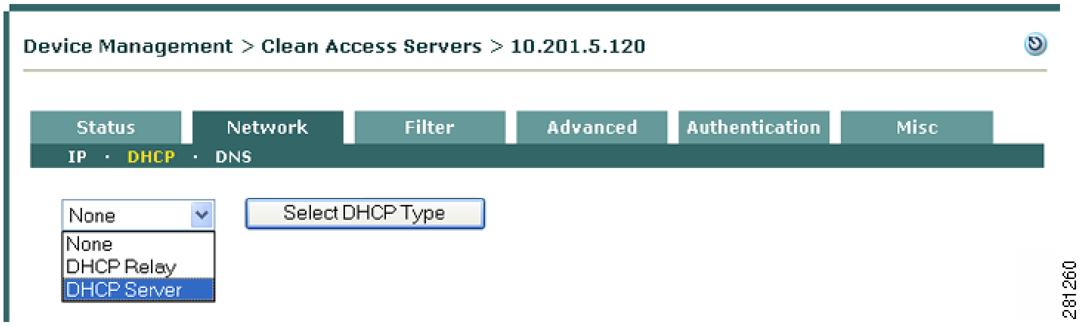
Enable the DHCP Module

You can enable DHCP Relay or DHCP Server mode on a Clean Access Server that is in Real-IP Gateway mode. When a CAS is a Virtual Gateway, it is always in DHCP Passthrough mode (see Figure 5-4).

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 5-1).

Figure 5-1 Select DHCP Type (CAS in Real-IP Gateway Mode)

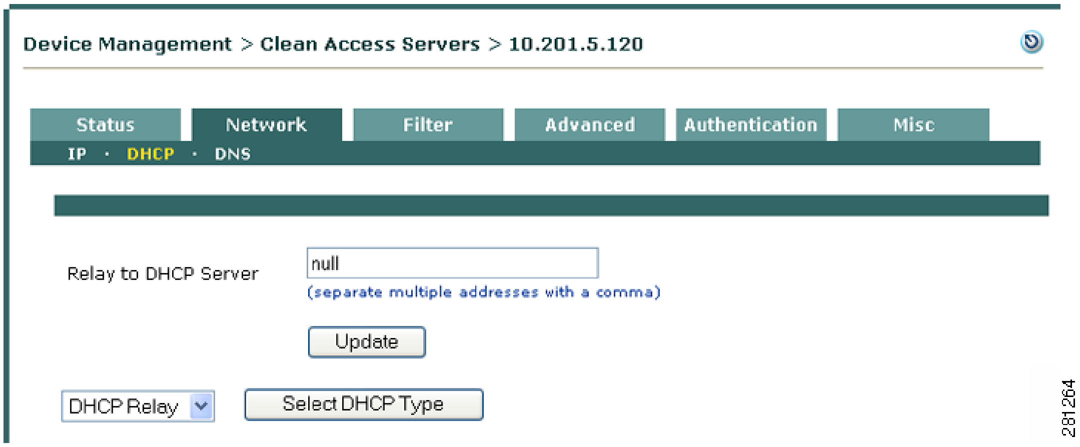


3. From the DHCP Type dropdown menu, select one of the following options and click the **Select DHCP Type** button (note that this button label toggles to **Select DHCP Type and Reboot Clean Access Server** when in DHCP Server mode.) Options are as follows:

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 5-2). Type the IP address of the external DHCP server in the **Relay to DHCP server** field, and click the **Update** button.

Figure 5-2 Configuring DHCP Relay


Device Management > Clean Access Servers > 10.201.5.120

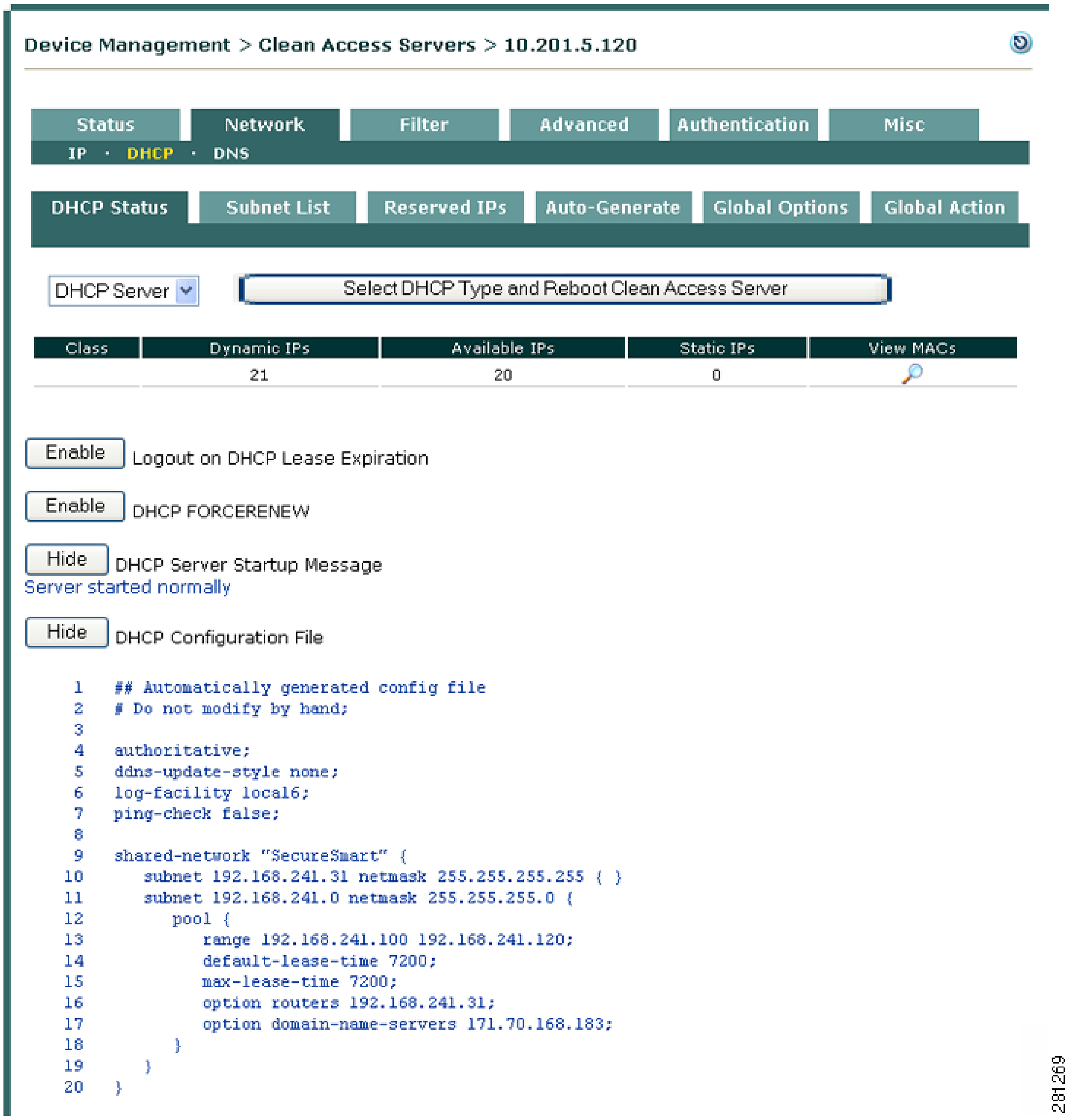
Relay to DHCP Server: null

(separate multiple addresses with a comma)

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 5-3). 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 5-5.

Figure 5-3 DHCP Server Mode



Class	Dynamic IPs	Available IPs	Static IPs	View MACs
	21	20	0	🔍

Enable Logout on DHCP Lease Expiration

Enable DHCP FORCERENEW

Hide DHCP Server Startup Message

Server started normally

Hide DHCP Configuration File

```
## Automatically generated config file
# Do not modify by hand;

authoritative;
ddns-update-style none;
log-facility local6;
ping-check false;

shared-network "SecureSmart" {
    subnet 192.168.241.31 netmask 255.255.255.255 { }
    subnet 192.168.241.0 netmask 255.255.255.0 {
        pool {
            range 192.168.241.100 192.168.241.120;
            default-lease-time 7200;
            max-lease-time 7200;
            option routers 192.168.241.31;
            option domain-name-servers 171.70.168.183;
        }
    }
}
```

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 5-3.

Cisco NAC Appliance offers two DHCP enable/disable functions 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 or Web session 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

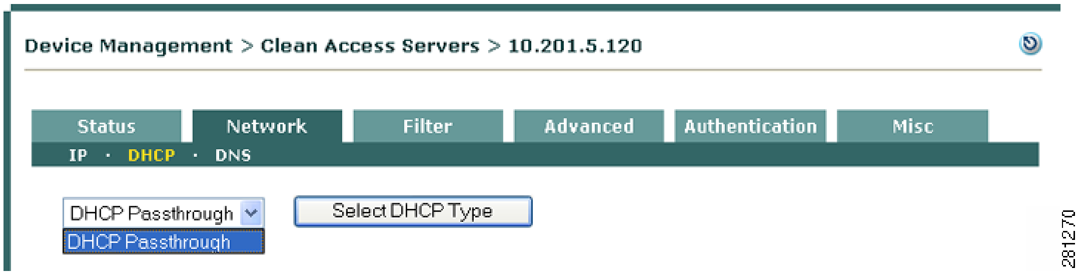
When this button is clicked, the DHCP configuration file is displayed. In some cases, the startup message displays an error for a particular line of the configuration. Clicking this button allows you to view the configuration file line-by-line.

For further information on the **DHCP Status** tab see Working with Subnets, page 5-15.

For additional information on DHCP configuration, see User-Specified DHCP Options, page 5-23.

Note A Virtual Gateway CAS is always in DHCP Passthrough mode (Figure 5-4).

Figure 5-4 CAS VGW DHCP Type



Device Management > Clean Access Servers > 10.201.5.120

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 5-2 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 5-2 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 5-3 shows the addressing for an automatically-generated IP range of four /30 subnets starting at address 10.1.100.12.

Table 5-3 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

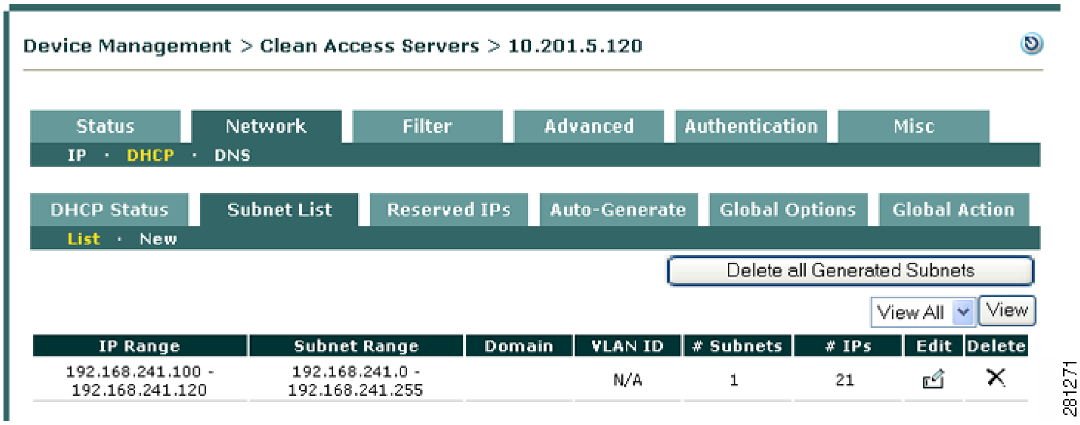
To create an IP pool manually, you also need to define the subnet in which the pool resides. There are three ways to arrive at the subnet address and netmask values for a manually generated pool:

- 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 5-5 New Subnet List Subtab Link

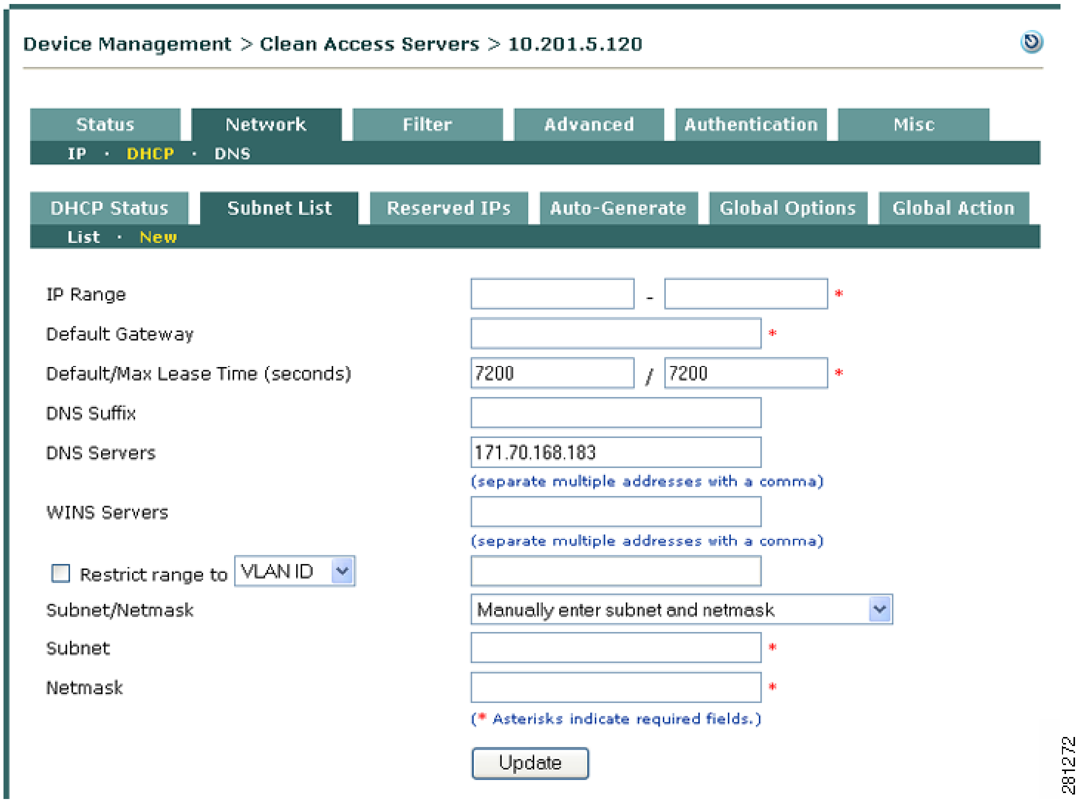


Device Management > Clean Access Servers > 10.201.5.120

IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.241.100 - 192.168.241.120	192.168.241.0 - 192.168.241.255		N/A	1	21	✎	✕

2. The new IP pool form appears.

Figure 5-6 New Subnet Form



IP Range	- *
Default Gateway	*
Default/Max Lease Time (seconds)	7200 / 7200 *
DNS Suffix	
DNS Servers	171.70.168.183 (separate multiple addresses with a comma)
WINS Servers	 (separate multiple addresses with a comma)
□ Restrict range to VLAN ID	
Subnet/Netmask	Manually enter subnet and netmask
Subnet	*
Netmask	* (* Asterisks indicate required fields.)

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 4-25 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 4-25 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 5-23 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

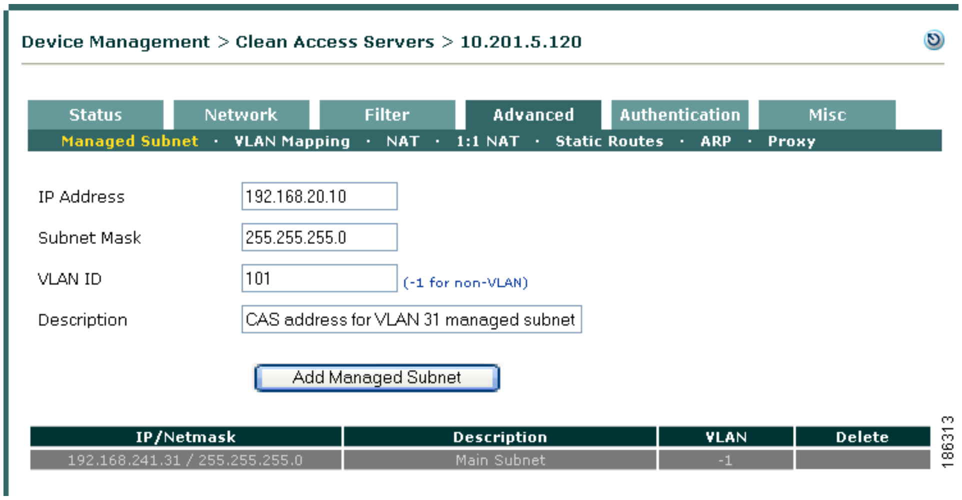
By automatically generating subnets, you can quickly divide your network into small segments. Segmenting your network into small subnets can be an effective security measure in response to a worm attack, since a network comprised of many small subnets (with one host per subnet possible) limits the ability 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 4-27).

Figure 5-7 Add Managed Subnet


Device Management > Clean Access Servers > 10.201.5.120
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add Managed Subnet
186313

IP Address 192.168.20.10

Subnet Mask 255.255.255.0

VLAN ID 101 (-1 for non-VLAN)

Description CAS address for VLAN 31 managed subnet

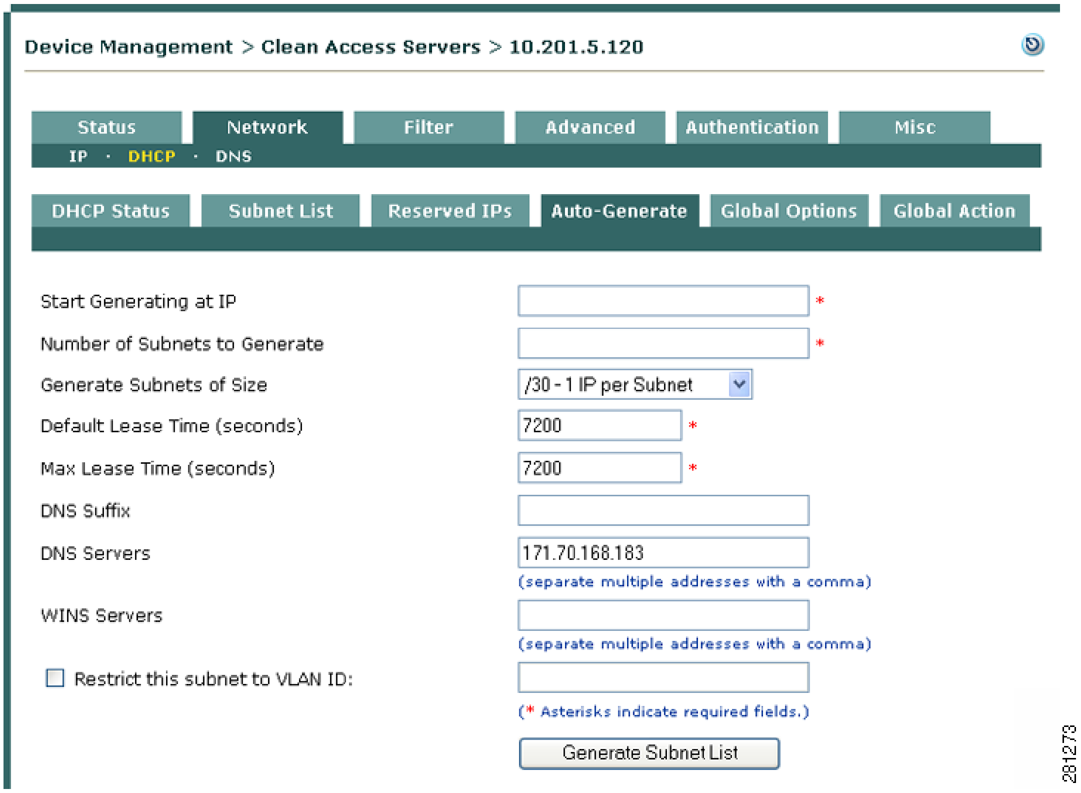
IP/Netmask	Description	VLAN	Delete
192.168.241.31 / 255.255.255.0	Main Subnet	-1	

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:

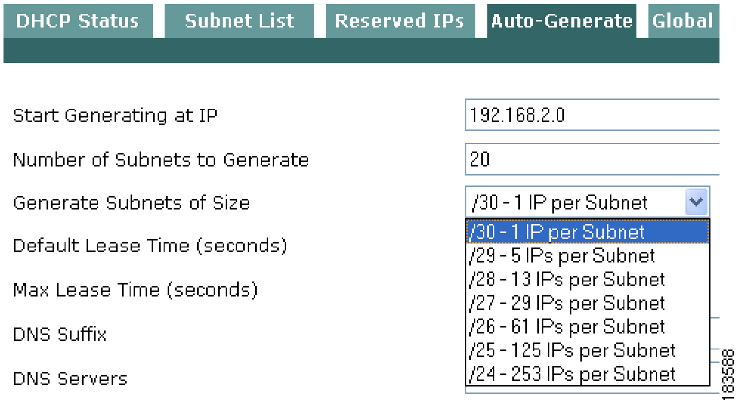
Figure 5-8 DHCP—Auto-Generate Subnet Form



Device Management > Clean Access Servers > 10.201.5.120

Start Generating at IP	*
Number of Subnets to Generate	*
Generate Subnets of Size	/30 - 1 IP per Subnet
Default Lease Time (seconds)	7200 *
Max Lease Time (seconds)	7200 *
DNS Suffix	
DNS Servers	171.70.168.183 (separate multiple addresses with a comma)
WINS Servers	(separate multiple addresses with a comma)
□ Restrict this subnet to VLAN ID:	(* Asterisks indicate required fields.)

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



Start Generating at IP	192.168.2.0
Number of Subnets to Generate	20
Generate Subnets of Size	/30 - 1 IP per Subnet
Default Lease Time (seconds)	
Max Lease Time (seconds)	
DNS Suffix	
DNS Servers	

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.

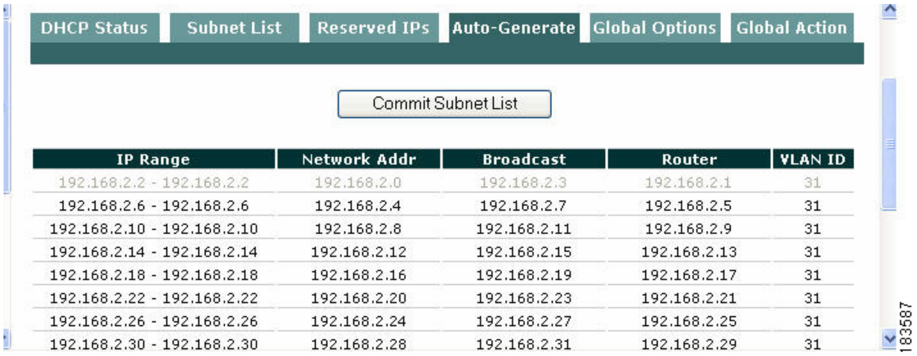
3. In the **Number of Subnets to Generate** field, type the number of subnets to generate. As mentioned, the maximum recommended size is 1000. Exceeding this number can impose a burden on the server's system resources.

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 5-23 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 5-9 Commit Subnet List

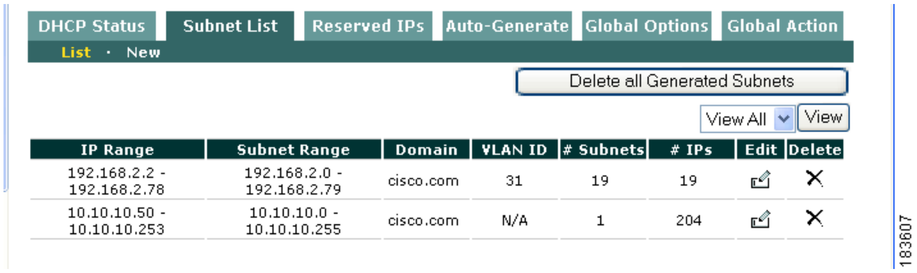


IP Range	Network Addr	Broadcast	Router	VLAN ID
192.168.2.2 - 192.168.2.2	192.168.2.0	192.168.2.3	192.168.2.1	31
192.168.2.6 - 192.168.2.6	192.168.2.4	192.168.2.7	192.168.2.5	31
192.168.2.10 - 192.168.2.10	192.168.2.8	192.168.2.11	192.168.2.9	31
192.168.2.14 - 192.168.2.14	192.168.2.12	192.168.2.15	192.168.2.13	31
192.168.2.18 - 192.168.2.18	192.168.2.16	192.168.2.19	192.168.2.17	31
192.168.2.22 - 192.168.2.22	192.168.2.20	192.168.2.23	192.168.2.21	31
192.168.2.26 - 192.168.2.26	192.168.2.24	192.168.2.27	192.168.2.25	31
192.168.2.30 - 192.168.2.30	192.168.2.28	192.168.2.31	192.168.2.29	31

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 5-10 Subnet List— List

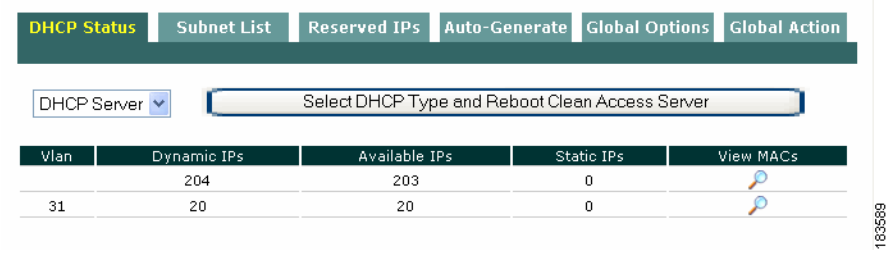
\



IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs	Edit	Delete
192.168.2.2 - 192.168.2.78	192.168.2.0 - 192.168.2.79	cisco.com	31	19	19	✎	✕
10.10.10.50 - 10.10.10.253	10.10.10.0 - 10.10.10.255	cisco.com	N/A	1	204	✎	✕

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).

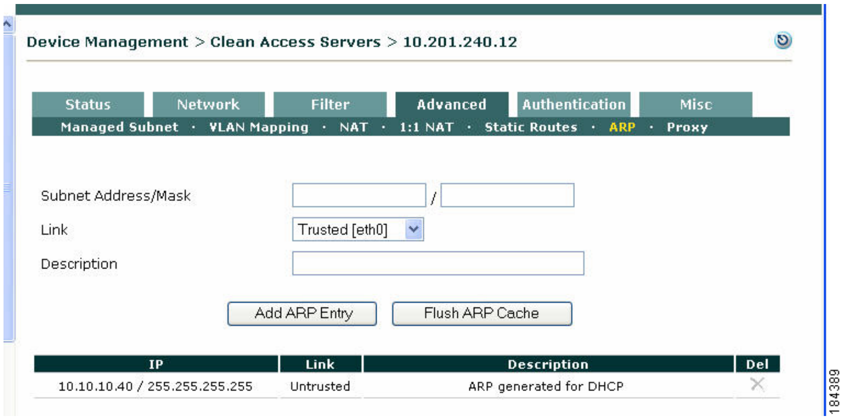
Figure 5-11 DHCP Status



Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	204	203	0	🔍
31	20	20	0	🔍

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 5-12. Deleting generated subnets also removes the corresponding ARP entries.

Figure 5-12 ARP Entries Generated for DHCP


Device Management > Clean Access Servers > 10.201.240.12
Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add ARP Entry
Flush ARP Cache
184389

Subnet Address/Mask /

Link Trusted [eth0]

Description

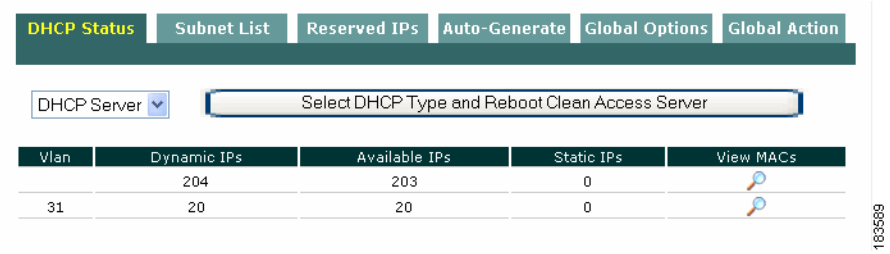
IP	Link	Description	Del
10.10.10.40 / 255.255.255.255	Untrusted	ARP generated for DHCP	✕

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.

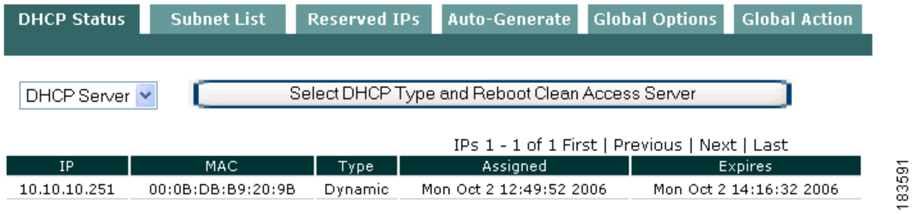
Figure 5-13 DHCP Status — VLANs



Vlan	Dynamic IPs	Available IPs	Static IPs	View MACs
	204	203	0	🔍
31	20	20	0	🔍

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 5-14.

Figure 5-14 View MAC Address



IPs 1 - 1 of 1 First | Previous | Next | Last

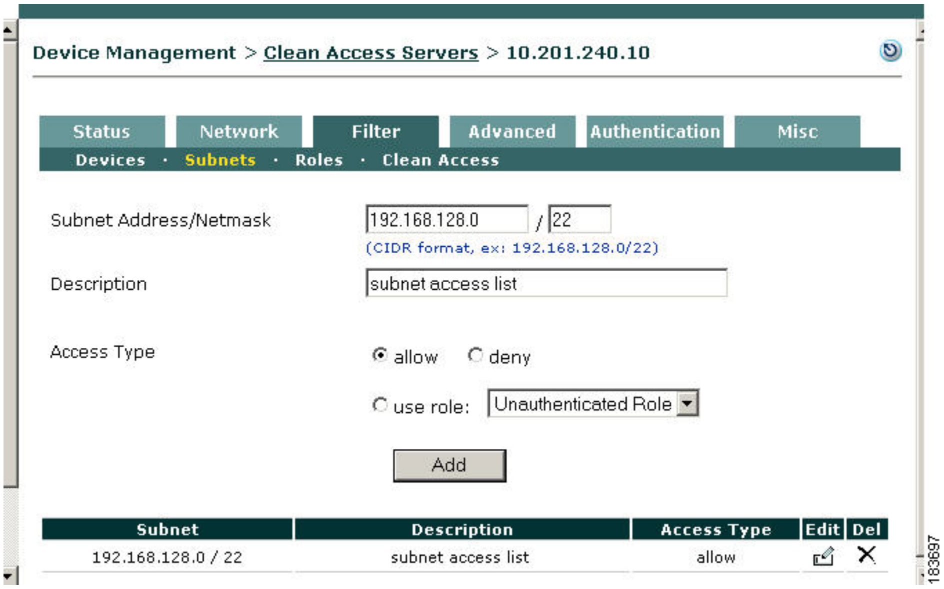
IP	MAC	Type	Assigned	Expires
10.10.10.251	00:0B:DB:B9:20:9B	Dynamic	Mon Oct 2 12:49:52 2006	Mon Oct 2 14:16:32 2006

- 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 5-15 Subnet List—List



Device Management > Clean Access Servers > 10.201.240.10

Subnet Address/Netmask: 192.168.128.0 / 22
(CIDR format, ex: 192.168.128.0/22)

Description: subnet access list

Access Type: ● allow ○ deny
○ use role: Unauthenticated Role

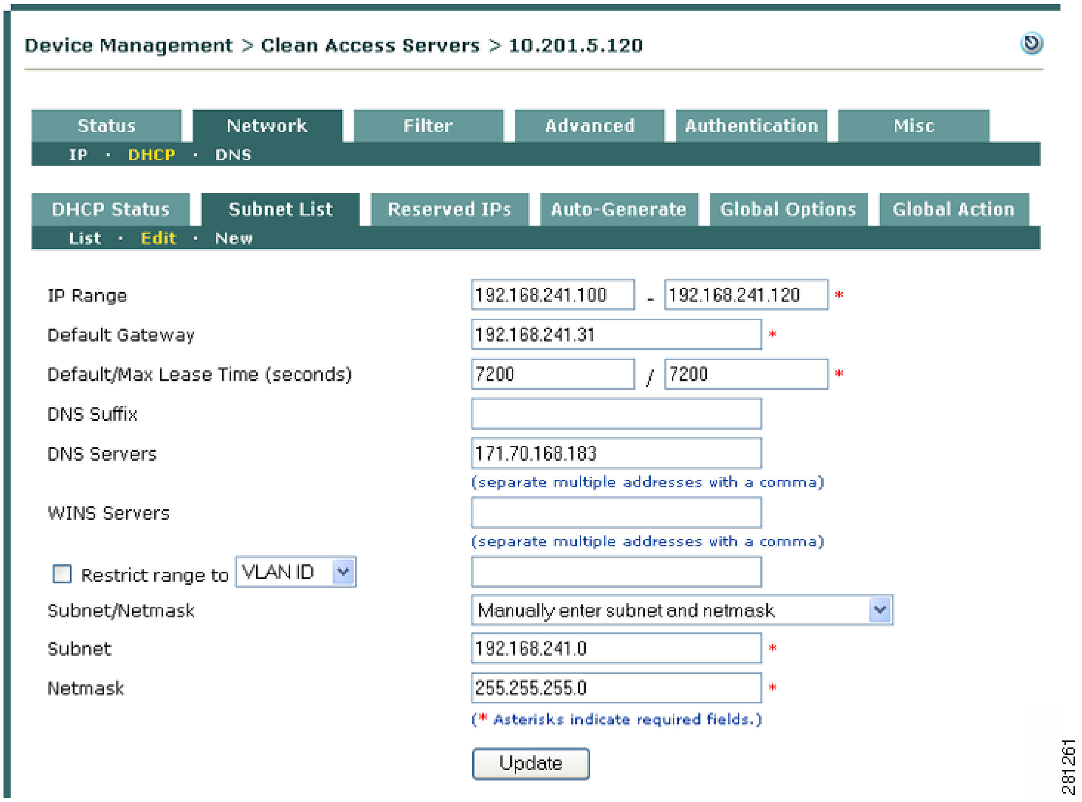
Subnet	Description	Access Type	Edit	Del
192.168.128.0 / 22	subnet access list	allow		✕

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. This action 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. Figure 5-16 shows the **Edit** form for an auto-generated subnet. (The **Edit** form for a manually-generated subnet is similar to Figure 5-6 on page 5-9.)

Figure 5-16 Edit Subnet List



IP Range	192.168.241.100 - 192.168.241.120 *
Default Gateway	192.168.241.31 *
Default/Max Lease Time (seconds)	7200 / 7200 *
DNS Suffix	
DNS Servers	171.70.168.183 (separate multiple addresses with a comma)
WINS Servers	 (separate multiple addresses with a comma)
□ Restrict range to VLAN ID	
Subnet/Netmask	Manually enter subnet and netmask
Subnet	192.168.241.0 *
Netmask	255.255.255.0 *

(* Asterisks indicate required fields.)

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.

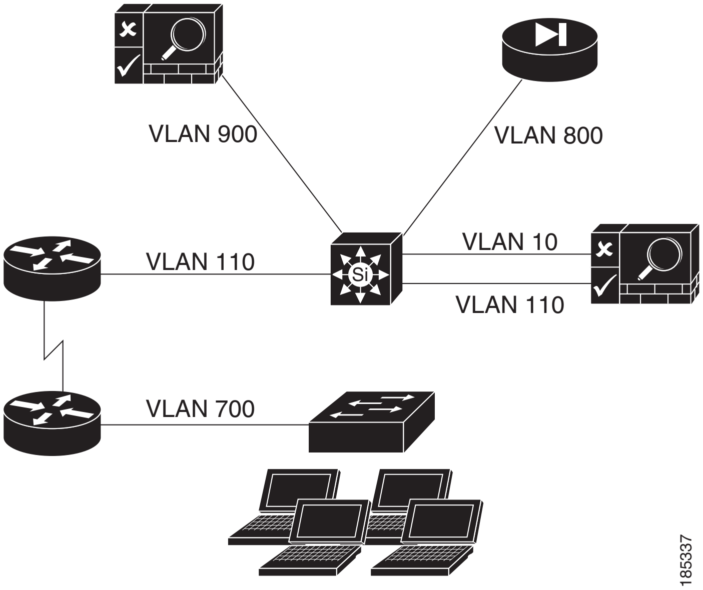
Configuring a Real-IP CAS as DHCP Server for L3 Clients

Typically, when a Clean Access Server is configured as a DHCP server it is in Layer 2 mode. The CAS acts as a DHCP server for the Layer 2 VLANs which are trunked to it. In Layer 2 mode, you configure a DHCP scope for that VLAN on the CAS and then configure a managed subnet for that VLAN so that the CAS can communicate to clients in that VLAN.

However, Layer 3 clients are one or multiple hops away from the CAS and therefore work differently. L3 clients are not adjacent to the CAS and DHCP discover broadcast from these clients will never reach the CAS (DHCP server). Therefore, a DHCP scope for these clients cannot be created based on VLAN.

Figure 5-17 illustrates an example scenario.

Figure 5-17 Example L3 Scenario



In this example:

- CAM is on VLAN 900
- CAS trusted interface is on VLAN 10 and untrusted interface is on VLAN 100.
- Client machines in VLAN 700 are multiple hops away from the CAS
- CAS is required to act as a DHCP server for these clients

As previously mentioned, DHCP discover broadcast from these L3 clients are not able to cross the VLAN 700 boundary. Therefore, an “IP helper address” needs to be configured under the router interface acting as the gateway for VLAN 700, for example:

```
Interface vlan 700
 Ip address 10.60.60.1 255.255.255.0
 ip helper-address x.x.x.x
```

Where `x.x.x.x` is the untrusted side (eth1) IP address of the CAS (e.g. 10.20.20.1).

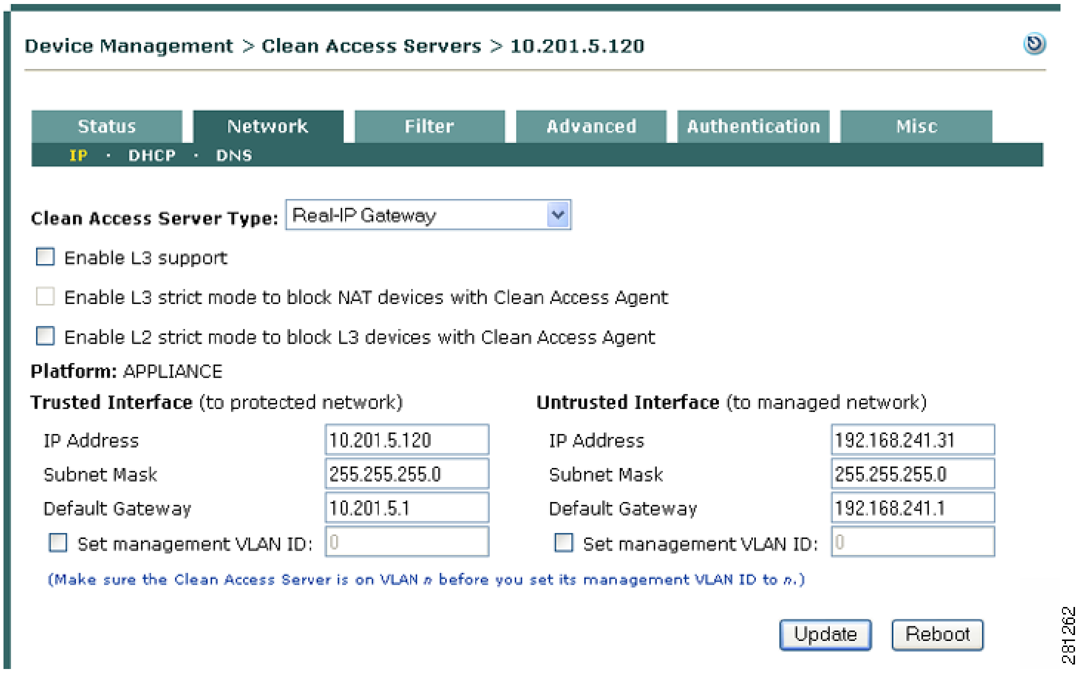
On the CAS, the following needs to be configured:

- A DHCP scope for clients in VLAN 700 with an “IP RELAY” of 10.60.60.1
- A route for 10.60.60.0/24 (VLAN 700) pointing towards the untrusted side

Figure 5-18 shows the IP information of the CAS configured as a Real-IP Gateway:

- Trusted (eth0) interface IP address is 10.2.2.1
- Trusted Default Gateway is 10.2.2.2
- Untrusted (eth1) interface IP address is 10.20.20.1
- Untrusted Default Gateway is 10.20.20.3

Figure 5-18 CAS IP Configuration



Device Management > Clean Access Servers > 10.201.5.120

Clean Access Server Type: Real-IP Gateway

□ Enable L3 support

□ Enable L3 strict mode to block NAT devices with Clean Access Agent

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

Platform: APPLIANCE

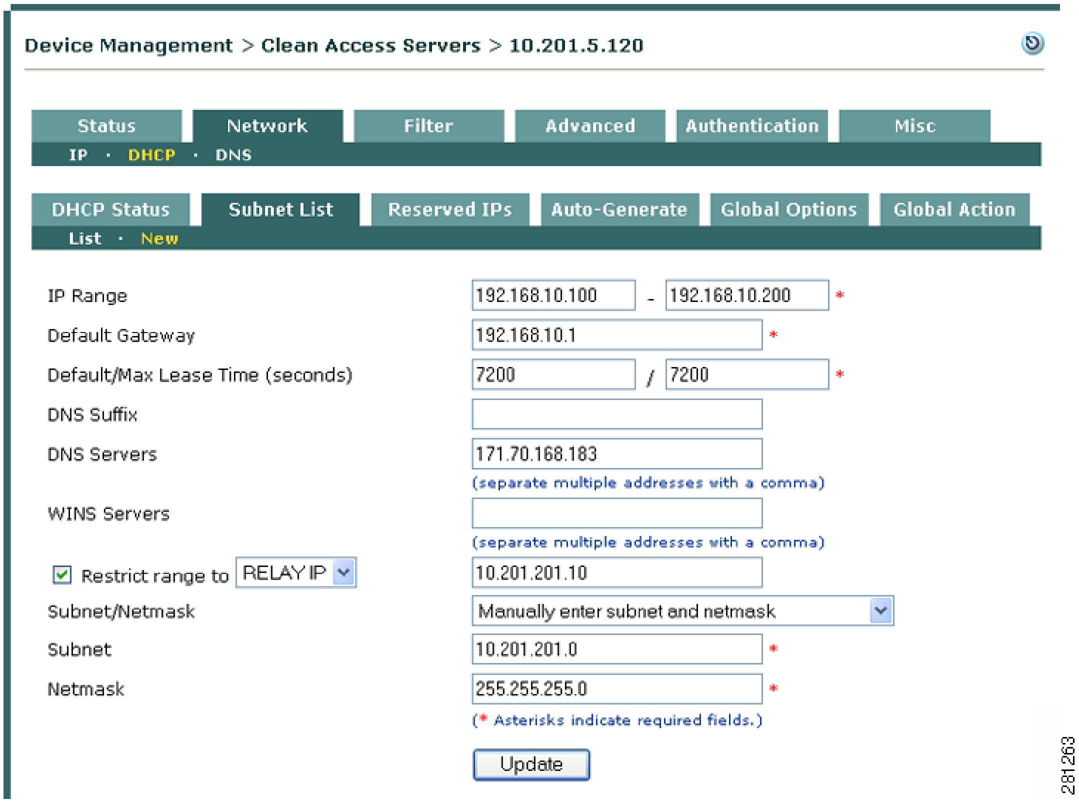
Trusted Interface (to protected network)		Untrusted Interface (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

The CAS has already been enabled as a **DHCP Server** (as described in Enable the DHCP Module, page 5-2). Figure 5-19 shows the New Subnet list form configured under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Subnet List > New** with:

- A client IP range of 10.60.60.100-10.60.60.200
- Default gateway of 10.60.60.1
- **Restrict range to RELAY IP** is chosen with 10.60.60.1 entered as the IP relay.
- Subnet of 10.60.60.0 and subnet mask of 255.255.255.0 manually entered
- Click **Update** to create the new DHCP scope.

Figure 5-19 Restrict Subnet List to Relay IP

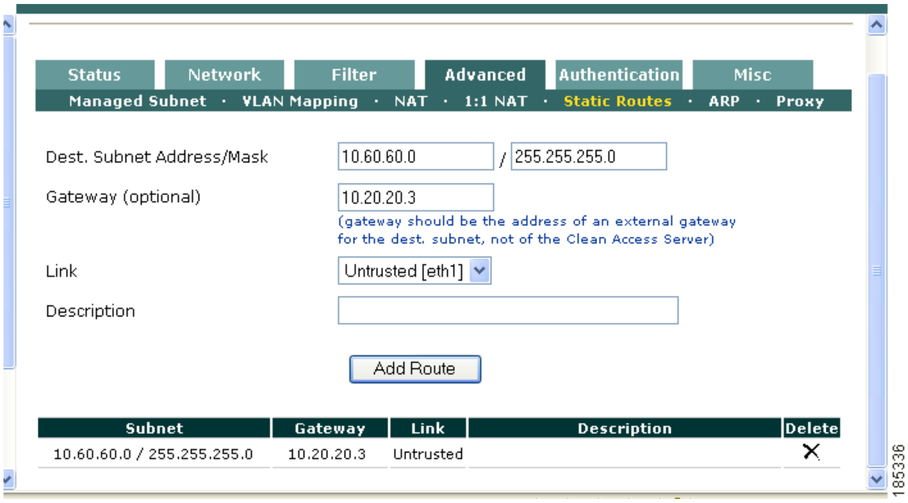


IP Range	192.168.10.100 - 192.168.10.200 *
Default Gateway	192.168.10.1 *
Default/Max Lease Time (seconds)	7200 / 7200 *
DNS Suffix	
DNS Servers	171.70.168.183 (separate multiple addresses with a comma)
WINS Servers	 (separate multiple addresses with a comma)
☑ Restrict range to RELAY IP	10.201.201.10
Subnet/Netmask	Manually enter subnet and netmask
Subnet	10.201.201.0 *
Netmask	255.255.255.0 *
	(* Asterisks indicate required fields.)

Figure 5-20 shows the Static Routes form configured under **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes** with:

- Destination Subnet Address of **10.60.60.0** and Subnet Mask of 255.255.255.0 (the subnet/netmask configured in Figure 5-19).
- **Untrusted[eth1]** chosen as the Link.
- Gateway of **10.20.20.3**, which is the CAS eth1 default gateway shown in Figure 5-18
- Click **Add Route** to add this static route to the CAS.

Figure 5-20 Create Static Route


Status
Network
Filter
Advanced
Authentication
Misc
Managed Subnet · VLAN Mapping · NAT · 1:1 NAT · Static Routes · ARP · Proxy
Add Route
185336

Dest. Subnet Address/Mask 10.60.60.0 / 255.255.255.0

Gateway (optional) 10.20.20.3

(gateway should be the address of an external gateway for the dest. subnet, not of the Clean Access Server)

Link Untrusted [eth1]

Description

Subnet	Gateway	Link	Description	Delete
10.60.60.0 / 255.255.255.0	10.20.20.3	Untrusted		✕

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 5-4 lists several rules that apply to reserved IP addresses.

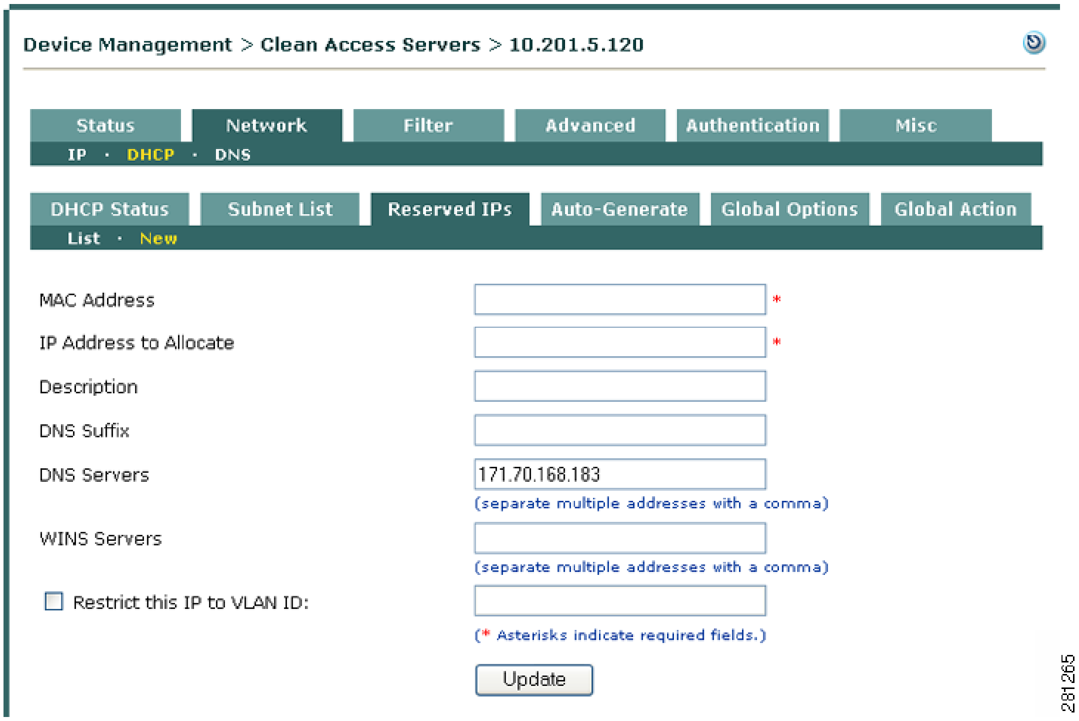
Table 5-4 Reserved IP Address Rules

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 5-21 Reserved IPs—New



MAC Address	*
IP Address to Allocate	*
Description	
DNS Suffix	
DNS Servers	171.70.168.183 (separate multiple addresses with a comma)
WINS Servers	(separate multiple addresses with a comma)
□ Restrict this IP to VLAN ID:	

(* Asterisks indicate required fields.)

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 5-22) 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 5-28.

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.

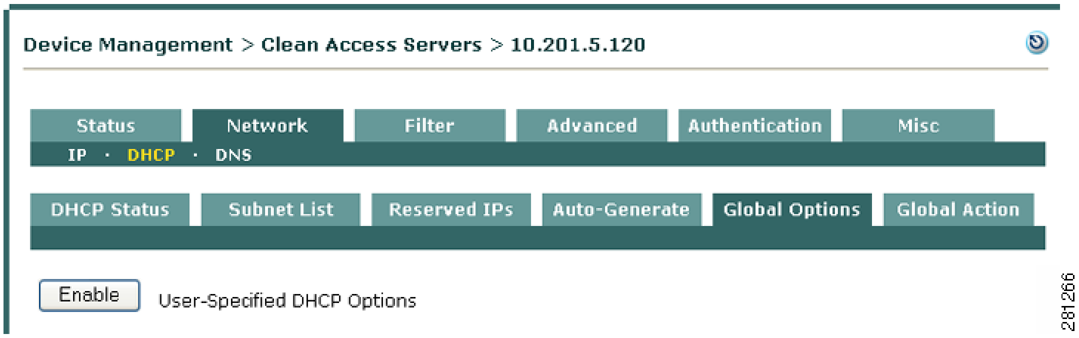
A server directive instructs the DHCP server to behave differently, while a DHCP option refers to a specific piece of data to be returned by the DHCP server. For example, the "allow-bootp" server directive (disabled by default) instructs the DHCP server to allow older BOOTP clients to connect. See Table 5-5 "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 5-22).

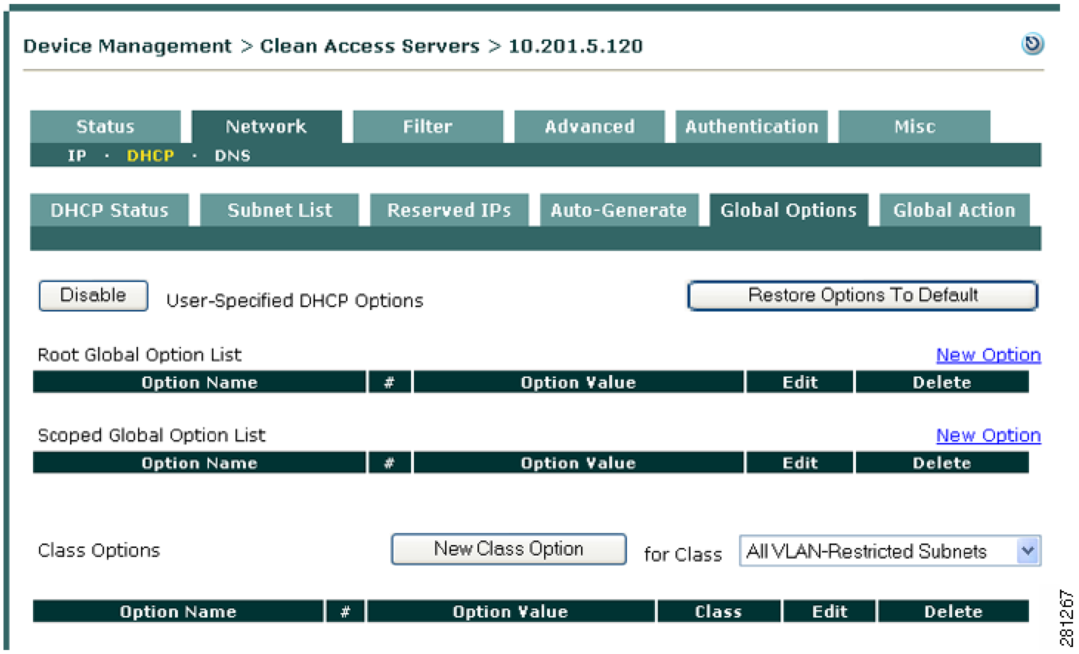
Figure 5-22 DHCP Global Options - Enable



2. With **Global Options** enabled on the CAS (Figure 5-23), 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 5-23 DHCP Global Options



Root Global Option List

Option Name	#	Option Value	Edit	Delete

Scoped Global Option List

Option Name	#	Option Value	Edit	Delete

Class Options — for Class: All VLAN-Restricted Subnets

Option Name	#	Option Value	Class	Edit	Delete

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.

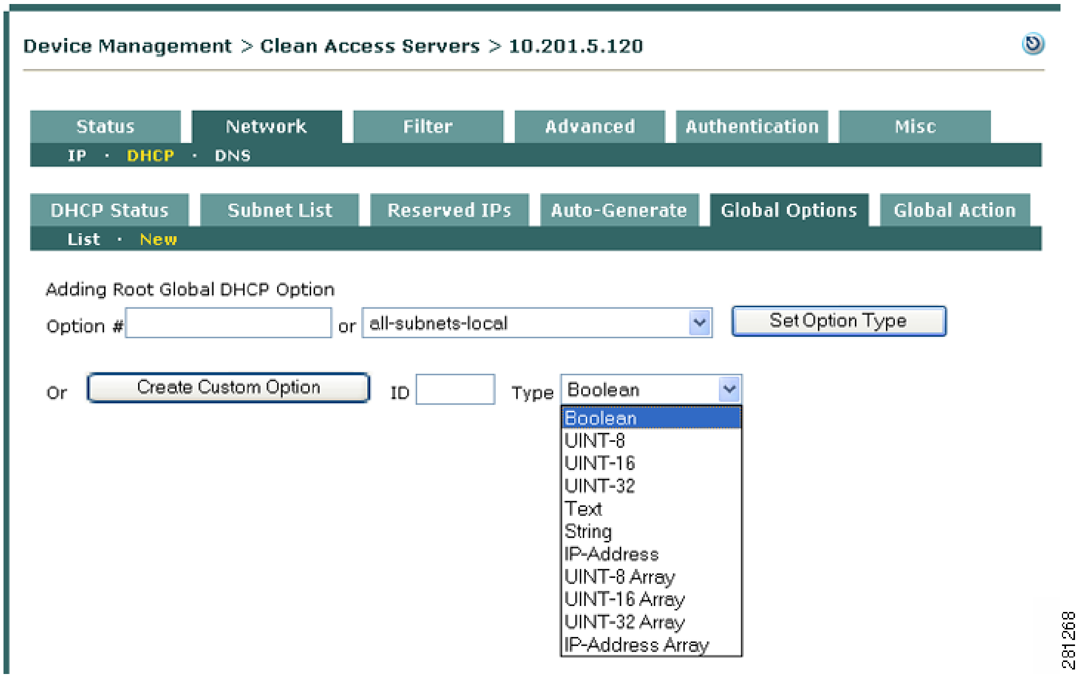
If the desired option number is not known, or if specifying a server directive which changes server behavior but has no corresponding DHCP option number, then select the name of the option or directive from the dropdown menu next to the **Set Option Type** button. In either case, click the **Set Option 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 5-24). This form allows you to enter text directly into the DHCP configuration file at the root level.

Figure 5-24 DHCP Global Options - New Root Global (Custom Option)



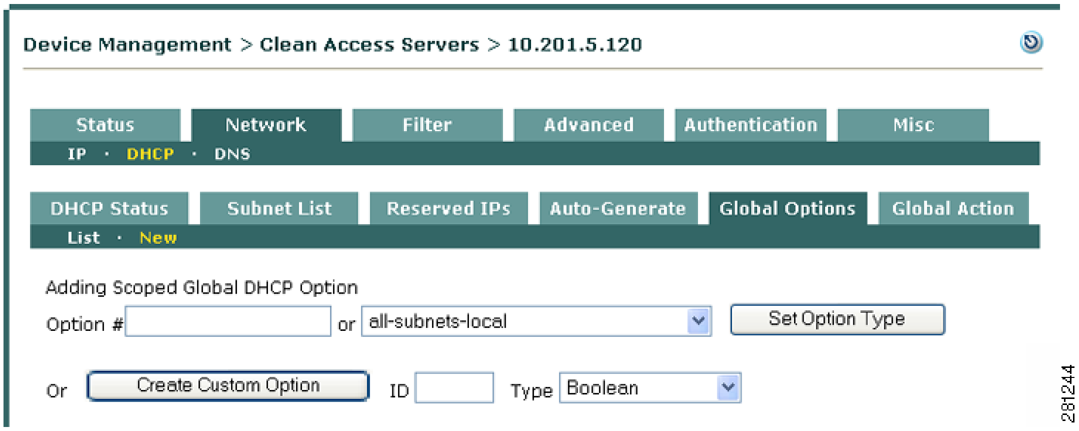
4. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.

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 5-23), 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 5-24). This form allows you to enter text directly into the DHCP configuration file at the subnet scope level.

Figure 5-25 DHCP Global Options - New Scoped Global



Device Management > Clean Access Servers > 10.201.5.120

Adding Scoped Global DHCP Option

Option # or all-subnets-local

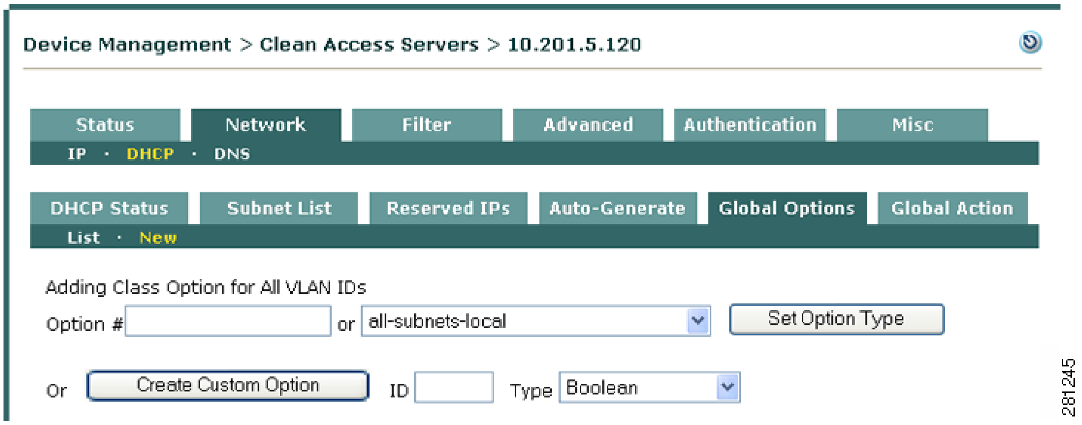
Or ID Type Boolean

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 5-23), 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 5-25).

Figure 5-26 DHCP Global Options - New Class Option For All VLAN IDs (VLAN Restricted Subnets)



Adding Class Option for All VLAN IDs

Option # or all-subnets-local

ID Type Boolean

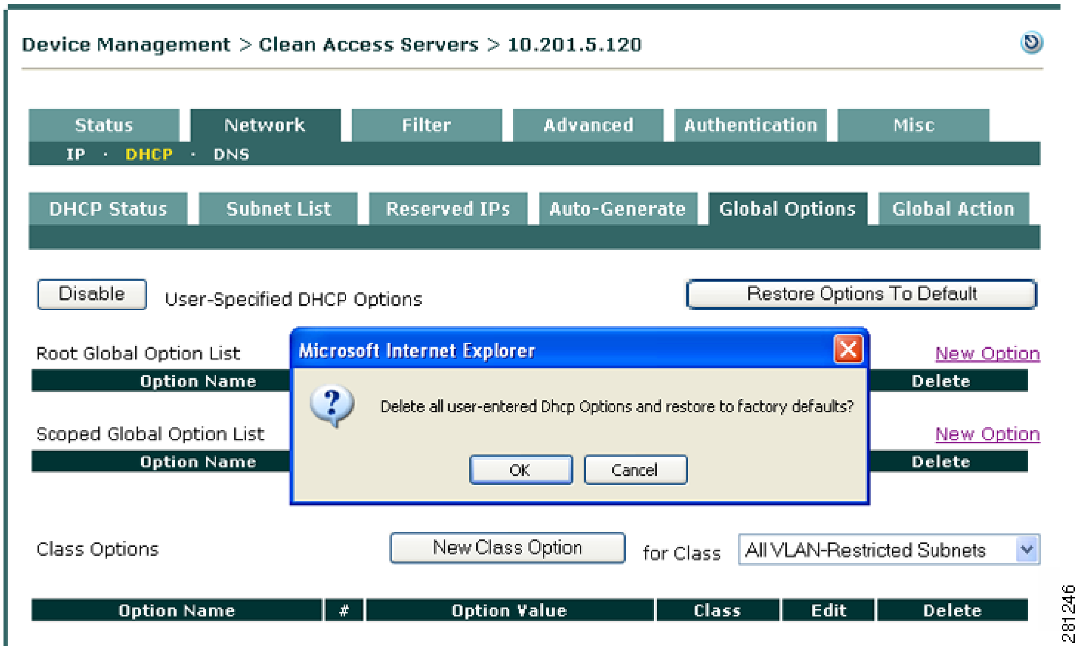
11. Either type the **Option #**, or choose the option type from the dropdown list (providing an alphabetized list of commonly-used options), and click **Set Option Type**.

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 5-27).

Figure 5-27 Restore Global Options to Default



Delete all user-entered Dhcp Options and restore to factory defaults?

for Class All VLAN-Restricted Subnets

Disable DHPC Options

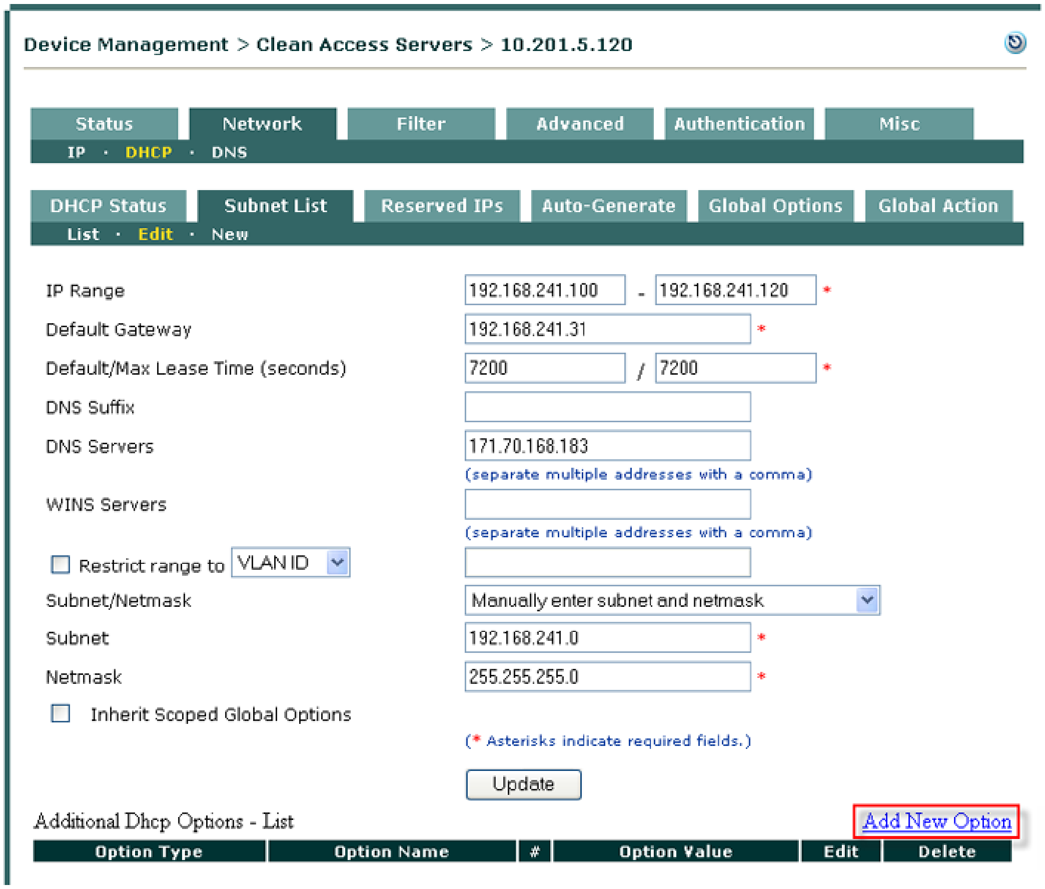
To disable admin-specified DHCP options, click the Disable button at the top-left side of he **Global Options > List** page (Figure 5-23 on page 5-24).

Add Local Scoped DHCP Option

1. Make sure DHCP options are enabled as described in Enable User-Specified DHCP Options, page 5-24.
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 5-28 Edit Subnet List Form (Local Scoped DHCP Option

)



Device Management > Clean Access Servers > 10.201.5.120

IP Range 192.168.241.100 - 192.168.241.120 *

Default Gateway 192.168.241.31 *

Default/Max Lease Time (seconds) 7200 / 7200 *

DNS Suffix

DNS Servers 171.70.168.183
(separate multiple addresses with a comma)

WINS Servers
(separate multiple addresses with a comma)

□ Restrict range to VLAN ID

Subnet/Netmask Manually enter subnet and netmask

Subnet 192.168.241.0 *

Netmask 255.255.255.0 *

□ Inherit Scoped Global Options

(* Asterisks indicate required fields.)

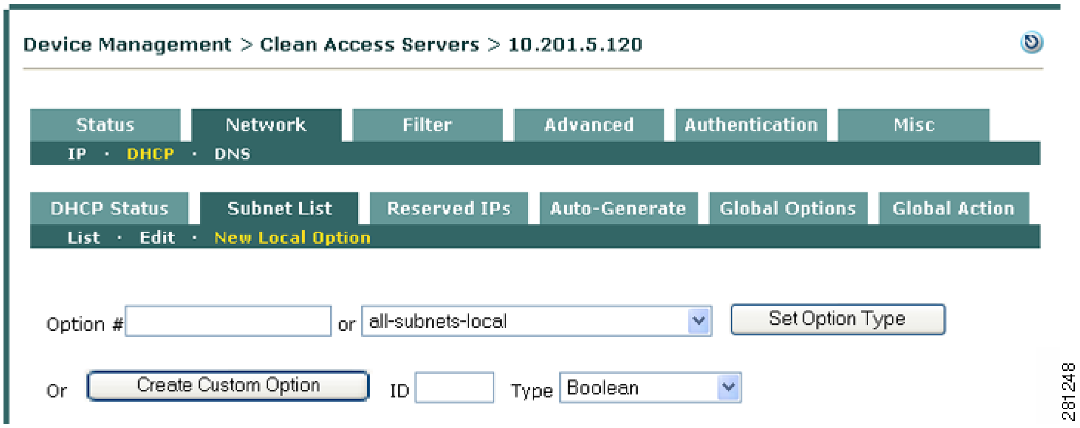
Additional Dhcp Options - List

Option Type	Option Name	#	Option Value	Edit	Delete

281247

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

Figure 5-29 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**.

Table 5-5 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.
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.

Table 5-5 DHCP Server Directives (continued)

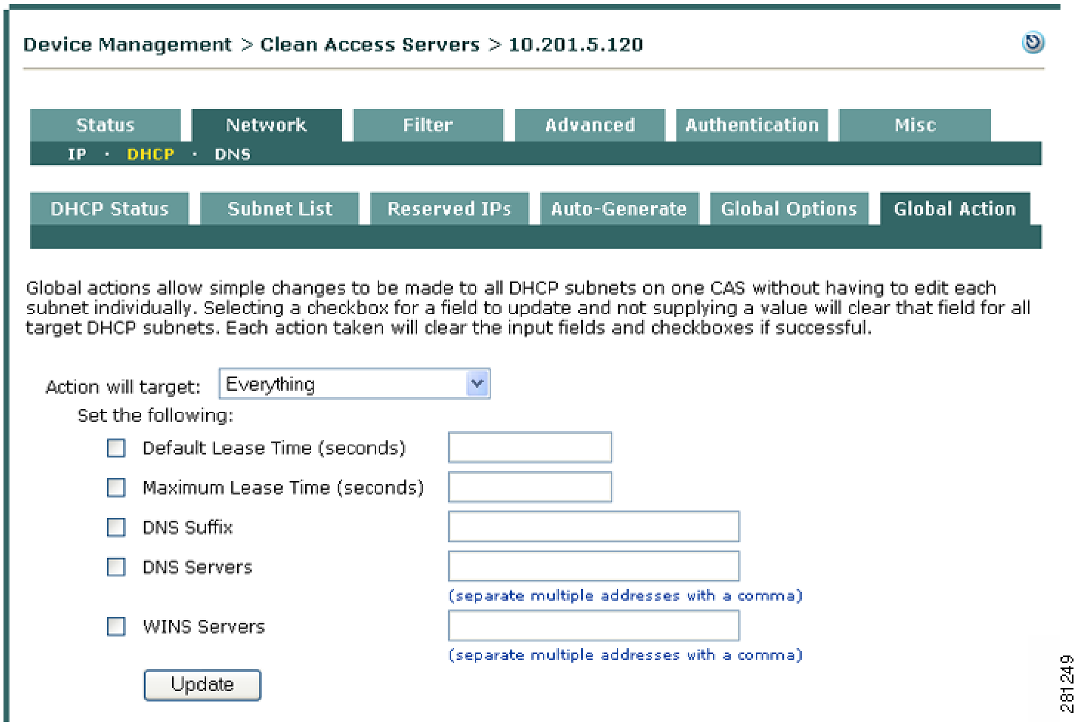
Server Directive	Description
filename	Instructs the DHCP server to fill out the filename portion of the DHCP packet. This is not an option, as it does not appear in the DHCP options list. This server directive can be specified as a scoped global or local option.
get-lease-hostname	Instructs the server 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 5-30).

Figure 5-30 Global Action



Global actions allow simple changes to be made to all DHCP subnets on one CAS without having to edit each subnet individually. Selecting a checkbox for a field to update and not supplying a value will clear that field for all target DHCP subnets. Each action taken will clear the input fields and checkboxes if successful.

Action will target: Everything

Set the following:

□ Default Lease Time (seconds)

□ Maximum Lease Time (seconds)

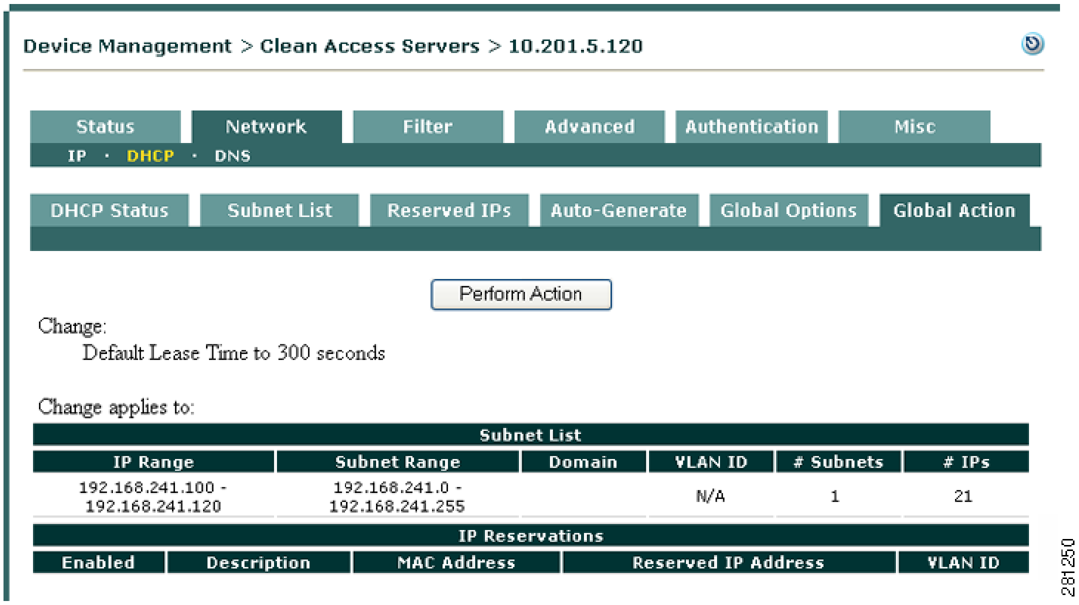
□ DNS Suffix

□ DNS Servers (separate multiple addresses with a comma)

□ WINS Servers (separate multiple addresses with a comma)

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 5-31).

Figure 5-31 Example Global Action



Change:

Default Lease Time to 300 seconds

Change applies to:

Subnet List

IP Range	Subnet Range	Domain	VLAN ID	# Subnets	# IPs
192.168.241.100 - 192.168.241.120	192.168.241.0 - 192.168.241.255		N/A	1	21

IP Reservations

Enabled	Description	MAC Address	Reserved IP Address	VLAN ID

CHAPTER 6

Integrating with Cisco VPN Concentrators

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

- Overview, page 6-1
- Configure Cisco NAC Appliance for VPN Concentrator Integration, page 6-4
- Cisco NAC Appliance Agent with VPN Concentrator and SSO, page 6-18
- View Active VPN Clients, page 6-19

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 Nessus Scanning process again.
- In order for clients to discover the CAS when they are one or more L3 hops away, the 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 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 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 topology and configuration required is fairly straightforward. Figure 6-1 illustrates a Cisco NAC Appliance network integrated with a VPN concentrator. Figure 6-2 illustrates the VPN concentrator configuration "before" and Figure 6-3 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 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 6-19.

See Configure Single Sign-On (SSO) on the CAS/CAM, page 6-10 for further details.

Figure 6-1 VPN Concentrator Integrated with Cisco NAC Appliance

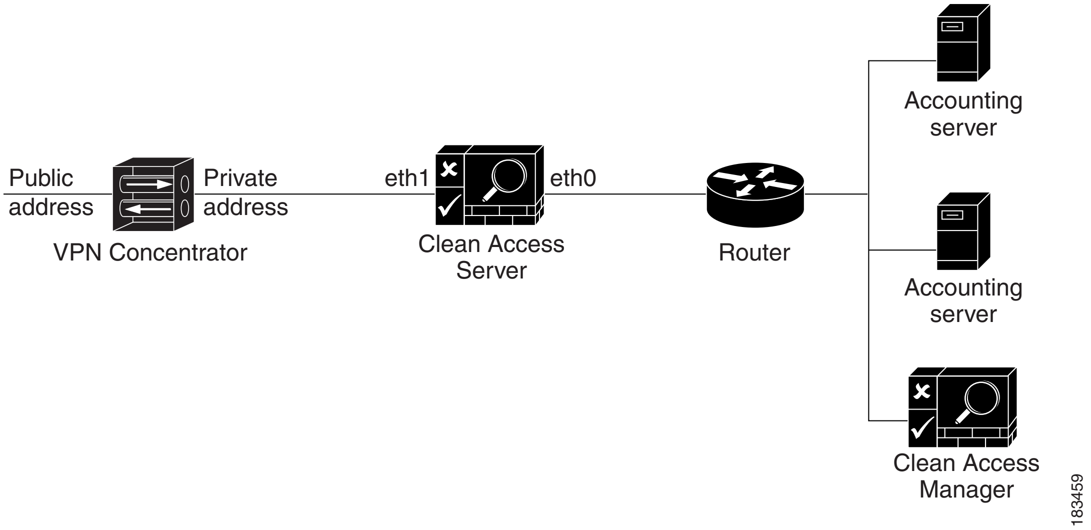


Figure 6-2 VPN Concentrator Before Cisco NAC Appliance Integration

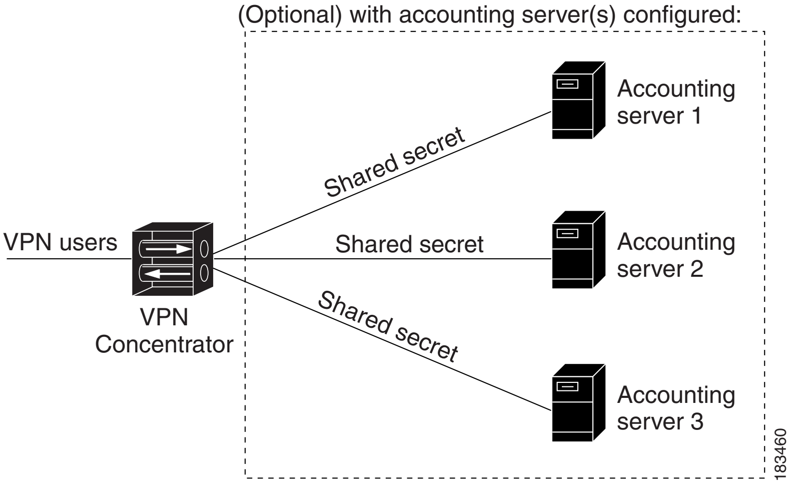
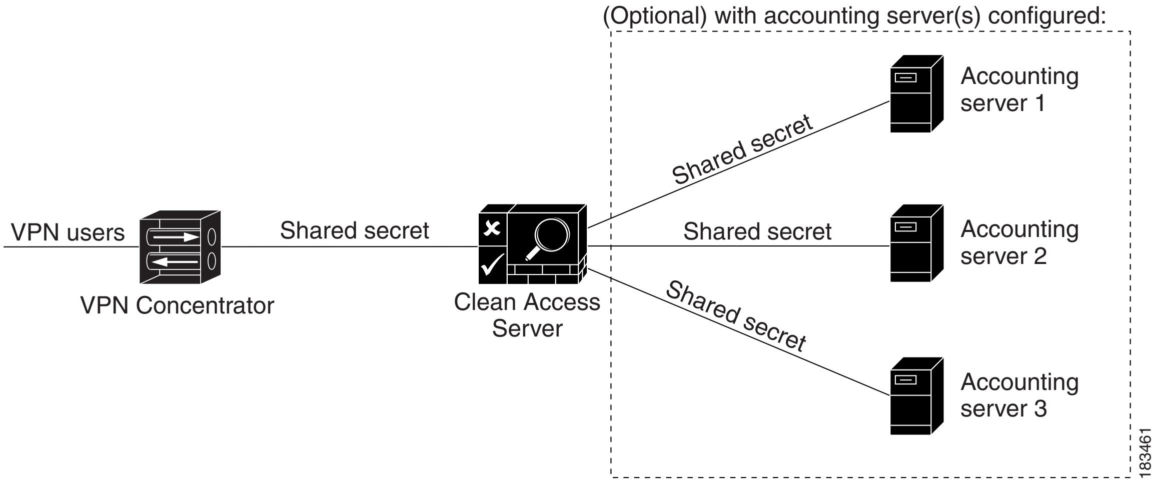


Figure 6-3 VPN Concentrator After Cisco NAC Appliance Integration



Configure Cisco NAC Appliance 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 Requirements for your VPN users

Step 3 Enable L3 Support on the CAS

Step 4 Verifying the Discovery Host

Step 5 Adding/Editing VPN Concentrator Entries

Step 6 Make CAS the RADIUS Accounting Server for VPN Concentrator

Step 7 Adding/Editing Accounting Server Entries

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

Step 9 Create (Optional) Auth Server Mapping Rules

Step 10 Add VPN Concentrator as a Floating Device

Step 11 Configure Single Sign-On (SSO) on the CAS/CAM

Step 12 Configure VPN SSO in a FIPS 140-2 Compliant Deployment (if FIPS 140-2 compliant deployment)

Step 13 Create (Optional) Auth Server Mapping Rules on the CAM for Cisco VPN SSO

Step 14 Test as Cisco NAC Appliance Agent with VPN Concentrator and SSO

Step 15 View Active VPN Clients (for troubleshooting)

Add Default Login Page

For both web login users and Agent users, a login page must be added and present in the system in order for the user to authenticate via the 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 Configuration Guide, Release 4.8(1)* for complete details on login page configuration options.

Configure User Roles and Requirements

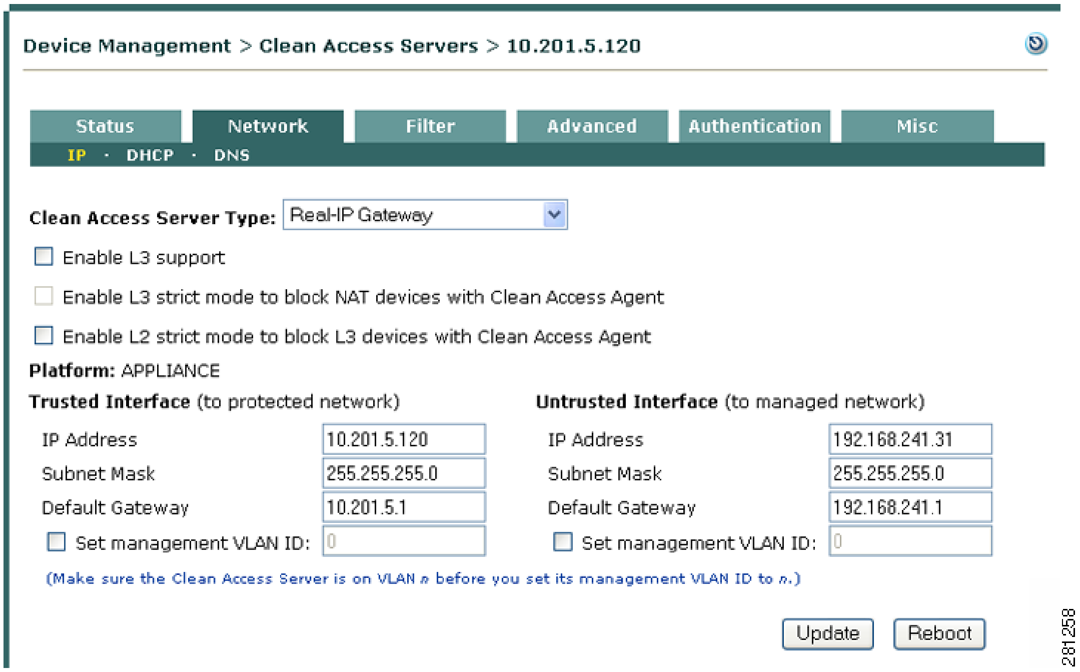
User roles must be configured along with requirements to enforce client posture assessment on VPN users. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for configuration details.

Enable L3 Support on the CAS

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

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

Figure 6-4 CAS Network Tab — Enable L3 Support



Device Management > Clean Access Servers > 10.201.5.120

Clean Access Server Type: Real-IP Gateway

□ Enable L3 support

□ Enable L3 strict mode to block NAT devices with Clean Access Agent

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

Platform: APPLIANCE

Trusted Interface (to protected network)		Untrusted Interface (to managed network)	
IP Address	10.201.5.120	IP Address	192.168.241.31
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	192.168.241.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0

(Make sure the Clean Access Server is on VLAN *n* before you set its management VLAN ID to *n*.)

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 disables the other.

See also Enable L3 Support, page 4-15.

Verifying the Discovery Host

There must be a Discovery Host enabled in order for the 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 8906 discovery packets to the network of the CAS. The CAS uses these packets to learn that an Agent is active, and discards the packets before they ever reach the CAM. (This function does not apply to the Cisco NAC Web Agent.) 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.

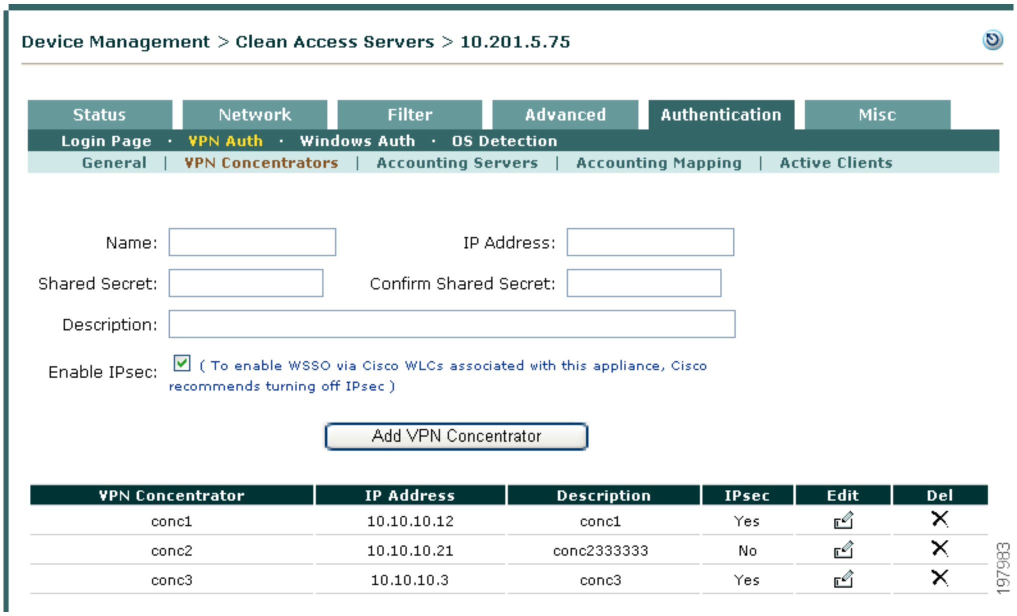
See VPN/L3 Access for Agents, page 4-16, and the "Configuring Agent Distribution/Installation" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for additional information.

Adding/Editing VPN Concentrator Entries

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

Step 2 If you are editing an existing VPN concentrator entry, click on the **Edit** icon for that entry in the list at the bottom of the configuration window, update any information necessary according to the following steps, and click **Save**. Otherwise, skip to Step 3 to add a new VPN concentrator entry.

Figure 6-5 Add VPN Concentrator


Device Management > Clean Access Servers > 10.201.5.75
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add VPN Concentrator
197983

Name: IP Address:

Shared Secret: Confirm Shared Secret:

Description:

Enable IPsec: ☑ (To enable WSSO via Cisco WLCs associated with this appliance, Cisco recommends turning off IPsec)

VPN Concentrator	IP Address	Description	IPsec	Edit	Del
conc1	10.10.10.12	conc1	Yes	✎	✕
conc2	10.10.10.21	conc2333333	No	✎	✕
conc3	10.10.10.3	conc3	Yes	✎	✕

Step 3 Type a **Name** for the concentrator.

Step 4 Type the Private **IP Address** of the concentrator.

Step 5 Type a **Shared Secret** between the CAS and VPN concentrator. The same secret must be configured on the concentrator itself.

Step 6 Retype the secret in the **Confirm Shared Secret** field.

Step 7 Enter an optional **Description**.

Step 8 For a FIPS 140-2 compliant deployment, activate the **Enable IPsec** checkbox to ensure you can establish a secure IPSec tunnel for authentication traffic. See also, Configure VPN SSO in a FIPS 140-2 Compliant Deployment, page 6-13.

Step 9 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_eol_series_home.html

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

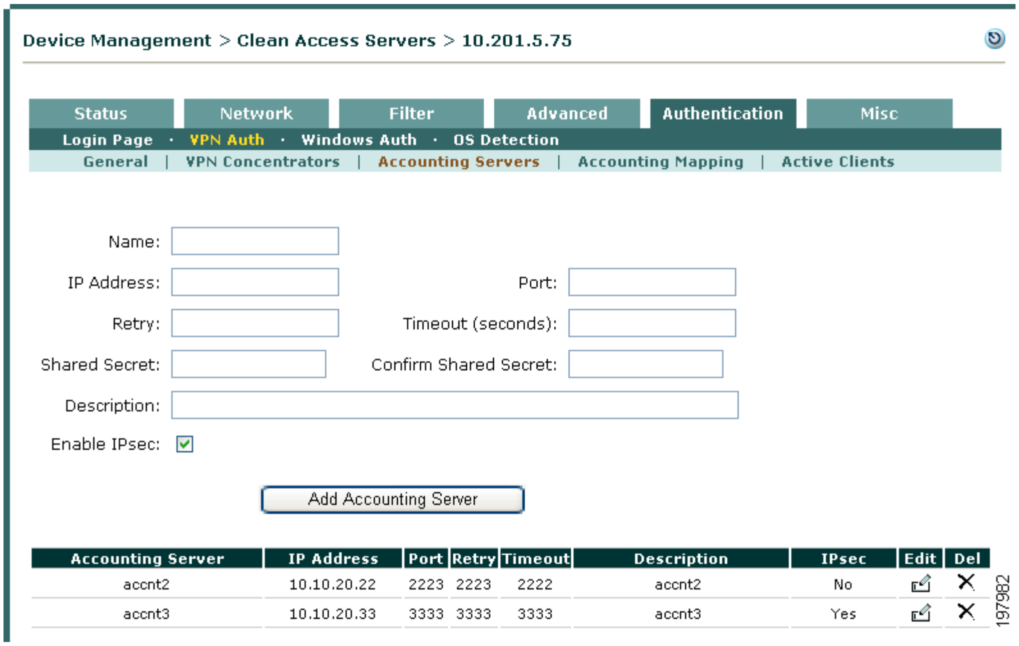
Adding/Editing Accounting Server Entries

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.

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

Step 2 If you are editing an existing accounting server entry, click on the **Edit** icon for that entry in the list at the bottom of the configuration window, update any information necessary according to the following steps, and click **Save**. Otherwise, skip to Step 3 to add a new accounting server entry.

Figure 6-6 Add Accounting Server(s)


Device Management > Clean Access Servers > 10.201.5.75
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add Accounting Server
197982

Name:

IP Address: Port:

Retry: Timeout (seconds):

Shared Secret: Confirm Shared Secret:

Description:

Enable IPsec: ☑

Accounting Server	IP Address	Port	Retry	Timeout	Description	IPsec	Edit	Del
accnt2	10.10.20.22	2223	2223	2222	accnt2	No	✎	✕
accnt3	10.10.20.33	3333	3333	3333	accnt3	Yes	✎	✕

Step 3 Type a **Name** for the accounting server.

Step 4 Type the **IP Address** of the accounting server.

Step 5 Type the **Port** of the accounting server (typically 1813)

Step 6 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.

Step 7 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.

Step 8 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.

Step 9 Retype the secret in the **Confirm Shared Secret** field.

Step 10 Enter an optional **Description.**

Step 11 For a FIPS 140-2 compliant deployment, activate the **Enable IPsec** checkbox to ensure you can establish a secure IPSec tunnel for authentication traffic.

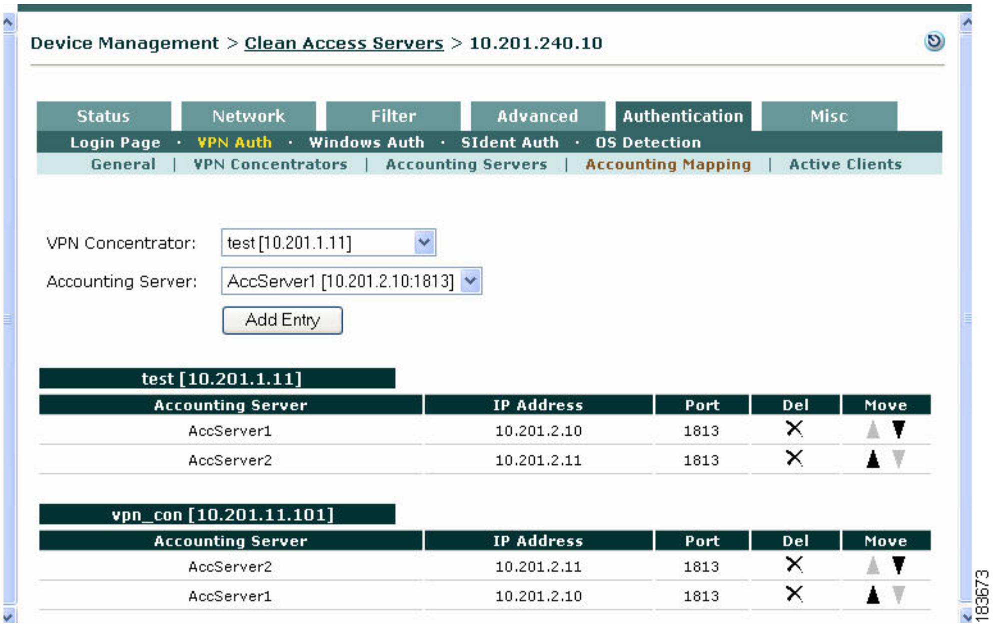
Step 12 Click **Add Accounting Server**.

Mapping 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.

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

Figure 6-7 Accounting Mapping


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · SIdent Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Add Entry
183673

VPN Concentrator: test [10.201.1.11]

Accounting Server: AccServer1 [10.201.2.10:1813]

test [10.201.1.11]

Accounting Server	IP Address	Port	Del	Move
AccServer1	10.201.2.10	1813	✕	▲ ▼
AccServer2	10.201.2.11	1813	✕	▲ ▼

vpn_con [10.201.11.101]

Accounting Server	IP Address	Port	Del	Move
AccServer2	10.201.2.11	1813	✕	▲ ▼
AccServer1	10.201.2.10	1813	✕	▲ ▼

Step 2 Choose a **VPN Concentrator** from the dropdown menu. The menu displays all VPN concentrators added to the CAS.

Step 3 Choose an **Accounting Server** from the dropdown menu. The menu displays all accounting servers configured for the CAS.

Step 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 Cisco NAC Appliance will be required to meet 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 Configuration Guide, Release 4.8(1)* 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 posture assessment 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 posture assessment directly without having to also login on the Clean Access Server. SSO is configured on both the CAS and CAM as described below.

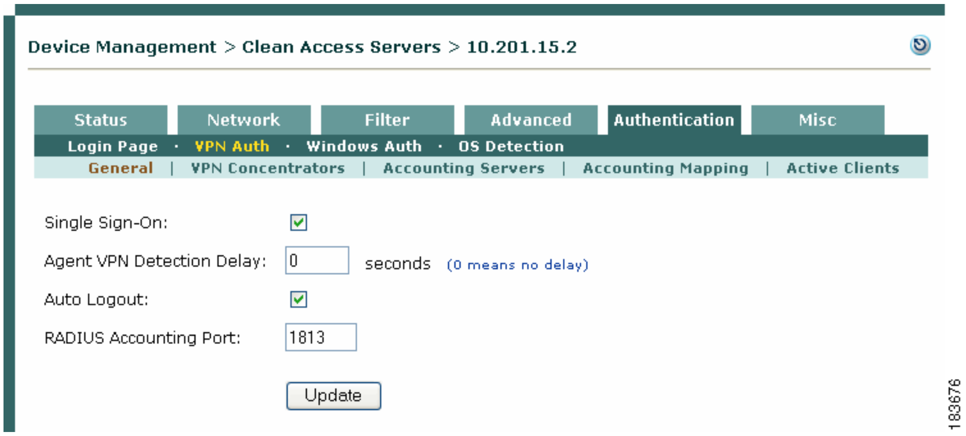
The most important attributes needed from RADIUS accounting packets are User_Name, Framed_IP_address, Calling_Station_ID. For a user to be qualified for SSO through the Clean Access Server, either the Framed_IP_address or Calling_Station_ID attribute (sent for the client's IP address) must be in the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

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

Figure 6-8 General Settings (SSO / Logout / RADIUS Accounting Port)



Device Management > Clean Access Servers > 10.201.15.2
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Update
183676

Single Sign-On: ☑

Agent VPN Detection Delay: 0 seconds (0 means no delay)

Auto Logout: ☑

RADIUS Accounting Port: 1813

Step 2 Click the checkbox for **Single Sign-On** to enable VPN SSO on the CAS.

Step 3 Enter a time period (in seconds) for the **Agent VPN Detection Delay** value. If the CAS has not received the required RADIUS accounting information before the Agent attempts VPN SSO, the Agent will prompt for user login. The **Agent VPN Detection Delay** field allows you to specify the amount of time the CAS should wait before prompting for authentication from the remote user's Agent that is transmitting SWISS UDP discovery packets.

This option ensures that the CAS has time to receive updates for users who are already connected via VPN before prompting them for login credentials that the CAS normally leverages from VPN login. If the CAS learns of the existing connection during the specified waiting period, it automatically yields to the VPN SSO function. Otherwise, once the specified waiting period has passed with no indication that the user connection is already established via VPN, the CAS prompts the user to enter their login credentials.

Note The **Agent VPN Detection Delay** applies to all VPN SSO users until the delay expires.

When this value is 0, the CAS requests the Agent to perform VPN SSO immediately. Set this value to 0 if the first RADIUS accounting packet received by the CAS has enough information to perform VPN SSO when the VPN is connected.

When this value is any number other than 0, the CAS informs the Agent in the SWISS packet to wait for the specified delay before attempting VPN SSO login. Set this field to a non-zero value if:

- The Agent is prompting for user authentication because the first RADIUS accounting packet is delayed.
- The VPN concentrator requires a second accounting packet to update the VPN IP address sent in the first accounting packet. In this case, the CAS will not see this VPN connection as valid after the first accounting packet, and the Agent will prompt for user login if the **Agent VPN Detection Delay** is set to 0.

Step 4 Click the checkbox for **Auto-Logout** to automatically terminate the VPN session for users when they log out.

Step 5 Leave the default port (1813) or configure a new one for **RADIUS Accounting Port**.

Note A CAS deployed as a Real-IP gateway supporting VPN SSO opens the Accounting port only on the trusted (eth0) interface.

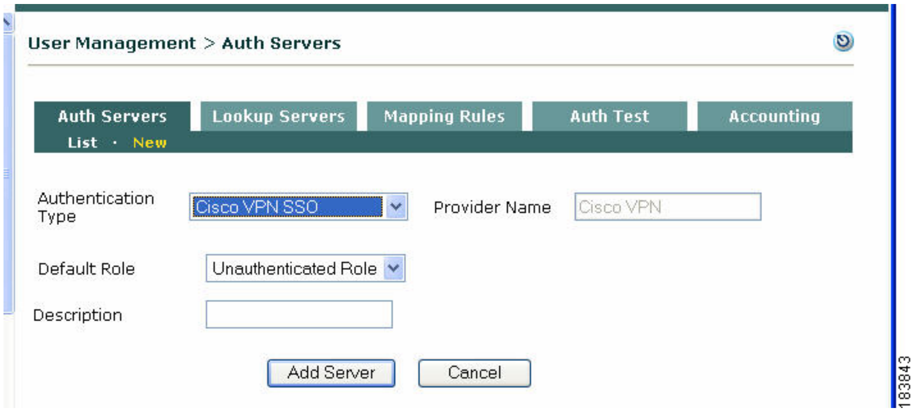
Step 6 Click **Update**.

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 6-9 Add New Auth Server (in CAM)



Authentication Type: Cisco VPN SSO

Provider Name: Cisco VPN

Default Role: Unauthenticated Role

Description:

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 Rol**e dropdown, choose the user role you want VPN client users to be assigned to for the posture assessment 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 Configuration Guide, Release 4.8(1)* for further details.

Configure VPN SSO in a FIPS 140-2 Compliant Deployment

Setting up IPSec communication between your FIPS compliant Cisco NAC Appliance system and Cisco ASA covers three primary phases:

- Import a Trusted CA
- Set up Identity certificate
- Create a Site-to-Site VPN to CAS

Import a Trusted CA

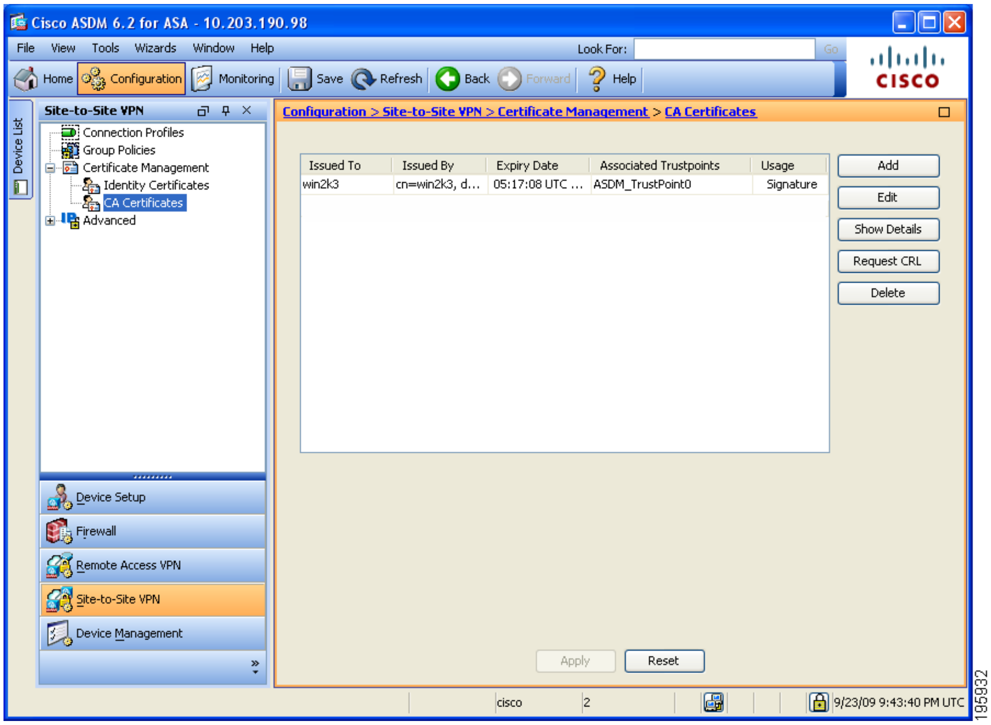
To import your trusted Certificate Authority (CA) into the ASA VPN concentrator:

Step 1 In ASDM, click the **Configuration** toolbar button.

Step 2 Select the **Site-to-Site VPN** tab.

Step 3 Go to **Panel Certificate Management > CA Certificates** (Figure 6-10).

Figure 6-10 Import CA Certificate



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage
win2k3	cn=win2k3, d...	05:17:08 UTC ...	ASDM_TrustPoint0	Signature

Step 4 Click **Add** and enter a trustpoint name for your CA.

Step 5 Click **Browse** and select your CA certificate file.

Step 6 Click **Install Certificate**.

Set up Identity certificate

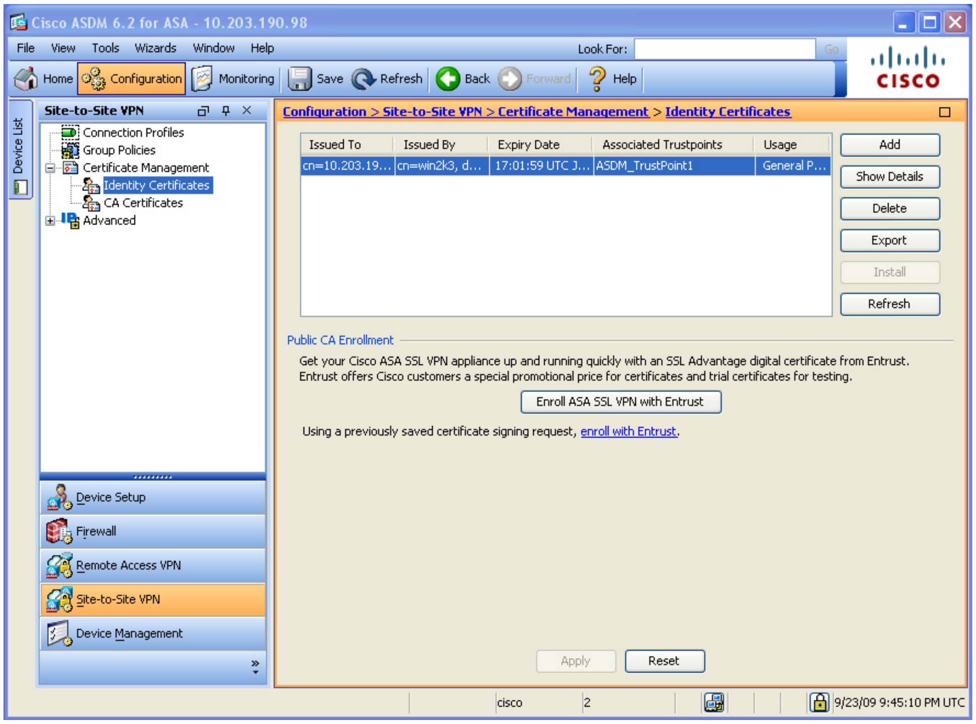
To set up an Identity Certificate on the ASA VPN concentrator:

Step 1 Go to **Certificate Management > Identity Certificates**.

Step 2 Specify a trustpoint name.

Step 3 Choose the **Import the identity certificate from a file** option (Figure 6-11).

Figure 6-11 Import Identity Certificate



Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage
cn=10.203.19...	cn=win2k3, d...	17:01:59 UTC J...	ASDM_TrustPoint1	General P...

Get your Cisco ASA SSL VPN appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

Using a previously saved certificate signing request, enroll with Entrust.

Step 4 Enter the **Decryption Passphrase** for your certificate (which is the password you specified when you exported the trusted CA certificate).

Step 5 Click **Browse** and select the identity certificate.

This certificate/key pair should be in pkcs12 format. If not, you can use the following OpenSSL command to convert separate key/certificate files into one single pkcs12 format:

```
openssl pkcs12 -export -in cert.pem -inkey key.pem -out ASACert.p12
```

Step 6 Specify the Identity Certificate password (which is the same as the **Decryption Passphrase** for your certificate).

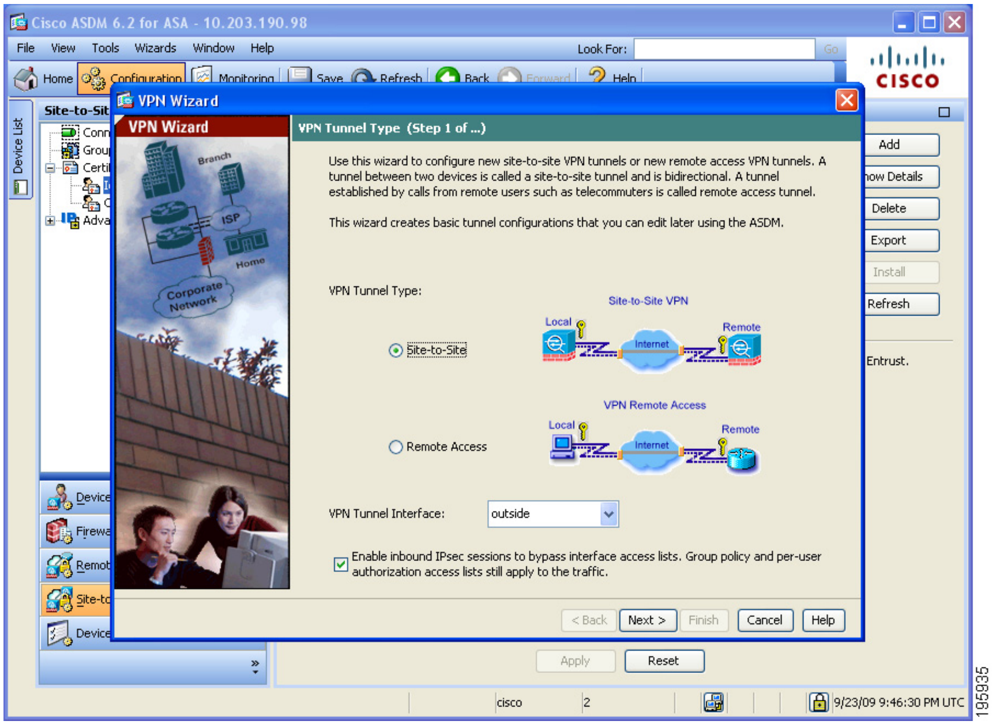
Step 7 Click **Add Certificate**.

Create a Site-to-Site VPN to CAS

Note Use ASDM version 6.2(1) (asdm-621.bin) for the following procedure.

Step 1 Select **Wizards > IPsec VPN Wizard** (Figure 6-12).

Figure 6-12 VPN Wizard



Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

● Site-to-Site

○ Remote Access

VPN Tunnel Interface: outside

☑ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Step 2 Specify the following tunnel attributes:

- VPN Tunnel Type: **Site-to-Site**
- VPN Tunnel Interface: **inside**

Step 3 Check the "**Enable inbound IPsec sessions**…" option and click **Next**.

Step 4 Specify the following attributes:

- Peer IP Address: <*CAS trusted IP address*>
- Authentication method: **Certificate**
- Certificate Name: <*trustpoint name you entered when importing identity certificate*>
- Tunnel Group Name: <*CAS IP address*> (default setting)

Step 5 Click **Next**.

Step 6 Specify the following IKE Policy attributes:

- Encryption: **AES-128**
- Authentication: **SHA**
- Diffie-Hellman Group: **2**

Step 7 Click **Next**.

Step 8 Specify the following IPsec Rule attributes:

- Encryption: **AES-128**
- Authentication: **SHA**
- Check the **Enable Perfect Forward Secrecy** option
- Diffie-Hellman Group: **2**

Step 9 Click **Next**.

Step 10 Specify the following Hosts and Networks attributes:

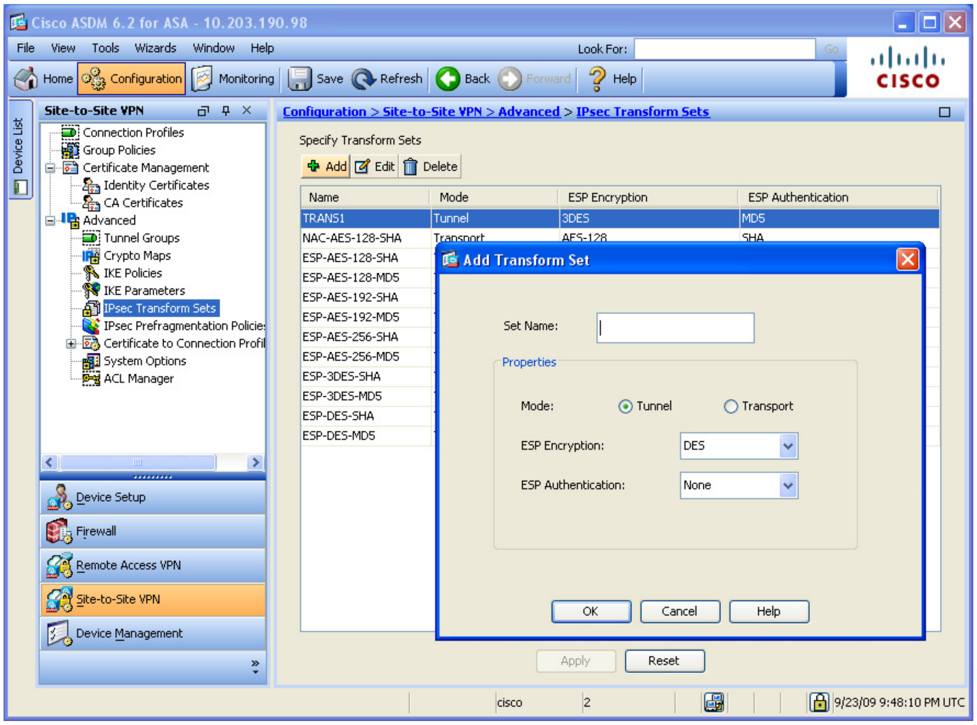
- Action: **Protect**
- Local Networks: <*inside IP address of ASA*>
- Remote Networks: <*CAS IP address*>

Step 11 Check the **Exempt ASA side host/network** option and click **Next**.

Step 12 Verify the configuration summary and click **Finish**.

Step 13 Go to **Configuration > Site-to-Site VPN > Advanced > IPSec Transform Sets** (Figure 6-13).

Figure 6-13 Add IPSec Transform Set



Configuration > Site-to-Site VPN > Advanced > IPsec Transform Sets

Specify Transform Sets

Add Edit Delete

Name	Mode	ESP Encryption	ESP Authentication
TRANS1	Tunnel	3DES	MD5
NAC-AES-128-SHA	Transport	AES-128	SHA
ESP-AES-128-SHA			
ESP-AES-128-MD5			
ESP-AES-192-SHA			
ESP-AES-192-MD5			
ESP-AES-256-SHA			
ESP-AES-256-MD5			
ESP-3DES-SHA			
ESP-3DES-MD5			
ESP-DES-SHA			
ESP-DES-MD5			

Add Transform Set

Set Name:

Properties

Mode: ● Tunnel ○ Transport

ESP Encryption: DES

ESP Authentication: None

OK Cancel Help

Step 14 Click **Add**.

Step 15 Specify the following attributes:

- Set Name: **NAC-AES-128-SHA**
- Mode: **Transport**
- ESP Encryption: **AES-128**

- ESP Authentication: **SHA**

Step 16 Click **OK**.

Step 17 Go to **Configuration > Site-to-Site VPN > Connection Profiles**.

Step 18 Select the IPSec connection you created and click **Edit**.

Step 19 Under Encryption Algorithms, click **Manage** (next to IKE Proposal).

Step 20 In the Configure IKE Proposals dialog box, click **Edit**.

Step 21 Select the **aes-128/sha/2/rsa-sig** proposal and edit it so that the **Lifetime** attribute is set to **8 hours**.

Step 22 Click **OK**.

Step 23 Specify the IPSec Proposal to be **NAC-AES-128-SHA** and click **OK**.

Step 24 Click **Apply**.

Step 25 Select **Tools > Command Line Interface** and enter `ping <CA Sip address>`.

Be sure to verify the ping output.

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 Configuration Guide, Release 4.8(1)*.

Cisco NAC Appliance Agent with VPN Concentrator and SSO

The Agent supports multi-hop L3 deployment and VPN/L3 access from the Agent. The Agent:

1. Checks the client network for the Clean Access Server (L2 deployments), and if not found,
2. Attempts 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 Agent download web page (i.e. via web login)
- By client upgrade to the latest Cisco NAC Agent or auto-upgrade to Agent version 4.6.2.113 or later. For the Agent auto-upgrade process to work, clients must have an earlier version of the 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 4-15 for details.

Note For VPN SSO deployments, if the Agent is not downloaded from the CAS, but is instead downloaded by other means, the Agent is not able to determine the runtime IP information of the CAM and does not automatically pop up, nor does it scan the client machine. For Cisco NAC Agent users, you can work around this issue by specifying a DiscoveryHost setting in the Agent configuration XML file.

Note

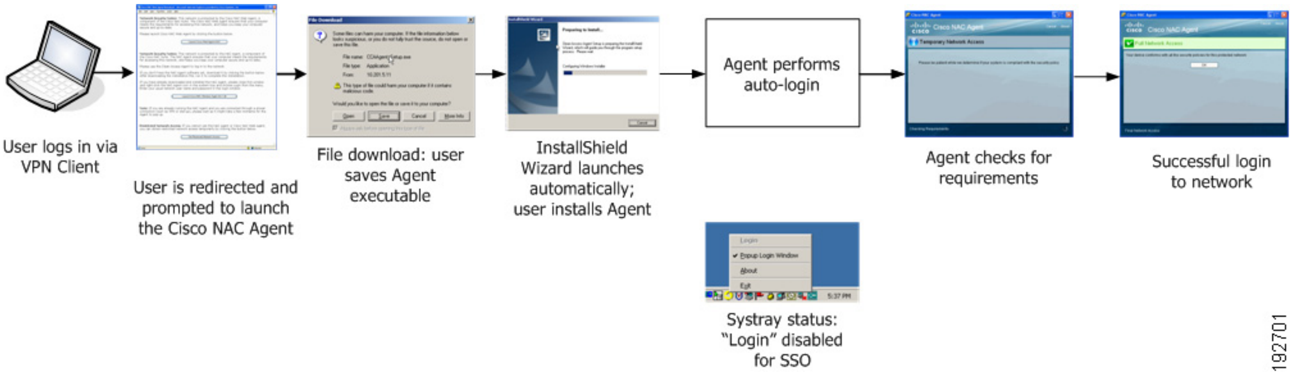
- Uninstalling the Agent while still on the VPN connection does not terminate the VPN connection, although the (if configured) the client machine is removed from the Certified Devices List and the user is removed from the Online Users List.
- If a 3.5.0 or earlier version of the Clean Access Agent is already installed, or if the Agent is installed through non-CAS means, 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.

Cisco NAC Appliance Agent Layer 3 VPN Concentrator User Experience

1. Launch the VPN connection application configured to work with Cisco NAC Appliance.
2. Once logged in, open a browser and attempt to go to an intranet or extranet site.

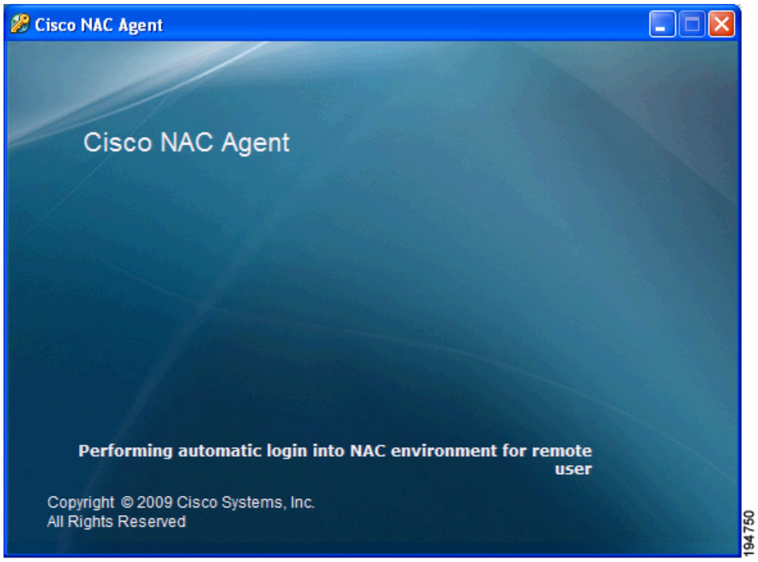
Cisco NAC Appliance enables administrators to deploy the CAS in-band behind a VPN concentrator, or router, or multiple routers. Cisco NAC Appliance supports multi-hop Layer 3 in-band deployment by allowing the CAM and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. With Layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before. Figure 6-14 illustrates the login and posture assessment process for a VPN user using the Agent with Single Sign-On. Note that the initial download of the Agent must be performed via the VPN connection.

Figure 6-14 Agent with SSO for VPN Users


User logs in via VPN Client
User is redirected and prompted to launch the Cisco NAC Agent
File download: user saves Agent executable
InstallShield Wizard launches automatically; user installs Agent
Agent performs auto-login
Agent checks for requirements
Successful login to network
Systray status: "Login" disabled for SSO
192701

With Single Sign-On, the Agent performs automatic login and scanning as shown Figure 6-15.

Figure 6-15 Agent Auto-Login Screen (User View)



Performing automatic login into NAC environment for remote user

Copyright © 2009 Cisco Systems, Inc.
All Rights Reserved

Note Web login always works in Layer 2 or Layer 3 mode, and Layer 3 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:

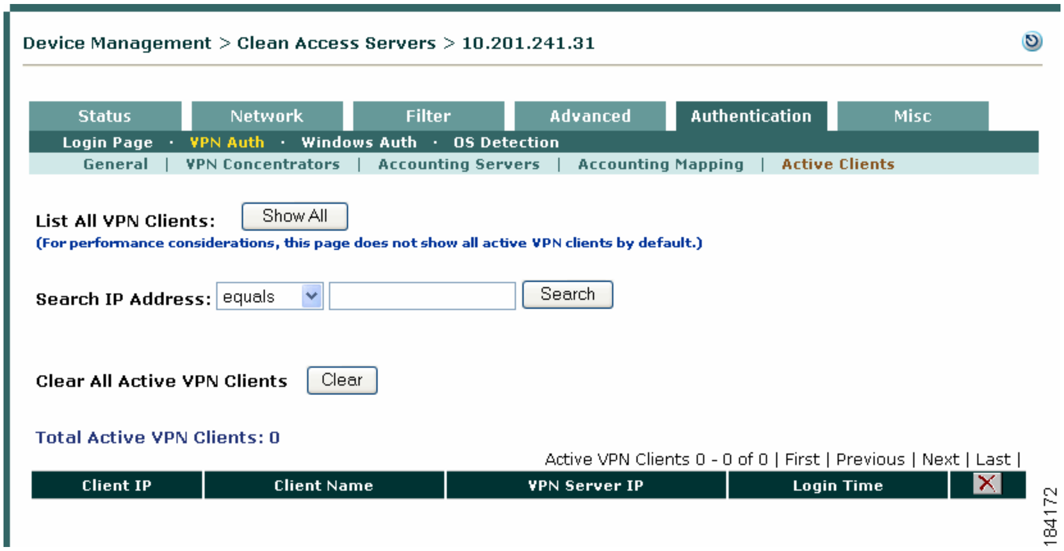
- Account-Status-type = 1 (indicating it is a START packet)
- Calling-station-Id (showing end machine's IP address)

When the user tries to browse, or runs the Agent, the CAM/CAS compares the Active VPN Client information to its mapping rules to determine what role to put the user in.

To view active VPN clients:

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

Figure 6-16 Active Clients (VPN Concentrator)


Device Management > Clean Access Servers > 10.201.241.31
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
General | VPN Concentrators | Accounting Servers | Accounting Mapping | Active Clients
Show All
equals
Search
Clear
Active VPN Clients 0 - 0 of 0 | First | Previous | Next | Last |
184172

List All VPN Clients:

(For performance considerations, this page does not show all active VPN clients by default.)

Search IP Address: equals

Clear All Active VPN Clients

Total Active VPN Clients: 0

Client IP	Client Name	VPN Server IP	Login Time	☒

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.

   – **Login Time**—The date/time that the active VPN client session was established.

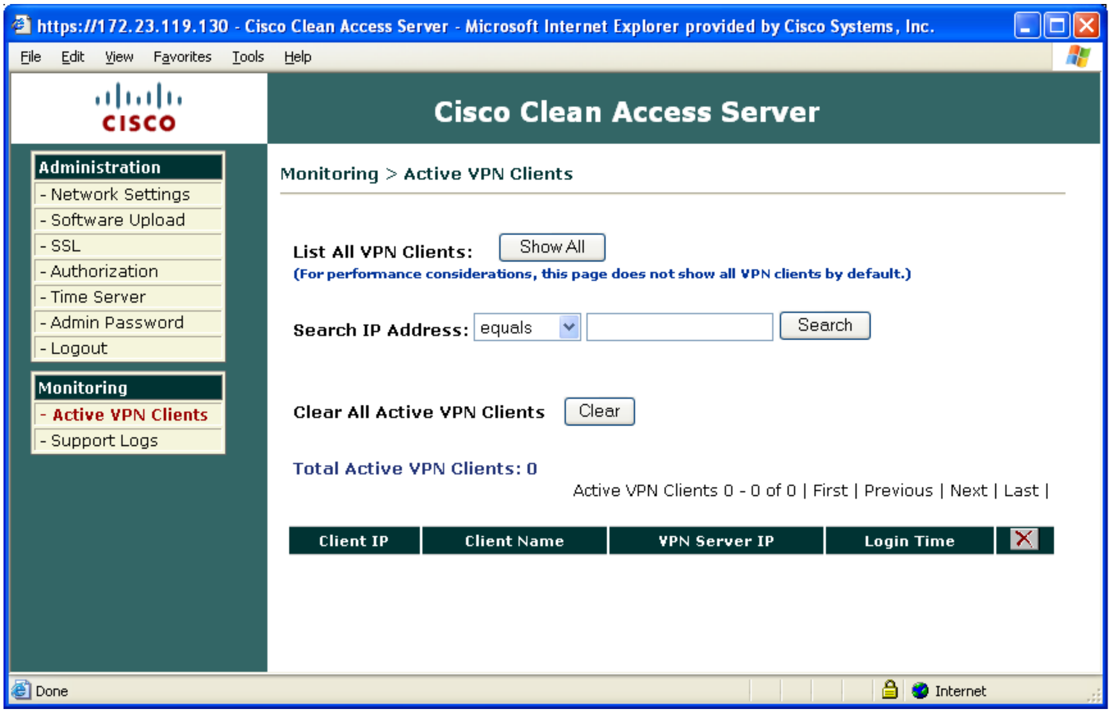
Note Clicking **Show All** or performing a new search refreshes the page with the latest SSO table information.

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_eth0_IP_address>/admin**), from the **Monitoring > Active VPN Clients** page (Figure 6-17).

Figure 6-17 CAS Direct Access Console—Monitoring Active VPN Clients


https://172.23.119.130 - Cisco Clean Access Server - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Clean Access Server
Administration
- Network Settings
- Software Upload
- SSL
- Authorization
- Time Server
- Admin Password
- Logout
Monitoring
- Active VPN Clients
- Support Logs
Monitoring > Active VPN Clients
Show All
equals
Search
Clear
Done
Internet
189271

List All VPN Clients:
(For performance considerations, this page does not show all VPN clients by default.)

Search IP Address: equals

Clear All Active VPN Clients

Total Active VPN Clients: 0

Active VPN Clients 0 - 0 of 0 | First | Previous | Next | Last |

Client IP	Client Name	VPN Server IP	Login Time	☒

CHAPTER 7

Local Traffic Control Policies

This chapter describes how to set up traffic filtering rules in the Clean Access Server. Topics include:

- Overview, page 7-1
- Local vs. Global Traffic Policies, page 7-2
- View Local Traffic Control Policies, page 7-3
- Add Local IP-Based Traffic Control Policies, page 7-4
- Add Local Host-Based Traffic Control Policies, page 7-6
- Controlling Bandwidth Usage, page 7-14

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 Agent Temporary and Quarantine roles.

Cisco NAC Appliance offers three types of traffic policies:

IP-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—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 primarily for 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.

Layer 2 Ethernet traffic policies—To support data transfer or similar operations originating at the Layer 2 level, Cisco NAC Appliance Layer 2 Ethernet traffic control policies enable you to allow or deny Layer 2 Ethernet traffic through the CAS based on the type of traffic. Network Frames except for IP, ARP, and RARP frames constitute standard Layer 2 traffic.

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

Traffic control policies are directional. IP-based and Layer 2 Ethernet traffic 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.

By default, when you create a new user role:

- 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.*).

Example 4 (Layer 2 Ethernet - Virtual Gateway mode only):

1. Allow SNA IBM Systems Network Architecture
2. Block ALL All Traffic

Result: Allow only IBM Systems Network Architecture (SNA) Layer 2 traffic and deny all other Layer 2 traffic.

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.

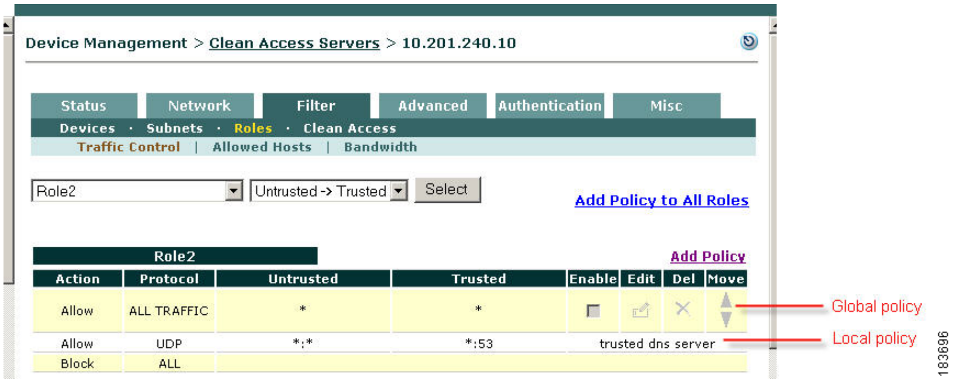
Global policies can only be accessed and modified from the **User Management > User Roles > Traffic Control** global forms. For details, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

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 7-1.

Figure 7-1 Local Traffic Control Policies



Device Management > Clean Access Servers > 10.201.240.10

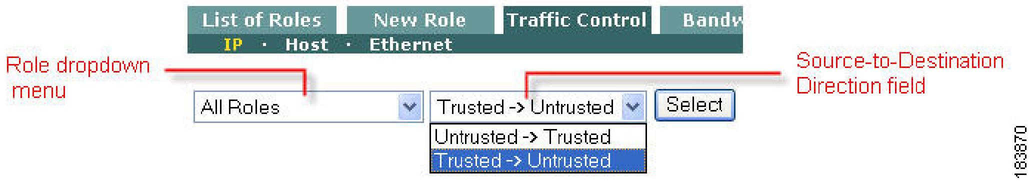
Role2 | Untrusted -> Trusted | Select

Role2

Action	Protocol	Untrusted	Trusted	Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*				
Allow	UDP	*:*	*:53	trusted dns server			
Block	ALL						

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 7-2 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.

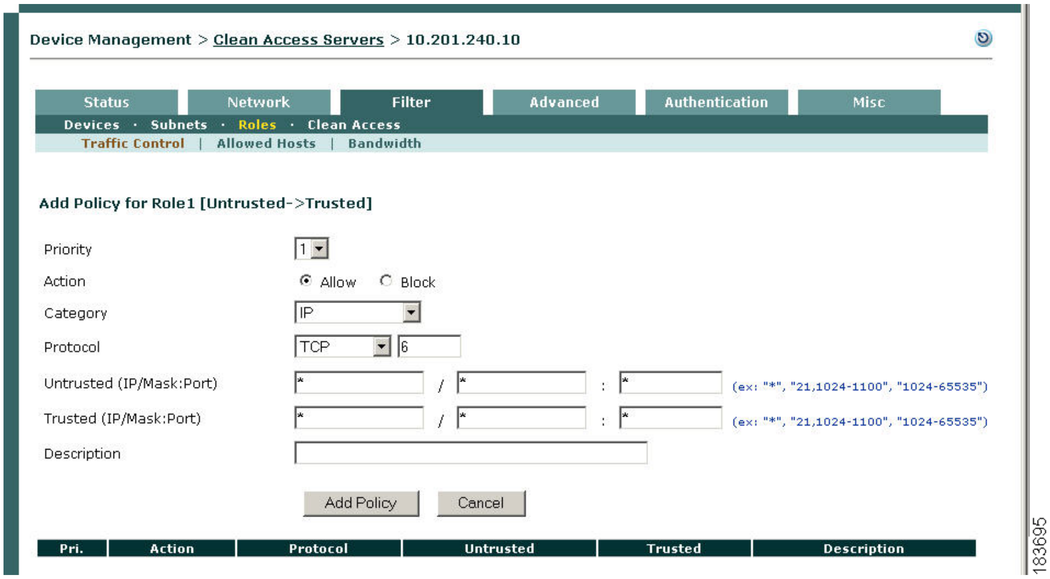
Add / Edit Local IP-Based Traffic Policy

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 7-3 shows the Add Policy form.

Figure 7-3 Add New Local IP Policy


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Traffic Control | Allowed Hosts | Bandwidth
Add Policy
Cancel
183695

Add Policy for Role1 [Untrusted->Trusted]

Priority	1					
Action	● Allow ○ Block					
Category	IP					
Protocol	TCP	6				
Untrusted (IP/Mask:Port)	*	/	*	:	*	(ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	*	/	*	:	*	(ex: "*", "21,1024-1100", "1024-65535")
Description						

Pri.	Action	Protocol	Untrusted	Trusted	Description

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 Cisco NAC Appliance **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 the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* 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 by redirecting user session packets to a local Proxy Server or to the URL of a preconfigured Proxy PAC (Proxy Auto Configuration) file reachable from the CAS.

When the **Parse Proxy Traffic** 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** option for this feature to take effect.

Note When administrators apply Host Policies to the Unauthenticated Role, the CAS acts as a proxy for the client machine. If the CAS itself requires a proxy to access the network, you must modify the **/perfigo/access/apache/conf/httpd.conf** file configuration to feature a **`ProxyRemote * http://`***`<proxy>`***`:`***`<port>`* statement associated with an appropriate **`ProxyAllow`** statement.

The following example illustrates a part of sample **httpd.conf** file that shows the **`ProxyRemote`** statement associated with an appropriate **`ProxyAllow`** statement:

```
<VirtualHost _default_:880>
    # TRACE OFF
    TraceEnable off
    RewriteEngine On
    RewriteRule ^perfigo$ "/perfigo/access/apache/www/fcgi-bin/proxy.fcgi"
    ProxyAllow "/proc/click/dnshandler/proxyallow"
    ProxyRemote http://proxyID.mycompany.com:<port-number>/
    ProxyRequests On
</VirtualHost>
```

Note Refer to http://httpd.apache.org/docs for more apache syntax/usage references.

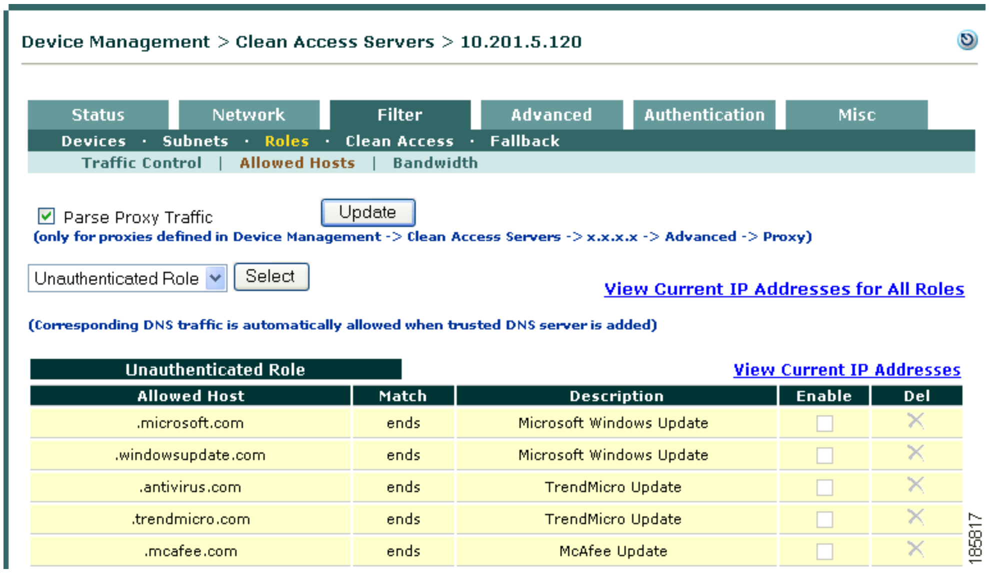
To enable host policies when traffic is going through proxy server specified on the CAS:

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

Step 2 Specify the proxy source as described in Configure Proxy Server Settings on the CAS, page 4-47.

Step 3 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Allowed Hosts** (see Figure 7-4).

Figure 7-4 CAS—Allowed Hosts


Device Management > Clean Access Servers > 10.201.5.120
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access · Fallback
Traffic Control | Allowed Hosts | Bandwidth
Update
Select
View Current IP Addresses for All Roles
View Current IP Addresses
185817

☑ Parse Proxy Traffic

(only for proxies defined in Device Management -> Clean Access Servers -> x.x.x.x -> Advanced -> Proxy)

Unauthenticated Role

(Corresponding DNS traffic is automatically allowed when trusted DNS server is added)

Unauthenticated Role

Allowed Host	Match	Description	Enable	Del
.microsoft.com	ends	Microsoft Windows Update	□	✕
.windowsupdate.com	ends	Microsoft Windows Update	□	✕
.antivirus.com	ends	TrendMicro Update	□	✕
.trendmicro.com	ends	TrendMicro Update	□	✕
.mcafee.com	ends	McAfee Update	□	✕

Step 4 Enable the **Parse Proxy Traffic** option. This setting applies to all roles (Unauthenticated, Temporary, Quarantine, and normal user login roles).

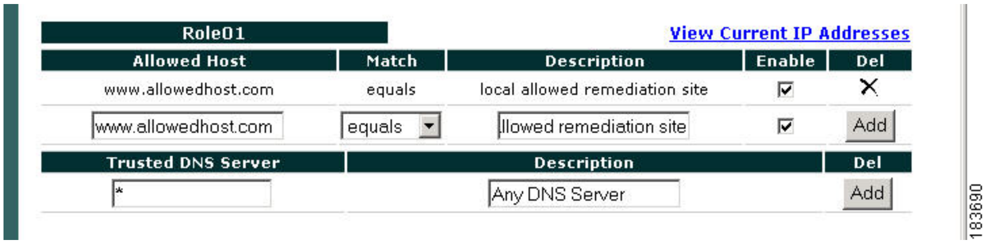
When the **Parse Proxy Traffic** option is enabled for an individual CAS, the CAS checks the payloads of GET, POST and CONNECT HTTP/HTTPS/FTP requests to make sure that the host is on the host policy list before allowing traffic to the proxy server specified on the **Proxy** page. This allows users to access only the host sites enabled for the associated role when the specified proxy server is used. Note that you must specify the Proxy server IP and port (as described above) before enabling the **Parse Proxy Traffic** option on *each* CAS in your deployment.

Note When using proxy settings, also make sure DNS settings are properly configured on the CAS under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS**. See Configure DNS Servers on the Network, page 4-24 for details.

Step 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.



Role01

Allowed Host	Match	Description	Enable	Del
www.allowedhost.com	equals	local allowed remediation site	☑	✕
www.allowedhost.com	equals	llowed remediation site	☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	Add

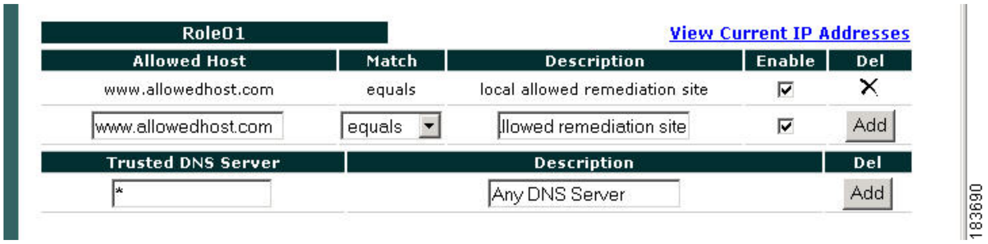
2. Type the hostname in the **Allowed Host** field (e.g. "allowedhost.com").
3. In the **Match** dropdown menu, select an operator to match the host name: equals, ends, begins, or contains.
4. Type a description for the host in the **Description** field, such as "Allowed Host Update".
5. Click **Enable**.
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

To add a local trusted DNS server:

1. Enter an IP address in the **Trusted DNS Server** field, or enter an asterisk "*" to specify any DNS server.



Role01

View Current IP Addresses

Allowed Host	Match	Description	Enable	Del
www.allowedhost.com	equals	local allowed remediation site	☑	✕
www.allowedhost.com	equals ▾	llowed remediation site	☑	Add

Trusted DNS Server	Description	Del
*	Any DNS Server	Add

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.

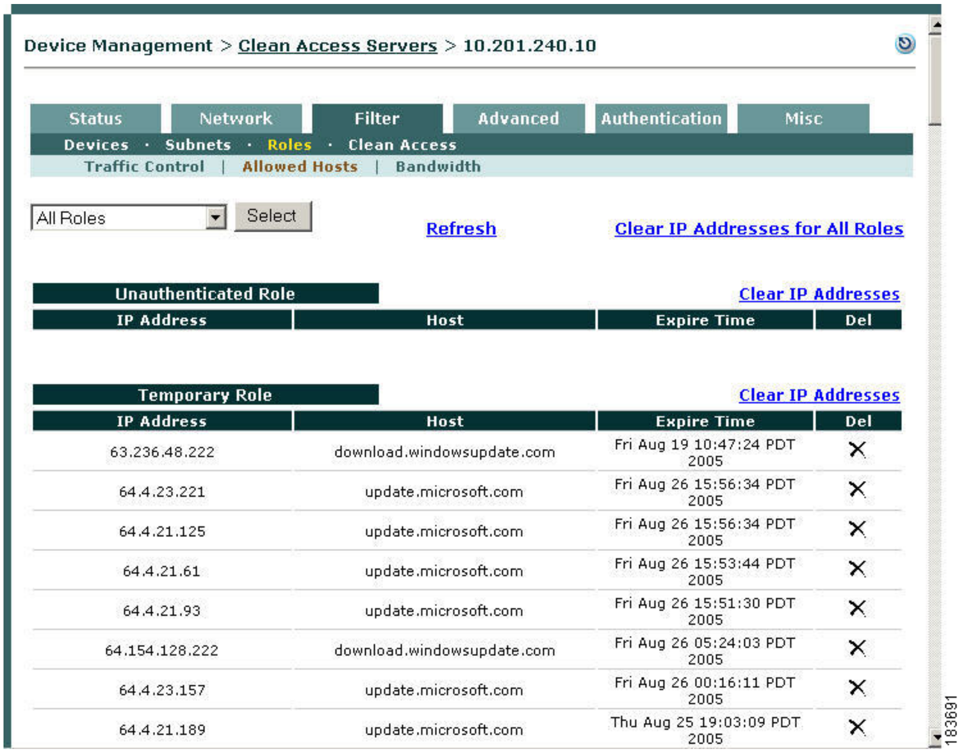
Note When you add a specific DNS server, then use this form later to add any ("*") DNS server, the previously added server becomes a subset of the overall policy allowing all DNS servers, and will not be displayed. If you later delete the any ("*") DNS server policy, the specific trusted DNS server you 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 7-5 View Current IP Addresses for All Roles


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Traffic Control | Allowed Hosts | Bandwidth
All Roles
Select
Refresh
Clear IP Addresses for All Roles
Clear IP Addresses
Clear IP Addresses
183691

Unauthenticated Role

IP Address	Host	Expire Time	Del

Temporary Role

IP Address	Host	Expire Time	Del
63.236.48.222	download.windowsupdate.com	Fri Aug 19 10:47:24 PDT 2005	✕
64.4.23.221	update.microsoft.com	Fri Aug 26 15:56:34 PDT 2005	✕
64.4.21.125	update.microsoft.com	Fri Aug 26 15:56:34 PDT 2005	✕
64.4.21.61	update.microsoft.com	Fri Aug 26 15:53:44 PDT 2005	✕
64.4.21.93	update.microsoft.com	Fri Aug 26 15:51:30 PDT 2005	✕
64.154.128.222	download.windowsupdate.com	Fri Aug 26 05:24:03 PDT 2005	✕
64.4.23.157	update.microsoft.com	Fri Aug 26 00:16:11 PDT 2005	✕
64.4.21.189	update.microsoft.com	Thu Aug 25 19:03:09 PDT 2005	✕

Note You can view this list 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 Configuration Guide, Release 4.8(1)* 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. 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.

Add Layer 2 Ethernet Traffic Control Policies

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

Layer 2 Ethernet traffic control policies enable administrators to allow or block Layer 2 Ethernet traffic based on the type of Layer 2 traffic passing through the CAS.

Default traffic control policies for the Unauthenticated, Temporary, and Quarantine roles are automatically retrieved and updated after an Agent **Update** or **Clean Update** is performed from the CAM.

Note

- After a software upgrade, new default Layer 2 Ethernet traffic control policies are disabled by default but enable/disable settings for existing Ethernet traffic control policies are preserved.
- After a Clean Update, all existing Layer 2 Ethernet traffic control policies are removed and new default Ethernet traffic control policies are added with default disabled settings.

See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details on the automatic **Updates** downloaded to the CAM under **Device Management > Clean Access > Updates**.

Enable Layer 2 Ethernet Traffic Control

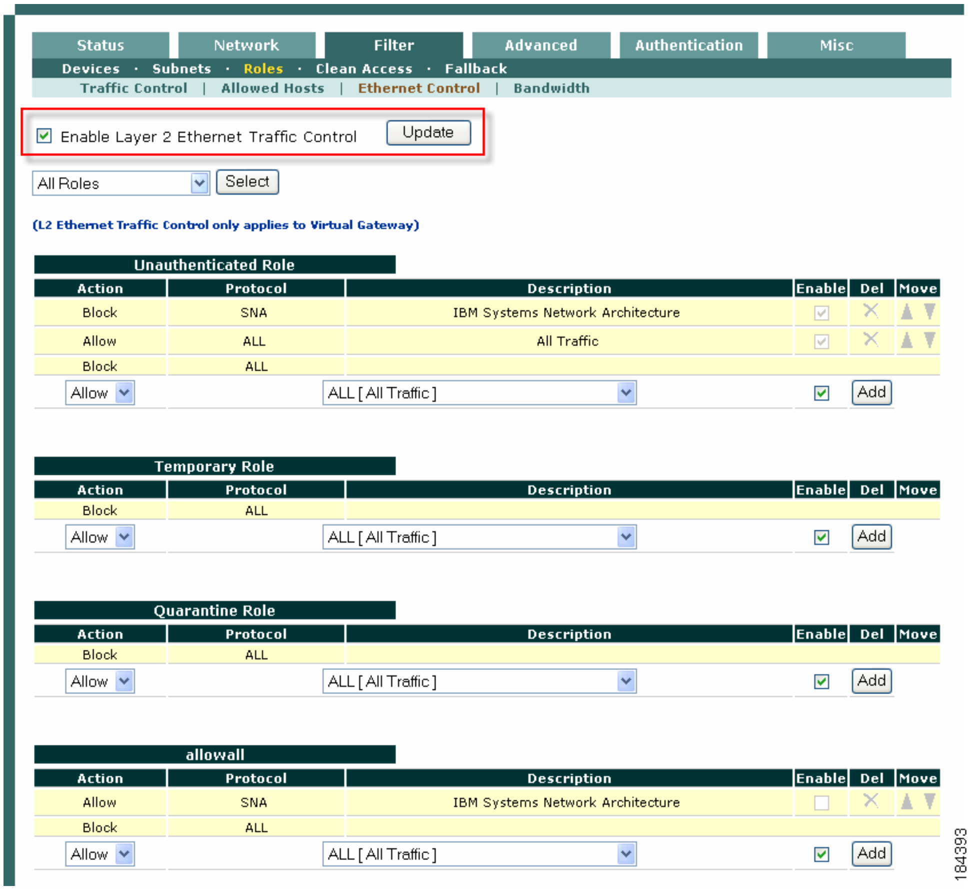
You can configure an individual CAS to allow or block specified Layer 2 Ethernet traffic based on control policies.

When the **Enable Layer 2 Ethernet Traffic Control** option is checked for an individual CAS, the CAS will apply relevant Layer 2 Ethernet traffic control policies to the traffic passing through the CAS, allowing or blocking packets based on the type of Layer 2 traffic passing through the CAS.

To enable Layer 2 Ethernet traffic control on the CAS:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control** (see Figure 7-6).

Figure 7-6 CAS—Ethernet Control


Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access · Fallback
Traffic Control | Allowed Hosts | Ethernet Control | Bandwidth
184393

☑ Enable Layer 2 Ethernet Traffic Control Update

All Roles ▾ Select

(L2 Ethernet Traffic Control only applies to Virtual Gateway)

Unauthenticated Role

Action	Protocol	Description	Enable	Del	Move
Block	SNA	IBM Systems Network Architecture	☑	✕	▲ ▼
Allow	ALL	All Traffic	☑	✕	▲ ▼
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

Temporary Role

Action	Protocol	Description	Enable	Del	Move
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

Quarantine Role

Action	Protocol	Description	Enable	Del	Move
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

allowall

Action	Protocol	Description	Enable	Del	Move
Allow	SNA	IBM Systems Network Architecture	□	✕	▲ ▼
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

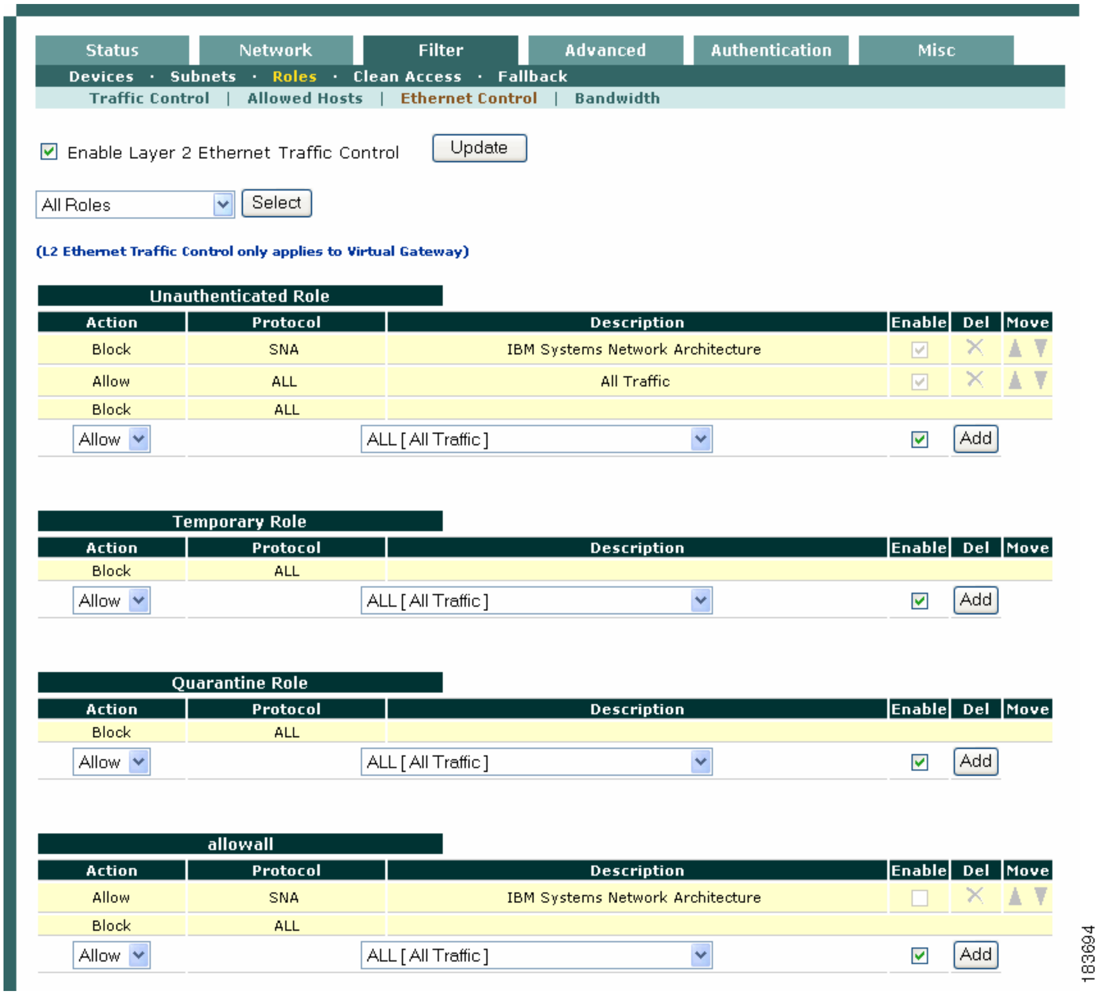
2. Click the checkbox for **Enable Layer 2 Ethernet Traffic Control**.
3. Click the **Update** button.

Add Layer 2 Ethernet Traffic Control

To add a Layer 2 Ethernet traffic control policy:

1. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Roles > Ethernet Control** and select the role for which to allow or block Layer 2 Ethernet traffic.

Figure 7-7 Adding Layer 2 Ethernet Traffic Control


Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access · Fallback
Traffic Control | Allowed Hosts | Ethernet Control | Bandwidth
Update
Select
Add
183694

☑ Enable Layer 2 Ethernet Traffic Control

All Roles ▾

(L2 Ethernet Traffic Control only applies to Virtual Gateway)

Unauthenticated Role

Action	Protocol	Description	Enable	Del	Move
Block	SNA	IBM Systems Network Architecture	☑	✕	▲ ▼
Allow	ALL	All Traffic	☑	✕	▲ ▼
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

Temporary Role

Action	Protocol	Description	Enable	Del	Move
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

Quarantine Role

Action	Protocol	Description	Enable	Del	Move
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

allowall

Action	Protocol	Description	Enable	Del	Move
Allow	SNA	IBM Systems Network Architecture	□	✕	▲ ▼
Block	ALL				
Allow ▾		ALL [All Traffic] ▾	☑	Add	

2. Select either **Allow** or **Block** from the **Action dropdown** menu.

3. Specify the type of Layer 2 Ethernet traffic to either allow or block in the **Protocol** dropdown menu.

Note Except for allowing all Layer 2 traffic, only the "IBM Systems Network Architecture (SNA)" protocol is available with Cisco NAC Appliance release 4.1(1) and later. Additional preset options may become available through the Cisco NAC Appliance update service on the Clean Access Manager.

4. Click **Enable**.

5. Click **Add**.

After you "Add" a traffic control policy, the CAM automatically populates the Description column for the entry with the description of the option you specified in the **Protocol** dropdown menu.

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 CASs, 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.

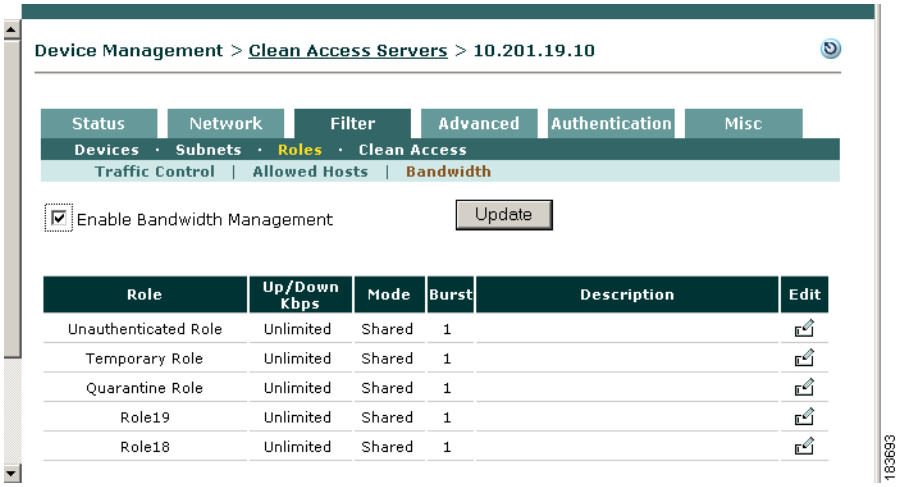
With bursting, you can allow for brief deviations from a bandwidth constraint. This accommodates users who need bandwidth resources intermittently (for example, when downloading and reading pages), while users attempting to stream content or transfer large files are subject to the bandwidth constraint.

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 7-8 Enable Bandwidth Management for the CAS

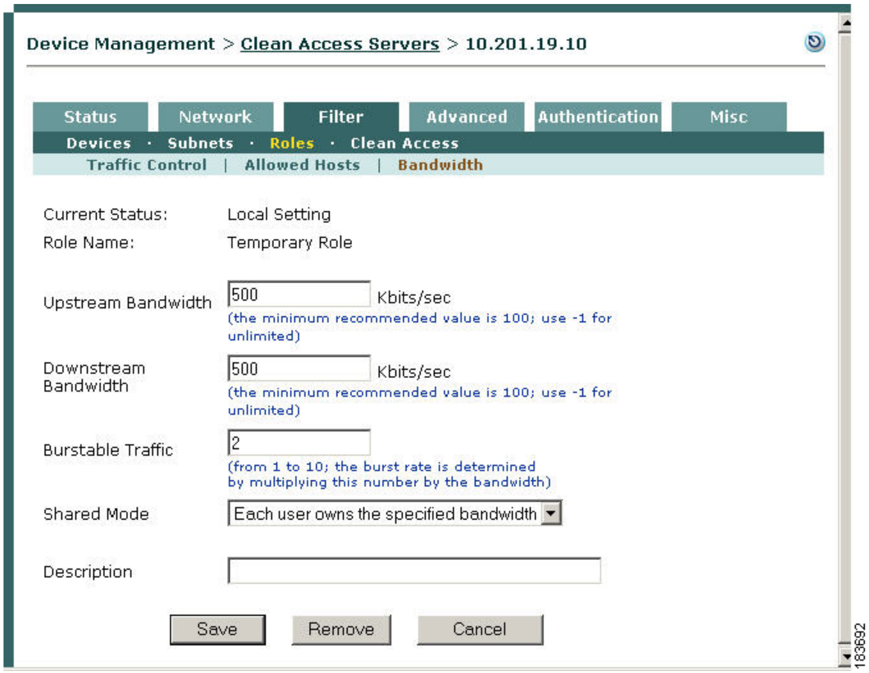

Device Management > Clean Access Servers > 10.201.19.10
Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Traffic Control | Allowed Hosts | Bandwidth
Update
183693

☑ Enable Bandwidth Management

Role	Up/Down Kbps	Mode	Burst	Description	Edit
Unauthenticated Role	Unlimited	Shared	1		✎
Temporary Role	Unlimited	Shared	1		✎
Quarantine Role	Unlimited	Shared	1		✎
Role19	Unlimited	Shared	1		✎
Role18	Unlimited	Shared	1		✎

3. Click the **Edit** button next to the role for which you want to set bandwidth limitations. The **Role Bandwidth** form appears.

Figure 7-9 Local Bandwidth Form for User Role



Device Management > Clean Access Servers > 10.201.19.10

Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Traffic Control | Allowed Hosts | Bandwidth

Current Status: Local Setting

Role Name: Temporary Role

Upstream Bandwidth 500 Kbits/sec
(the minimum recommended value is 100; use -1 for unlimited)

Downstream Bandwidth 500 Kbits/sec
(the minimum recommended value is 100; use -1 for unlimited)

Burstable Traffic 2
(from 1 to 10; the burst rate is determined by multiplying this number by the bandwidth)

Shared Mode Each user owns the specified bandwidth

Description

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 Configuration Guide, Release 4.8(1)* for additional details on bandwidth management.

CHAPTER 8

Configuring Active Directory Single Sign-On (AD SSO)

This chapter describes how to configure Active Directory (AD) Single Sign-On (SSO) for the Cisco NAC Appliance.

Topics include:

- Overview, page 8-1
- AD SSO Configuration Step Summary, page 8-5
- Add Active Directory SSO Auth Server, page 8-6
- Configure Traffic Policies for Unauthenticated Role, page 8-7
- Configure AD SSO on the CAS, page 8-11
- Configuring a CAS User on the AD Server for AD SSO, page 8-14
- Configure AD SSO in a Windows 7 Client Environment, page 8-34
- Configure Active Directory for FIPS 140-2 Compliant AD SSO, page 8-36
- Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos), page 8-40
- Confirm Active AD SSO Service, page 8-41
- Enable GPO Updates, page 8-41
- Enabling a Login Script (Optional), page 8-43
- Add LDAP Lookup Server for Active Directory SSO (Optional), page 8-46
- Troubleshooting, page 8-48

Overview

You can configure Cisco NAC Appliance to automatically authenticate Agent users who are already logged into a Windows domain. AD SSO allows users logging into AD on their Windows systems to automatically go through authentication and posture assessment without ever having to log in via the Agent.

Note Users logging into Cisco NAC Appliance via AD SSO must be running Windows Vista or Windows 7 and have the latest Cisco NAC Agent (version 4.7.1.15 or 4.8.0.32) installed on their client machine in order to remain FIPS 140-2 compliant. Windows XP clients performing AD SSO do not conform to FIPS 140-2 compliance requirements.

Note The Cisco NAC Web Agent does not support AD SSO functions.

Cisco NAC Appliance Agent/AD Server Compatibility for AD SSO

Cisco NAC Appliance supports Windows Single Sign-On (SSO) on Windows 7/Vista/XP client machines and AD on Windows 2000/2003/2008 servers. See *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later* for full compatibility details.

Note You can configure AD SSO for all deployment types (L2/L3, In-Band/Out-of-Band). For OOB, client ports are put on the Auth VLAN first prior to Windows domain authentication.

With AD SSO, Cisco NAC Appliance *authenticates* the user with Kerberos, but *authorizes* the user with LDAP. Cisco NAC Appliance leverages the cached credentials/Kerberos ticket from the client machine login and uses it to validate the user authentication with the backend Windows 2000/2003/2008 server Active Directory. After the user authentication is validated, authorization (role-mapping) is then performed as a separate lookup in Active Directory using LDAP.

You can also use the CAMs **Auth Test** function to test AD SSO authentication in Cisco NAC Appliance, For details, see the "Auth Test" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

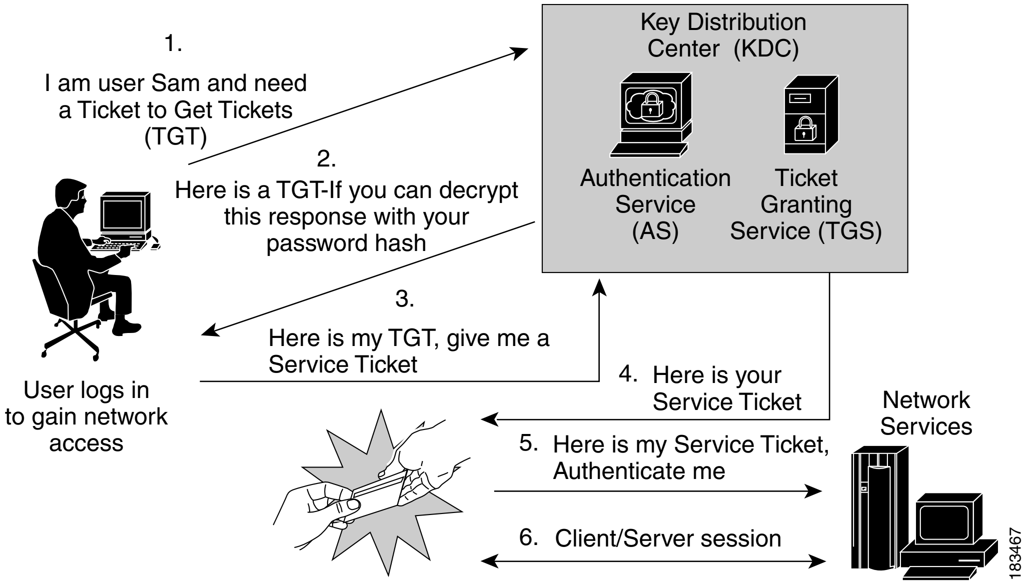
Note The LDAP user account must have privileges sufficient to provide a "Search DN/ Password" that can be used to look up any attribute.

Windows SSO Process (Kerberos Ticket Exchange)

Windows SSO is the ability for Cisco NAC Appliance to automatically authenticate users already authenticated to a backend Kerberos Domain Controller (Active Directory server). Figure 8-1 on page 8-3 shows the general process for Kerberos ticket exchange.

Note AD SSO fails in Cisco NAC Appliance when the CAS and Cisco NAC Agent attempt to exchange Kerberos tickets with the AD domain that are larger than 16kB.

Figure 8-1 General Process for Kerberos Ticket Exchange


Key Distribution Center (KDC)
Authentication Service (AS)
Ticket Granting Service (TGS)
1. I am user Sam and need a Ticket to Get Tickets (TGT)
2. Here is a TGT-If you can decrypt this response with your password hash
3. Here is my TGT, give me a Service Ticket
4. Here is your Service Ticket
5. Here is my Service Ticket, Authenticate me
6. Client/Server session
User logs in to gain network access
Network Services
183467

When the Clean Access Server is configured for AD SSO, it essentially replaces the “Network Services” component shown in Figure 8-1. The general sequence is as follows:

- Windows User and the CAS both have an account on the Active Directory server.
- User logs onto Windows AD (or uses cached credentials).
- Credentials are sent to the AD. The AD authenticates and gives a Ticket Granting Ticket (TGT) to the user.
  - The NAC Agent on the client machine asks the Windows user for a Kerberos Service Ticket (ST) from AD, so that the NAC Agent can communicate with the CAS.
  - The client requests a Service Ticket from the AD.
  - The AD sends the new ST to the client and the client provides this ST to the NAC Agent.
  - The NAC Agent presents this ST to the CAS as part of the authentication process to establish communication with the CAS.
- The CAS sends back packets and mutually authenticates the client as part of the ADSSO process.
- The CAS uses this information to sign the client onto Cisco NAC Appliance and hence SSO authentication takes place.
- For additional user role mapping (for authentication and posture assessment), an LDAP lookup server with attribute mapping can be configured.

Note Starting from Cisco NAC Appliance Release 4.5(1), the default timeout setting that monitors responses from the CAS changed to 60 seconds. which could impact AD SSO behavior if the response takes longer to come back to the Cisco NAC Appliance system. (For example, if the complete AD SSO process takes 2 minutes, once the 60 second timeout has elapsed, the CAM times out assuming that no response is forthcoming from the CAS that is communicating with the AD domain and automatically moves to the next CAS. If you then examine the CAS following the full 2-minute AD SSO process, you see that the service is actually working.) To help ensure reliable AD SSO behavior, Cisco also recommends verifying that your network DNS servers are functioning and accessible along with your Active Directory servers.

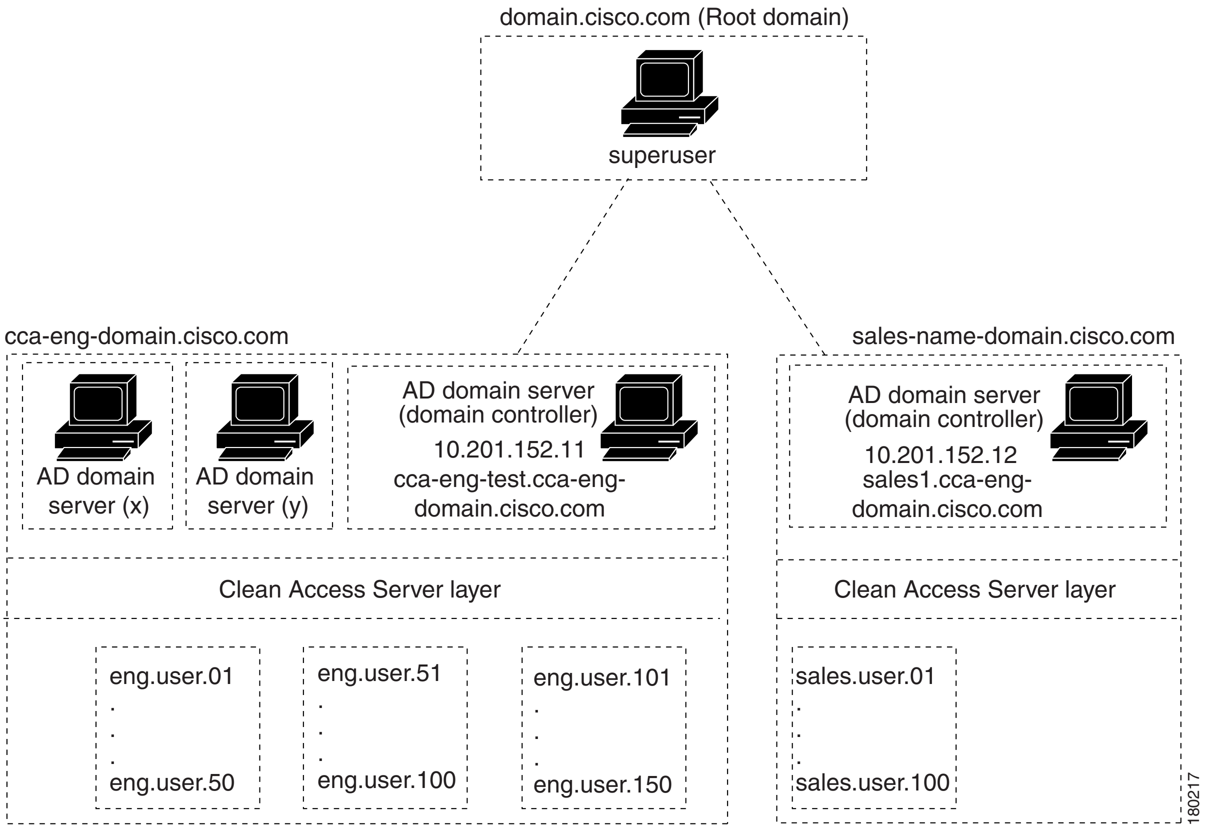
CAS Communication with AD Server

Figure 8-2 illustrates the general setup for Clean Access Server communication with the AD server for Active Directory SSO.

The CAS reads user login traffic only to the AD servers under the root domain. As shown in Figure 8-2, the sales domain (sales-name-domain.cisco.com) and the engineering domain (cca-eng-name.domain.cisco.com) are configured under different Clean Access Servers. Taking the cca-eng domain as an example, the CAS user only needs to be created and configured on the cca-eng-test.cca-eng-domain.cisco.com AD server.

Users under cca-eng-domain.cisco.com can log into any AD server in the domain. In addition, the KTPass command (described in Configuring a CAS User on the AD Server for AD SSO, page 8-14) only needs to be executed on the cca-eng-test.cca-eng-domain.cisco.com server.

Figure 8-2 Configuring the CAS User Account on the AD Server


domain.cisco.com (Root domain)
superuser
cca-eng-domain.cisco.com
AD domain server (x)
AD domain server (y)
AD domain server (domain controller)
10.201.152.11
cca-eng-test.cca-eng-domain.cisco.com
sales-name-domain.cisco.com
AD domain server (domain controller)
10.201.152.12
sales1.cca-eng-domain.cisco.com
Clean Access Server layer
Clean Access Server layer
eng.user.01
.
.
.
eng.user.50
eng.user.51
.
.
.
eng.user.100
eng.user.101
.
.
.
eng.user.150
sales.user.01
.
.
.
sales.user.100
180217

AD SSO Configuration Step Summary

Administrators should start with a good understanding of their network layout with respect to their AD servers prior to configuring Active Directory SSO.

Configuration Prerequisites

To configure Active Directory SSO, you will need to have the following:

- You *must* use Windows Server 2008 Enterprise SP1 (32-bit) with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or WIndows 7 with Cisco NAC Agent version 4.7.1.15 or 4.8.0.32 installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO.
- The number of AD servers (domain controllers) to be configured. Typically, the CAS will correspond to one AD server, but you can also associate the CAS with an entire AD domain.
- The Windows 2000 or Windows 2003 server installation CD for the AD server. This is needed to install support tools for the KTPass command. The KTPass command is required to be run only on the AD server (domain controller) to which the CAS is logging in.
- The appropriate version of **ktpass.exe** installed. (To determine the correct version of KTPass to support your Cisco NAC Appliance/AD SSO deployment, see *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.)
- The IP address of each AD server (to configure Unauthenticated role traffic policies). You will need to allow traffic on the CAS for every AD server that is in charge of that domain. For example, if users can log into multiple AD servers in the domain, you should allow traffic to all the multiple AD servers for the Unauthenticated role.

Note In OOB deployments, ICMP (ping) is used to find the "closest AD server" by the workstation, and *must* work to all AD servers referenced in sites and services for the Authentication VLAN(s), or all AD servers in the domain if sites and services has not been set up.

- If setting up a connection between the CAS and a single AD server, the FQDN of the Active Directory server that the CAS logs into (for CAS configuration).
- DNS server settings correctly configured on the CAS **(under Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS**) to resolve the FQDN for the AD server on the CAS.
- The date and time of the CAM, CAS, and AD server synchronized within 5 minutes of each other. The time on the AD server and the CAS must be synchronized to not more than 300 seconds clock skew (Kerberos is sensitive to time).
- The Active Directory Domain Name in Kerberos format (Windows 2000 and above). This is needed for both CAS configuration and CLI configuration of the AD server.

Note The host principal name in the KTPass command (i.e. "<AD_DomainServer>") must exactly match the case of the "Full computer name" of the AD server (under **Control Panel > System > Computer Name | Full computer name**.) See Run the ktpass.exe Command, page 8-22 for details.

- Client systems must already have the Agent installed. Refer to the "Distributing the Agent" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for additional information on Agent distribution and installation.

Configuration Step Summary

Step 1 Add Active Directory SSO Auth Server, page 8-6.

On the CAM, add a new auth server of type Active Directory SSO and specify a default role for users.

Step 2 Configure Traffic Policies for Unauthenticated Role, page 8-7.

Open ports on the CAS to allow client authentication traffic to pass through the CAS to/from the Active Directory server.

Step 3 Configure AD SSO on the CAS, page 8-11.

From the CAS management pages, configure the Active Directory server settings, CAS user account settings, and auth server settings for the CAS corresponding to the domain of the users.

Step 4 Configuring a CAS User on the AD Server for AD SSO, page 8-14.

Add a CAS account on the Windows 2000/2003/2008 AD server with which the CAS will communicate, and configure encryption parameters to support the Linux operating system of the CAS.

Step 5 Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos), page 8-40.

Step 6 Confirm Active AD SSO Service, page 8-41.

Step 7 Enable GPO Updates, page 8-41.

Step 8 Enabling a Login Script (Optional), page 8-43.

Step 9 Add LDAP Lookup Server for Active Directory SSO (Optional), page 8-46.

Optionally configure LDAP lookup servers to map users to multiple roles after authentication.

Step 10 Refer to Troubleshooting, page 8-48 if necessary.

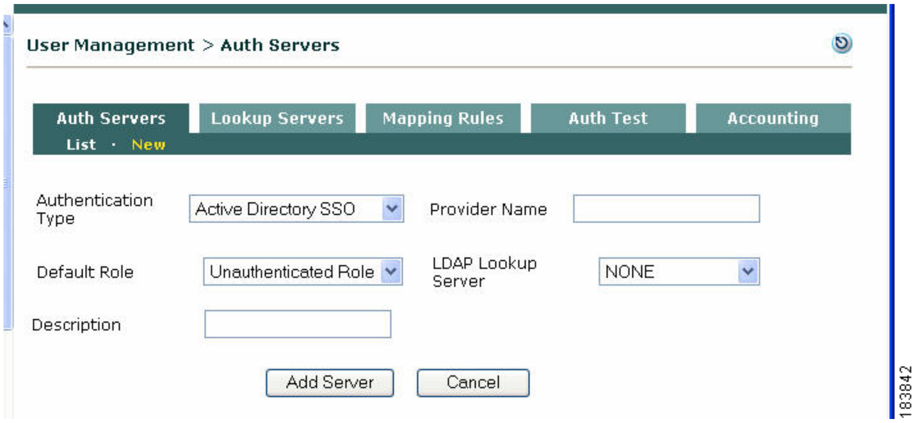
Add Active Directory SSO Auth Server

To create an AD SSO auth server on the CAM, and map the AD server to a default role for users and a secondary LDAP lookup server (if configured), follow these steps:

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

Step 2 From the **Authentication Type** dropdown menu, choose **Active Directory SSO**.

Figure 8-3 Active Directory SSO



User Management > Auth Servers

Authentication Type: Active Directory SSO
Provider Name:
Default Role: Unauthenticated Role
LDAP Lookup Server: NONE
Description:

Step 3 Choose a **Default Role** from the dropdown menu. If no additional lookup is required to map users to roles, all users performing authentication via Active Directory single sign-on will be assigned to the default role. Posture assessment/Nessus Scanning should be configured for this role.

Step 4 Type a **Provider Name** that will identify the AD SSO auth server on the list of authentication providers. Do not use spaces or special characters in the name.

Step 5 You can leave the **LDAP Lookup Server** dropdown menu at the default NONE setting if you plan to assign your users to one default role, and no additional lookup is required. If you plan on mapping Windows domain SSO users to multiple roles, the CAM will need to perform a second-level lookup using the LDAP Lookup server you configure as described in Add LDAP Lookup Server for Active Directory SSO (Optional), page 8-46. In this case, select the LDAP Lookup server you have already configured from the **LDAP Lookup Server** dropdown.

Step 6 Click **Add Server**.

Note For AD SSO users, the **Online Users** and **Certified Devices** pages will display `AD_SSO` in the **Provider** field and both the username and domain of the user (for example, `user1@domain.name.com`.) in the **User/User Name** field.

Note The **Auth Test** feature cannot be used to test SSO Auth providers (e.g. AD SSO or VPN SSO).

Configure Traffic Policies for Unauthenticated Role

A user in the domain logging into his/her Windows machine sends credentials to the root domain controller to perform the first portion of Kerberos ticket exchange (as shown in Figure 8-1). Once the machine receives a Service Ticket, the Agent uses it to validate the client authentication through the CAS. Only when the CAS validates the authentication is the user allowed network access, and there is no need for a separate user login through the Agent.

As Figure 8-2 illustrates, the CAS is configured to read the login credentials of user machines as they authenticate to the Active Directory (AD) server. Ports must be opened on the CAS to allow the authentication traffic to pass through the CAS to/from the AD server. The administrator can open either TCP or UDP ports, depending on what the AD server uses.

Note If AD SSO traffic may include fragmented packets, you might need to enable the **IP FRAGMENT** option according to the guidelines in the Add IP-Based Policy section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Configure traffic policies for the Unauthenticated role to allow these ports on the trusted-side IP address of the AD server. This allows the client to authenticate to the AD server and for GPO and scripts to run. Cisco recommends that you install Cisco Security Agent (CSA) on the AD server/DMZ AD server.

TCP/UDP Ports Supporting AD SSO Implementation

The following list is an initial comprehensive list of ports to open when implementing AD SSO in your Cisco NAC Appliance network. You may be required to open other ports to support AD services not included in this list.

Table 8-1 Recommended Ports to Support AD SSO

Action	Protocol	Untrusted	Trusted	Purpose/Description
Recommended TCP Ports				
Allow	TCP	*:*	IP address DC Port 88	Kerberos
Allow	TCP	*:*	IP address DC Port 135	EpMap
Allow	TCP	*:*	IP address DC Port 139	Netbios-ssn
Allow	TCP	*:*	IP address DC Port 389[1]	LDAP
Allow	TCP	*:*	IP address DC Port 445	MS-DC/SMB
Allow	TCP	*:*	IP address DC Port 636	LDAP with SSL
Allow	TCP	*:*	IP address DC Port 1025	MS-AD
Allow	TCP	*:*	IP address DC Port 1026	MS-AD
Recommended UDP Ports				
Allow	UDP	*:*	IP address DC Port 88	Kerberos
Allow	UDP	*:*	IP address DC Port 123	NTP
Allow	UDP	*:*	IP address DC Port 137	Netbios-ns

Table 8-1 Recommended Ports to Support AD SSO

Action	Protocol	Untrusted	Trusted	Purpose/Description
Recommended TCP Ports				
Allow	TCP	*:*	IP address DC Port 88	Kerberos
Allow	UDP	*:*	IP address DC Port 389	LDAP
Allow	UDP	*:*	IP address DC Port 636	LDAP with SSL
Other Ports				
Allow	ICMP request	*:*	IP address DC	Ping
Allow	IP fragments	*:*	IP address DC	IP packet fragments

[1] When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

Note Typically, the LDAP protocol uses plain text when sending traffic on TCP/UDP port 389. If encryption is required for LDAP communications, use TCP/UDP port 636 (LDAP with SSL encryption) instead.

When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

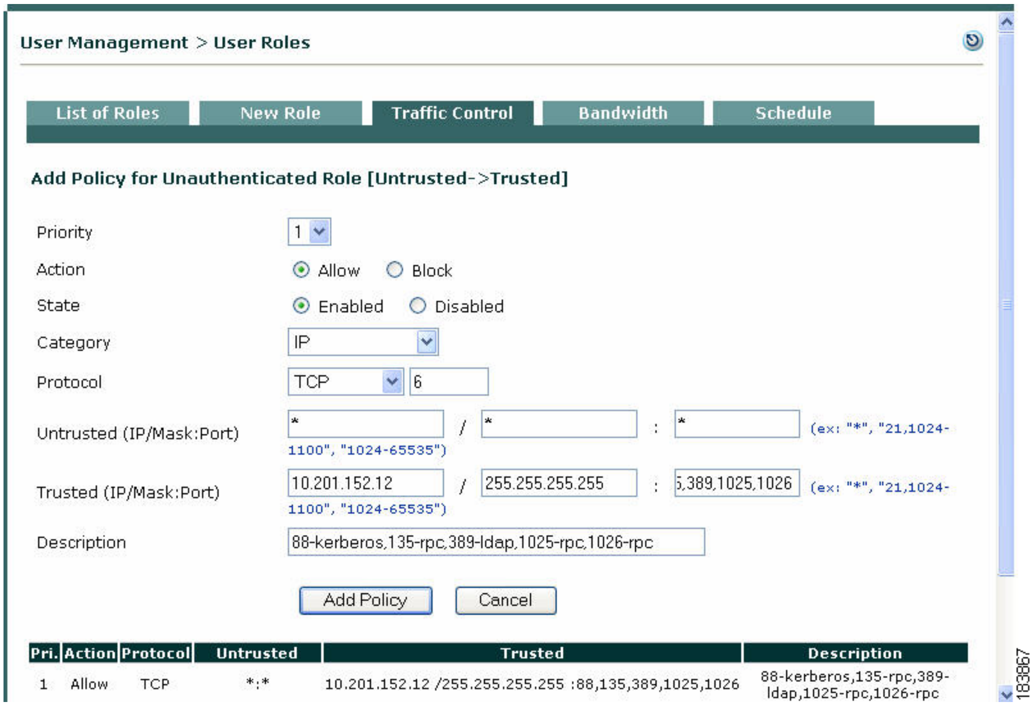
Add Policy for AD Server

To Add Policies for AD Server, follow these steps:

Step 1 Go to **User Management > User Roles > List of Roles > Policies [Unauthenticated Role]**. This brings up the **IP** traffic policy form for the Unauthenticated Role.

Step 2 With the direction dropdown set for Untrusted -> Trusted, click the **Add Policy** link. The Add Policy form appears (Figure 8-4).

Figure 8-4 Configure Traffic Policy for CAS to AD Server



Add Policy for Unauthenticated Role [Untrusted->Trusted]

Priority	1
Action	● Allow ○ Block
State	● Enabled ○ Disabled
Category	IP
Protocol	TCP 6
Untrusted (IP/Mask:Port)	* / * : * (ex: "*", "21,1024-1100", "1024-65535")
Trusted (IP/Mask:Port)	10.201.152.12 / 255.255.255.255 : 5,389,1025,1026 (ex: "*", "21,1024-1100", "1024-65535")
Description	88-kerberos,135-rpc,389-ldap,1025-rpc,1026-rpc

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	TCP	*:*	10.201.152.12 /255.255.255.255 :88,135,389,1025,1026	88-kerberos,135-rpc,389-ldap,1025-rpc,1026-rpc

Step 3 Leave the following fields at their defaults:

- **Action**: Allow
- **State**: Enabled
- **Category**: IP
- **Protocol**: TCP 6
- **Untrusted (IP/Mask:Port)**: * / * / *

Step 4 For **Trusted (IP/Mask:Port)**, enter:

- The IP address of the Active Directory server
- 255.255.255.255 as the subnet mask (for just the AD server)
- Ports (using commas to separate port numbers)

For example: `10.201.152.12 / 255.255.255.255 / 88,135,1025,1026,3268`

Note When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of *all* directory partitions in both single and multi domain environments.

Step 5 Type an optional **Description**.

Step 6 Click **Add Policy**.

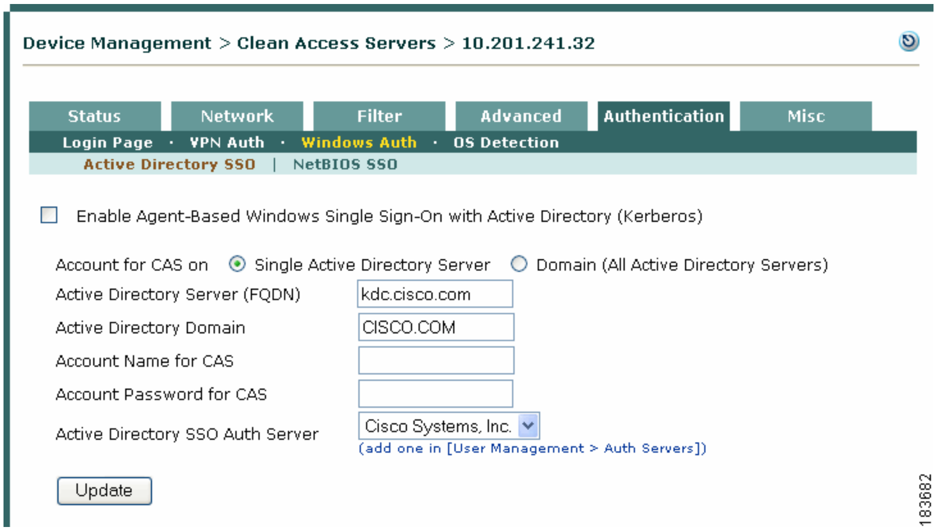
Note When testing, Cisco recommends opening complete access to the AD server/DC first, then restricting ports as outlined above once AD SSO is working. When logging into the client PC, make sure to log into the domain using Windows domain credentials (not Local Account).

Configure AD SSO on the CAS

To configure the CAS corresponding to the domain of the users, follow these steps:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

Figure 8-5 Active Directory SSO



Device Management > Clean Access Servers > 10.201.241.32

Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO

☐ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on ● Single Active Directory Server ○ Domain (All Active Directory Servers)

Active Directory Server (FQDN): kdc.cisco.com

Active Directory Domain: CISCO.COM

Account Name for CAS:

Account Password for CAS:

Active Directory SSO Auth Server: Cisco Systems, Inc.

(add one in [User Management > Auth Servers])

Step 2 Do *not* click the checkbox for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)** yet. The service should only be enabled after you Configuring a CAS User on the AD Server for AD SSO, page 8-14. You can configure the other fields of this page and click **Update**, as described below.

Note Until you perform the configuration on the AD server, the following message will appear:

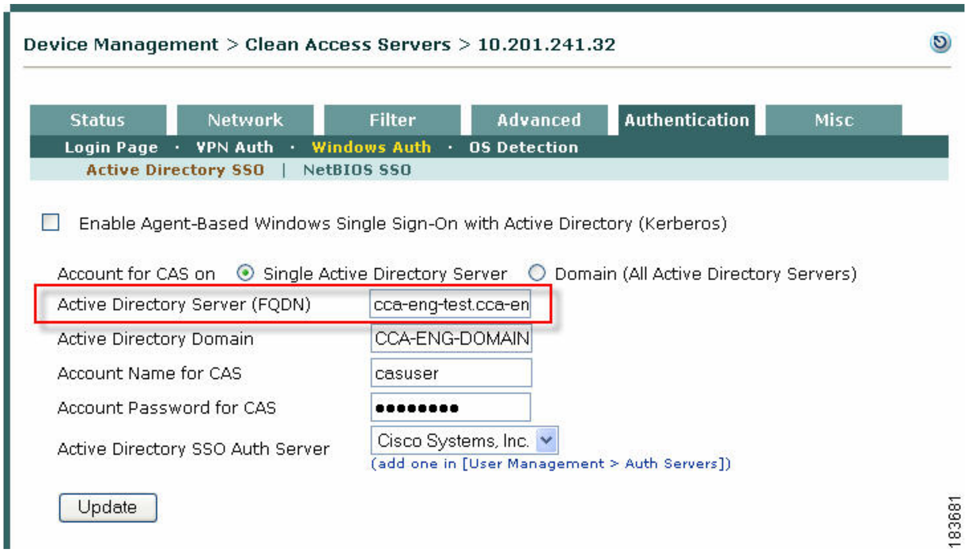
```
Error: Could not start the SSO service. Please check the configuration.
```

Step 3 For **Account for CAS on**, specify whether the CAS account resides on a **Single Active Directory Server** or multiple servers within a **Domain (All Active Directory Servers)**.

Note Make sure the CAS can resolve the name you type in the **Active Directory Server (FQDN)** field via DNS. A DNS server must be correctly configured on the CAS (under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS)** so that the CAS can resolve the FQDN for the AD server.

a. If you specify that the CAS account resides on a **Single Active Directory Server**, enter the fully qualified domain name of the AD server in the **Active Directory Server (FQDN) field (for example,** `cca-eng-test.cca-eng-domain.cisco.com`). This field cannot be an IP address, and must exactly match CASE-BY-CASE the name of the AD server it appears under **Control Panel > System > Computer Name | Full computer name** on the AD server (see Figure 8-7).

Figure 8-6 AD SSO—Single Active Directory Server


Device Management > Clean Access Servers > 10.201.241.32

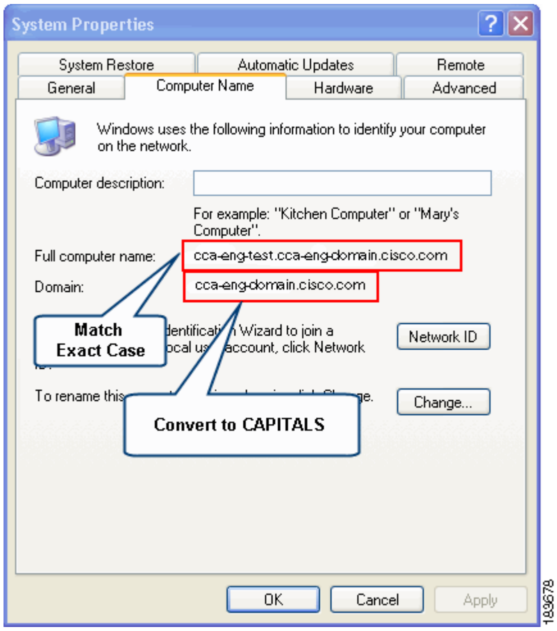
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO

□ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on ● Single Active Directory Server ○ Domain (All Active Directory Servers)

Active Directory Server (FQDN)	cca-eng-test.cca-en
Active Directory Domain	CCA-ENG-DOMAIN
Account Name for CAS	casuser
Account Password for CAS	●●●●●●●●
Active Directory SSO Auth Server	Cisco Systems, Inc. (add one in [User Management > Auth Servers])

Figure 8-7 Control Panel > System > Computer Name | Full computer name



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: cca-eng-test.cca-eng-domain.cisco.com

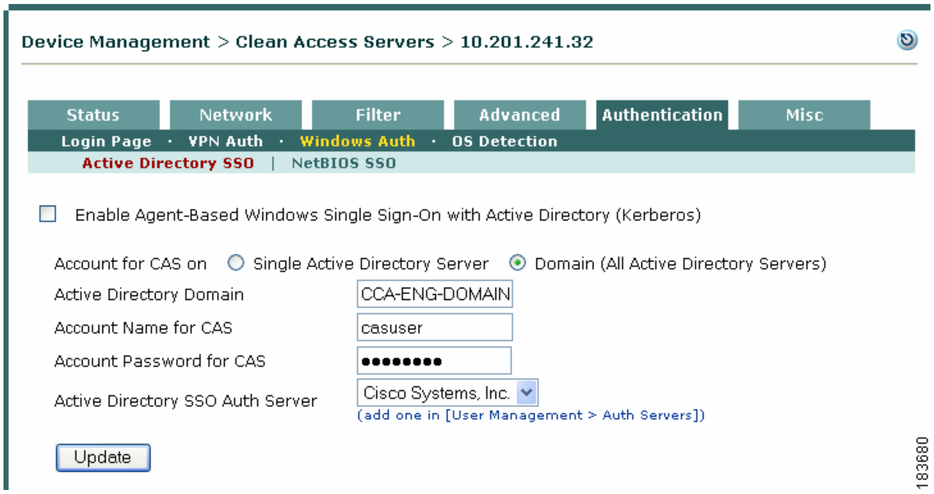
Domain: cca-eng-domain.cisco.com

dentificati n Wizard to join a ocal us account, click Network

To rename this ge.

b. If you select the **Domain (All Active Directory Servers)** option, the **Active Directory Server (FQDN)** field disappears (Figure 8-8). DNS automatically resolves the Active Directory domain specified to the primary domain controller (DC) and, if the primary DC becomes inaccessible, the secondary DC. In this case, you specify only the domain and not the full FQDN of the AD server. Note also that the KTPass command syntax also changes based on whether you specify the **Single Active Directory Server** or **Domain (All Active Directory Servers)** option. For details, see Run the ktpass.exe Command, page 8-22.

Figure 8-8 AD SSO—Domain (All Active Directory Servers)


Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO
Update
183680

Device Management > Clean Access Servers > 10.201.241.32

□ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on ○ Single Active Directory Server ● Domain (All Active Directory Servers)

Active Directory Domain: CCA-ENG-DOMAIN

Account Name for CAS: casuser

Account Password for CAS: ●●●●●●●●

Active Directory SSO Auth Server: Cisco Systems, Inc.
(add one in [User Management > Auth Servers])

Step 4 For **Active Directory Domain**, type the name of the domain for the KDC/Active Directory server **in UPPER CASE** (see Figure 8-7). The “Active Directory Domain” is equivalent to “Kerberos Realm”. For example:

```
CCA-ENG-DOMAIN.CISCO.COM
```

Step 5 For **Account Name for CAS**, type the name of the Clean Access Server user you have created on the AD server, for example: `casuser`.
The CAS user account allows the CAS to log into the AD server.

Step 6 For **Account Password for CAS**, type the password for the CAS user on the AD server.

Note The password is case sensitive. From the CAS side, there is no limitation on the number of characters, and standard characters are allowed. Since this password is based of the mapping created using the KTPass command, observe any limitations from the Windows server side (e.g. password policies).

Step 7 From the **Active Directory SSO Auth Server** dropdown, choose the Active Directory SSO Server you configured on the CAM. This field maps the auth provider created on the CAM to the CAS (along with the Default Role, and secondary LDAP Lookup server, if configured).

Step 8 Click **Update**.

Note If the Active Directory server is not reachable from the CAS at the time of CAS startup, AD SSO service is not started. If this occurs, the administrator must go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO** and click the **Update** button to restart the AD SSO service.

Configuring a CAS User on the AD Server for AD SSO

You can choose to set up AD SSO with or without running KTPass. In either case you must create the CAS user and then set up encryption according to the following sections:

- Create the CAS User, page 8-14
- Specify encryption using one of the following:
  - Install and Run KTPass, page 8-18
  - Configure AD SSO Without KTPass, page 8-26

Create the CAS User

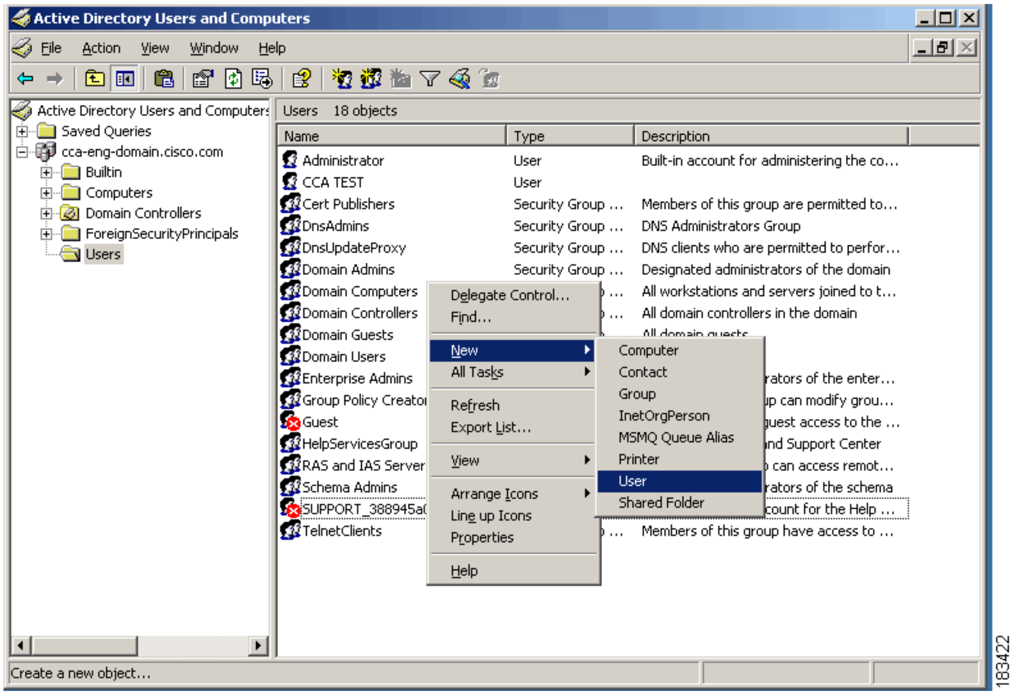
To create a CAS user, follow these steps:

Step 1 Login as the administrator on the Active Directory server machine.

Step 2 Open the Active Directory Management console from **All Programs > Admin Tools > Active Directory Users and Computers**.

Step 3 From the left-hand pane of the **Active Directory Users and Computers** window, navigate to the domain for which you want to configure the CAS, for example, **cca-eng-domain.cisco.com**.

Figure 8-9 Create New User on AD Server



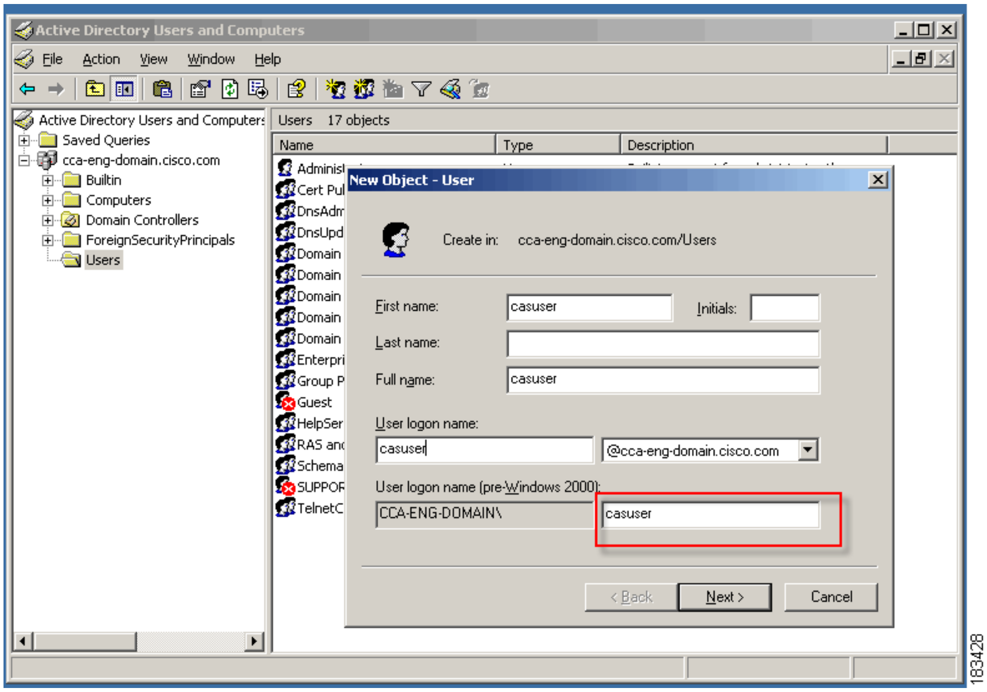
Name	Type	Description
Administrator	User	Built-in account for administering the co...
CCA TEST	User	
Cert Publishers	Security Group ...	Members of this group are permitted to...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permitted to perfor...
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Computers	) ...	All workstations and servers joined to t...
Domain Controllers	) ...	All domain controllers in the domain
Domain Guests		All domain guests
Domain Users		
Enterprise Admins		rators of the enter...
Group Policy Creato		p can modify grou...
Guest		uest access to the ...
HelpServicesGroup		nd Support Center
RAS and IAS Server		can access remot...
Schema Admins		rators of the schema
SUPPORT_388945a(		count for the Help ...
TelnetClients	) ...	Members of this group have access to ...

Step 4 Right-click the **Users** folder. In the menu that appears, select **New > User** (Figure 8-9).

Step 5 In the first **New Object - User** dialog(Figure 8-10), configure the fields for the Clean Access Server user as follows:

Enter the name you want the CAS to use in the **First name** field, for example: **`casuser`**. This automatically populates the **Full name** and **User logon name** fields. The **User logon name** must be one word. Make sure First name= Full name = User name for the user account.

Figure 8-10 Configure the CAS User



Create in: cca-eng-domain.cisco.com/Users

First name: casuser

Initials:

Last name:

Full name: casuser

User logon name: casuser @cca-eng-domain.cisco.com

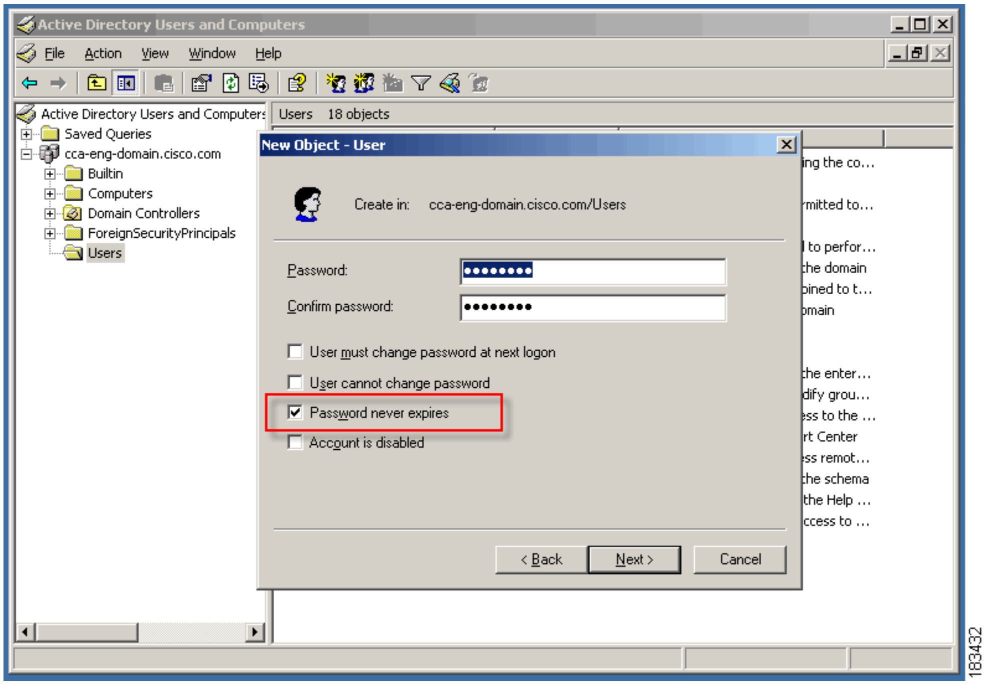
User logon name (pre-Windows 2000): CCA-ENG-DOMAIN\ casuser

Step 6 Click **Next** to bring up the second **New Object - User** dialog.

Step 7 In the second **New Object - User** dialog (Figure 8-11), configure the following:

- Type and retype the password for the CAS user in the **Password** and **Confirm Password** fields.
- Make sure the **Password never expires** option is CHECKED.
- Make sure the **User must check password at next login** option is UNCHECKED.

Figure 8-11 Configure Password for CAS User



Create in: cca-eng-domain.cisco.com/Users

Password: ••••••••

Confirm password: ••••••••

☐ User must change password at next logon

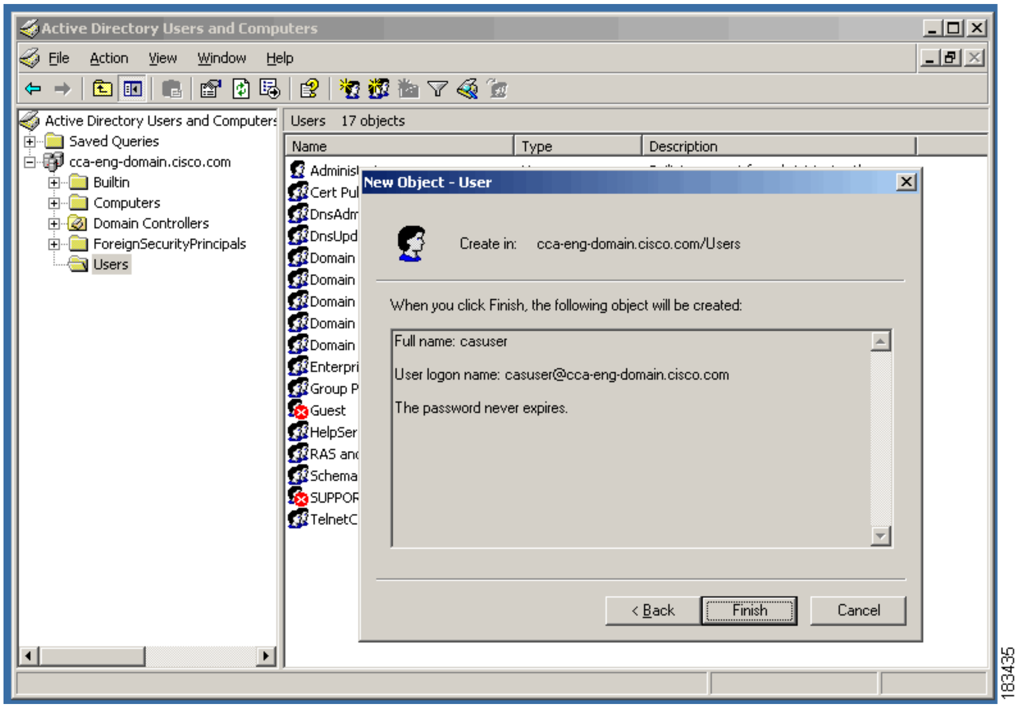
☐ User cannot change password

☑ Password never expires

☐ Account is disabled

Step 8 Click **Next** to bring up the confirmation **New Object - User** dialog (Figure 8-12).

Figure 8-12 Confirm CAS User Properties



Create in: cca-eng-domain.cisco.com/Users

When you click Finish, the following object will be created:

Full name: casuser

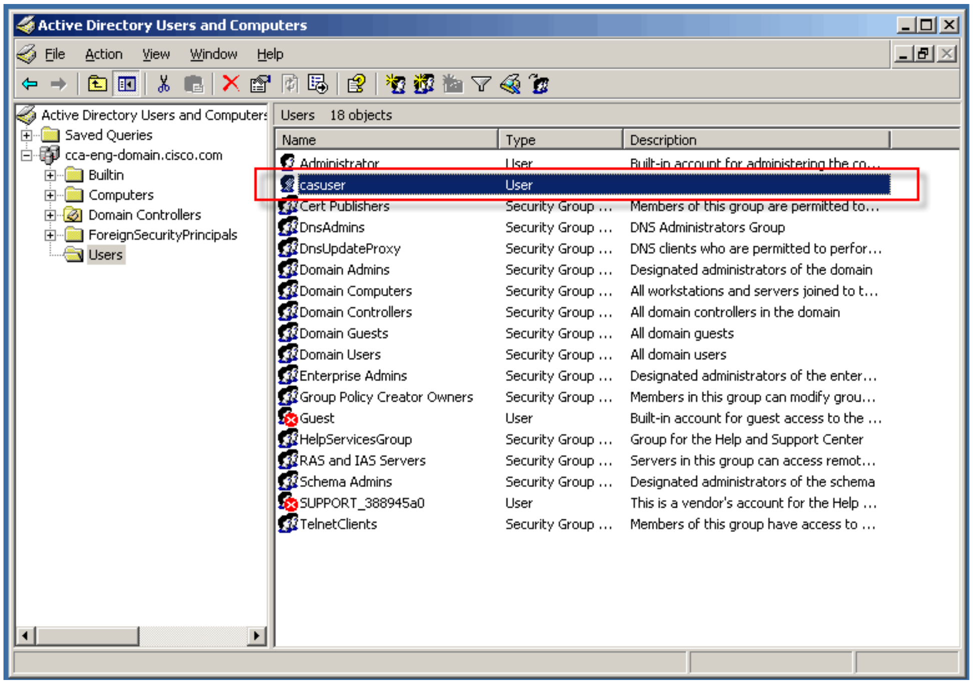
User logon name: casuser@cca-eng-domain.cisco.com

The password never expires.

Step 9 Confirm the properties for the CAS user and click **Finish** to conclude, or click **Back** if you need to make corrections.

Step 10 The CAS user is successfully added to the AD domain (Figure 8-13).

Figure 8-13 CAS User is Added


Active Directory Users and Computers
File Action View Window Help
183439

- Active Directory Users and Computers
  - Saved Queries
  - cca-eng-domain.cisco.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

Users 18 objects

Name	Type	Description
Administrator	User	Built-in account for administering the co...
casuser	User	
Cert Publishers	Security Group ...	Members of this group are permitted to...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permitted to perfor...
Domain Admins	Security Group ...	Designated administrators of the domain
Domain Computers	Security Group ...	All workstations and servers joined to t...
Domain Controllers	Security Group ...	All domain controllers in the domain
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators of the enter...
Group Policy Creator Owners	Security Group ...	Members in this group can modify grou...
Guest	User	Built-in account for guest access to the ...
HelpServicesGroup	Security Group ...	Group for the Help and Support Center
RAS and IAS Servers	Security Group ...	Servers in this group can access remot...
Schema Admins	Security Group ...	Designated administrators of the schema
SUPPORT_388945a0	User	This is a vendor's account for the Help ...
TelnetClients	Security Group ...	Members of this group have access to ...

Install and Run KTPass

This section addresses the following two topics:

- Install the Correct Version of ktpass.exe to Support Your AD SSO Deployment, page 8-18
- Run the ktpass.exe Command, page 8-22

Install the Correct Version of ktpass.exe to Support Your AD SSO Deployment

The **ktpass.exe** tool is available as part of the Windows 2000/2003/2008 Server support tools on the Microsoft support site: http://support.microsoft.com/. The KTPass executable is not installed by default in Windows Server 2000/2003. Therefore, if you are configuring in a Windows Server 2000/2003 environment, you must retrieve the executable from the Microsoft Support site prior to installation. To determine the correct version of **ktpass.exe** to support your Cisco NAC Appliance/AD SSO deployment, see *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

Note To ensure successful KTPass operation, obtain and install the correct version of **ktpass.exe** according to the AD SSO support table in *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.)
You *must* use Windows Server 2008 with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or Windows 7 with an appropriate version of the Cisco NAC Agent installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO.

Cisco has tested the following versions of Windows AD Server and KTPass for the purposes of enabling AD SSO for Windows 7 client authentication.

Table 8-2 Windows AD Server and KTPass Version Compatibility for Windows 7 Clients

Windows AD Server Version	KTPass Version
Windows 2008 Server SP2 [1,2]	6.0.6002.18005
Windows 2008 Server R2 [2]	6.1.7600.16385
Windows 2008 Server Enterprise SP1[3]	6.0.6001.18000
Windows 2003 Server	5.2.3790.1830

[1] Window Server 2008 SP2 servers need to perform a Windows Update before running KTPass. Make sure Windows Hotfix KB951191 is installed. Without this Windows Update, the AD SSO service in the CAS might not start. This applies to the KTPass version to be used for Windows 2008 SP2 – 6.0.6002.18005 and for Windows 2008 R2 enterprise it is 6.1.7600.16385.

[2] If the AD system is based on an upgrade from Windows Server 2003, you must raise the domain functionality to Windows Server 2008 level for Cisco NAC appliance to perform SSO on Windows 7 clients. Without this you will not be able to automatically login to the Cisco NAC Appliance network.

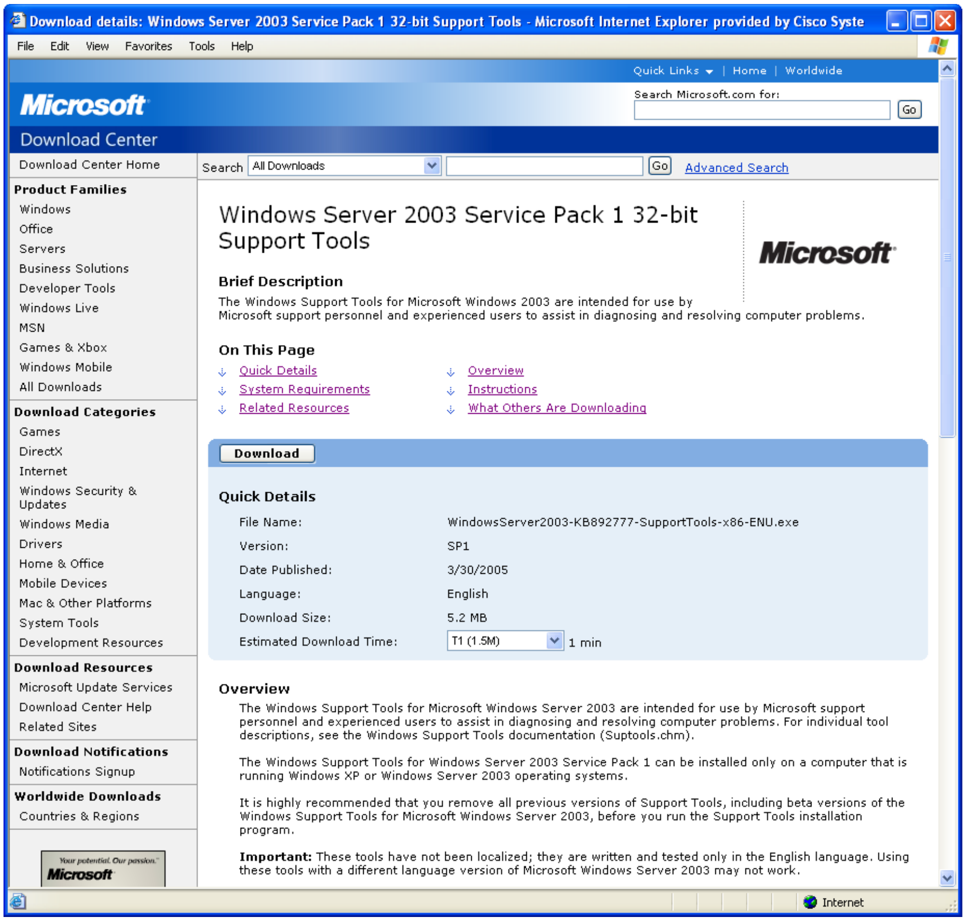
[3] Server running at 2003 functional level.

To install the **ktpass.exe** tool, follow these steps:

Step 1 Open a web browser and navigate to http://support.microsoft.com/.

Step 2 Locate the Windows Server 2000/2003/2008 Support Tools section(s) of the Microsoft web site.

Figure 8-14 Support Tools for Windows 2003 Server



Windows Server 2003 Service Pack 1 32-bit Support Tools

Brief Description

The Windows Support Tools for Microsoft Windows 2003 are intended for use by Microsoft support personnel and experienced users to assist in diagnosing and resolving computer problems.

On This Page

- Quick Details
- System Requirements
- Related Resources
- Overview
- Instructions
- What Others Are Downloading

Download

Quick Details

File Name:	WindowsServer2003-KB892777-SupportTools-x86-ENU.exe
Version:	SP1
Date Published:	3/30/2005
Language:	English
Download Size:	5.2 MB
Estimated Download Time:	T1 (1.5M) 1 min

Overview

The Windows Support Tools for Microsoft Windows Server 2003 are intended for use by Microsoft support personnel and experienced users to assist in diagnosing and resolving computer problems. For individual tool descriptions, see the Windows Support Tools documentation (Suptools.chm).

The Windows Support Tools for Windows Server 2003 Service Pack 1 can be installed only on a computer that is running Windows XP or Windows Server 2003 operating systems.

It is highly recommended that you remove all previous versions of Support Tools, including beta versions of the Windows Support Tools for Microsoft Windows Server 2003, before you run the Support Tools installation program.

Important: These tools have not been localized; they are written and tested only in the English language. Using these tools with a different language version of Microsoft Windows Server 2003 may not work.

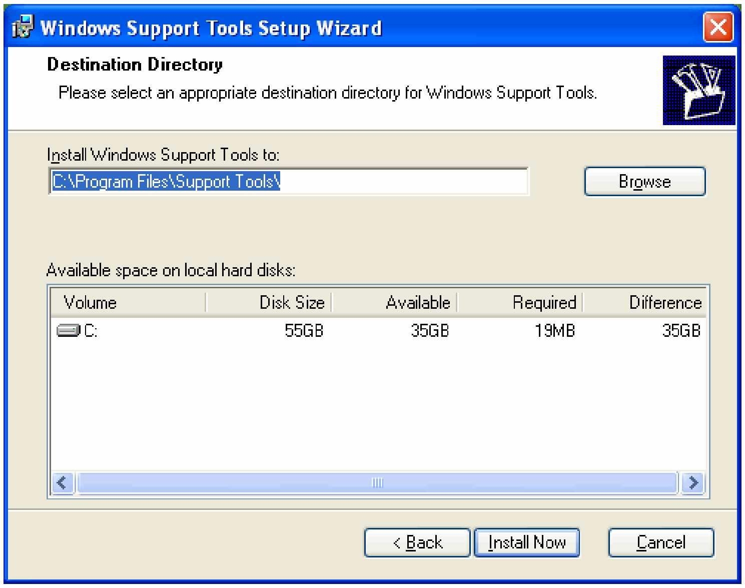
Step 3 Click the **Download** button.

Step 4 Do one of the following:

- Click **Save** to save a copy of the Windows Server 2000/2003/2008 Support Tools Self-Extractor executable on your local machine.
- Click **Run** to begin installing the Windows Server 2000/2003/2008 Support Tools on your local machine.

When you launch the Self-Extractor or click **Run**, Windows automatically launches the **Windows Support Tools Setup Wizard**.

Figure 8-15 Installing Windows Server 2003 Support Tools


Windows Support Tools Setup Wizard

Destination Directory

Please select an appropriate destination directory for Windows Support Tools.

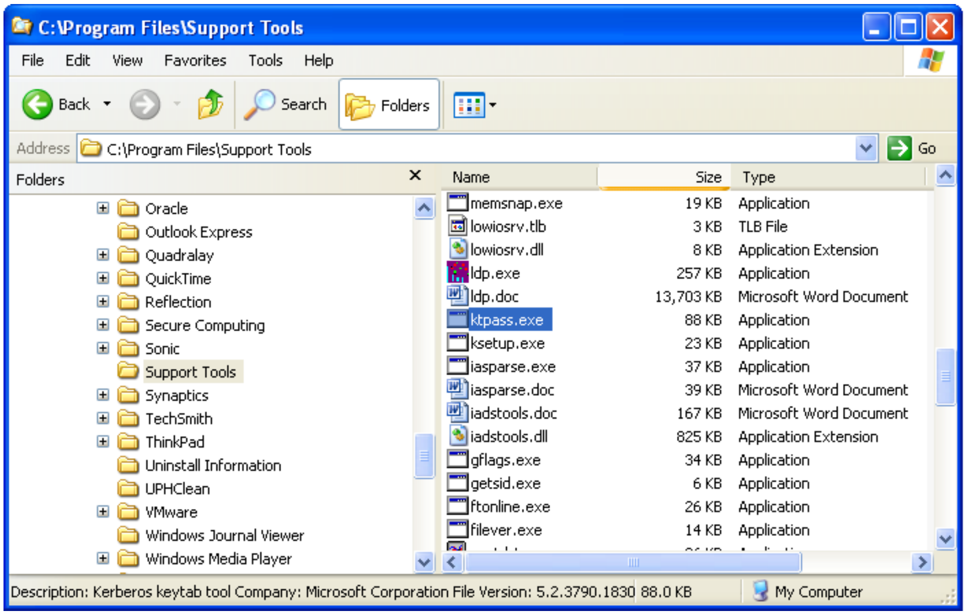
Install Windows Support Tools to: C:\Program Files\Support Tools\

Available space on local hard disks:

Volume	Disk Size	Available	Required	Difference
C:	55GB	35GB	19MB	35GB

Step 5 Once the installation is complete, open Windows Explorer and navigate to the C:\Program Files\Support Tools directory (or another directory you may have specified in the Setup Wizard session), and verify that the **ktpass.exe** component appears in the file list. (See Figure 8-16.)

Figure 8-16 Support Tools—ktpass.exe


C:\Program Files\Support Tools

Address C:\Program Files\Support Tools

Folders: Oracle, Outlook Express, Quadralay, QuickTime, Reflection, Secure Computing, Sonic, Support Tools, Synaptics, TechSmith, ThinkPad, Uninstall Information, UPHClean, VMware, Windows Journal Viewer, Windows Media Player

Name	Size	Type
memsnap.exe	19 KB	Application
lowiosrv.tlb	3 KB	TLB File
lowiosrv.dll	8 KB	Application Extension
ldp.exe	257 KB	Application
ldp.doc	13,703 KB	Microsoft Word Document
ktpass.exe	88 KB	Application
ksetup.exe	23 KB	Application
iasparse.exe	37 KB	Application
iasparse.doc	39 KB	Microsoft Word Document
iadstools.doc	167 KB	Microsoft Word Document
iadstools.dll	825 KB	Application Extension
gflags.exe	34 KB	Application
getsid.exe	6 KB	Application
ftonline.exe	26 KB	Application
filever.exe	14 KB	Application

Description: Kerberos keytab tool Company: Microsoft Corporation File Version: 5.2.3790.1830 88.0 KB

Step 6 Execute the **ktpass.exe** command according to the directions in the next section, Run the ktpass.exe Command.

Note Do not double-click the **ktpass.exe** command in Windows Explorer; it must be run from a command prompt.

Run the ktpass.exe Command

This section is designed to execute the KTPass executable for non-Windows 7 client machines to perform SSO. If you are setting up an environment for Windows 7 client machines, see Configure AD SSO in a Windows 7 Client Environment, page 8-34.

When a CAS is configured to interact with a single AD server, you also need to run the KTPass command on the AD server configured in the CAS.

If you are associating the CAS with an entire AD domain, you must run the KTPass command on any single AD server (not all AD servers) in the AD domain. The information in the KTPass command operation is then automatically propagated to the other members of the AD domain.

See *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later* for a list of the Windows server versions supported.

Note When running **ktpass.exe**, it is very important to observe the following case sensitivity:.

- The computer name that is entered between "/" and "@" in the command (e.g. "AD_DomainServer") must exactly match CASE-BY-CASE the name of the AD server as it appears under **Control Panel > System > Computer Name | Full computer name** on the AD server.
- The realm name that is entered after "@" (e.g. "AD_DOMAIN") must always be in **UPPER CASE**. You must convert the Domain name that appears under **Control Panel > System > Computer Name | Domain** on the AD server to UPPER CASE when entering it in the KTPass command. (See Figure 8-19.)
- No warnings should appear after you execute **ktpass.exe**.
- Execution of the command must display the following output:

```
Account <CAS user> has been set for DES-only encryption
```

To run **ktpass.exe** on a non-Windows 7 client machine:

Step 1 Open a command prompt and cd to C:\Program Files\Support Tools\. The **ktpass.exe** command should be in the folder.

Step 2 Enter one of the following commands:

If your Active Directory domain consists of only one server

- **ktpass -princ** <*CAS_username*>**/**<*AD_DomainServer*>**.**<*AD_Domain*>**@**<*AD_DOMAIN*> **-mapuser** <*CAS_username*> **-pass** <*CAS_password*> **-out c:\**<*CAS_username*>**.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly**

  Use this command syntax when you specify the **Account for CAS on Single Active Directory Server** option in Configure AD SSO on the CAS, page 8-11.

  For example (see also Figure 8-17):

```
C:\Program Files\Support Tools> ktpass -princ
casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser
casuser -pass Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
```

If your Active Directory domain consists of multiple servers

While adding new servers to an already existing multi-server domain, it is not required to run the ktpass command again. This includes adding a 2008 server to an existing multi-server domain running in a 2003 domain functional level.

- **ktpass -princ** <*CAS_username*>**/**<*AD_Domain*>**@**<*AD_DOMAIN*> **-mapuser** <*CAS_username*> **-pass** <*CAS_password*> **-out c:\**<*CAS_username*>**.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly**

  Use this command syntax when you specify the **Account for CAS on Domain (All Active Directory Servers) option** in Configure AD SSO on the CAS, page 8-11.

  For example (see also Figure 8-17):

  ```
  C:\Program Files\Support Tools> ktpass -princ
  casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass
  Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
  ```

The output of the command should be as follows (see also Figure 8-18):

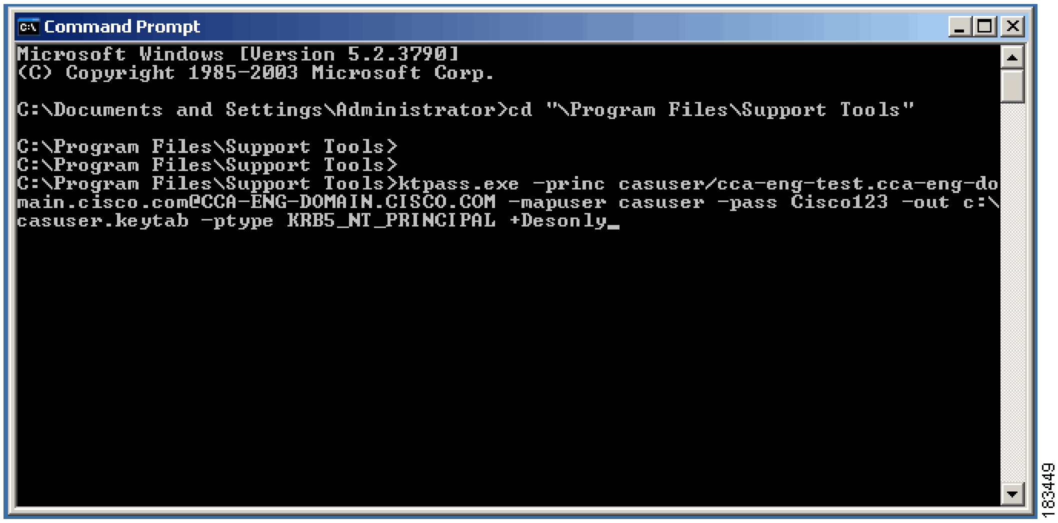
```
Targeting domain controller: cca-eng-test.cca-eng-domain.cisco.com
Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser.
Key created.
Output keytab to c:\casuser.keytab:
Keytab version: 0x502
keysize 97 casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0xbc5120bcfeda01f8)
Account casuser has been set for DES-only encryption.
```

Note The "**`Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser`**" response confirms that the **`casuser`** account is mapped correctly.

In the example above, the service principal name (SPN), `casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM`, is the key to ensuring that any AD server within a managed domain can appropriately resolve user credentials passed from the CAS.

Step 3 **Save** the exact command you ran and the output to a text file (you do not need to save the CAS user password). For troubleshooting purposes, this will facilitate TAC support.

Figure 8-17 Execute ktpass.exe Command

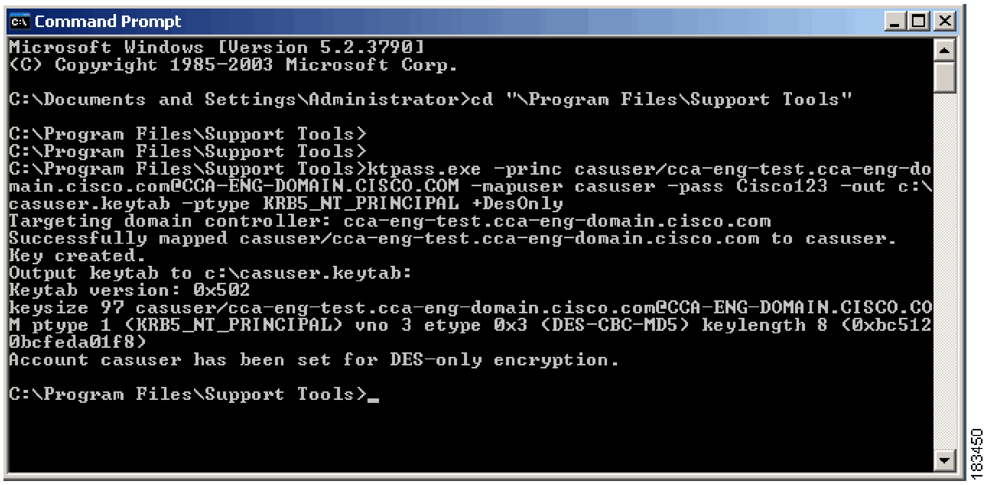


```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files\Support Tools"

C:\Program Files\Support Tools>
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>ktpass.exe -princ casuser/cca-eng-test.cca-eng-do
main.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass Cisco123 -out c:\
casuser.keytab -ptype KRB5_NT_PRINCIPAL +Desonly_
```

Figure 8-18 ktpass.exe Command Output



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files\Support Tools"

C:\Program Files\Support Tools>
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>ktpass.exe -princ casuser/cca-eng-test.cca-eng-do
main.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass Cisco123 -out c:\
casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
Targeting domain controller: cca-eng-test.cca-eng-domain.cisco.com
Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser.
Key created.
Output keytab to c:\casuser.keytab:
Keytab version: 0x502
keysize 97 casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.CO
M ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0xbc512
0bcfeda01f8)
Account casuser has been set for DES-only encryption.

C:\Program Files\Support Tools>_
```

Table 8-3 provides further parameter details.

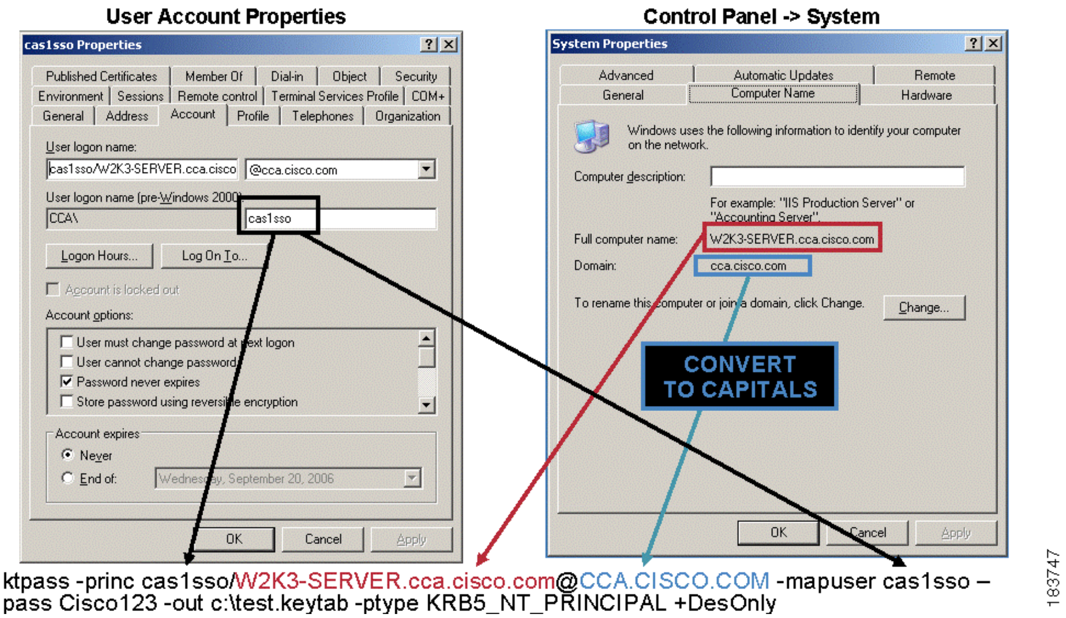
Table 8-3 ktpass.exe Parameters

Parameter	Description
`-princ`	Service principal name (SPN) identifier The entire SPN string, itself, is constructed as follows: `<CAS_username>/[<AD_DomainServer>|<AD_Domain>]@<AD_DOMAIN>`
`<CAS_username>`	UserName
`<AD_DomainServer>`	FQDN machine name for a single AD server. This parameter must exactly match (including the case) the *name* of the AD server under **Control Panel > System > Computer Name | Full computer name**.
`<AD_Domain>`	The name of the AD domain the CAS uses to authenticate user credentials. This parameter must exactly match (including the case) the *domain* of the AD server(s) under **Control Panel > System > Domain**.
`<AD_DOMAIN>`	Domain name (must be in UPPER CASE)
`-mapuser`	Maps the CAS user to the domain
`-pass`	CAS user password
`-out`	Outputs the "c:\**<CAS_user_name>**.keytab" key to generate a key tab (similar to a certificate) for this user
c:\**<CAS_user_name>**.keytab	Required parameter
`-ptype`	Principal type (required parameter)
`KRB5_NT_PRINCIPAL`	The Principal provided is of this type. By default AD servers should use this type, but some do not.
`+DesOnly`	Flag for DES encryption

Example KTPass Command Execution

Figure 8-19 shows how parameters are derived from the CAS user account properties and AD server computer name to run the KTPass command. Note that the values in this figure are example values only; they do not match the configuration example steps outlined in this chapter.

Figure 8-19 Example of How KTPass is Run—SAMPLE VALUES


User Account Properties
cas1sso Properties
Published Certificates | Member Of | Dial-in | Object | Security
Environment | Sessions | Remote control | Terminal Services Profile | COM+
General | Address | Account | Profile | Telephones | Organization
Logon Hours...
Log On To...
OK
Cancel
Apply
Control Panel -> System
System Properties
Advanced | Automatic Updates | Remote
General | Computer Name | Hardware
Change...
OK
Cancel
Apply
CONVERT TO CAPITALS
183747

User logon name: cas1sso/W2K3-SERVER.cca.cisco @cca.cisco.com

User logon name (pre-Windows 2000): CCA\ cas1sso

□ Account is locked out

Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, September 20, 2006

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: W2K3-SERVER.cca.cisco.com

Domain: cca.cisco.com

To rename this computer or join a domain, click Change.

```
ktpass -princ cas1sso/W2K3-SERVER.cca.cisco.com@CCA.CISCO.COM -mapuser cas1sso –
pass Cisco123 -out c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
```

Configure AD SSO Without KTPass

The following procedure guides you through the process necessary to configure an AD SSO user account for both Windows Server 2003 and Windows Server 2008 Active Directory entities operating at their respective full functional levels without having to run KTPass. (This method does not support a Server 2008 AD operating at a 2003 domain functional level.)

Note AD SSO user accounts configured to connect with Server 2008 AD entities are not FIPS 140-2 compliant.

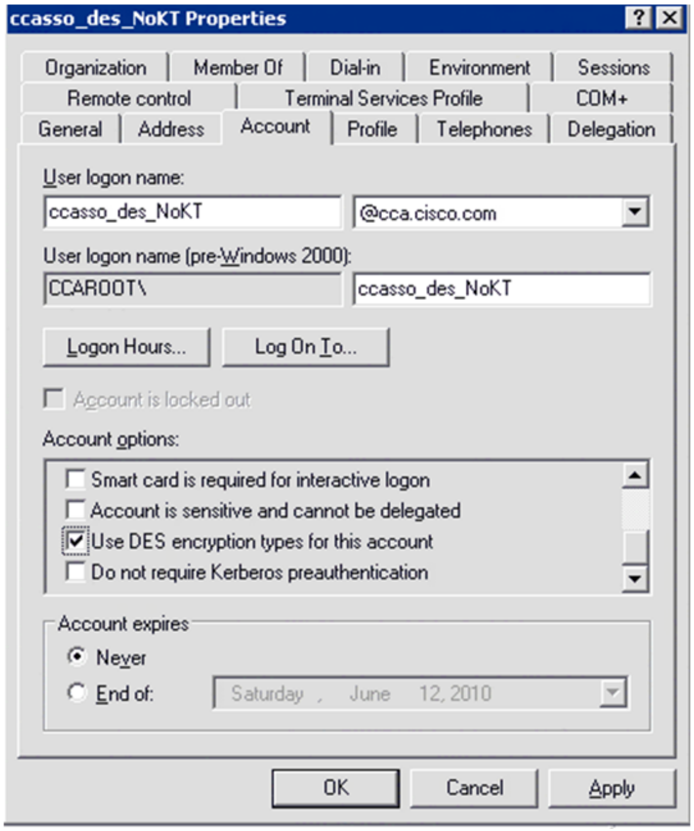
The following steps apply for DES only encryption type.

Step 1 Open the **Properties** dialog for an Active Directory account you created using Create the CAS User, page 8-14.

Step 2 To require DES encryption for the new CAS user account, click on the **Account** tab, enable (check) the **Use DES encryption types for this account** (Server 2003) or **Use Kerberos DES encryption types for this account** (Server 2008) option under Account options, and click **OK**. (See Figure 8-20 and Figure 8-21.)

Note To set up a Windows 7 client machine for DES encryption, refer to Manually Enable DES on Individual Windows 7 Client Machines.

Figure 8-20 Server 2003 Example—Account Properties



ccasso_des_NoKT Properties

User logon name: ccasso_des_NoKT @cca.cisco.com

User logon name (pre-Windows 2000): CCAROOT\ ccasso_des_NoKT

□ Account is locked out

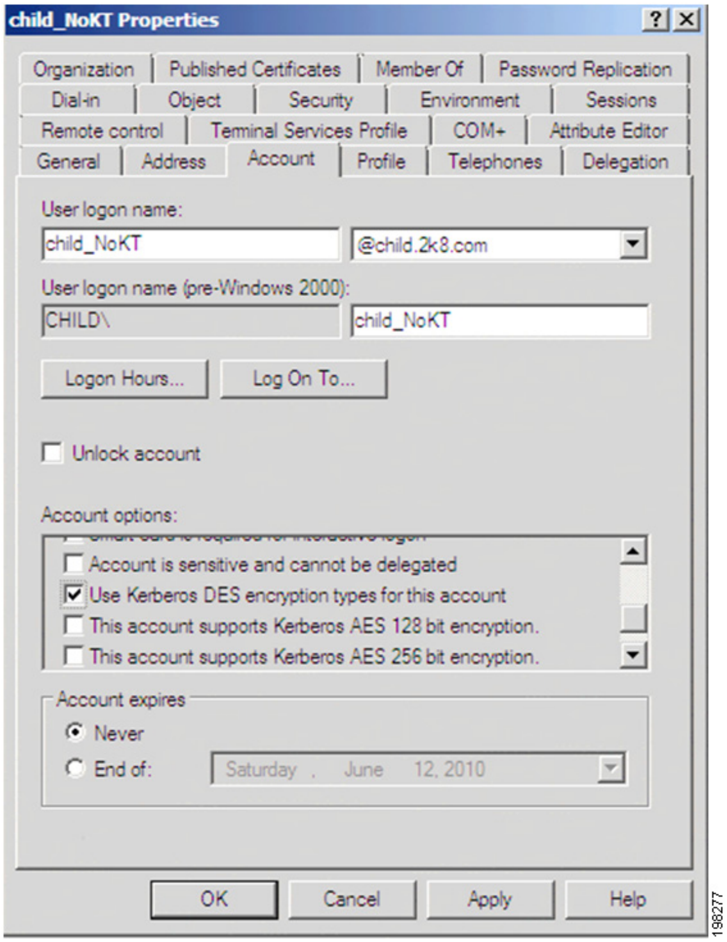
Account options:

- □ Smart card is required for interactive logon
- □ Account is sensitive and cannot be delegated
- ☑ Use DES encryption types for this account
- □ Do not require Kerberos preauthentication

Account expires

- ● Never
- ○ End of: Saturday , June 12, 2010

Figure 8-21 Server 2008 Example—Account Properties



User logon name:
child_NoKT @child.2k8.com

User logon name (pre-Windows 2000):
CHILD\ child_NoKT

□ Unlock account

Account options:
- □ Account is sensitive and cannot be delegated
- ☑ Use Kerberos DES encryption types for this account
- □ This account supports Kerberos AES 128 bit encryption.
- □ This account supports Kerberos AES 256 bit encryption.

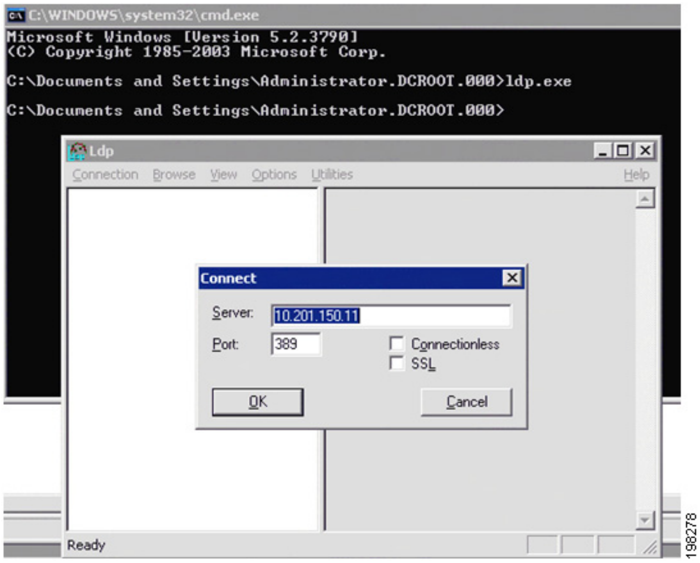
Account expires
- ● Never
- ○ End of: Saturday , June 12, 2010

Step 3 Open a DOS prompt on the AD server and enter `ldp.exe` (Figure 8-22 background). An additional **Ldp** application window opens.

> **Note** If you do not have a local copy of the **ldp.exe** file, you can locate it under Support Tools in the Microsoft Windows Server Resource Kit.

Step 4 In the **Ldp** window, connect to the Active Directory domain controller using the **Connection > Connect** command and entering the domain controller's IP address or domain name (Figure 8-22 and Figure 8-23). For example, in the **Connect** dialog, enter `10.201.150.11` or `child.2k8.com`.

Figure 8-22 Ldp Application Connection > Connect—Server 2003 Example



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator.DCROOT.000>ldp.exe

C:\Documents and Settings\Administrator.DCROOT.000>
```

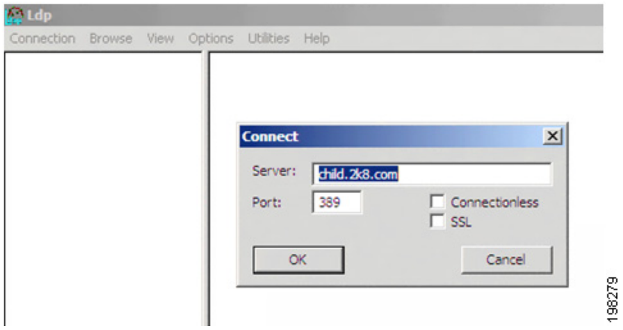
Server: 10.201.150.11

Port: 389

□ Connectionless

□ SSL

Figure 8-23 Ldp Application Connection > Connect—Server 2008 Example



Server: child.2k8.com

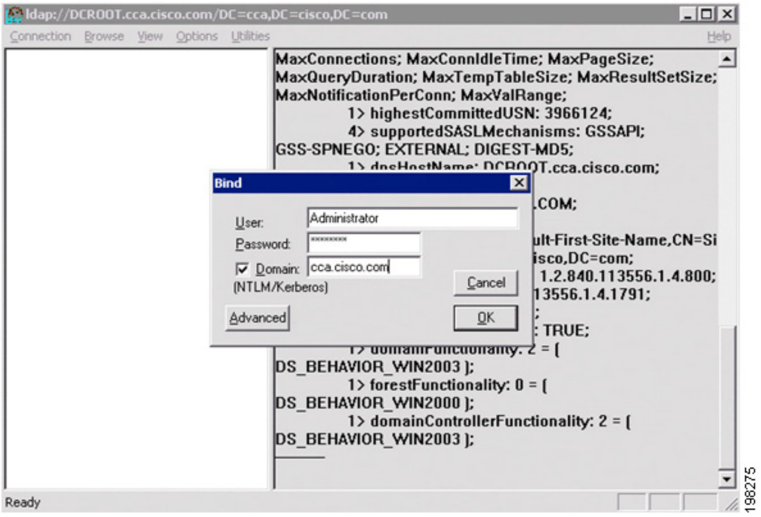
Port: 389

□ Connectionless

□ SSL

Step 5 After you are connected to the domain controller, use the **Connection > Bind** command to bind to the AD domain as an administrator (Figure 8-24 and Figure 8-25). (You can specify the same ID that you used to create the user account).

Figure 8-24   Connection > Bind—Server 2003 Example



```
MaxConnections; MaxConnIdleTime; MaxPageSize;
MaxQueryDuration; MaxTempTableSize; MaxResultSetSize;
MaxNotificationPerConn; MaxValRange;
            1> highestCommittedUSN: 3966124;
            4> supportedSASLMechanisms: GSSAPI;
GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
            1> dnsHostName: DCROOT.cca.cisco.com;
                              .COM;
                              ult-First-Site-Name,CN=Si
                              isco,DC=com;
                               1.2.840.113556.1.4.800;
                              13556.1.4.1791;
                              ;
                              : TRUE;
            1> domainFunctionality: 2 = (
DS_BEHAVIOR_WIN2003 );
            1> forestFunctionality: 0 = (
DS_BEHAVIOR_WIN2000 );
            1> domainControllerFunctionality: 2 = (
DS_BEHAVIOR_WIN2003 );
```

Bind

User: Administrator

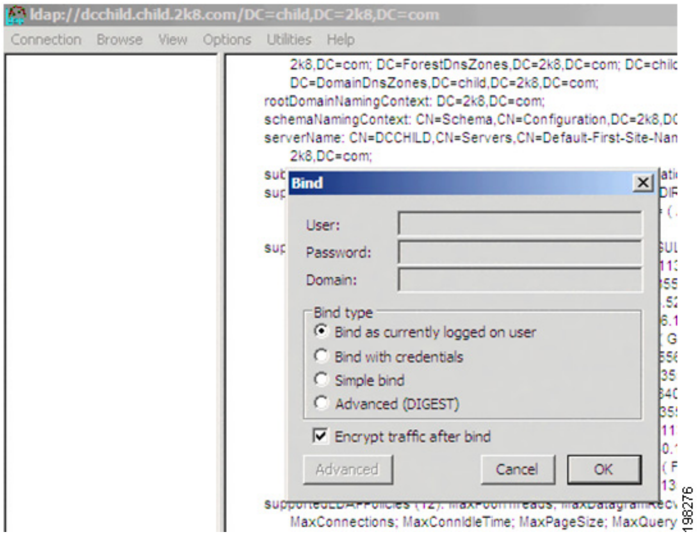
Password: ********

☑ Domain: cca.cisco.com

(NTLM/Kerberos)

Advanced   Cancel   OK

Figure 8-25   Connection > Bind—Server 2008 Example



```
    2k8,DC=com; DC=ForestDnsZones,DC=2k8,DC=com; DC=chilc
    DC=DomainDnsZones,DC=child,DC=2k8,DC=com;
rootDomainNamingContext: DC=2k8,DC=com;
schemaNamingContext: CN=Schema,CN=Configuration,DC=2k8,DC
serverName: CN=DCCHILD,CN=Servers,CN=Default-First-Site-Nan
    2k8,DC=com;
sub
sup
sup
supportedLDAPPolicies (12): MaxPoolThreads; MaxDatagramRecv
    MaxConnections; MaxConnIdleTime; MaxPageSize; MaxQuery
```

Bind

User:

Password:

Domain:

Bind type

● Bind as currently logged on user

○ Bind with credentials

○ Simple bind

○ Advanced (DIGEST)

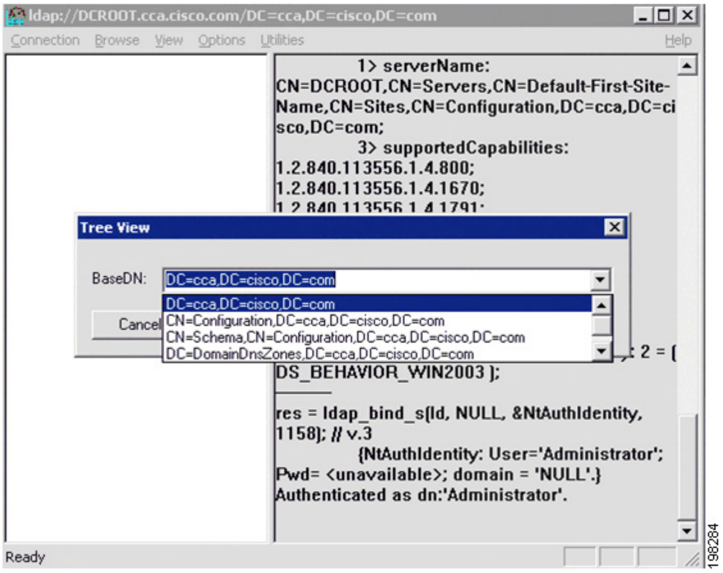
☑ Encrypt traffic after bind

Advanced   Cancel   OK

Step 6 Display a list of known domain suffixes using the **View > Tree** command and expanding the pull-down menu that appears (Figure 8-26).

Step 7 Choose **DC=cca,DC=cisco,DC=com** and click **OK**.

Figure 8-26 "DC=cca,DC=cisco,DC=com" Tree View


ldap://DCROOT.cca.cisco.com/DC=cca,DC=cisco,DC=com
Connection Browse View Options Utilities Help
Tree View
Cancel
Ready
198284

```
        1> serverName:
CN=DCROOT,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=cca,DC=ci
sco,DC=com;
        3> supportedCapabilities:
1.2.840.113556.1.4.800;
1.2.840.113556.1.4.1670;
1.2.840.113556.1.4.1791;
```

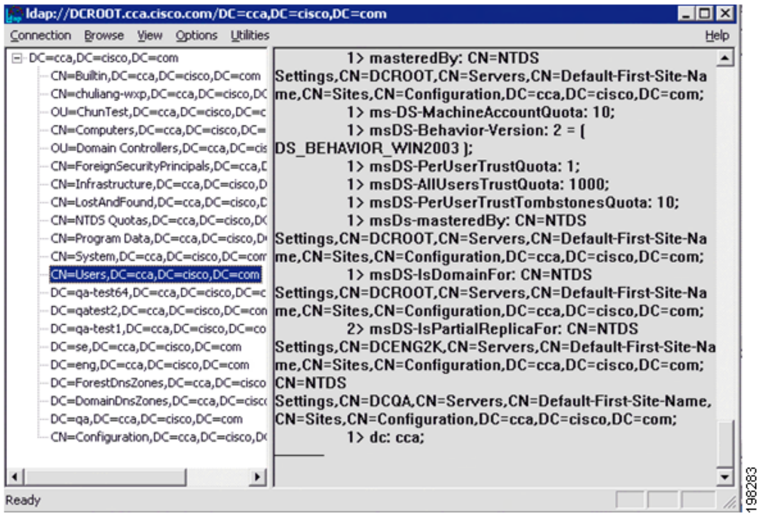
BaseDN: DC=cca,DC=cisco,DC=com

```
DC=cca,DC=cisco,DC=com
CN=Configuration,DC=cca,DC=cisco,DC=com
CN=Schema,CN=Configuration,DC=cca,DC=cisco,DC=com
DC=DomainDnsZones,DC=cca,DC=cisco,DC=com
```

```
                                        : 2 = (
DS_BEHAVIOR_WIN2003 );
-----------
res = ldap_bind_s(ld, NULL, &NtAuthIdentity,
1158); // v.3
        {NtAuthIdentity: User='Administrator';
Pwd= <unavailable>; domain = 'NULL'.}
Authenticated as dn:'Administrator'.
```

Step 8 Expand the **DC=cca,DC=cisco,DC=com** tree and double-click on **CN=Users,DC=cca,DC=cisco,DC=com** (Figure 8-27).

Figure 8-27 Expanded Tree View

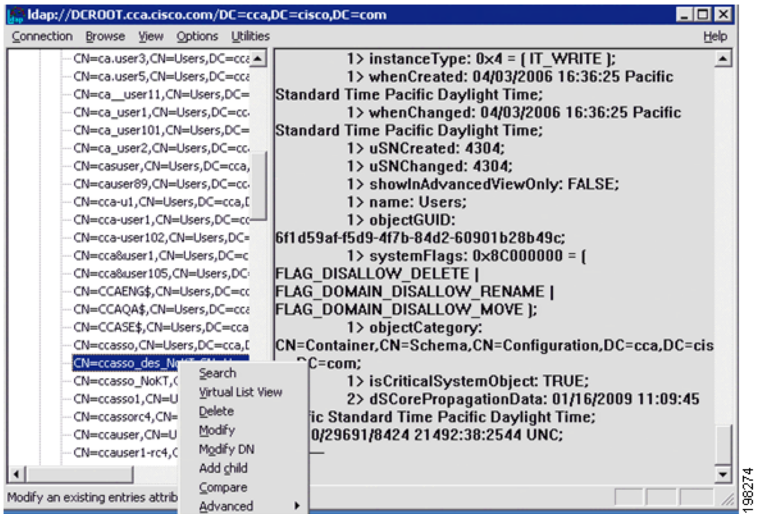

ldap://DCROOT.cca.cisco.com/DC=cca,DC=cisco,DC=com
Connection Browse View Options Utilities Help
Ready
198283

```
DC=cca,DC=cisco,DC=com
    CN=Builtin,DC=cca,DC=cisco,DC=com
    CN=chuliang-wxp,DC=cca,DC=cisco,DC
    OU=ChunTest,DC=cca,DC=cisco,DC=c
    CN=Computers,DC=cca,DC=cisco,DC=
    OU=Domain Controllers,DC=cca,DC=cis
    CN=ForeignSecurityPrincipals,DC=cca,D
    CN=Infrastructure,DC=cca,DC=cisco,D
    CN=LostAndFound,DC=cca,DC=cisco,D
    CN=NTDS Quotas,DC=cca,DC=cisco,DC
    CN=Program Data,DC=cca,DC=cisco,D
    CN=System,DC=cca,DC=cisco,DC=com
    CN=Users,DC=cca,DC=cisco,DC=com
    DC=qa-test64,DC=cca,DC=cisco,DC=c
    DC=qatest2,DC=cca,DC=cisco,DC=con
    DC=qa-test1,DC=cca,DC=cisco,DC=co
    DC=se,DC=cca,DC=cisco,DC=com
    DC=eng,DC=cca,DC=cisco,DC=com
    DC=ForestDnsZones,DC=cca,DC=cisco
    DC=DomainDnsZones,DC=cca,DC=cisc
    DC=qa,DC=cca,DC=cisco,DC=com
    CN=Configuration,DC=cca,DC=cisco,DC
```

```
        1> masteredBy: CN=NTDS
Settings,CN=DCROOT,CN=Servers,CN=Default-First-Site-Na
me,CN=Sites,CN=Configuration,DC=cca,DC=cisco,DC=com;
        1> ms-DS-MachineAccountQuota: 10;
        1> msDS-Behavior-Version: 2 = (
DS_BEHAVIOR_WIN2003 );
        1> msDS-PerUserTrustQuota: 1;
        1> msDS-AllUsersTrustQuota: 1000;
        1> msDS-PerUserTrustTombstonesQuota: 10;
        1> msDs-masteredBy: CN=NTDS
Settings,CN=DCROOT,CN=Servers,CN=Default-First-Site-Na
me,CN=Sites,CN=Configuration,DC=cca,DC=cisco,DC=com;
        1> msDS-IsDomainFor: CN=NTDS
Settings,CN=DCROOT,CN=Servers,CN=Default-First-Site-Na
me,CN=Sites,CN=Configuration,DC=cca,DC=cisco,DC=com;
        2> msDS-IsPartialReplicaFor: CN=NTDS
Settings,CN=DCENG2K,CN=Servers,CN=Default-First-Site-Na
me,CN=Sites,CN=Configuration,DC=cca,DC=cisco,DC=com;
CN=NTDS
Settings,CN=DCQA,CN=Servers,CN=Default-First-Site-Name,
CN=Sites,CN=Configuration,DC=cca,DC=cisco,DC=com;
        1> dc: cca;
-----------
```

Step 9 Locate the user account you created in Step 1, right-click on the account entry, and click **Modify** (Figure 8-28). The account **Modify** dialog box opens.

Figure 8-28 Modify the User Account Entry



```
CN=ca.user3,CN=Users,DC=cca
CN=ca.user5,CN=Users,DC=cca
CN=ca__user11,CN=Users,DC=
CN=ca_user1,CN=Users,DC=cc.
CN=ca_user101,CN=Users,DC=
CN=ca_user2,CN=Users,DC=cc.
CN=casuser,CN=Users,DC=cca,
CN=causer89,CN=Users,DC=cc.
CN=cca-u1,CN=Users,DC=cca,[
CN=cca-user1,CN=Users,DC=cc
CN=cca-user102,CN=Users,DC=
CN=cca&user1,CN=Users,DC=c
CN=cca&user105,CN=Users,DC
CN=CCAENG$,CN=Users,DC=cc
CN=CCAQA$,CN=Users,DC=cca
CN=CCASE$,CN=Users,DC=cca
CN=ccasso,CN=Users,DC=cca,[
CN=ccasso_des_N
CN=ccasso_NoKT,C
CN=ccasso1,CN=U
CN=ccassorc4,CN=
CN=ccauser,CN=U
CN=ccauser1-rc4,C
```

```
        1> instanceType: 0x4 = ( IT_WRITE );
        1> whenCreated: 04/03/2006 16:36:25 Pacific
Standard Time Pacific Daylight Time;
        1> whenChanged: 04/03/2006 16:36:25 Pacific
Standard Time Pacific Daylight Time;
        1> uSNCreated: 4304;
        1> uSNChanged: 4304;
        1> showInAdvancedViewOnly: FALSE;
        1> name: Users;
        1> objectGUID:
6f1d59af-f5d9-4f7b-84d2-60901b28b49c;
        1> systemFlags: 0x8C000000 = (
FLAG_DISALLOW_DELETE |
FLAG_DOMAIN_DISALLOW_RENAME |
FLAG_DOMAIN_DISALLOW_MOVE );
        1> objectCategory:
CN=Container,CN=Schema,CN=Configuration,DC=cca,DC=cis
   C=com;
        1> isCriticalSystemObject: TRUE;
        2> dSCorePropagationData: 01/16/2009 11:09:45
  ic Standard Time Pacific Daylight Time;
  0/29691/8424 21492:38:2544 UNC;
```

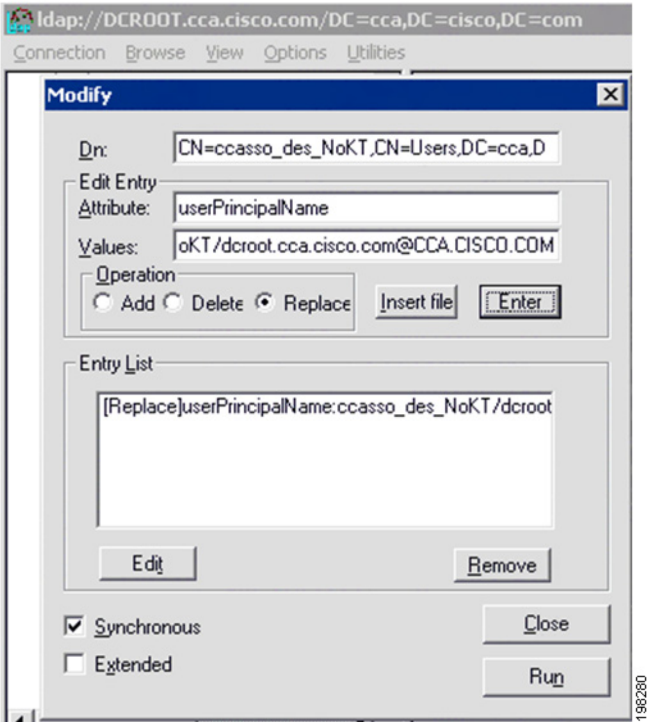
Modify an existing entries attrib

Step 10 Specify **`userPrincipalName`** in the **Attribute** field and enter a *<username>*/*<FQDN>*@*<REALM>* value. For example, enter **`ccasso_des_NoKT/dcroot.cca.cisco.com@CCA.CISCO.COM`** (Figure 8-29).

Note If there are multiple servers in the Active Directory domain, the value must be *<username>*/*<AD_domain>*@*<AD_DOMAIN>*
(e.g., **`casuser_des_NoKT/qa-test1.cca.cisco.com@QA-TEST1.CCA.CISCO.COM`**).

Step 11 Complete the change by choosing the **Replace** operation and clicking **Enter**.

Figure 8-29 Modify the userPrincipalName Attribute



Dn: CN=ccasso_des_NoKT,CN=Users,DC=cca,D

Attribute: userPrincipalName

Values: oKT/dcroot.cca.cisco.com@CCA.CISCO.COM

Operation: ○ Add ○ Delete ● Replace

[Replace]userPrincipalName:ccasso_des_NoKT/dcroot

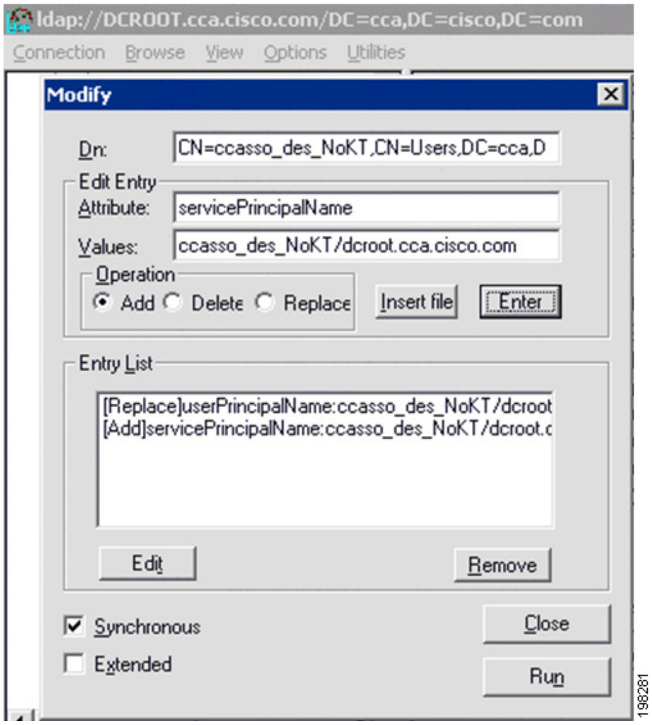
☑ Synchronous

□ Extended

Step 12 Specify **`servicePrincipalName`** in the attribute field and enter *`<username>`*`/`*`<FQDN>`*. For example, enter a **`ccasso_des_NoKT/dcroot.cca.cisco.com`** value (Figure 8-30).

Step 13 Complete the addition by choosing the **Add** operation and clicking **Enter**.

Figure 8-30 Add the servicePrincipalName Attribute



Dn: CN=ccasso_des_NoKT,CN=Users,DC=cca,D

Attribute: servicePrincipalName

Values: ccasso_des_NoKT/dcroot.cca.cisco.com

Operation: ● Add ○ Delete ○ Replace

Entry List:

[Replace]userPrincipalName:ccasso_des_NoKT/dcroot
[Add]servicePrincipalName:ccasso_des_NoKT/dcroot.c

☑ Synchronous

□ Extended

Step 14 Verify that there are two lines representing your changes in the Entry List display and click **Run**.

Step 15 Once complete, the bottom of the **Ldp** application window should display “Modified <*userDN*>” without errors.

```
Modified
“CN=ccasso_des_NoKT,CN=Users,DC=cca,DC-cisco,DC=com”.
```

Step 16 To confirm, double-click on the user account name on the left side of the application window and verify that your changes are present in the user account entry.

Configure AD SSO in a Windows 7 Client Environment

Administrators who configured AD SSO prior to Release 4.7(1) can provide only limited support for Windows 7 clients after upgrade. An unmodified Windows 7 client machine with the Cisco NAC Agent installed still prompts the user with a manual login dialog because Microsoft has disabled DES encryption on Windows 7 client machines by default.

To enable Windows 7 client machines to authenticate via AD SSO in your Cisco NAC Appliance network, you can do one of the following:

Option 1 (Recommended)

Allow AD SSO for Windows 7 by enabling additional algorithms on the Microsoft Active Directory servers (see Enable Additional Algorithms on Existing AD Servers).

Option 2 (Recommended Only for Small Client Group Testing)

Enable the DES algorithm on the Windows 7 client machines so that they can communicate via the CASs existing AD SSO DES service account configuration (see Manually Enable DES on Individual Windows 7 Client Machines).

Enable Additional Algorithms on Existing AD Servers

Step 1 Create a new AD SSO service account according to the guidelines in Add Active Directory SSO Auth Server, page 8-6. Cisco recommends that the current AD SSO account remain unchanged to allow you to quickly switch between the original DES encryption system and the this multi-algorithm option.

Step 2 Run KTPass to allow multiple algorithms for this new service account (see Table 8-2).

- For Windows 2008 Server at full functional level:

```
ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass
PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL -crypto All
```

- For Windows 2008 Server at 2003 Server functional level:

```
ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass
PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

Note Before performing the following step, Cisco strongly recommends making a backup copy of the CAS's **/perfigo/access/tomcat/conf/krb.txt** file.

After running the **ktpass** command above, manually modify two files on the CAS as follows:

- In the CAS CLI, navigate to **/perfigo/access/tomcat/conf/krb.txt** and add the following lines:

```
[libdefaults]
   kdc_timeout = 20000
   default_tkt_enctypes = RC4-HMAC
   default_tgs_enctypes = RC4-HMAC
   permitted_enctypes = RC4-HMAC
```

- Navigate to **/perfigo/access/bin/starttomcat**.

  Search for **CATALINA_OPTS**.

  Add **-DKRB_OVERRIDE=true** to the value of **CATALINA_OPTS**.

  For example:

```
Old value: CATALINA_OPTS="-server ..."
New Value: CATALINA_OPTS="-server ... -DKRB_OVERRIDE=true"
```

Note If you are applying this change to an existing HA pair, you must perform the above update on both the HA-Primary and HA-Secondary CAS just as you would upgrade a pair of HA-enabled CASs. For more information, see the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

- Restart the CAS by entering the **service perfigo stop** and **service perfigo start** commands.

- For Windows 2003 Server at full functional level:

```
ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass
PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
```

Step 3 Change the AD SSO service account on the CAM to the new service account according to the guidelines in Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos), page 8-40.

a. Log in to the CAM web console and go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

b. Modify the AD SSO account name and password.

c. Click the checkbox for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)**.

d. Click **Update**.

Manually Enable DES on Individual Windows 7 Client Machines

Step 1 Login to the Windows 7 client machine as an administrator.

Step 2 Go to Start > Control Panel > System and Security > Administrative Tools > Local Security Policy > Local Policies/Security > Options.

Step 3 Choose **Network security > Configure encryption types allowed** and enable all of the options except for the last one ("Future encryption types") by checking the boxes corresponding to each in the **Local Security Settings** tab.

Configure Active Directory for FIPS 140-2 Compliant AD SSO

This section describes how to configure your Windows Server 2008 environment to communicate with a FIPS 140-2 compliant Cisco NAC Appliance deployment. This section covers the following topics:

- Prerequisites
- Configuring Your Windows Environment for FIPS 140-2 Compliance

Prerequisites

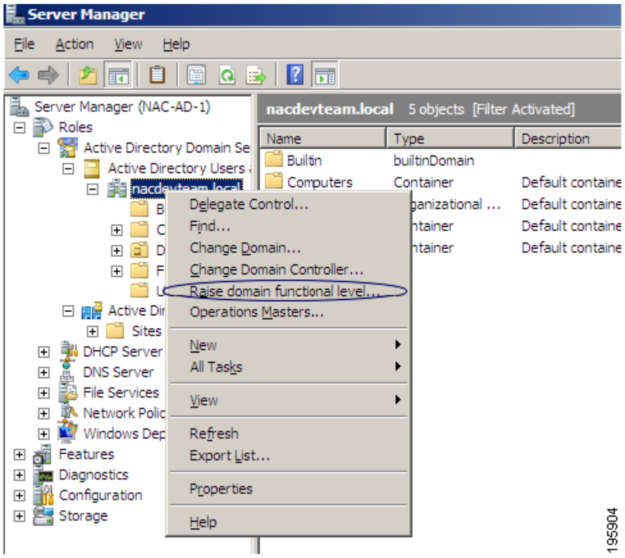
- You *must* use Windows Server 2008 with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or Windows 7 with Cisco NAC Agent version 4.7.1.15 or 4.8.0.32 installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO. (It is assumed that the user has already configured an Active Directory domain on this system.)
- The Clean Access Manager and Clean Access Server should be configured in FIPS mode and must be running Cisco NAC Appliance Release 4.7(0) or later.

Configuring Your Windows Environment for FIPS 140-2 Compliance

To set up your Windows environment for FIPS 140-2 compliant AD SSO with the Cisco NAC Appliance system:

Step 1 If the AD system is based on an upgrade from Windows Server 2003, you must raise the domain functionality to Windows Server 2008 level for Cisco NAC appliance to operate in FIPS mode, as shown in Figure 8-31. Without this you will not be able connect to the Cisco NAC Appliance network.

Figure 8-31 Update the Domain Functional Level

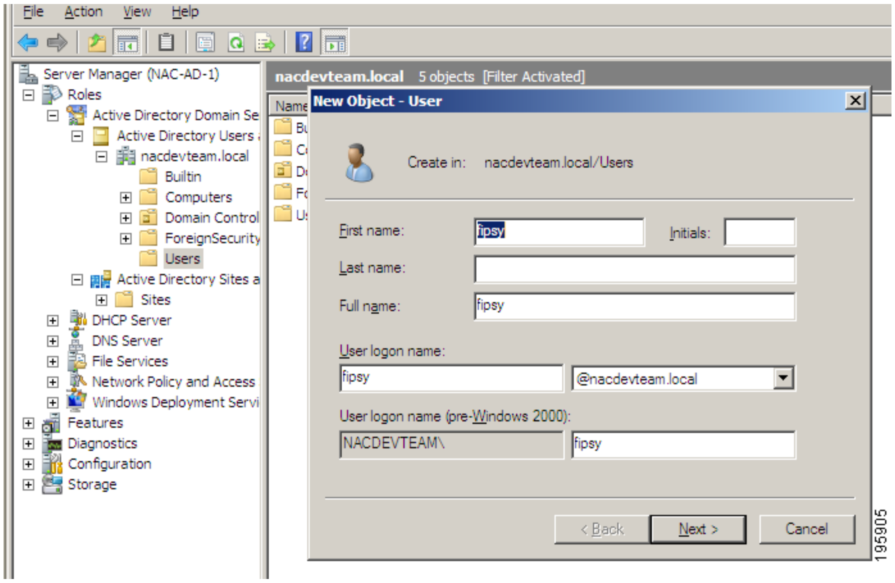


Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default containe
	ganizational ...	Default containe
	ntainer	Default containe
	ntainer	Default containe

Configure the User Profile

Step 2 Create the user in Windows. The example in this procedure uses the name “fipsy.”

Figure 8-32 Create a New User



Create in: nacdevteam.local/Users

First name: fipsy

Initials:

Last name:

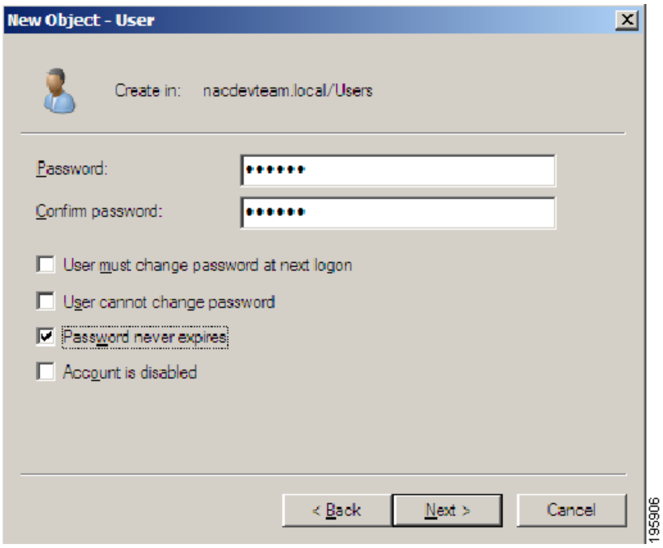
Full name: fipsy

User logon name: fipsy @nacdevteam.local

User logon name (pre-Windows 2000): NACDEVTEAM\ fipsy

Step 3 Ensure you click the **Password never expires** option and leave the other user options unchecked (especially, ensure that you *do not* require the password to be changed on first login).

Figure 8-33 New User Settings



Create in: nacdevteam.local/Users

Password: ••••••

Confirm password: ••••••

☐ User must change password at next logon

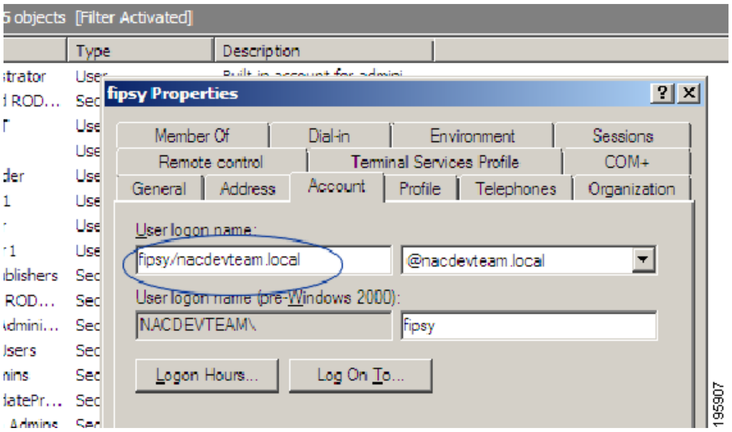
☐ User cannot change password

☑ Password never expires

☐ Account is disabled

Step 4 Open the user Properties and update the username to include the domain, as shown in Figure 8-34.

Figure 8-34 User Properties

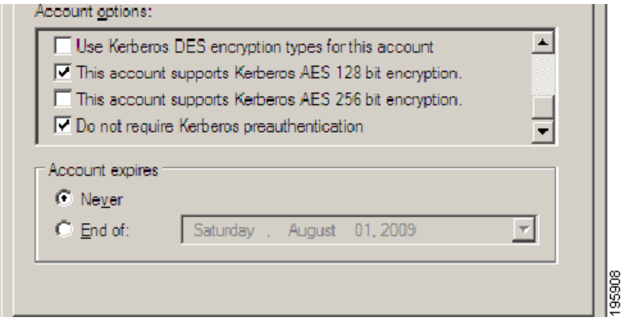


User logon name:
fipsy/nacdevteam.local @nacdevteam.local

User logon name (pre-Windows 2000):
NACDEVTEAM\ fipsy

Step 5 Specify Account Options as shown in Figure 8-35.

Figure 8-35 Specify Account Options



Account options:

□ Use Kerberos DES encryption types for this account
☑ This account supports Kerberos AES 128 bit encryption.
□ This account supports Kerberos AES 256 bit encryption.
☑ Do not require Kerberos preauthentication

Account expires
● Never
○ End of: Saturday , August 01, 2009

Step 6 Ensure you have Administrator privileges on the client machine and open a CMD prompt. Verify whether or not KTPass is available by entering **ktpass** at the CMD prompt. If KTPass is not available, navigate to the **\Windows\System32\** directory and try again.

Note KTPass is available on Windows 2008 Server by default.

Step 7 Run the KTPass command as follows:

```
ktpass -princ fipsy/nac-ad-1.nacdevteam.local@NACDEVTEAM.LOCAL -mapuser fipsy -pass
Pass1234
-out c:\fipsy.keytab -ptype KRB5_NT_PRINCIPAL -crypto AES128-SHA1
```

Step 8 Configure the Clean Access Server for AD SSO, as described in Configure AD SSO on the CAS, page 8-11.

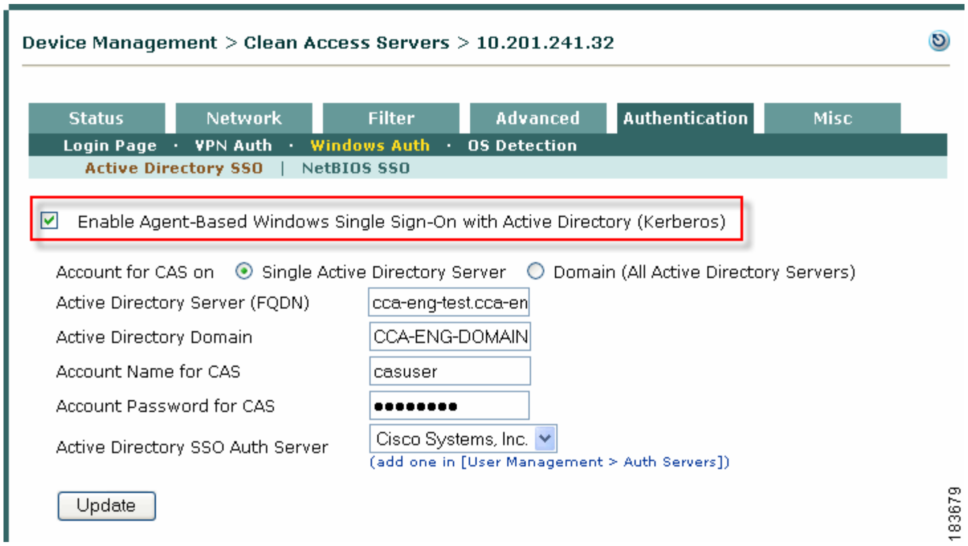
Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

After the AD server configuration is completed, perform the final step.

To enable the Agent-Based Windows single sign-on with Active Directory (AD), follow these steps:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

Figure 8-36 Active Directory SSO


Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO
Update
183679

Device Management > Clean Access Servers > 10.201.241.32

☑ Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on ● Single Active Directory Server ○ Domain (All Active Directory Servers)

Active Directory Server (FQDN): cca-eng-test.cca-en

Active Directory Domain: CCA-ENG-DOMAIN

Account Name for CAS: casuser

Account Password for CAS: ••••••••

Active Directory SSO Auth Server: Cisco Systems, Inc.
(add one in [User Management > Auth Servers])

Step 2 Click the checkbox for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)**.

Step 3 Click **Update**.

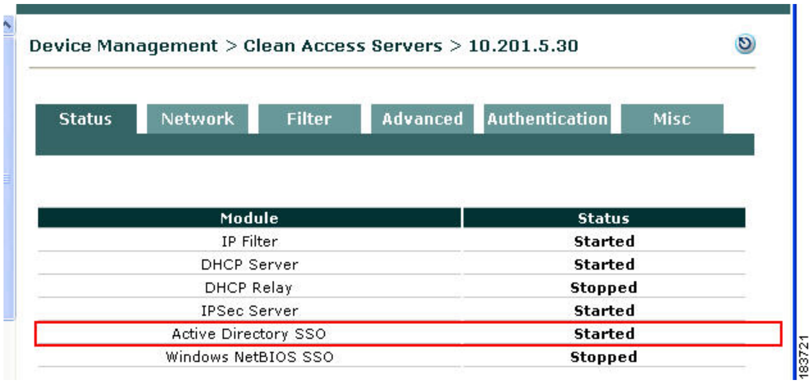
Note See Configure AD SSO on the CAS, page 8-11 for further details on **Active Directory SSO** page fields.

Confirm Active AD SSO Service

Once you have performed all the configuration outlined in AD SSO Configuration Step Summary, page 8-5, make sure the AD SSO service starts on the Clean Access Server.

Go to **Device Management > CCA Servers > Manage [CAS_IP] > Status** (see Figure 8-37).

Figure 8-37 AD SSO Service Is Started



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

Make sure **Active Directory SSO** is listed with a Status of **Started**.

Note You can also confirm that the CAS trusted interface (eth0) is listening on TCP port 8910 (used for Windows SSO) via SSH command: `netstat -a | grep 8910`.

Enable GPO Updates

When a user is not yet authenticated/certified by Cisco NAC Appliance (or is on the Authentication VLAN), access to the Windows Domain Controller is limited; and as a result, a complete group policy update might not finish. In addition, the next refresh for group policies occurs every 90 minutes by default. In order to accomplish a GPO update, administrators can force a group policy refresh for Agent users immediately after AD SSO login by enabling the **Refresh Windows domain group policy after login** option.

Administrators can configure the Agent to retrigger a Group Policy Object (GPO) update after the AD SSO user login finishes. If configured in the CAM web console, the Agent calls the "gpupdate" command to re-trigger the Group Policy update after users are logged in.

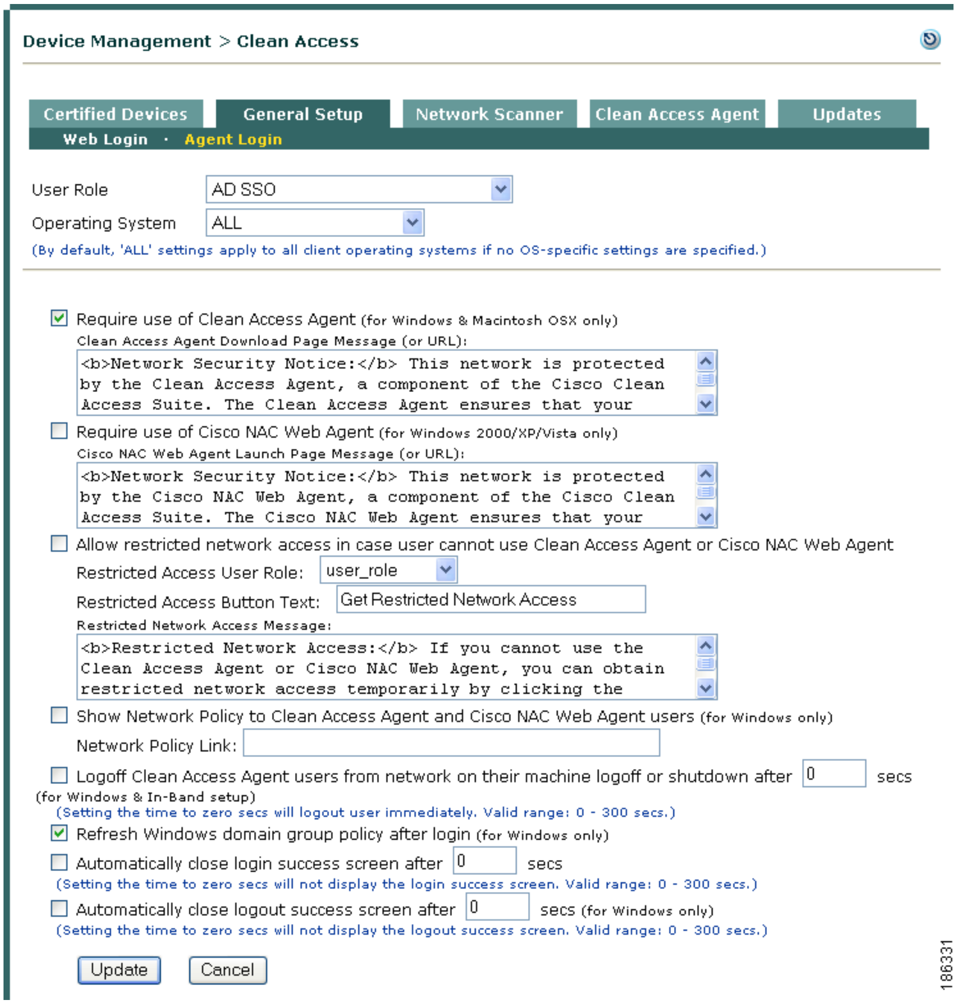
Login scripts are controlled by the Domain Controller and require a login event to run. For more information about how to use login script in a Windows environment, see Enabling a Login Script (Optional), page 8-43.

Note Because Microsoft Group Policies are only available since the advent of Active Directory (Windows 2000 and later), the GPO trigger update feature is only available on Windows 7/Vista/XP machines.

To enable GPO update, follow these steps:

Step 1 Go to **Device Management > Clean Access > General Setup > Agent Login**.

Figure 8-38 Agent Login—General Setup



User Role: AD SSO

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

☑ Require use of Clean Access Agent (for Windows & Macintosh OSX only)

Clean Access Agent Download Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Clean Access Agent, a component of the Cisco Clean
Access Suite. The Clean Access Agent ensures that your
```

□ Require use of Cisco NAC Web Agent (for Windows 2000/XP/Vista only)

Cisco NAC Web Agent Launch Page Message (or URL):

```
<b>Network Security Notice:</b> This network is protected
by the Cisco NAC Web Agent, a component of the Cisco Clean
Access Suite. The Cisco NAC Web Agent ensures that your
```

□ Allow restricted network access in case user cannot use Clean Access Agent or Cisco NAC Web Agent

Restricted Access User Role: user_role

Restricted Access Button Text: Get Restricted Network Access

Restricted Network Access Message:

```
<b>Restricted Network Access:</b> If you cannot use the
Clean Access Agent or Cisco NAC Web Agent, you can obtain
restricted network access temporarily by clicking the
```

□ Show Network Policy to Clean Access Agent and Cisco NAC Web Agent users (for Windows only)

Network Policy Link:

□ Logoff Clean Access Agent users from network on their machine logoff or shutdown after 0 secs (for Windows & In-Band setup)

(Setting the time to zero secs will logout user immediately. Valid range: 0 - 300 secs.)

☑ Refresh Windows domain group policy after login (for Windows only)

□ Automatically close login success screen after 0 secs

(Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)

□ Automatically close logout success screen after 0 secs (for Windows only)

(Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)

Step 2 From the **User Role** dropdown, choose the role to which to apply the GPO update.

Step 3 From the **Operating System** dropdown, choose the OS to which to apply the GPO update (must be Windows XP or later).

Step 4 Click the checkbox for **Refresh Windows domain group policy after login (for Windows).**

Step 5 Click **Update**.

Enabling a Login Script (Optional)

Caution This step is optional and this section provides reference information for convenience only. Cisco Technical Assistance Center (TAC) does not support questions or troubleshooting for Microsoft login scripts. Refer to http://support.microsoft.com for additional support.

GPO update objects, such as login scripts, require an event to trigger them, such as login, or they fail. Running a script in a Windows environment prior to login fails because users do not have access to drive mappings to the AD server or drive resources.

Network-based login scripts and local login scripts are handled differently:

- Local login scripts run locally on a client machine. If you introduce an artificial delay with a script, they work correctly.
- Network-based scripts require continuous access to a AD server for initialization. Depending on your network deployment, you can use a combination of steps to use them. Network-based scripts typically reside on the AD server in the %Sysvol%\scripts folder.

Table 8-4 lists the options for handling network-based scripts.

Table 8-4 Network-Based Login Script Options

Deployment	Option
In Band	Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.
Out-of-Band without IP change	Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.
Out-of-Band with IP change	Use a combination of scripts to copy a script that introduces delay locally, run it, and then delete it. **Note** A security concern exists while the script resides on the client machine because it can be viewed or copied.

In any type of deployment, you need to create an artificial delay script to run during authentication in order for local or network-based scripts to work correctly. See Introducing a Delay to Allow Script Use, page 8-44.

For network-based script use in Out-of-Band deployments with IP address changes, you must also:

- Append the delete command to the end of the “delay” script.
- Use a reference script that copies the “delay” script to the client machine and then launches it.

For more information, see Using Network-Based Scripts in Out-of-Band Mode with IP Address Changes, page 8-45.

Introducing a Delay to Allow Script Use

You can introduce delay by calling a persistent check action that fails until authentication finishes. For example, you can use ping, Telnet, nslookup, or another action that requires network connectivity to succeed. The following example is a .bat script, but you can use other types of scripts.

When using ping, remember:

- You can ping any IP address that is reachable after successful Cisco NAC Appliance login.
- The IP address used for the ping and the AD server do not have to be the same.

Caution If you ping a protected device that has a real IP address, the user will be able to see the IP address while the delay script runs. You can add a statement to the script to hide the DOS window.

- You only need one IP address.
- All of your mappings can be assigned after the ping succeeds.

Example

```
:CHECK
@echo off
echo Please wait...
ping -n 1 -l 1 192.168.88.128
if errorlevel 1 goto CHECK
@echo on
netuse L:\\192.168.88.128\Scripttest
```

In the example, ping runs in the background until it succeeds. After succeeding, the loop is broken; the system maps to drive L:\ on the same node, where the network-based script resides, and then that script runs. The user sees a DOS window in the background.

Note You can enhance the script with statements to hide or minimize the DOS window from the user.

Table 8-5 lists the script statements and meanings.

Table 8-5 Reference Script Statements and Meaning

Statement	Meaning
`:CHECK`	Begin the script.
`@echo off`	Only display the command output.
echo Please wait...	Show the words “Please wait...” to the end user.
`ping -n 1 -l 1 192.168.88.128`	Use the ping utility to check if the IP address 192.168.88.128 is reachable: **-n**—do not look up a hostname. **1**—send one packet. **-l**—use the ODBC driver or library. **1**—wait one second.
`if errorlevel 1 goto CHECK`	If the ping utility did not reach 192.168.88.128 successfully, then start again from :CHECK.

Table 8-5 Reference Script Statements and Meaning (continued)

Statement	Meaning
`@echo on`	Display debug messages.
`netuse L:\\192.168.88.128\Scripttest`	Map the file share at 192.168.88.128 to the L: drive.

Using Network-Based Scripts in Out-of-Band Mode with IP Address Changes

In Out-of-Band mode with an IP address change, you need to create and run two scripts before calling the targeted network-based script:

- A reference script to copy over and launch the local copy of the script.
- A delay script with a line added to delete the network script after it runs.

Caution Copying a network script to a user machine that has not been granted network access is a security concern. While the script resides on the user machine, the user can copy or view the script.

Reference Script

Create a script similar to the following example. The script is named "refer.bat", and it copies over a delay script named "actual.bat" and then launches it.

```
@echo off
echo Please wait...
copy \\192.168.88.228\notlogon\actual.bat actual.bat
actual.bat
```

Table 8-6 lists the script statements and the meaning of each line.

Table 8-6 Reference Script Statements and Meaning

Statement	Meaning
`@echo off`	Only display the command output.
echo Please wait...	Show the words "Please wait..." to the end user.
`copy \\192.168.88.228\notlogon\actual.bat actual.bat`	Copy the script "actual.bat" from the "notlogon" folder on the AD server at IP address 192.168.88.228.
`actual.bat`	Launch the script named "actual.bat".

Delay Script with Delete Command

To create a script that delays script initialization, refer to the "Introducing a Delay to Allow Script Use" section on page 8-44. As shown in the following example add the **del** command and the name of the script that you want to delete to the end of the delay script. The script is named "actual.bat".

Caution We recommend that you reduce network vulnerability by deleting the local copy of the script residing on the end user machine. The last line of the sample script performs the deletion or clean up function.

Example

```
:CHECK
@echo off
echo Please wait...
ping -n 1 -l 1 192.168.88.128
if errorlevel 1 goto CHECK
@echo on
netuse L:\\192.168/88/128/Scripttest
del actual.bat
```

Add LDAP Lookup Server for Active Directory SSO (Optional)

Note The LDAP Lookup server is only needed if you want to configure mapping rules so that users are placed into user roles based on AD attributes after AD SSO authentication. For basic AD SSO without role mapping, or for testing purposes, it is not necessary to configure an LDAP Lookup Server.

If you plan on mapping Windows domain SSO users to multiple user roles, you will need to configure a secondary LDAP Lookup server so that the CAM can perform the mapping. You then specify this LDAP Lookup server for the Active Directory SSO auth provider, as described in Add Active Directory SSO Auth Server, page 8-6. You can configure your LDAP Lookup server to use one of the following two authentication mechanisms:

- **SIMPLE**—The CAM and LDAP server pass user ID and password information between themselves without encrypting the data.
- **GSSAPI**—(Generic Security Services Application Programming Interface) Provides an option to encrypt user ID and password information passed between the CAM and the specified LDAP server to help ensure privacy.

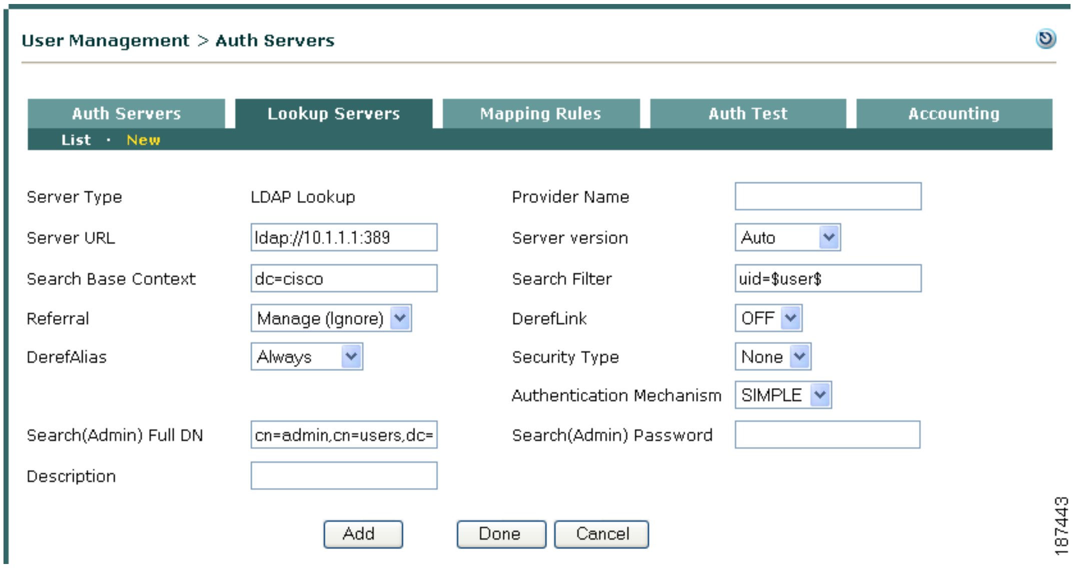
Note To ensure complete DNS capability when using GSSAPI, you must ensure that all Domain Controllers, child domains, and hosts conform to strict DNS naming conventions and that you have the ability to perform both forward- and reverse-DNS.

In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See the “Kerberos” section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for more information.

Configure an LDAP Lookup Server

Step 1 Go to **User Management > Auth Servers > Lookup Servers**. The **Server Type** is automatically set to **LDAP Lookup**.

Figure 8-39 Lookup Server (LDAP)—SIMPLE Authentication Method



Server Type	LDAP Lookup	Provider Name	
Server URL	ldap://10.1.1.1:389	Server version	Auto
Search Base Context	dc=cisco	Search Filter	uid=$user$
Referral	Manage (Ignore)	DerefLink	OFF
DerefAlias	Always	Security Type	None
		Authentication Mechanism	SIMPLE
Search(Admin) Full DN	cn=admin,cn=users,dc=	Search(Admin) Password	
Description			

The configuration page for the LDAP Lookup Server features the same fields as the LDAP Authentication Provider configuration page. For complete details on configuring SIMPLE and GSSAPI authentication methods, refer to the "LDAP" configuration section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Cross-Forest Group Mapping using LDAP Lookup

Step 1 Set up a bidirectional trust between two AD forests.

Step 2 Create an LDAP Lookup Server with **GSSAPI** in the CAM Web Console.

Step 3 In the **Base/Realm Mapping** field, specify the base context and realm mapping of the AD forest. For example, if the realm of the first AD forest is CCA.CISCO.COM and other AD forest is NAC.PERFIGO.COM respectively, the base/realm mapping will be as follows:

dc=cca,dc=cisco,dc=com/CCA.CISCO.COM

dc=nac,dc=perfigo,dc=com/NAC.PERFIGO.COM

Step 4 Create an ADSSO server with the LDAP Lookup server.

You can use the **Auth Test** function to test AD SSO authentication in Cisco NAC Appliance. For details, see the "Auth Test" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

In the **Auth Test** tab, the realm name must be entered in addition to the username. For example, if the username is **nacuser** and the realm is **NAC.PERFIGO.COM**, then you must enter **nacuser@NAC.PERFIGO.COM**.

You can test with users available in either or both the AD forests.

Troubleshooting

General

- Make sure the date and time of the CAM, CAS, and AD server are all synchronized within 5 minutes of each other or AD SSO will not work. You will have to delete the account on AD, synchronize the times and recreate the account. If the AD server still keeps a record of the old account even though you have deleted it, you may need to create a new account with a different name.
- When setting up the CAS account on the AD server, make sure that the CAS account does not require Kerberos pre-authentication.
- In OOB deployments, ICMP (ping) is used to find the "closest AD server" by the workstation, and *must* work to all AD servers referenced in sites and services for the Authentication VLAN(s), or all AD servers in the domain if sites and services has not been set up.
- In a NAT environment, ensure that the CAM is configured with the NAT entry, for the AD SSO to work properly.

Note Perform a **`service perfigo restart`** on the CAS to make sure it is not using old cached credentials.

KTPass Command

- Make sure the AD domain name (for multiple servers) or single AD server name you enter between "/" and "@" in the KTPass command (e.g. "AD_DomainServer") exactly matches case-by-case the domain or single AD server name as it appears under **Control Panel > System > Computer Name | Full computer name**. See Run the ktpass.exe Command, page 8-22 for details.
- Make sure you enter the realm name after "@" (e.g. "AD_DOMAIN") in the KTPass command in all **upper case characters**. You must convert the Domain name that appears under **Control Panel > System > Computer Name | Domain** on the AD server to UPPER CASE when entering it in the KTPass command.

Cannot Start AD SSO Service on CAS

If the AD SSO service cannot start on the CAS, this typically indicates a communication issue between the AD server and the CAS.

- If the Active Directory server is not reachable from the CAS at the time of CAS startup, AD SSO service is not started. As a workaround, the administrator must go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO** and click the **Update** button to restart the AD SSO service.

- Check that the KTPass command is run correctly. Verify the fields are correct as described in Run the ktpass.exe Command, page 8-22. If KTPass was run incorrectly, delete the account, create a new account on the AD server, and run KTPass again.
- Make sure the time on the CAS is synchronized with the AD server. This can be done by pointing them both to the same time server (or, in lab setups by just pointing the CAS to the AD server itself for time (AD server runs Windows time)). Kerberos is sensitive to clock timing and the clock skew cannot be greater than 5 minutes (300 seconds).
- Make sure the Active Directory Domain is in UPPERCASE (Realm) and that the CAS can resolve the FQDN in DNS. (For lab setups you can point to a AD server that runs DNS, as AD requires at least one DNS server).
- Make sure the following are correct: CAS username on the AD server, Active Directory Domain (Kerberos Realm) on the CAS (uppercase), Active Directory Server (FQDN) on the CAS.
- When creating a TAC support case, login to CAS directly at **https://<CAS_IP-address>/admin**, click on Support Logs and change the logging level for Active Directory communication logging to “INFO”. Recreate the problem and download support logs. Make sure to restart the CAS or change the log level back to the default after the support logs are downloaded. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for further details.

AD SSO Service Starts, But Client Not Performing SSO

If AD SSO service is started on the CAS, but the client machine is not performing Windows Single Sign-On, this typically indicates a communication issue between the AD server and client PC or between the client PC and the CAS. Check that:

- The client does have Kerberos keys.
- Ports are open in the Unauthenticated role to the AD server so that the client can connect.

Note When you test, Cisco recommends first opening complete access to the AD server/DC, then restricting ports once AD SSO is working. When logging into the client PC, make sure to log into the domain using Windows domain credentials (not Local Account).

- The client PC time/clock is synchronized with the AD server.
- The CAS trusted interface (eth0) is listening on TCP port 8910. A sniffer trace on the client PC can help.
- The user is logged in using the Windows domain account and not the local account.

Note The CAS and Agent do not support using multiple NICs on the client machine. The client machine Wireless NIC must be turned OFF when the Wired NIC is turned ON.

Kerbtray

Kerbtray is a free tool available from Microsoft Support Tools that can be used to confirm that the client has obtained the Kerberos Tickets (TGT and ST), and can also be used to purge Kerberos Tickets on a client machine. The ST (Service Ticket) is of concern for the CAS user account that is created on the AD Server. A green Kerbtray icon on the system tray indicates that the client has active Kerberos tickets. However the ticket needs to be verified as correct (valid) for the CAS user account.

Note AD SSO fails in Cisco NAC Appliance when the CAS and Cisco NAC Agent attempt to exchange Kerberos tickets with the AD domain that are larger than 16kB.

CAS Log Files

Note The log file of interest on the CAS is **/perfigo/access/tomcat/logs/nac_server.log**.

If AD SSO Service does not start on CAS, this indicates a CAS-AD server communication issue:

- Clock is not synchronized between CAS and the Domain Controller:

```
SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37)
Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
```

- Username is incorrect. Note the wrong username "ccass," error code 6 and the last warning:

```
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos
database (6)
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
WARNING: GSSServer loginSubject could not be created.
```

- Password is incorrect or Realm is invalid (e.g. not uppercase, bad FQDN, or KTPass run incorrectly). Note error code 24 and last warning:

```
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
SEVERE: startServer - SSO Service authentication failed. Pre-authentication
information was invalid (24)
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
WARNING: GSSServer loginSubject could not be created.
```

The following error indicates a client-CAS communication issue, seen when the client PC's time is not synchronized with AD server. (Note the difference between this error and the one in which the CAS time is not synchronized with the AD server.)

```
Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew
too great (37))
```

"Integrity check on decrypted field failed" Error

If AD SSO is not working, and the CAS logs show a "SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Integrity check on decrypted field failed (31))" message, check the account name/password in the AD configuration and KTPass command.

The CAS typically returns error messages such as "Integrity check on decrypted field failed" when the password or key is incorrect. For example, this error could appear if you run KTPass on the same account existing on multiple AD servers. Executing the KTPass command again on a new account from a single AD server should resolve the issue.

CHAPTER 9

Local Authentication Settings

This chapter describes **Authentication** tab settings in the CAS management pages (other than **VPN Auth** settings which are described in Chapter 6, "Integrating with Cisco VPN Concentrators"). Topics include:

- Overview, page 9-1
- Local Heartbeat Timer, page 9-1
- Local Login Page, page 9-3
- Enable Active Directory SSO Login, page 9-7
- Enable Windows NetBIOS SSO Login, page 9-8
- OS Detection, page 9-9

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 an 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.

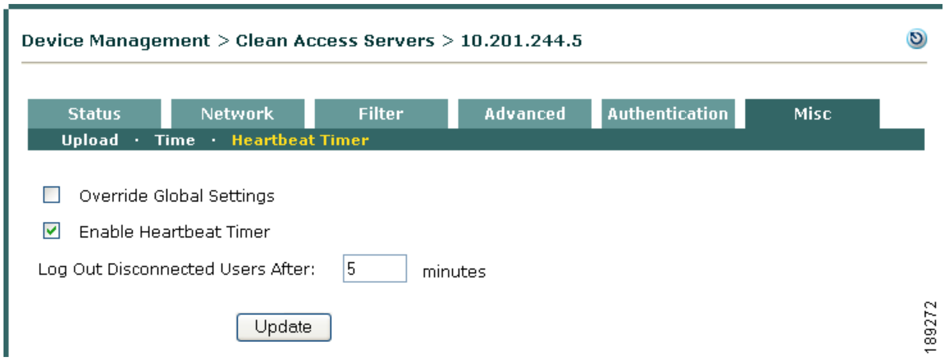
The timer is configurable globally when accessed from **User Management > User Roles > Schedule > Heartbeat Timer**. By configuring a local setting in the Clean Access Server, you can override the global setting in the Clean Access Manager for that particular CAS.

Note For information on user session Heartbeat Timer capabilities and behavior, see the "Configure User Session and Heartbeat Timeouts" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

To configure timeout properties based on connection status:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Heartbeat Timer**.

Figure 9-1 Local Heartbeat Timer


Device Management > Clean Access Servers > 10.201.244.5
Status
Network
Filter
Advanced
Authentication
Misc
Upload · Time · Heartbeat Timer
Update
189272

☐ Override Global Settings

☑ Enable Heartbeat Timer

Log Out Disconnected Users After: 5 minutes

Step 2 To override the global setting configured using the **User Management > User Roles > Schedule > Heartbeat Timer** web console page, click the **Override Global Settings** checkbox. The global heartbeat timer setting is overridden for user sessions established using this specific CAS.

Step 3 Click the **Enable Heartbeat Timer** checkbox.

Note If the CAS enters Fallback mode and this option is enabled, user sessions are still terminated and cleared from the Online Users List and Certified Devices List after the specified time period has passed. For more information, see CAS Fallback Policy, page 4-44.

Step 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.

Step 5 Click **Update**.

For complete details on user session timeouts, see the "User Management: Traffic Control, Bandwidth, Schedule" chapter in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

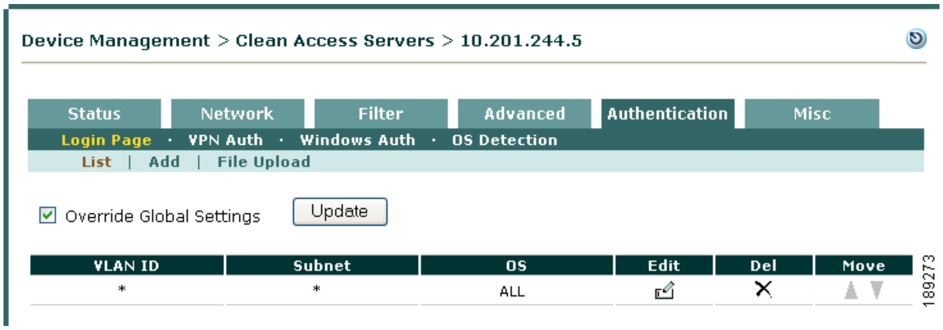
Local Login Page

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 9-2 Override Global Login Page



Device Management > Clean Access Servers > 10.201.244.5

☑ Override Global Settings

VLAN ID	Subnet	OS	Edit	Del	Move
*	*	ALL	✎	✕	▲▼

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 an 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.

DHCP IP addresses can be refreshed for client machines using the Agent or ActiveX Control/Java Applet without requiring port bouncing after authentication and posture assessment. This feature is intended to facilitate NAC Appliance OOB deployment in VoIP environments.

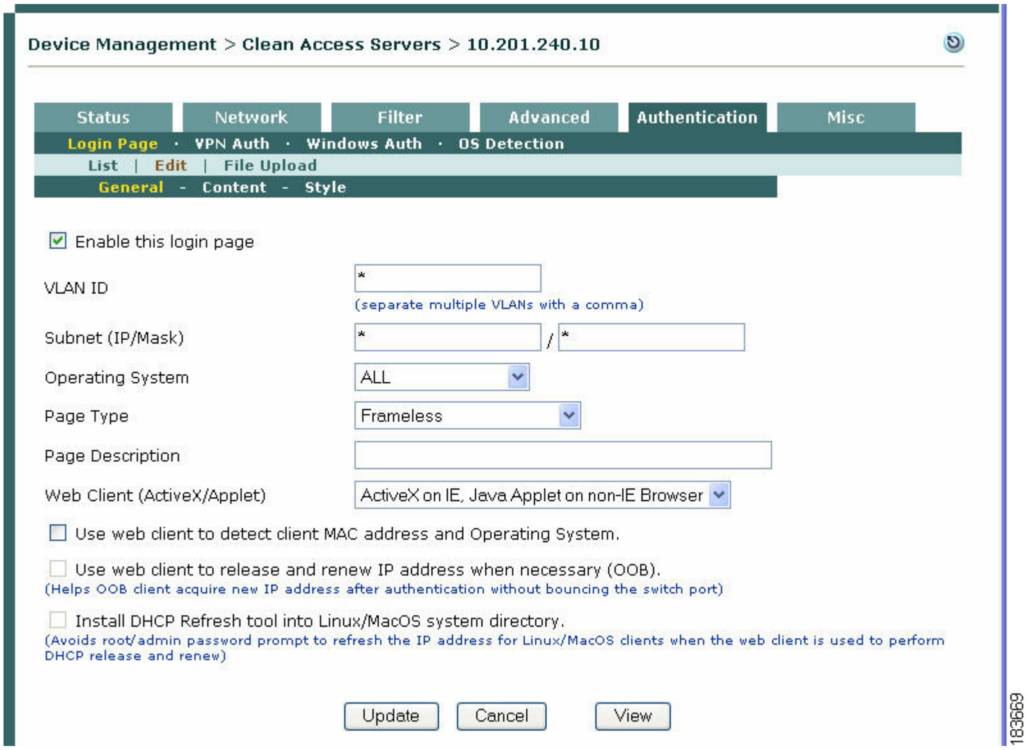
Note For complete details, refer to "Configuring User Login Page and Guest Access" in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

For detailed information on Access to Authentication VLAN change detection, refer to the "Configuring Access to Authentication VLAN Change Detection" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

To enable the web client:

Step 1 Go to **Administration > User Pages > Login Page > Edit | General**.

Figure 9-3 Enable ActiveX/Java Applet for L3 OOB


Device Management > Clean Access Servers > 10.201.240.10
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
List | Edit | File Upload
General - Content - Style
Update
Cancel
View
183669

☑ Enable this login page

VLAN ID: *
(separate multiple VLANs with a comma)

Subnet (IP/Mask): * / *

Operating System: ALL

Page Type: Frameless

Page Description:

Web Client (ActiveX/Applet): ActiveX on IE, Java Applet on non-IE Browser

□ Use web client to detect client MAC address and Operating System.

□ Use web client to release and renew IP address when necessary (OOB).
(Helps OOB client acquire new IP address after authentication without bouncing the switch port)

□ Install DHCP Refresh tool into Linux/MacOS system directory.
(Avoids root/admin password prompt to refresh the IP address for Linux/MacOS clients when the web client is used to perform DHCP release and renew)

Step 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, ActiveX is preferred because it runs faster than the Java Applet.

- **ActiveX Only**—Only runs ActiveX. If ActiveX fails, does not attempt to run Java Applet.
- **Java Applet Only**—Only runs Java Applet. If Java Applet fails, does not attempt to run ActiveX.
- **ActiveX Preferred**—Runs ActiveX first. If ActiveX fails, attempts to run Java Applet.
- **Java Applet Preferred**—Runs Java Applet first. If Java Applet fails, attempts to run ActiveX.

- **ActiveX on IE, Java Applet on non-IE Browser** (Default)—Runs ActiveX if Internet Explorer is detected, and runs Java Applet if another (non-IE) browser is detected. If ActiveX fails on IE, the CAS attempts to run a Java Applet. For non-IE browsers, only the Java Applet is run.

Step 3 Two options need to be checked to use the ActiveX/Applet web client to refresh the client's IP address:

a. Click the checkbox for **Use web client to detect client MAC address and Operating System**.

b. 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.

Note This option can introduce unpredictable results for OOB clients if not configured correctly for your specific network topology. For detailed information on Access to Authentication VLAN change detection, refer to the "Configuring Access to Authentication VLAN Change Detection" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Step 4 When you enable web client use for IP address release/renew, for Linux/Mac OS X clients, you can optionally click the **Install DHCP Refresh tool into Linux/Mac OS system directory** checkbox. This will install a DHCP refresh tool on the client to avoid the root/admin password prompt when IP address is refreshed.

Step 5 Click **Update** to save settings.

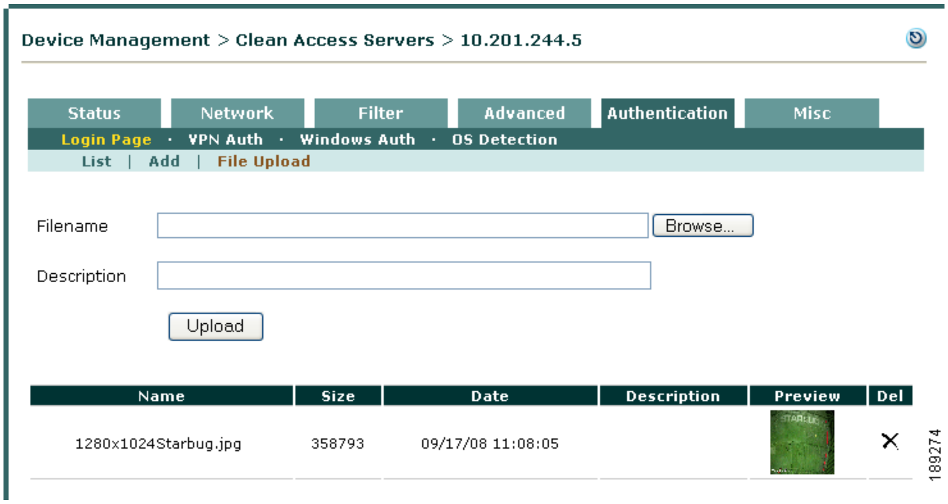
Note To use this feature. "Enable L3 support" must be enabled under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.

See Chapter 3, "Configuring Layer 3 Out-of-Band (L3 OOB)" and the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* 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 9-4 Upload Local File to CAS


Device Management > Clean Access Servers > 10.201.244.5
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
List | Add | File Upload
Browse...
Upload
189274

Filename

Description

Name	Size	Date	Description	Preview	Del
1280x1024Starbug.jpg	358793	09/17/08 11:08:05			✕

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] > Authentication > 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/data/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 Configuration Guide, Release 4.8(1)* for further details.

Enable Active Directory SSO Login

See Chapter 8, "Configuring Active Directory Single Sign-On (AD SSO)" 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. Cisco recommends configuring Active Directory SSO instead. Refer to the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details.

Implementing Windows NetBIOS SSO login involves several steps:

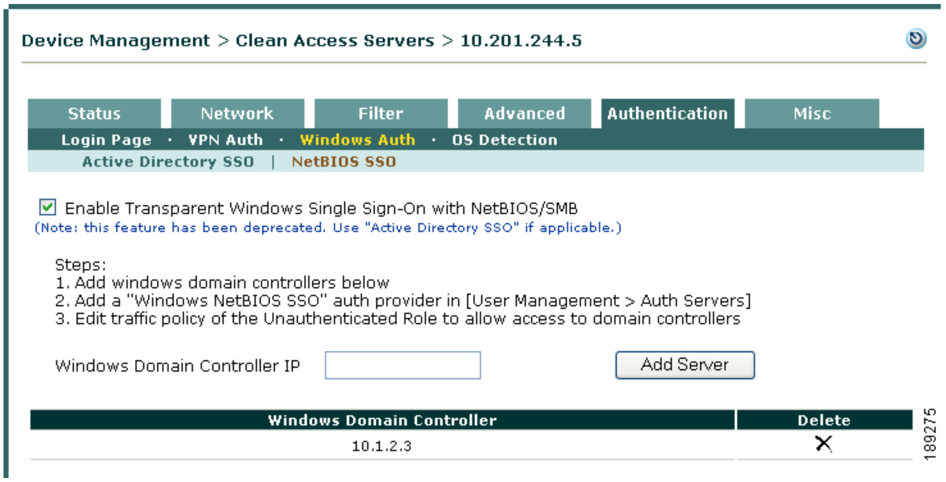
1. Add a Windows NetBIOS SSO authentication provider to the list of authentication servers in the CAM.
(See the "User Management: Auth Servers" chapter in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.)
2. Modify the policy of the Unauthenticated role to allow users access to the domain controller.
(See the "User Management: Traffic Control, Bandwidth, Schedule" chapter in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.)
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:

Step 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 9-5 Enable Transparent Windows Login


Device Management > Clean Access Servers > 10.201.244.5
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
Active Directory SSO | NetBIOS SSO
Add Server
189275

☑ Enable Transparent Windows Single Sign-On with NetBIOS/SMB
(Note: this feature has been deprecated. Use "Active Directory SSO" if applicable.)

Steps:
1. Add windows domain controllers below
2. Add a "Windows NetBIOS SSO" auth provider in [User Management > Auth Servers]
3. Edit traffic policy of the Unauthenticated Role to allow access to domain controllers

Windows Domain Controller IP

Windows Domain Controller	Delete
10.1.2.3	✕

Step 2 Click the **Enable Transparent Windows Single Sign-On with NetBIOS** checkbox and then click **Update**.

Step 3 Type the IP address of your Windows domain controller in the **Windows Domain Controller IP** field.

Step 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 Configuration Guide, Release 4.8(1)* 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.

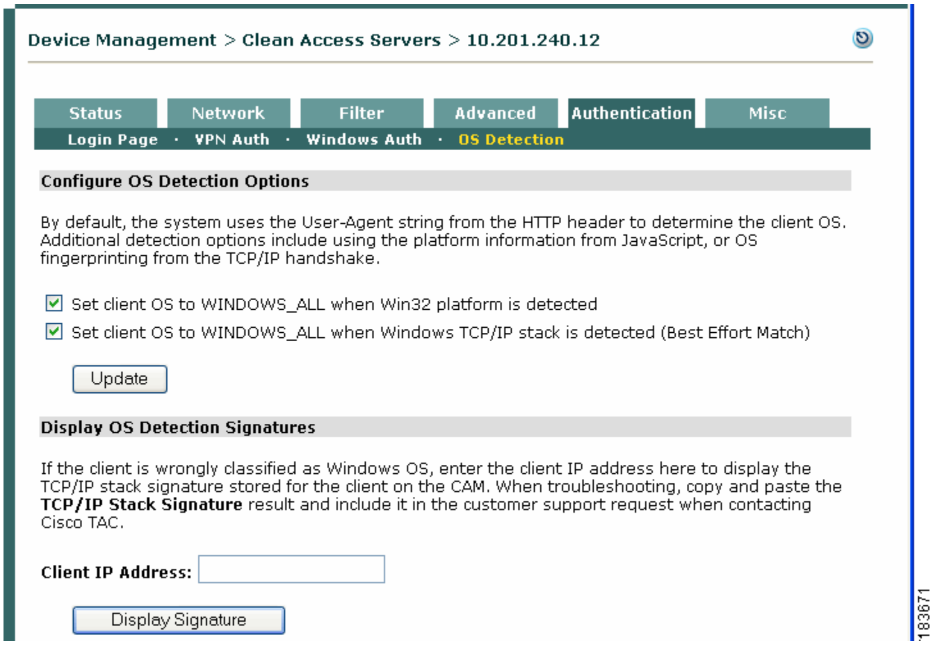
Note

- 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 Agent on client machines or requiring users to log in using the Cisco NAC Web Agent.
- The OS Detection feature supports OS fingerprinting for Windows operating systems only. For example, Cisco NAC Appliance can detect and block a Windows OS disguised as another OS (e.g. Linux, Mac OS X); however it will not support detecting a Mac OS X disguised as Linux.
- In a FIPS 140-2 compliant network where both the CAMs and CASs are configured in failover mode, Cisco NAC Appliance does not correctly report the operating system of a client machine following a failover event and subsequent synchronization. Once the CAM/CAS detect client HTTP/HTTPS traffic, the CAM/CAS are able to "rediscover" the client machine operating system following the failover event.

To Set OS Detection Settings:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection** in the CAS management pages of the web console.

Figure 9-6 OS Detection



Device Management > Clean Access Servers > 10.201.240.12
Status
Network
Filter
Advanced
Authentication
Misc
Login Page · VPN Auth · Windows Auth · OS Detection
183671

Configure OS Detection Options

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. Additional detection options include using the platform information from JavaScript, or OS fingerprinting from the TCP/IP handshake.

☑ Set client OS to WINDOWS_ALL when Win32 platform is detected

☑ Set client OS to WINDOWS_ALL when Windows TCP/IP stack is detected (Best Effort Match)

Update

Display OS Detection Signatures

If the client is wrongly classified as Windows OS, enter the client IP address here to display the TCP/IP stack signature stored for the client on the CAM. When troubleshooting, copy and paste the **TCP/IP Stack Signature** result and include it in the customer support request when contacting Cisco TAC.

Client IP Address:

Display Signature

Step 2 Click the checkbox for **Set client OS to WINDOWS_ALL when Win32 platform is detected** to add this as an additional detection option.

Step 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.

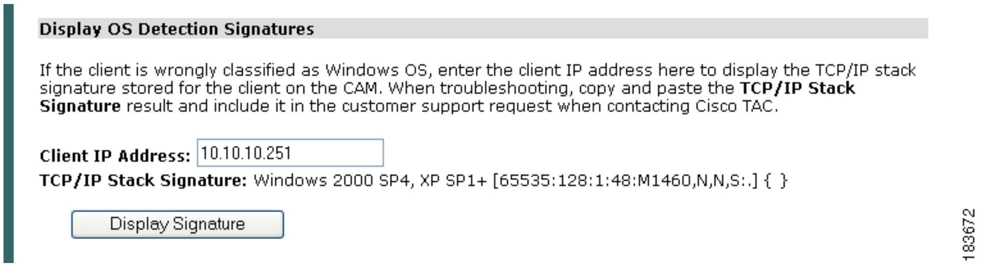
Step 4 Click **Update**.

When troubleshooting, the TCP/IP Stack Signature result can copied/pasted for inclusion in the customer support request when contacting Cisco TAC.

To Troubleshoot OS Detection Signatures:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection**.

Figure 9-7 Display TCP/IP Stack Signature



Display OS Detection Signatures

If the client is wrongly classified as Windows OS, enter the client IP address here to display the TCP/IP stack signature stored for the client on the CAM. When troubleshooting, copy and paste the **TCP/IP Stack Signature** result and include it in the customer support request when contacting Cisco TAC.

Client IP Address: 10.10.10.251

TCP/IP Stack Signature: Windows 2000 SP4, XP SP1+ [65535:128:1:48:M1460,N,N,S:.] { }

Display Signature

Step 2 In the **Client IP Address** field, type the client IP address to be tested.

Step 3 Click **Display Signature**. The OS signature result displays in the **TCP/IP Stack Signature** field.

Step 4 Copy and paste the **TCP/IP Stack Signature** result to your support request when contacting Cisco TAC.

CHAPTER 10

Local Certified and Floating Devices

This chapter describes local settings that can be configured at the CAS level for Cisco NAC Appliance implementation. For complete information on Cisco NAC Appliance configuration in the CAM web console, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*. Topics in this chapter include:

- Overview, page 10-1
- Clear Certified Devices, page 10-3
- Add Exempt Devices, page 10-2
- Clear Exempt Devices, page 10-3
- Specify Floating Devices, page 10-4

Overview

Most elements of Cisco NAC Appliance, such as login pages, Nessus scan plugin behavior, Agent requirements, and user roles, are configured at the global level for all CASs. However, certain tasks can also be performed at the local level for an individual CAS. These include the following.

- Clearing certified devices

  The Cisco NAC Appliance 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 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 Agent users are always scanned for requirements at each login.

- Adding/clearing exempt devices

  An exempt device is one which is never subject to certification via network scanning (Nessus scans). You can specify a device as exempt to allow it to bypass network scanning, or you can clear an exempt device to force it to meet Cisco NAC Appliance requirements. Adding or clearing exempt devices is always done **manually**.

- Specifying floating devices

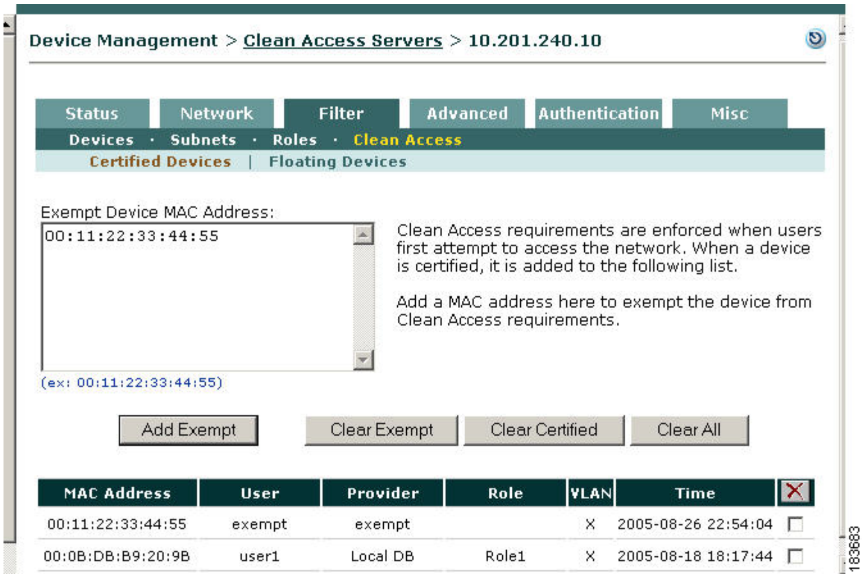
  A floating device requires authentication at every login and is certified only for the duration of a user session. Floating devices are always added manually.

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 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 network scanning certification process to certify that the device you are adding to the list is clean.

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices**.

Figure 10-1 Certified Devices (Local)



Device Management > Clean Access Servers > 10.201.240.10

Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Certified Devices | Floating Devices

Exempt Device MAC Address:

00:11:22:33:44:55

(ex: 00:11:22:33:44:55)

Clean Access requirements are enforced when users first attempt to access the network. When a device is certified, it is added to the following list.

Add a MAC address here to exempt the device from Clean Access requirements.

MAC Address	User	Provider	Role	VLAN	Time	☒
00:11:22:33:44:55	exempt	exempt		X	2005-08-26 22:54:04	□
00:0B:DB:B9:20:9B	user1	Local DB	Role1	X	2005-08-18 18:17:44	□

Step 2 Type the MAC address of the exempt device in the text field. Use line breaks to separate multiple addresses.

Step 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 Nessus Scanning. 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:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see Figure 10-1).

Step 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 Nessus Scanning again for the new CAS unless it has been manually added as an exempt device at the global level for all CASs. This allows for the case where one CAS has more restrictive 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 Cisco NAC Appliance 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 authentication process when it is still considered clean.

To manually clear devices from the list for a specific Clean Access Server:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Certified Devices** (see Figure 10-1).

Step 2 Click **Clear Exempt** to remove the devices that were added manually (using **Add Exempt**).

Step 3 Click **Clear Certified** to remove the devices that were added to the list after meeting Cisco NAC Appliance criteria.

Step 4 Click **Clear All** to remove both types.

Step 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.

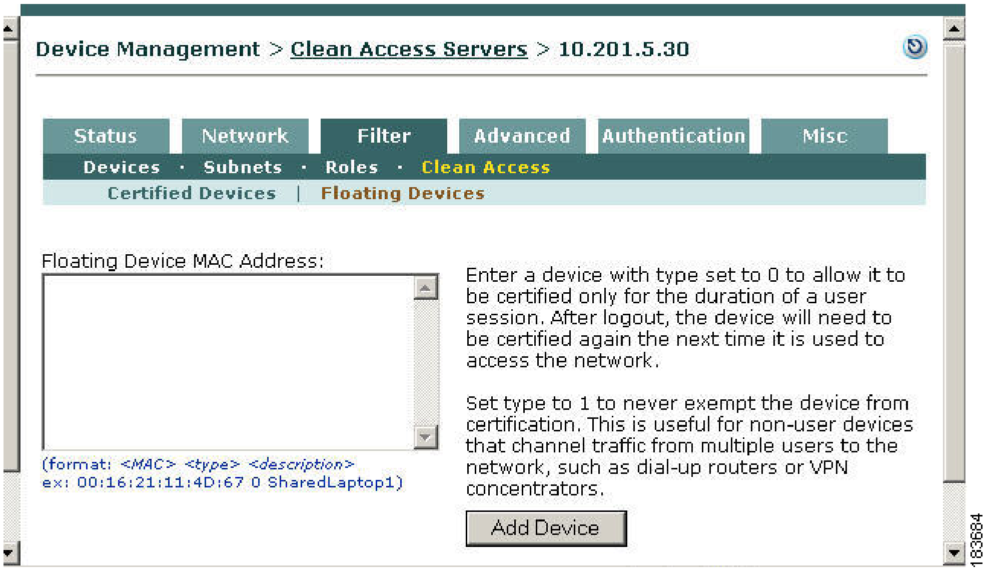
In this case, the users are distinguished by IP address. Note that users must have different IP addresses for this to work. If the router performs NATing services, the users are indistinguishable to the Clean Access Manager and only the first user will be certified.

See also Add VPN Concentrator as a Floating Device, page 6-10.

To specify a local floating device:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Clean Access > Floating Devices**.

Figure 10-2 Floating Devices (Local)



Device Management > Clean Access Servers > 10.201.5.30

Status
Network
Filter
Advanced
Authentication
Misc
Devices · Subnets · Roles · Clean Access
Certified Devices | Floating Devices

Floating Device MAC Address:

(format: <MAC> <type> <description>
ex: 00:16:21:11:4D:67 0 SharedLaptop1)

Enter a device with type set to 0 to allow it to be certified only for the duration of a user session. After logout, the device will need to be certified again the next time it is used to access the network.

Set type to 1 to never exempt the device from certification. This is useful for non-user devices that channel traffic from multiple users to the network, such as dial-up routers or VPN concentrators.

Step 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
```

Step 3 Click **Add Device** to save the setting.

Step 4 To remove a floating MAC address, click the **Delete** icon next to the address.

CHAPTER 11

Administering CAS Certificates, Time, and Support Logs

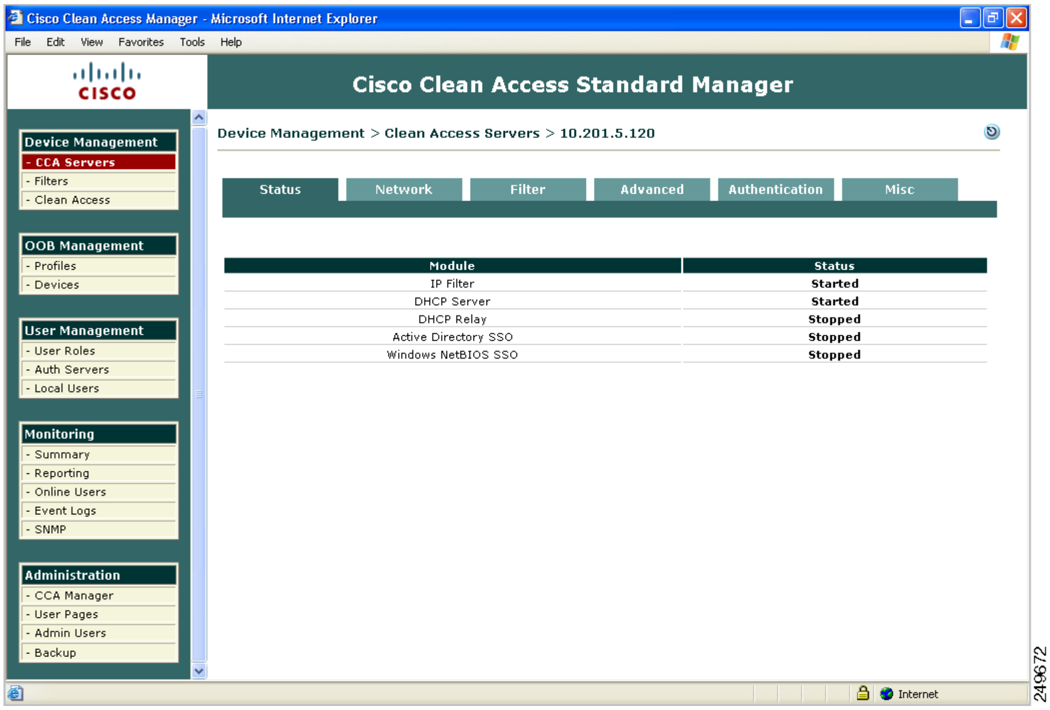
This chapter describes Clean Access Server (CAS) administration. Topics include:

- Status Tab, page 11-1
- Clean Access Server Direct Access Web Console, page 11-2
- Manage CAS SSL Certificates, page 11-6
- System Upgrade, page 11-33
- Synchronize System Time, page 11-35
- Support Logs and LogLevel Settings, page 11-37

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 11-1 CAS Management Pages Status Tab



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

- **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

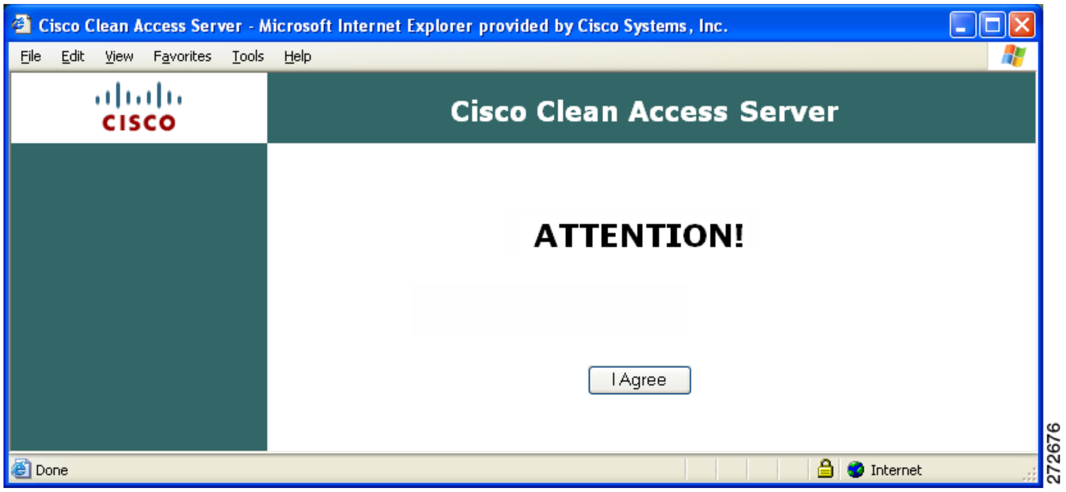
The CAS management pages of the CAM web admin console (Figure 11-1) are the primary configuration interface for the Clean Access Server(s). However, each Clean Access Server has its own web admin console that allows configuration of certain limited Administration and Monitoring settings directly on the CAS (Figure 11-4). 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 the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* 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:

Step 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_address>/admin** (for example, `https://172.16.1.2/admin`).

If you have chosen to enable the customizable Pre-login Banner for the CAS during initial configuration, the CAS admin web console displays in introductory Pre-login Banner (Figure 11-2). Otherwise, the CAS administrator credential entry page (Figure 11-3) appears.

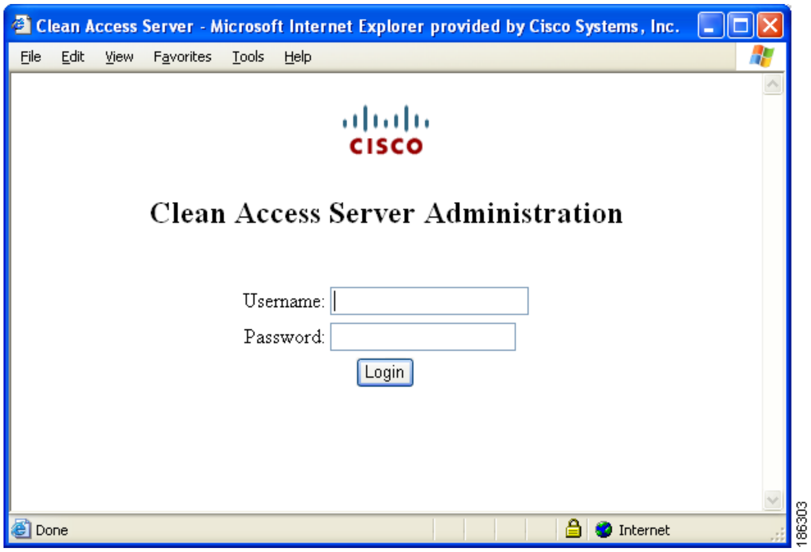
Figure 11-2 CAS Pre-Login Banner Example


Cisco Clean Access Server - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
CISCO
Cisco Clean Access Server
ATTENTION!
I Agree
Done
Internet
272676

The Pre-login Banner enables you to present a broad range of messages, including warnings, system/network status, access requirements, etc., to administrator users before they enter authentication credentials in the CAM/CAS. Administrators can specify the text of the Pre-login Banner by enabling this feature on the appliance, logging into the command-line console, and editing the **/root/banner.pre** file. The text of the Pre-login Banner appears in both the web console interface and the command-line interface when admin users are logging into the CAM/CAS.

You can enable or disable the Pre-login Banner during the initial CAM/CAS configuration CLI session and whenever you choose to alter your base CAM/CAS configuration with the `service perfigo config` CLI command.

Figure 11-3 CAS Direct Access Web Admin Console Login Page



Clean Access Server - Microsoft Internet Explorer provided by Cisco Systems, Inc.

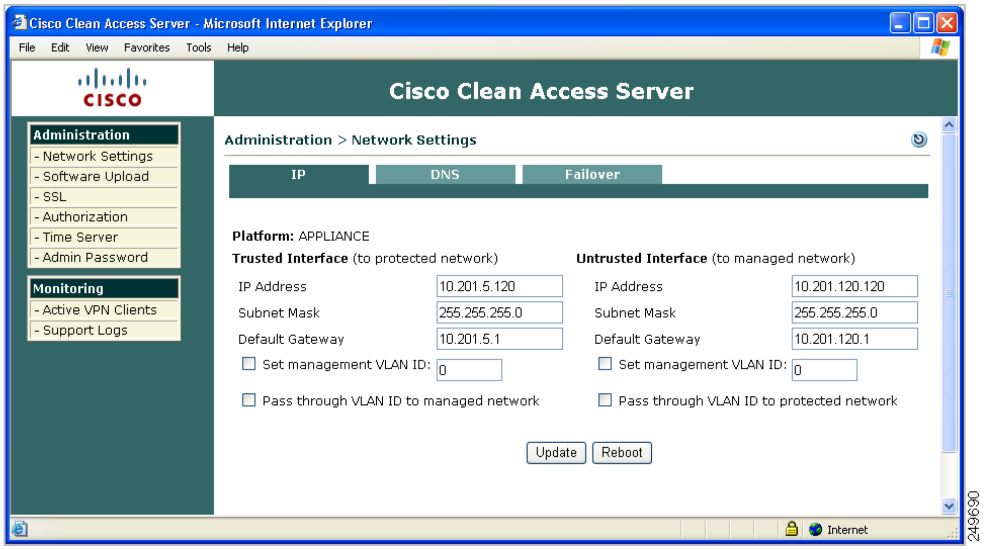
Clean Access Server Administration

Username:

Password:

Step 2 Accept the temporary certificate and log in as user **`admin`** with the associated password.

Figure 11-4 CAS Direct Access Web Admin Console—Cisco NAC-3300 Series



Cisco Clean Access Server - Microsoft Internet Explorer

Cisco Clean Access Server

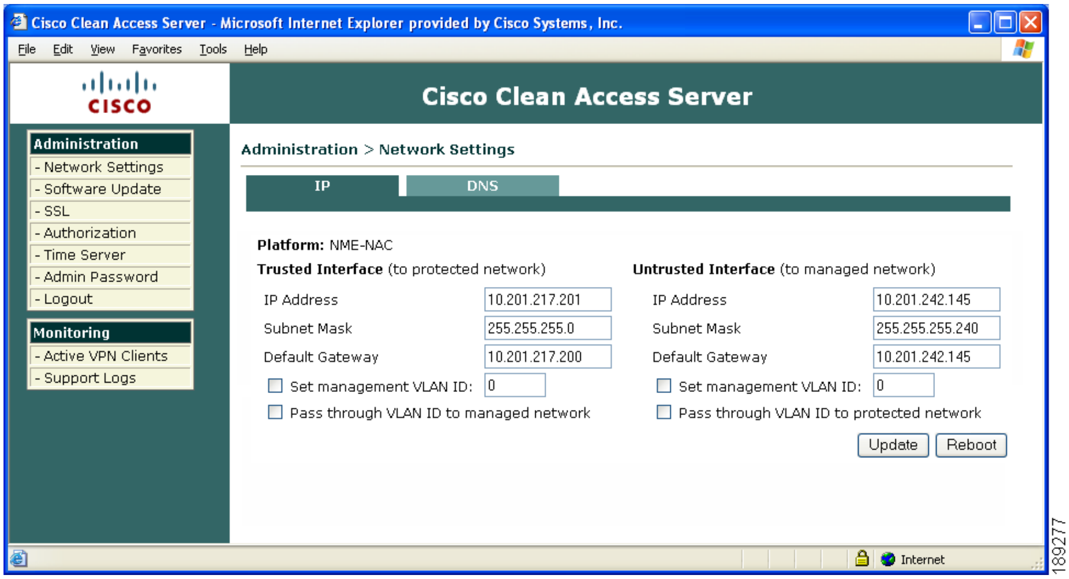
Administration > Network Settings

Platform: APPLIANCE

Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.201.5.120	IP Address	10.201.120.120
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.0
Default Gateway	10.201.5.1	Default Gateway	10.201.120.1
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0
□ Pass through VLAN ID to managed network		□ Pass through VLAN ID to protected network	

Note Because Cisco NAC network modules installed in Cisco Integrated Services Routers (ISRs) do not support high availability, the **Failover** tab is not available when you view the direct web admin console for a Cisco NAC network module.

Figure 11-5 CAS Direct Access Web Admin Console—Cisco NAC Network Module



Platform: NME-NAC

Trusted Interface (to protected network)		**Untrusted Interface** (to managed network)	
IP Address	10.201.217.201	IP Address	10.201.242.145
Subnet Mask	255.255.255.0	Subnet Mask	255.255.255.240
Default Gateway	10.201.217.200	Default Gateway	10.201.242.145
□ Set management VLAN ID:	0	□ Set management VLAN ID:	0
□ Pass through VLAN ID to managed network		□ Pass through VLAN ID to protected network	

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, Cisco recommends changing the 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**, **SSL**, **Admin Password**, and **Support Logs**. The CAS direct access web console provides the following Administration pages for the local CAS:

- Network Settings—IP, DNS, and Failover (Cisco NAC-3300 Series only)
- Software Update
- SSL (Generate Temporary Certificate, Import Certificate, Export CSR/Private Key/Certificate, and view and remove existing Trusted CAs)
- 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 4-11 and the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details.

Manage CAS SSL Certificates

This section describes the following:

- SSL Certificate Overview, page 11-6
- Typical SSL Certificate Setup on the CAS, page 11-10
- Generate Temporary Certificate, page 11-12
- Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14
- Manage Signed Certificate/Private Key, page 11-16
- Manage Trusted Certificate Authorities, page 11-19
- View Current Private Key/Certificate and Certificate Authority Information, page 11-21
- SSL Requirements for Mac OS X/CAS Communication, page 11-23
- Troubleshooting Certificate Issues, page 11-31

SSL Certificate Overview

The elements of Cisco NAC Appliance communicate securely over Secure Socket Layer (SSL) connections. Cisco NAC Appliance uses SSL connections for a number of purposes, including the following:

- Secure communications between the CAM and the CAS

Caution CAM-CAS communication and HA-CAM and/or HA-CAS peer communication can break down and adversely affect network functionality when SSL certificates expire. For more information, see HA Active-Active Situation Due to Expired SSL Certificates, page 11-31.

- Policy Import/Export operations between Policy Sync Master and Policy Sync Receiver CAMs
- CAM-to-LDAP authentication server communications where SSL has been enabled for the **LDAP** authentication provider using the **Security Type** option on the **User Management > Auth Servers > New | Edit** page
- Between the CAS and end-users connecting to the CAS
- Between the CAM/CAS and the browsers accessing the CAM/CAS web admin consoles

During installation, the configuration utility script for both the CAM and CAS requires you to generate a temporary SSL certificate for the appliance being installed (CAM or CAS). A corresponding Private Key is also generated with the temporary certificate. For the Clean Access Manager and Clean Access Servers operating strictly in a lab environment, it is not necessary to use a CA-signed certificate and you can continue to use a temporary certificate, if desired. For security reasons in a production deployment, however, you must replace the temporary certificate for the CAM and CAS with a third-party CA-signed SSL certificate.

At installation, a corresponding Private Key is also generated with the temporary certificate. Cisco NAC Appliance Release 4.7 uses two types of keys to support FIPS compliance: Private Keys and Shared Master Keys. Both of these key types are managed and stored using the FIPS card installed in the CAM/CAS. During installation, keys are created using the CAM/CAS setup utilities, the keys are then *moved* to the FIPS card for security, and key-generation files and/or directories are then removed from the CAM/CAS.

In Cisco NAC Appliance Release 4.7, you can no longer export private keys and you cannot generate CSRs using a FIPS 140-2 compliant CAM/CAS. To adhere to FIPS compliance guidelines, you can only import certificates from trusted third-party resources.

For details on managing SSL certificates for the CAM, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Note Cisco NAC Appliance supports 1024-, 2048-, and 4096-bit RSA key lengths for SSL certificates.

Note Cisco NAC Appliance does not support wildcard SSL certificates.

This Overview section discusses the following topics:

- Web Console Pages for SSL Certificate Management
- CA-Signed Certificates
- Intermediary Certificates
- Certificates for High Availability (HA) Pairs
- Regenerating Certificates for DNS Name Instead of IP

Web Console Pages for SSL Certificate Management

CAM SSL certificate files are kept on the CAM machine, and CAS SSL certificate files are kept on the CAS machine. The CAS certificate can be managed from:

- **Administration > SSL > X509 Certificate**—Use this configuration window to import and export temporary or CA-signed certificates, import Private Keys (FIPS and non-FIPS appliances), export Private Keys (non-FIPS appliances only), and generate new temporary certificates
- **Administration > SSL > Trusted Certificate Authorities**—Use this configuration window to view, add, and remove Certificate Authorities on the CAS
- **Administration > SSL > X509 Certification Request** (non-FIPS appliances only)—Use this configuration window to generate a new CA-signed certificate request for the CAS

For additional web console access information, refer to Clean Access Server Direct Access Web Console, page 11-2.

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 through its direct access web console. These settings include updating the SSL certificate, system time/time zone, DNS, or Service IP. See the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details.

CA-Signed Certificates

The CAS SSL certificate is used for communication between the CAS and the user's web browser and/or Agent, and for communication between the CAM and CAS. In a production deployment, you must replace the temporary certificate for the Clean Access Server with a third-party CA-signed SSL certificate. Cisco NAC Appliance provides a tool to generate and export a Certificate Signing Request (CSR) that you can send to your Certificate Authority on the **Administration > SSL > X509 Certification Request** page. The following reasons highlight the need to obtain and import a third-party CA-signed certificate on the CAS:

- The CAS certificate is visible to the end user. If the CAS has a temporary certificate, users have to explicitly accept the certificate from the CAS each time they login.
- The root certificate needs to be trusted by the client machine.

  Note The CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

- With public certification authorities (Thawte, Verisign, etc.), the root already exists on the client machine.
- For client machines running Windows Vista and/or Internet Explorer 7.0, Certificate Revocation List (CRL) checking is enabled by default. Cisco recommends obtaining a CA-signed certificate for the CAS if supporting Windows Vista/IE 7.0 client machines. For further details, see the section "Windows Vista and Windows 7—IE 7 and IE 8 Certificate Revocation List" in *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.
- For details on Mac OS X Agent certificates, refer to SSL Requirements for Mac OS X/CAS Communication, page 11-23.
- Temporary certificates are designed for lab environments only. When you deploy your CAS in a production environment, Cisco strongly recommends using a trusted certificate from a third-party Certificate Authority to help ensure network security.

In a strictly lab environment, it is not necessary to use a CA-signed certificate and you can continue to use a temporary certificate for the CAM and CAS, if desired. If you deploy your CAM and CAS in a production environment, however, you must use a third-party Trusted CA. For details on managing SSL certificates for the CAM, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1).*

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.

Any certificate that is not provided by a public CA or that is not the self-signed certificate is considered a non-standard certificate by the CAS.

Certification Authorities

A Certification Authority (CA) can be public (e.g. Thawte, Verisign) or private.

With a Public CA:

- You submit your CSR to the public CA and request a Webserver type or SSL type of certificate.
- Your CA should provide you a certificate based on the CSR.
- You can also request the CA's root or public key.
- Note that the CAM/CAS already have the public keys (root) of the most common public CAs.

With a Private CA:

- You can submit your CSR to a private or local CA such as Microsoft CA server.
- The private CA server provides the Certificate and root (Public key).
- However, this root will need to be loaded to CAM/CAS.

Intermediary Certificates

When one or more Intermediary CAs are involved, you will have multiple root certificates or public keys. Each CA has its own root. The root/public key information of all certification authorities in the chain needs to be combined into one single file (for example, **root.cer**) before it can be uploaded into the CAS. To do this, open the root certificate of each CA and copy the information from each root cert into Wordpad or a similar text editor. Include the "Begin Certificate" and "End Certificate' lines for each CA cert, and put each certificate one right after the other in the text file. Save this compiled **root.cer** file, then import it into the CAS.

Certificates for High Availability (HA) Pairs

If you are running HA-CAS pairs, you must generate the CSR for the Service IP of the HA pair and import the CA-signed certificate into one of the HA pairs (e.g. CAS-1). After that, the certificate information, i.e. the Private Key, Certificate, and Root, will need to be exported from the HA-Primary CAS and imported into the HA-Secondary CAS. Refer to the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for more information.

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:

- When you are generating a CSR for signing, always export and save the Private Key to a secure location (for safekeeping and to have the Private Key handy). 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 after you have exported the CSR will create a new private-public key combination, and the new Private Key will no longer match the CA-signed certificate.

- 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 4-24).
- For High-Availability (failover) configurations, use the DNS name for the Service IP (virtual DNS).
- When using a DNS-based certificate, if it is not CA-signed, the user is typically prompted to accept the certificate.

Typical SSL Certificate Setup on the CAS

The typical steps for managing CAS certificates are as follows:

Phase 1: Establish SSL Communication Between the CAS and CAM

Step 1 Synchronize time.

After CAM and CAS installation, make sure the time on the CAM and CAS is synchronized (within 3-5 minutes) before regenerating the temporary certificate on which the Certificate Signing Request will be based. See the next section, Synchronize System Time, page 11-35, for details.

Step 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 certificates, you will need to verify the CAS settings and regenerate a temporary certificate. See Regenerating Certificates for DNS Name Instead of IP, page 11-9 for details. For HA systems, you'll need to regenerate the certificates based on Service IP (see Generate Temporary Certificate, page 11-12).

Step 3 Generate Temporary Certificate, page 11-12.

During initial CAS installation/configuration, a temporary certificate and Private Key are automatically generated. If changing time or DNS settings on the CAM, regenerate the temporary certificate and Private Key.

Step 4 Ensure you export the certificate from your CAM, save it on a machine accessible from your CAS, and import the exported certificate on the CAS, and repeat the process in reverse to ensure the CAS certificate also resides on the CAM.

Phase 2: Set Up Your CAS and CAM For Production Deployment

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

Step 5 Export (Backup) the certificate to a local machine for safekeeping.

If you are altering your Cisco NAC Appliance SSL configuration, it is always a good idea to back up the certificate and Private Key corresponding to the current certificate to a local hard drive for safekeeping. See Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14.

Step 6 (Non-FIPS appliances only) Export (Backup) the Private Key to a local machine for safekeeping.

If you are altering your Cisco NAC Appliance SSL configuration, it is always a good idea to back up the certificate and Private Key corresponding to the current certificate to a local hard drive for safekeeping. See Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14.

Step 7 (Non-FIPS appliances only) Export (save) the Certificate Signing Request (CSR) to a local machine. (See Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14.)

Step 8 Send the CSR file to a Certification Authority (CA) authorized to issue trusted certificates.

Step 9 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 Manage Signed Certificate/Private Key, page 11-16.

Note Cisco strongly recommends removing this certificate authority before deploying your CAS in a production environment. If you are not deploying your CAS in a production environment, you can choose whether or not to remove this certificate authority.

Note The CAM and CAS require encrypted communication. Therefore, the CAM must contain the Trusted Certificate Authorities from which the certificates on all of its managed CASs originate, and all CASs must contain the same Trusted Certificate Authority from which the CAM certificate originates before deploying Cisco NAC Appliance in a production environment.

Step 10 If necessary, upload any required intermediate CA certificate(s) as a single PEM-encoded file to the CAS temporary store (see Intermediary Certificates, page 11-9).

Step 11 Test as a client accessing the Clean Access Server.

Phase 3: Adding a New CAM or CAS to an Existing Production Deployment

In production deployments, CA-signed certificates are used exclusively. Use the following steps when introducing new appliances (CAM or CAS) to a production deployment. The new appliance should not be added to the deployment until you have requested and are able to import a new third-party CA-signed certificate.

Step 1 Install and initially configure the new appliance as described in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8*.

Step 2 Follow the steps in Phase 1: Establish SSL Communication Between the CAS and CAM, page 11-10

Step 3 (Non-FIPS appliances only) Generate a CSR for the new appliance, as described in Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14.

Step 4 Obtain and install the CA-signed certificate as described in Import Signed Certificate/Private Key, page 11-16.

Step 5 Add the appliance to your existing production environment.

Generate Temporary Certificate

The following procedure describes how to generate a new temporary certificate for the CAS. Any time you change basic configuration settings on the CAM (date, time, associated DNS server, etc.) you should generate a new temporary certificate. See Regenerating Certificates for DNS Name Instead of IP, page 11-9 for additional details.

Note Before generating a certificate on the CAS, ensure you enter the CAS distinguished name (DN) in the CAM **Device Management > CCA Servers > Authorization** web console page.

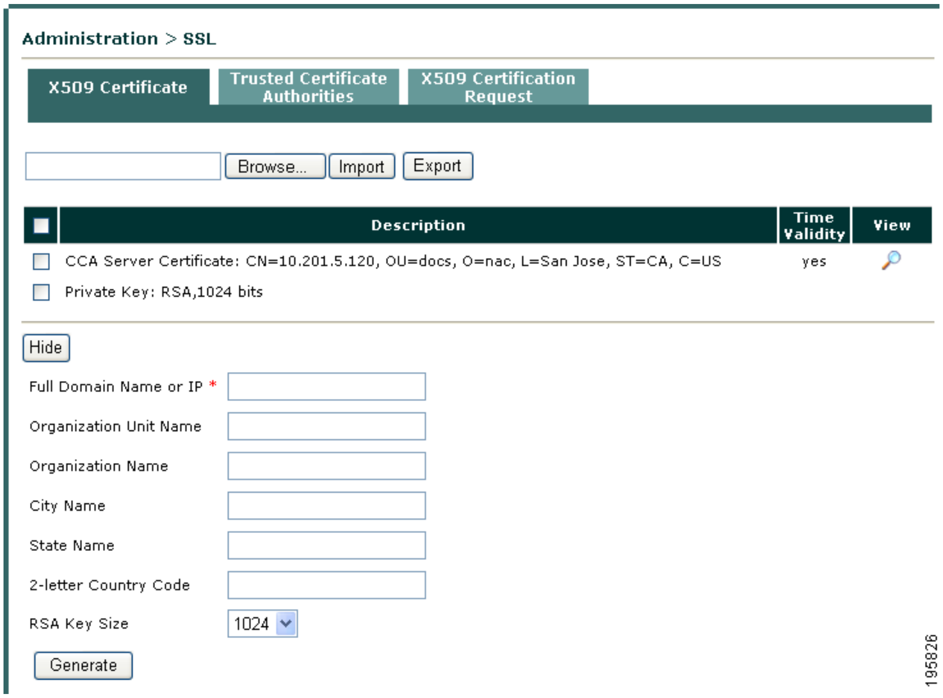
Caution If you are using FIPS 140-2 compliant appliances, be sure you have your current trusted-CA certificate and Private Key stored on an external machine so you can restore them following this procedure.

If you are using a CA-signed certificate on a non-FIPS appliance, Cisco recommends backing up the Private Key for the current certificate prior to generating any new certificate, as generating a new certificate also generates a new Private Key. See Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14 for more information.

Step 1 Go to **Administration > SSL > X509 Certificate**.

Step 2 Click **Generate Temporary Certificate** to expose the fields required to construct a temporary certificate (Figure 11-6).

Figure 11-6 Administration > SSL > X509 Certificate—Generate Temporary Certificate



Administration > SSL

□	Description	Time Validity	View
□	CCA Server Certificate: CN=10.201.5.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US	yes	🔍
□	Private Key: RSA,1024 bits		

Full Domain Name or IP *	
Organization Unit Name	
Organization Name	
City Name	
State Name	
2-letter Country Code	
RSA Key Size	1024

Step 3 Enter appropriate values for the form fields:

- **Full Domain Name or IP** – Either the fully qualified domain name (FQDN) or the IP address of the CAS for which the certificate applies, for example: **caserver.<your_domain_name>**.
  - If using an IP-based certificate, generate the certificate based on the Trusted Interface IP address (eth0) of the CAS.

    Note If the CAS is configured as an L3 Real-IP Gateway, generate the certificate based on the Untrusted Interface (eth1) IP address of the CAS.

  - If using a domain name, make sure that your DNS server can resolve the "Full Domain Name" entered.

  Note To support the Mac OS X Agent, the CAS/CAM **must** use the FQDN as the "**subject**" DN on the certificate (this is the "Full Domain Name or IP" on the CAS/CAM console). An IP address is not allowed. Refer to SSL Requirements for Mac OS X/CAS Communication, page 11-23 for details.

- **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.

Step 4 Specify whether you want the new temporary certificate to use a 1024-, 2048-, or 4096-bit **RSA Key Size**.

Step 5 When finished, click **Generate**. This generates a new temporary certificate and new Private Key.

Step 6 For FIPS 140-2 compliant appliances, be sure to be sure to restore your current trusted-CA certificate and Private Key from an external machine.

Note The **CCA Server Certificate** entry at the top of the certificate display table specifies the full distinguished name of the current CAS SSL certificate. You are required to enter the full distinguished name of the CAS in the CAM web console if you are setting up Authorization between your CAM and CASs. For more information, see Configure Clean Access Server-to-Clean Access Manager Authorization, page 4-6.

Generate and Export a Certification Request (Non-FIPS CAS Only)

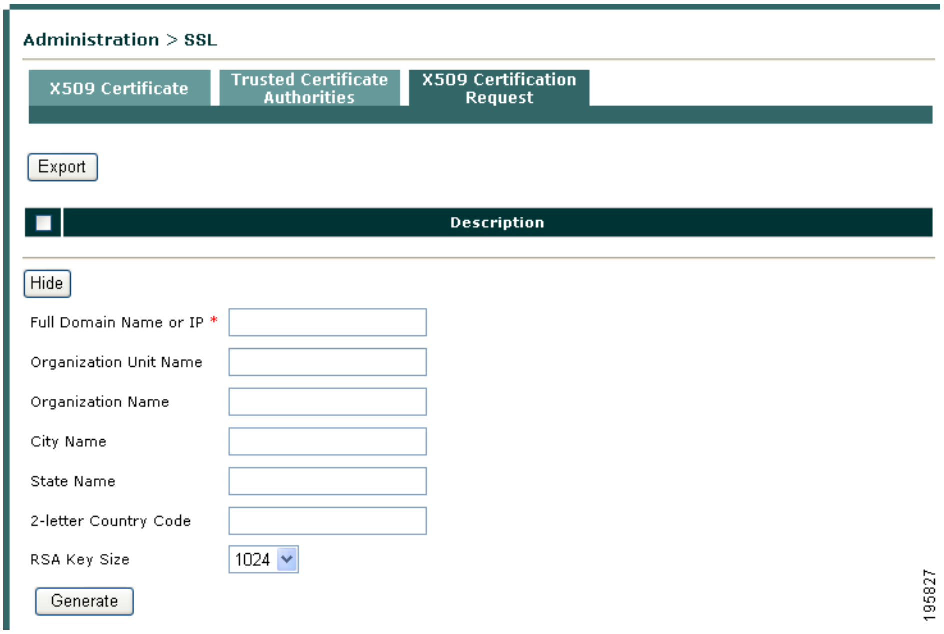
Note The **Administration > SSL > X509 Certification Request** tab does not appear in the CAS web console on a FIPS 140-2 compliant appliance.

Generating a CSR creates a PEM-encoded PKCS#10-formatted Certificate Signing Request (CSR) suitable for submission to a certificate authority. Before you send the CSR, make sure to export the existing certificate and Private Key to a local machine to back it up for safekeeping.

To export he CSR/Private Key and create a certificate request from the CAS web console:

Step 1 Go to **Administration > SSL > X509 Certification Request** (Figure 11-7).

Figure 11-7 Administration > SSL > X509 Certification Request



RSA Key Size 1024

Step 2 Click **Generate Certification Request** to expose the fields required to construct a certificate request.

Step 3 Type appropriate values for the following fields:

- **Full Domain Name or IP**—The fully qualified domain name or IP address of the Clean Access Manager for which the certificate is to apply. For example: `camanager.<your_domain_name>`

Note If requesting a CA-signed certificate for a CAS HA-pair, 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.

- **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.

Step 4 Specify whether you want the new temporary certificate to use a 1024-, 2048-, or 4096-bit **RSA Key Size**.

Step 5 Click **Generate** to generate a certificate request and Private Key pair. Make sure these are the ones for which you want to submit the CSR to the certificate authority.

Step 6 Before you submit the new CSR to the Certificate Authority, save the new certification request and Private Key used to generate the request to your local machine by enabling the checkboxes for the **Certification Request** and/or **Private Key** and clicking **Export**. You are prompted to save or open the file (see Default File Names for Exported Files, page 11-16). Save it to a secure location. 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.

Alternatively, you can immediately **Open** the CSR in Wordpad or a similar text editor if you are ready to fill out the certificate request form, but Cisco strongly recommends you also save a local copy of the CSR and Private Key to ensure you have them should the request process suffer some sort of mishap or your CAM basic configuration change between submitting the CSR and receiving your CA-signed certificate.

When you receive the CA-signed certificate back from the certification authority, you can import it into the Clean Access Server as described in Manage Signed Certificate/Private Key, page 11-16. 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.

Default File Names for Exported Files

The default file names for SSL Certificate files that can be exported from the CAS are as follows. When you actually save the file to your local machine, you can specify a different name for the file. For example, to keep from overwriting your **chain.pem** file containing your certificate chain information, you can specify your Private Key filename to be a more appropriate name like **priv_key.pem** or something similar.

Default File Name [1]	Description
cert_request.pem	CAS Certificate Signing Request (CSR)
chain.pem[2]	CAS Currently Installed Private Key and/or 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.

Manage Signed Certificate/Private Key

Import Signed Certificate/Private Key

You can import CA-signed PEM-encoded X.509 Certificates and Private Keys using the CAS web console on both FIPS 140-2 compliant and non-FIPS appliances. (Typically, you only need to re-import the Private Key if the current Private Key does not match the one used to create the original CSR on which the CA-Signed certificate is based.) There are two methods administrators can use to import CA-signed certificates, Private Keys, and associated Certificate Authority information into Cisco NAC Appliance:

1. Import the Certificate Authorities and the End Entity Certificates/Private Keys separately:
   a. Import the Certificate Authorities into the trust store using the procedures in Manage Trusted Certificate Authorities, page 11-19
   b. Import the CAS's end entity certificate and/or Private Key using the instructions below
2. Construct a PEM-encoded X.509 certificate chain (including the Private Key and End Entity, Root CA, and Intermediate CA certificates) and import the entire chain at once using the instructions below

If you have received a CA-signed PEM-encoded X.509 certificate for the Clean Access Server, you can also 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 and that you have obtained third-party certificates for both your CAM and CASs. If using a Certificate Authority for which intermediate CA certificates are necessary, make sure these files are also present and accessible if not already present on the CAS.

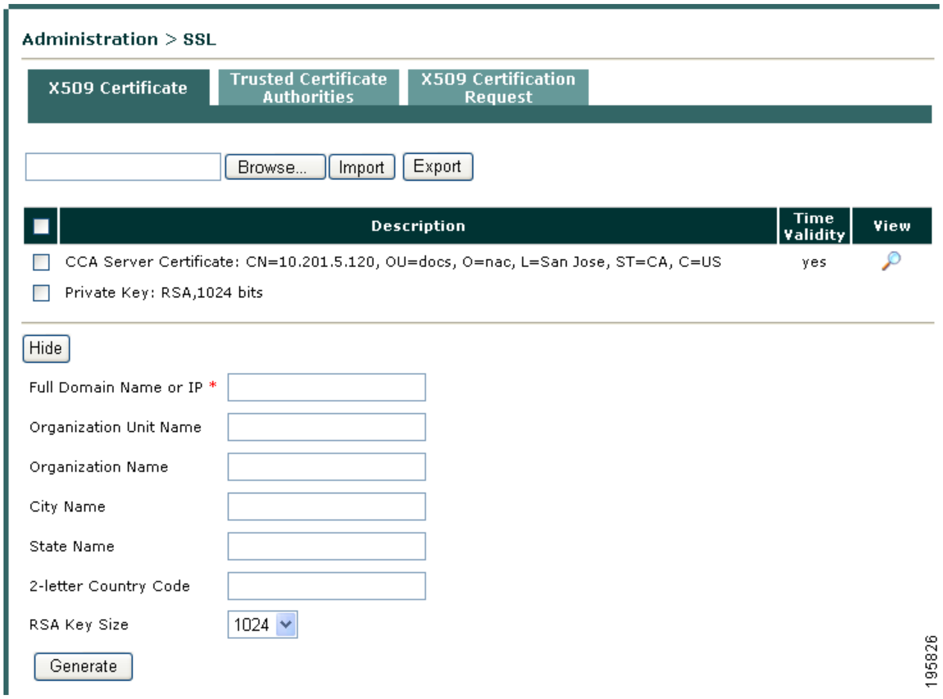
Note If obtaining a CA-signed certificate for a CAS HA-Pair, the CA-signed certificate must either be based on the Service IP or a host name/domain name resolvable to the Service IP through DNS.

Note Any certificate that is not provided by a public CA or that is not the self-signed certificate is considered a non-standard certificate by the CAM/CAS. When importing certificates to the CAS, make sure to obtain CA-signed certificates for authentication servers.

To import a certificate and/or Private Key for the CAS:

Step 1 Go to **Administration > SSL > X509 Certificate** (see Figure 11-8).

Figure 11-8 Administration > SSL > X509 Certificate—Import Certificate



□	Description	Time Validity	View
□	CCA Server Certificate: CN=10.201.5.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US	yes	🔎
□	Private Key: RSA,1024 bits		

Full Domain Name or IP *	
Organization Unit Name	
Organization Name	
City Name	
State Name	
2-letter Country Code	
RSA Key Size	1024

Step 2 Click **Browse** and locate the certificate file and/or Private Key on your local machine.

Note Make sure there are no spaces in the filename when importing files (you can use underscores).

Step 3 Click **Import**.

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.

If you already have other members of the certificate chain in the CAS trust store, you do not need to re-import them. The CAS can build the certificate chain from a combination of newly-imported and existing parts.

If you try to upload a root/intermediate CA certificate for the CAM that is already in the list, you may see an error message reading "This intermediate CA is not necessary." In this case, you must delete the uploaded Root/Intermediate CA in order to remove any duplicate files.

Export Certificate and/or Private Key

Note You cannot export the Private Key for a FIPS 140-2 compliant CAS. You can only export certificates.

To backup your certificate and/or Private Key in case of system failure or other loss, you can export your certificate and/or Private Key information and save a copy on your local machine. This practice also helps you manage certificate/Private Key information for a CAS HA-Pair. By simply exporting the certificate information from the HA-Primary CAS and importing it on the HA-Secondary CAS, you are able to push an exact duplicate of the certificate info required for CAM/CAS communication to the standby CAS.

Step 1 Go to **Administration > SSL > X509 Certificate** (Figure 11-8).

Step 2 To export existing certificate/Private Key information:

a. Select one or more certificates and/or the Private Key displayed in the certificates list by clicking on their respective left hand checkboxes.

b. Click **Export** and specify a location on your local machine where you want to save the resulting file.

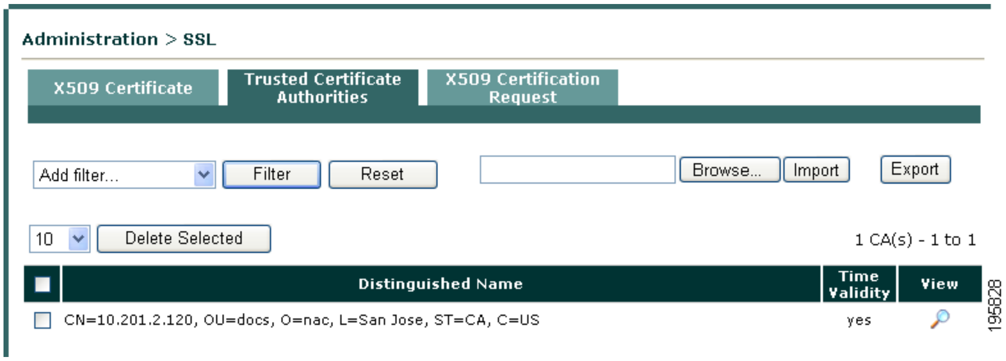
Manage Trusted Certificate Authorities

You can locate and remove Trusted CAs from the CAS database using the **Administration > SSL > Trusted Certificate Authorities** CAS web console page. To keep your collection of trusted certificate authority Cisco recommends keeping only trusted certificate authority information critical to Cisco NAC Appliance operations in the CAM trust store.

To view and/or remove Trusted CAs from the CAS:

Step 1 Go to **Administration > SSL > Trusted Certificate Authorities** (Figure 11-9).

Figure 11-9 Administration > SSL > Trusted Certificate Authorities



1 CA(s) - 1 to 1

□	Distinguished Name	Time Validity	View
□	CN=10.201.2.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US	yes	🔍

Viewing Trusted CAs

Step 2 If you want to refine the list of Trusted CAs displayed in the CAS web console:

a. Choose an option from the **Filter** dropdown menu:

- **Distinguished Name**—Use this option to refine the list of Trusted CAs according to whether the Trusted CA name contains or does not contain a specific text string.
- **Time**—Use this option to refine the display according to which Trusted CAs are currently valid or invalid.

  You can also combine these two options to refine the Trusted CAs display.

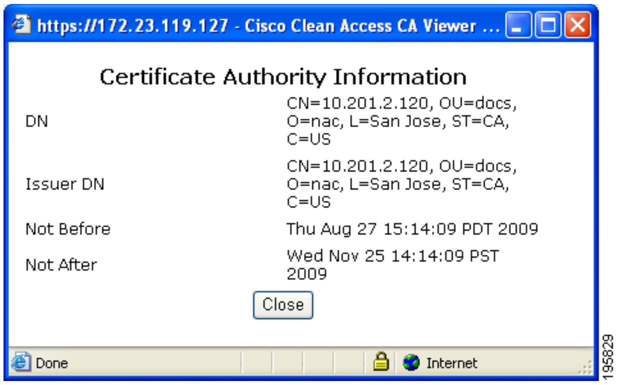
b. Click the **Filter** button after selecting and defining parameters for the search options to display a refined list of all Trusted CAs that match the criteria.

You can click **Reset** to negate any of the optional search criteria from the filter dropdown menu and return the Trusted CA display to default settings.

c. You can also increase or decrease the number of viewable items in the Trusted CAs list by choosing one of the options in the dropdown menu at the top-left of the list. The options are 10, 25, or 100 items.

d. If you want to view details about an existing Trusted CA, click the **View** button (far-right magnifying glass icon) to see information on the specific certificate authority, as shown in Figure 11-10.

Figure 11-10 Trusted Certificate Authority Information



Certificate Authority Information

DN	CN=10.201.2.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US
Issuer DN	CN=10.201.2.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US
Not Before	Thu Aug 27 15:14:09 PDT 2009
Not After	Wed Nov 25 14:14:09 PST 2009

Close

Removing Trusted CAs

Step 3 Select one or more Trusted CAs to remove by clicking on the checkbox for the respective Trusted CA in the list. (Clicking on the empty checkbox at the top of the Trusted CAs display automatically selects or unselects *all* Trusted CAs in the current list.)

Step 4 Click **Delete Selected**.

Once the CAS removes the selected Trusted CAs from the database, the CAS automatically restarts services to complete the update.

Import/Export Trusted Certificate Authorities

You can also use the Trusted Certificate Authorities web console page to import and export certificate information for the CAS.

Note For standard certificate import and export guidelines, refer to Generate and Export a Certification Request (Non-FIPS CAS Only), page 11-14 and Manage Signed Certificate/Private Key, page 11-16.

Step 1 Go to **Administration > SSL > Trusted Certificate Authorities**.

Step 2 To import a Trusted Certificate Authority:

a. Ensure you have the appropriate certificate file accessible to the CAS in the network and click **Browse**.

b. Locate and select the certificate file on your directory system and click **Open**.

c. Click **Import** to upload the Trusted Certificate Authority information to your CAS.

Step 3 To export existing Trusted Certificate Authority information:

a. Select one or more Trusted CAs displayed in the Trusted Certificate Authorities list by clicking on their respective left hand checkboxes.

b. Click **Export** and specify a location on your local machine where you want to save the resulting “caCerts” file.

View Current Private Key/Certificate and Certificate Authority Information

You can verify the following files by viewing them under **Administration > SSL > X509 Certificate** (see Figure 11-7):

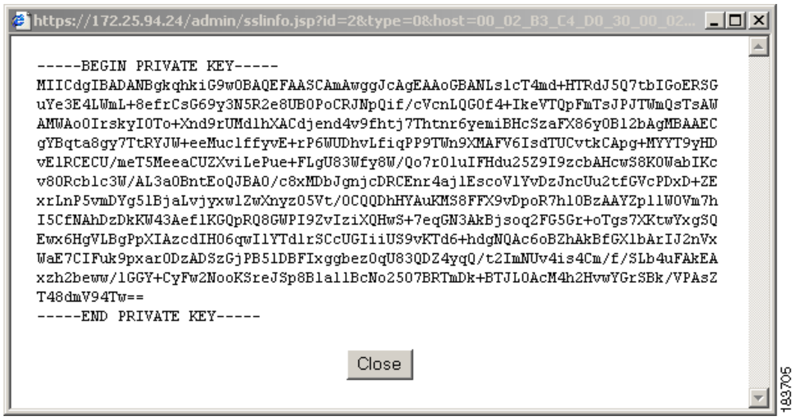
- Currently Installed Private Key
- Currently Installed End Entity, Root, and Intermediate CA Certificate
- Certificate Authority Information

Note You must be currently logged into your web console session to view any Private Key and/or certificate files.

View Currently Installed Private Key

You can view the CAM Private Key by exporting and opening the exported Private Key file in Wordpad or a similar text editor tool to bring up a dialog like the one in Figure 11-11 (BEGIN PRIVATE KEY/END PRIVATE KEY).

Figure 11-11 View Currently Installed Private Key


https://172.25.94.24/admin/sslinfo.jsp?id=2&type=0&host=00_02_B3_C4_D0_30_00_02...
Close
183705

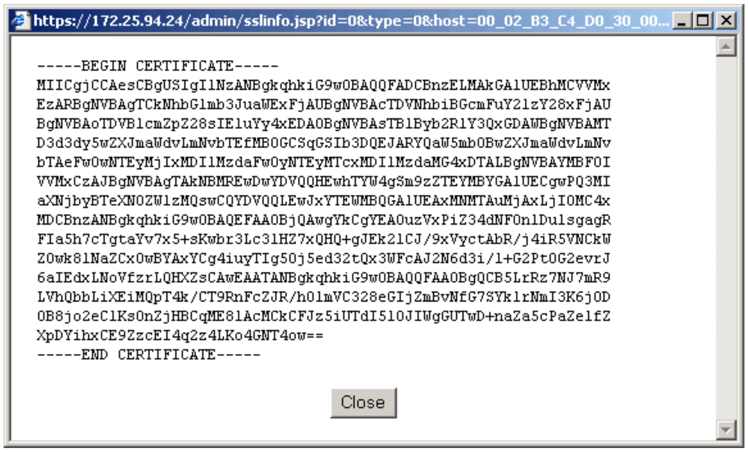
```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBANLslcT4md+HTRdJ5Q7tbIGoERSG
uYe3E4LWmL+8efrCsG69y3N5R2e8UB0PoCRJNpQif/cVcnLQG0f4+IkeVTQpFmTsJPJTWmQsTsAW
AMWAo0IrskyI0To+Xnd9rUMdlhXACdjend4v9fhtj7Thtnr6yemiBHcSzaFX86y0Bl2bAgMBAAEC
gYBqta8gy7TtRYJW+eeMuclffyvE+rP6WUDhvLfiqPP9TWn9XMAFV6IsdTUCvtkCApg+MYYT9yHD
vElRCECU/meT5MeeaCUZXviLePue+FLgU83Wfy8W/Qo7r0luIFHdu25Z9I9zcbAHcwS8K0WabIKc
v80Rcblc3W/AL3a0BntEoQJBA0/c8xMDbJgmjcDRCEnr4ajlEscoVlYvDzJncUu2tfGVcPDxD+ZE
xrLnP5vmDYg5lBjaLvjyxwlZwXnyz05Vt/0CQQDhHYAuKMS8FFX9vDpoR7hl0BzAAYZpllW0Vm7h
I5CfNAhDzDkKW43AeflKGQpRQ8GWPI9ZvIziXQHwS+7eqGN3AkBjsoq2FG5Gr+oTgs7XKtwYxgSQ
Ewx6HgVLBgPpXIAzcdIH06qwIlYTdlrSCcUGIiiUS9vKTd6+hdgNQAc6oBZhAkBfGXlbArIJ2nVx
WaE7CIFuk9pxar0DzADSzGjPB5lDBFIxggbez0qU83QDZ4yqQ/t2ImNUv4is4Cm/f/SLb4uFAkEA
xzh2beww/lGGY+CyFw2NooKSreJSp8Blal1BcNo2507BRTmDk+BTJL0AcM4h2HvwYGrSBk/VPAsZ
T48dmV94Tw==
-----END PRIVATE KEY-----
```

You can also use this method to view uploaded Private Keys before importing them into your CAM.

View Currently Certificate or Certificate Chain

You can view CAS Private Key and End Entity, Root CA, and Intermediate CA certificates by exporting and opening the saved file in Wordpad or a similar text editor tool to bring up a dialog like the one in Figure 11-12 (BEGIN CERTIFICATE/END CERTIFICATE).

Figure 11-12 View Currently Installed Certificate



https://172.25.94.24/admin/sslinfo.jsp?id=0&type=0&host=00_02_B3_C4_D0_30_00...
Close
183704

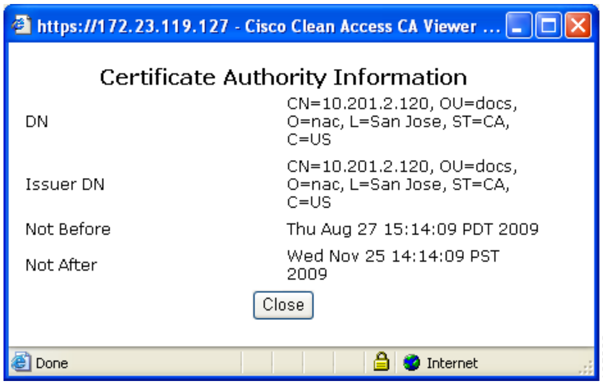
```
-----BEGIN CERTIFICATE-----
MIICgjCCAesCBgUSIgIlNzANBgkqhkiG9w0BAQQFADCBnzELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDVNhbiBGcmFuY2lzY28xFjAU
BgNVBAoTDVBlcmZpZ28sIEluYy4xEDAOBgNVBAsTBlByb2RlY3QxGDAWBgNVBAMT
D3d3dy5wZXJmaWdvLmNvbTEfMB0GCSqGSIb3DQEJARYQaW5mb0BwZXJmaWdvLmNv
bTAeFw0wNTEyMjIxMDIlMzdaFw0yNTEyMTcxMDIlMzdaMG4xDTALBgNVBAYMBF0I
VVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEYMBYGA1UECgwPQ3MI
aXNjbyBTeXN0ZWlzMQswCQYDVQQLEwJxYTEWMBQGA1UEAxMNMTAuMjAxLjI0MC4x
MDCBnzANBgkqhkiG9w0BAQEFAA0BjQAwgYkCgYEA0uzVxPiZ34dNF0nlDulsgagR
FIa5h7cTgtaYv7x5+sKwbr3Lc3lHZ7xQHQ+gJEk2lCJ/9xVyctAbR/j4iR5VNCkW
Z0wk8lNaZCx0wBYAxYCg4iuyTIg50j5ed32tQx3WFcAJ2N6d3i/l+G2Pt0G2evrJ
6aIEdxLNoVfzrLQHXZsCAwEAATANBgkqhkiG9w0BAQQFAA0BgQCB5LrRz7NJ7mR9
LVhQbbLiXEiMQpT4k/CT9RnFcZJR/h0lmVC328eGIjZmBvNfG7SYklrNmI3K6j0D
0B8jo2eClKs0nZjHBCqME8lAcMCkCFJz5iUTdI5l0JIWgGUTwD+naZa5cPaZelfZ
XpDYihxCE9ZzcEI4q2z4LKo4GNT4ow==
-----END CERTIFICATE-----
```

You can also use this method to view uploaded certificates before importing them into your CAM.

View Certificate Authority Information

You can view Certificate Authority information for CAM End Entity, Root, and Intermediate CA Certificates by clicking on the respective **View** icon (magnifying glass) in the right hand column to bring up a dialog like the one in Figure 11-13.

Figure 11-13 View Certificate Authority Information



Certificate Authority Information

DN	CN=10.201.2.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US
Issuer DN	CN=10.201.2.120, OU=docs, O=nac, L=San Jose, ST=CA, C=US
Not Before	Thu Aug 27 15:14:09 PDT 2009
Not After	Wed Nov 25 14:14:09 PST 2009

SSL Requirements for Mac OS X/CAS Communication

For the Mac OS X Agent to communicate with the Clean Access Server, the SSL communication between the Agent and CAS must meet certain requirements. The CAS must have one of the following:

- A valid name-based CA-signed certificate (from a trusted Certificate Authority)
- A name-based temporary certificate that meets the requirements described below

Note Ensure DNS can also resolve all name-based certificates.

CAS Temporary Certificate Requirements for SSL Connection to Mac OS X Agent

If using a temporary certificate for the CAS, make sure the following are in place:

Step 1 The CAS/CAM must use a fully qualified domain name (FQDN) as the "**subject**" DN on the certificate (this is the "Full Domain Name or IP" on the CAS/CAM console). An IP address is not allowed. This may require regenerating the certificate on your CAS. (See Generate Temporary Certificate, page 11-12for details.)

Step 2 On the Mac OS X machine, the root certificate which is used to sign the temporary certificate must be installed in the X509 Anchors in Keychain Access application. To do this, use one of the following set of steps for the Mac OS X version running on the machine:

- Installing the Root Certificate for Mac OS 10.4.x
- Installing the Root Certificate for Mac OS 10.5

Step 3 The Mac OS X machine must be able to correctly resolve the FQDN name via DNS. There are two approaches to this:

a. Add an entry into the DNS server which the Mac machine is using, or

b. For a test machine:

1. Enable your root account as described in Enable the Root User on Mac OS X, page 11-27
2. Edit the /etc/hosts file on the Macintosh client machine by running **`sudo vi /etc/hosts`** to add a new domain lookup entry.

Caution Because the CAS/CAM use the full domain name, you cannot use an IP address in the certificate. You must use the domain name instead.

Caution Make sure your machine's date and time are valid for the certificate. If the current date and time fall out of the range of the certificate, the Agent will not work.

Installing the Root Certificate for Mac OS 10.4.x

Note You must have administrative permissions on your computer in order to run these steps.

Step 1 Download the root certificate to your client machine (or desktop). See Obtaining the Root Certificate from the CAS, page 11-28 for details.

Step 2 Click the **Finder** icon in the Dock.

Step 3 From the **Go** menu, choose **Applications**.

Step 4 Open the **Utilities** folder.

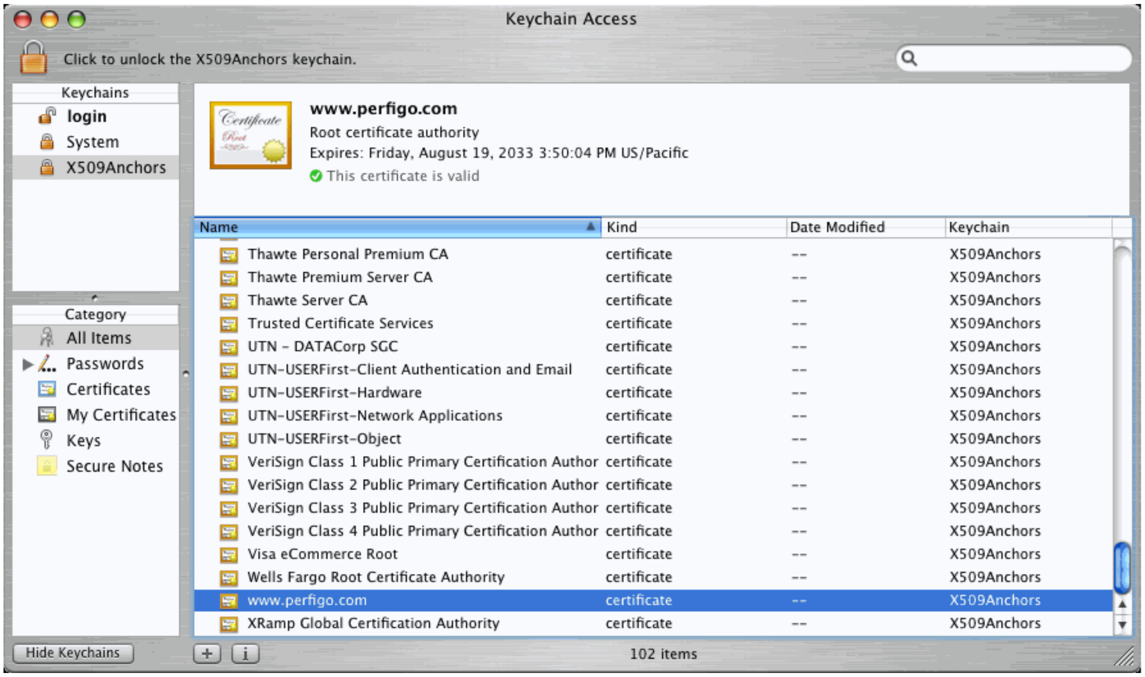
Step 5 Launch the **Keychain Access** application.

Step 6 Drag the root certificate to the **Keychain Access** application.

Step 7 In the **Add Certificates** dialog box, click **X509 Anchors** and click **OK**.

Step 8 The root certificate is added (Figure 11-14).

Figure 11-14 Root Certificate Added on Mac OS 10.4.x



www.perfigo.com
Root certificate authority
Expires: Friday, August 19, 2033 3:50:04 PM US/Pacific
This certificate is valid

Name	Kind	Date Modified	Keychain
Thawte Personal Premium CA	certificate	--	X509Anchors
Thawte Premium Server CA	certificate	--	X509Anchors
Thawte Server CA	certificate	--	X509Anchors
Trusted Certificate Services	certificate	--	X509Anchors
UTN - DATACorp SGC	certificate	--	X509Anchors
UTN-USERFirst-Client Authentication and Email	certificate	--	X509Anchors
UTN-USERFirst-Hardware	certificate	--	X509Anchors
UTN-USERFirst-Network Applications	certificate	--	X509Anchors
UTN-USERFirst-Object	certificate	--	X509Anchors
VeriSign Class 1 Public Primary Certification Author	certificate	--	X509Anchors
VeriSign Class 2 Public Primary Certification Author	certificate	--	X509Anchors
VeriSign Class 3 Public Primary Certification Author	certificate	--	X509Anchors
VeriSign Class 4 Public Primary Certification Author	certificate	--	X509Anchors
Visa eCommerce Root	certificate	--	X509Anchors
Wells Fargo Root Certificate Authority	certificate	--	X509Anchors
www.perfigo.com	certificate	--	X509Anchors
XRamp Global Certification Authority	certificate	--	X509Anchors

Installing the Root Certificate for Mac OS 10.5

Note You must have administrative permissions on your computer in order to run these steps.

Step 1 Download the root certificate to your client machine (or desktop). See Obtaining the Root Certificate from the CAS, page 11-28 for details.

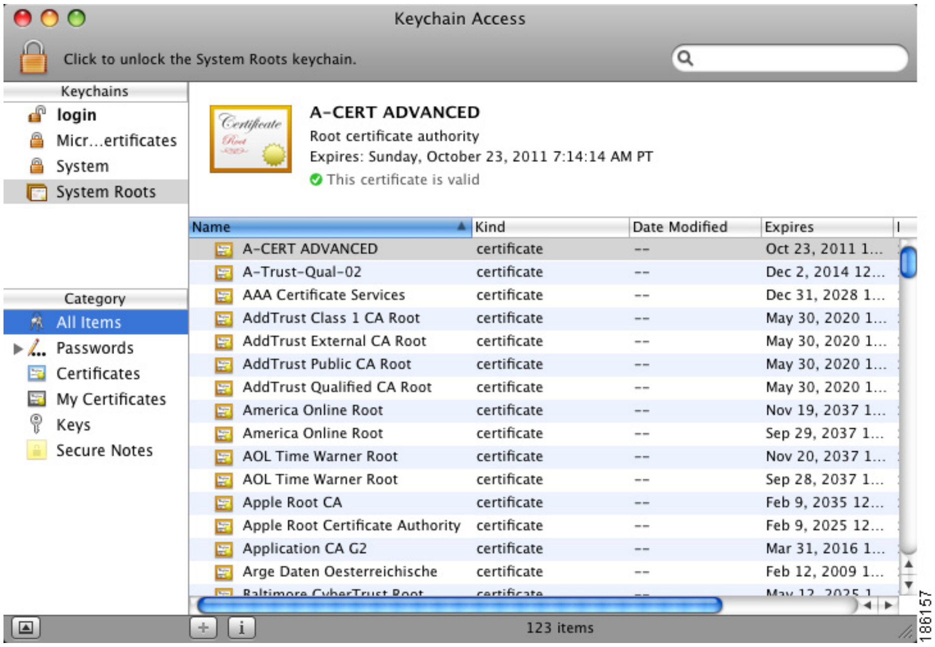
Step 2 Click the **Finder** icon in the Dock.

Step 3 From the **Go** menu, choose **Applications**.

Step 4 Open the **Utilities** folder.

Step 5 Launch the **Keychain Access** application.

Figure 11-15 Launch Keychain Access Application on Mac OS 10.5

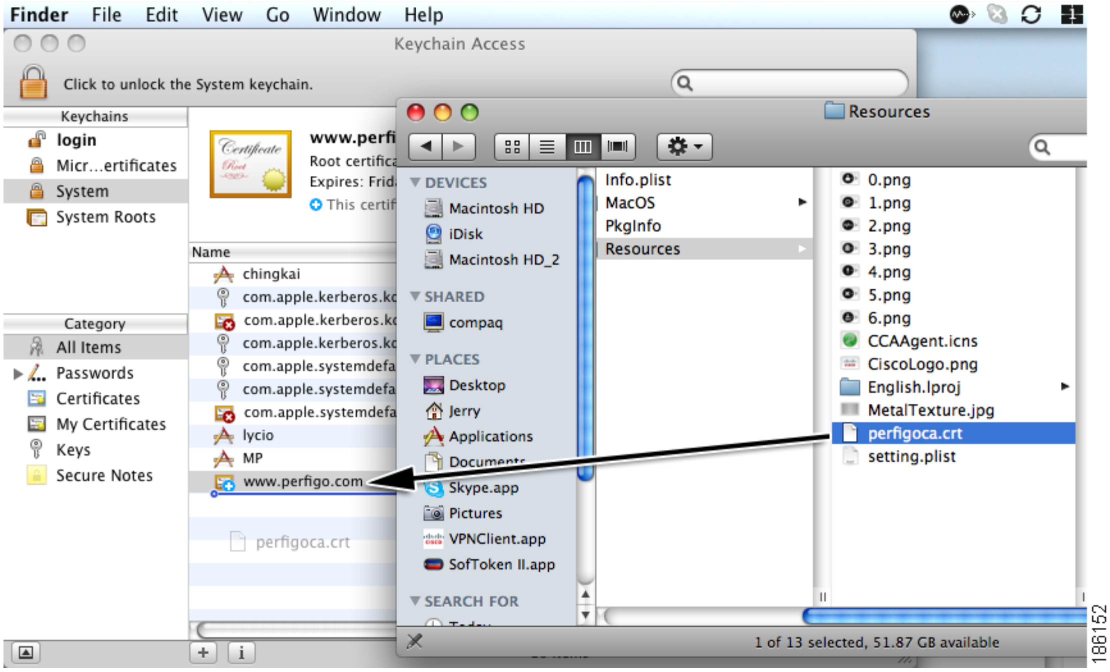


A-CERT ADVANCED
Root certificate authority
Expires: Sunday, October 23, 2011 7:14:14 AM PT
This certificate is valid

Name	Kind	Date Modified	Expires
A-CERT ADVANCED	certificate	--	Oct 23, 2011 1...
A-Trust-Qual-02	certificate	--	Dec 2, 2014 12...
AAA Certificate Services	certificate	--	Dec 31, 2028 1...
AddTrust Class 1 CA Root	certificate	--	May 30, 2020 1...
AddTrust External CA Root	certificate	--	May 30, 2020 1...
AddTrust Public CA Root	certificate	--	May 30, 2020 1...
AddTrust Qualified CA Root	certificate	--	May 30, 2020 1...
America Online Root	certificate	--	Nov 19, 2037 1...
America Online Root	certificate	--	Sep 29, 2037 1...
AOL Time Warner Root	certificate	--	Nov 20, 2037 1...
AOL Time Warner Root	certificate	--	Sep 28, 2037 1...
Apple Root CA	certificate	--	Feb 9, 2035 12...
Apple Root Certificate Authority	certificate	--	Feb 9, 2025 12...
Application CA G2	certificate	--	Mar 31, 2016 1...
Arge Daten Oesterreichische	certificate	--	Feb 12, 2009 1...
Baltimore CyberTrust Root	certificate	--	May 12, 2025 1...

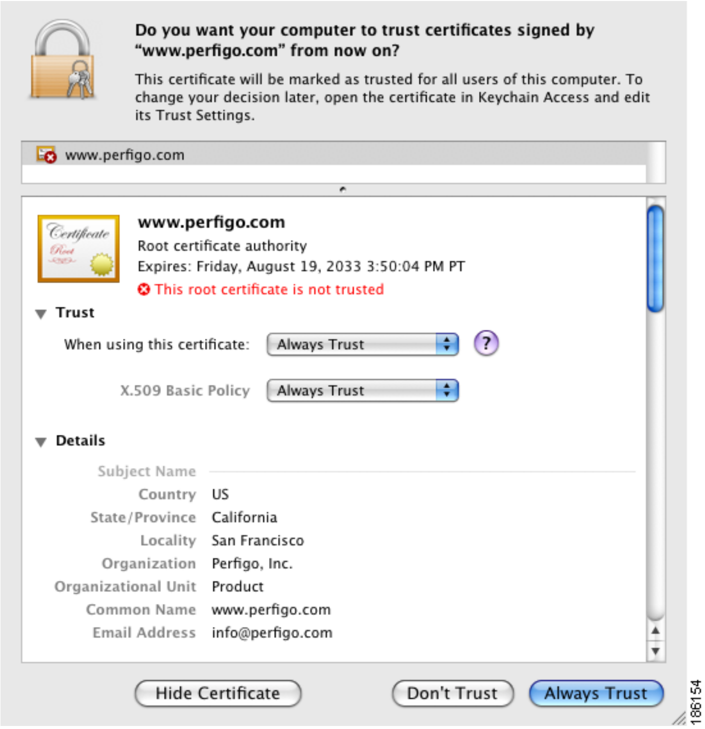
Step 6 Drag the root certificate to the **Keychain Access** application.

Figure 11-16 Drag and Drop the Certificate Into the Keychain Access Application on Mac OS 10.5



Step 7 Click **Always Trust** in the Certificate dialog.

Figure 11-17 Certificate Dialog on Mac OS 10.5



Do you want your computer to trust certificates signed by "www.perfigo.com" from now on?

This certificate will be marked as trusted for all users of this computer. To change your decision later, open the certificate in Keychain Access and edit its Trust Settings.

www.perfigo.com

www.perfigo.com
Root certificate authority
Expires: Friday, August 19, 2033 3:50:04 PM PT
This root certificate is not trusted

Trust

When using this certificate: Always Trust

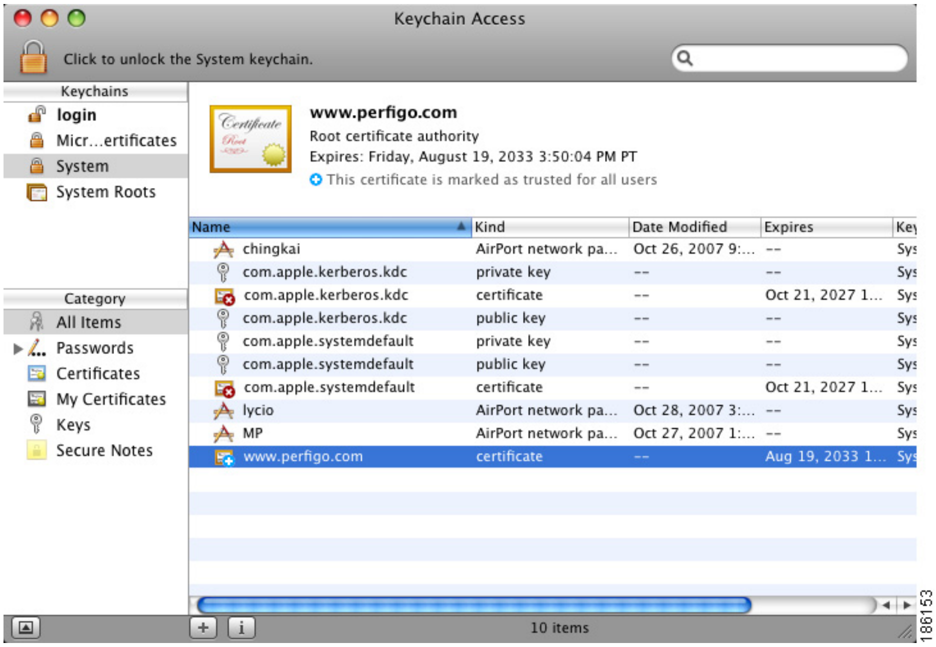
X.509 Basic Policy: Always Trust

Details

Subject Name	
Country	US
State/Province	California
Locality	San Francisco
Organization	Perfigo, Inc.
Organizational Unit	Product
Common Name	www.perfigo.com
Email Address	info@perfigo.com

Step 8 The root certificate is added (Figure 11-18).

Figure 11-18 Display the New Root Certificate on Mac OS 10.5



www.perfigo.com
Root certificate authority
Expires: Friday, August 19, 2033 3:50:04 PM PT
This certificate is marked as trusted for all users

Name	Kind	Date Modified	Expires	Key
chingkai	AirPort network pa…	Oct 26, 2007 9:…	--	Sys
com.apple.kerberos.kdc	private key	--	--	Sys
com.apple.kerberos.kdc	certificate	--	Oct 21, 2027 1…	Sys
com.apple.kerberos.kdc	public key	--	--	Sys
com.apple.systemdefault	private key	--	--	Sys
com.apple.systemdefault	public key	--	--	Sys
com.apple.systemdefault	certificate	--	Oct 21, 2027 1…	Sys
lycio	AirPort network pa…	Oct 28, 2007 3:…	--	Sys
MP	AirPort network pa…	Oct 27, 2007 1:…	--	Sys
www.perfigo.com	certificate	--	Aug 19, 2033 1…	Sys

Enable the Root User on Mac OS X

Note Ensure you are an administrator on the machine. You must have access to an account that has administrator privileges to perform the rest of these steps.

Step 1 Click the **Finder** icon in the Dock.

Step 2 From the **Go** menu, choose **Applications**.

Step 3 Open the **Utilities** folder.

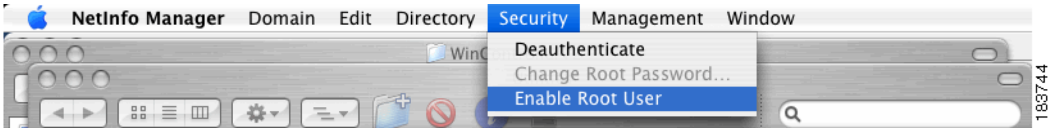
Step 4 Open the **NetInfo Manager** utility.

Step 5 Click the lock in the **NetInfo Manager** window (or go to **Security > Authenticate**).

Step 6 Type your administrator account **username** and **password** and click **OK**.

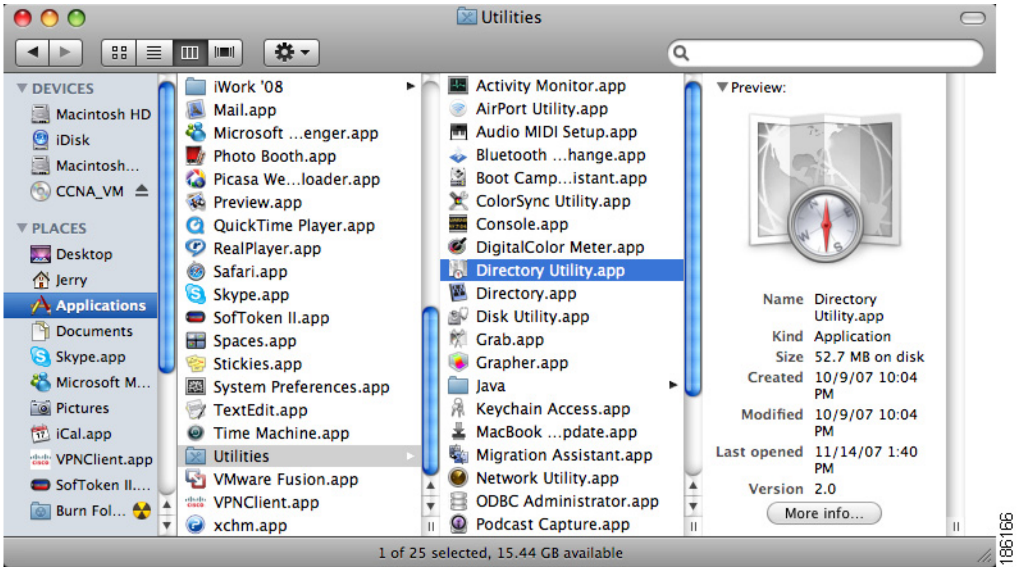
Step 7 For Mac OS 10.4.x, choose **Enable Root User** from the **Security** menu (Figure 11-19).

Figure 11-19 Enable Root User (Mac OS 10.4.x)



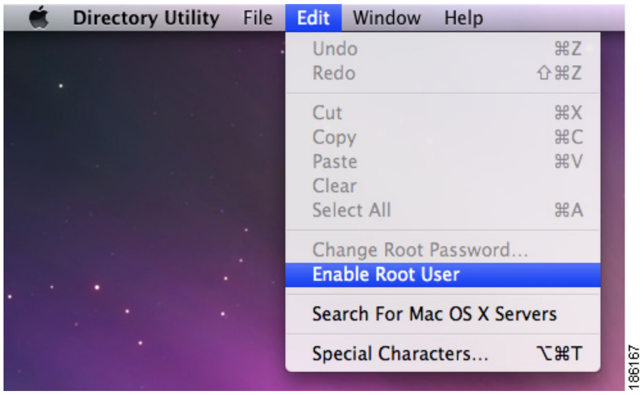
For Mac OS 10.5, launch **Applications > Utilities > Directory Utility.app** (Figure 11-20) and choose **Enable Root User** from the **Edit** menu (Figure 11-21).

Figure 11-20 Enable Root User > (Mac OS 10.5)



Name Directory Utility.app
Kind Application
Size 52.7 MB on disk
Created 10/9/07 10:04 PM
Modified 10/9/07 10:04 PM
Last opened 11/14/07 1:40 PM
Version 2.0

Figure 11-21 Enable Root User > Edit (Mac OS 10.5)



Step 8 Type a password for root to enable the root account. If you have not previously set a root password, an alert box may appear that says "NetInfo Error," indicating that the password is blank. Click **OK**.

Step 9 Type the root password you wish to use and click **Set**.

Step 10 Retype the password for verification and click **Verify**.

Step 11 The root user is now enabled.

Step 12 Click the lock again to prevent changes.

Note For additional reference, see http://docs.info.apple.com/article.html?artnum=106290#one.

For more information on the Mac OS X Agent, see the "Mac OS X Agent Dialogs" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Obtaining the Root Certificate from the CAS

Because Internet Explorer allows exporting of the CAS certificate, this section describes how to obtain the root certificate on a Windows system. Administrators can then transfer the certificate to their Mac via email as an attachment, FTP, or USB storage device.

There are three ways to retrieve the root certificate:

- Get the Root Certificate From the Mac OS X Agent Bundle
- Transfer the Root Certificate from Windows Using Internet Explorer
- Use Web Login to Get the Root Certificate

Get the Root Certificate From the Mac OS X Agent Bundle

Step 1 In the **Finder**, go to **/Applications/CCAAgent.app**.

Step 2 Ctrl-click on the **CCAAgent.app** to display the context menu.

Step 3 Choose **Show Package Contents** and search for the "perfigoca.crt" certificate in the **/Contents/Resources/** folder.

Step 4 Drag and drop the "perfigoca.crt" certificate to the keychain.

For more information, see SSL Requirements for Mac OS X/CAS Communication, page 11-23.

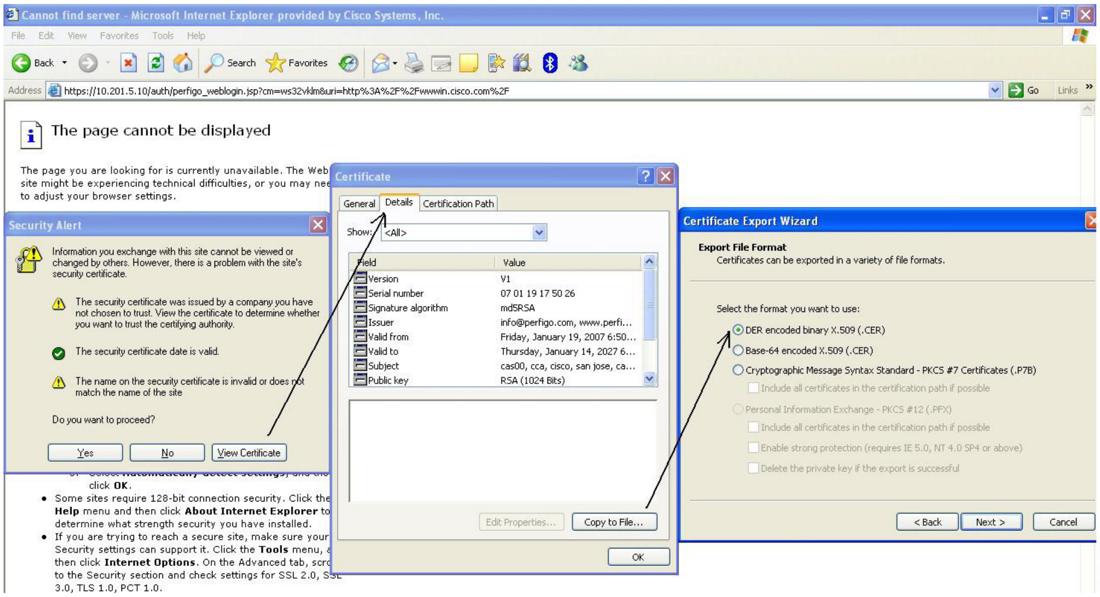
Transfer the Root Certificate from Windows Using Internet Explorer

If the temporary certificate has not yet been installed on the Windows system:

Figure 11-22 illustrates the steps to initially download the temporary certificate.

1. Open an IE browser and enter any address. The browser will redirect to the authentication page for web login.
2. Since the certificate has not been installed, the **Security Alert** dialog pops up from the browser. Click the **View Certificate** button in the **Security Alert** dialog.
3. Click the **Details** tab in the **Certificate** window that pops up.
4. Click the **Copy to File** button in the **Details** tab
5. Leave format option as **DER encoded binary x.509 (.CER)** on the **Certificate Export Wizard** and click **Next** to save the certificate on the Windows system.
6. Transfer the certificate to your Mac machine.

Figure 11-22 Download Certificate Option 1


Cannot find server - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Security Alert
Yes No View Certificate
Certificate
General Details Certification Path
Edit Properties... Copy to File...
OK
Certificate Export Wizard
< Back Next > Cancel
183745

https://10.201.5.10/auth/perfigo_weblogin.jsp?cm=ws32vklm&uri=http%3A%2F%2Fwwwin.cisco.com%2F

The page cannot be displayed

The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may nee to adjust your browser settings.

click **OK**.

- Some sites require 128-bit connection security. Click the **Help** menu and then click **About Internet Explorer** to determine what strength security you have installed.
- If you are trying to reach a secure site, make sure your Security settings can support it. Click the **Tools** menu, then click **Internet Options**. On the Advanced tab, scro to the Security section and check settings for SSL 2.0, SSL 3.0, TLS 1.0, PCT 1.0.

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Show: <All>

Field	Value
Version	V1
Serial number	07 01 19 17 50 26
Signature algorithm	md5RSA
Issuer	info@perfigo.com, www.perfi...
Valid from	Friday, January 19, 2007 6:50...
Valid to	Thursday, January 14, 2027 6...
Subject	cas00, cca, cisco, san jose, ca...
Public key	RSA (1024 Bits)

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

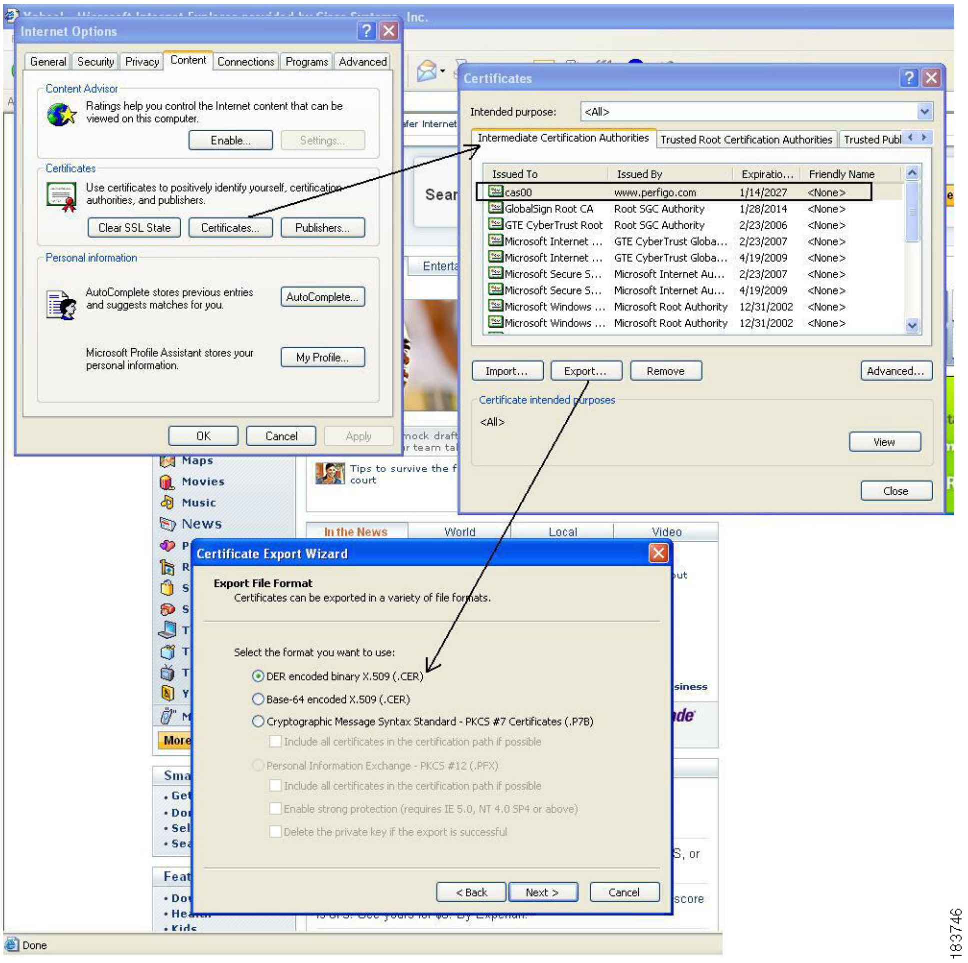
● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful

If the browser already has the temporary certificate installed:

Figure 11-23 illustrates the steps to download the certificate if already installed on the system.

1. Open the IE browser.
2. Go to **Tools > Internet Options**. Click the **Content** tab then the **Certificates** button.
3. Click the **Intermediate Root Certificate Authorities** tab in the **Certificates** window.
4. Highlight the certificate issued by **www.perfigo.com** and click the **Export** button.
5. Choose a location on your Windows machine to save the certificate.
6. Transfer the certificate to your Mac machine.

Figure 11-23 Download Certificate Option 2



Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
cas00	www.perfigo.com	1/14/2027	<None>
GlobalSign Root CA	Root SGC Authority	1/28/2014	<None>
GTE CyberTrust Root	Root SGC Authority	2/23/2006	<None>
Microsoft Internet ...	GTE CyberTrust Globa...	2/23/2007	<None>
Microsoft Internet ...	GTE CyberTrust Globa...	4/19/2009	<None>
Microsoft Secure S...	Microsoft Internet Au...	2/23/2007	<None>
Microsoft Secure S...	Microsoft Internet Au...	4/19/2009	<None>
Microsoft Windows ...	Microsoft Root Authority	12/31/2002	<None>
Microsoft Windows ...	Microsoft Root Authority	12/31/2002	<None>

<All>

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - □ Delete the private key if the export is successful

Use Web Login to Get the Root Certificate

Step 1 Change the CAM settings to enable the **Root CA Label** option (in the **Administration > User Pages > Login Page > Edit > Content** CAM web console configuration page). This shows the link to download the root certificate from the user login page in the browser.

Step 2 When users open a browser and go to the login page, they will see a link for downloading the root certificate. Instruct users to click on the link and save the "perfigoca.crt" certificate on their local client machine.

Step 3 Obtain the certificate from the user and drag and drop the "perfigoca.crt" certificate to the keychain.

For more information, see the guidelines "Administering the CAM" chapter in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)*.

Troubleshooting Certificate Issues

There can be issues with Cisco NAC Appliance certificate management 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 troubleshooting topics:

- HA Active-Active Situation Due to Expired SSL Certificates
- CAS Cannot Establish Secure Connection to CAM
- Private Key in Clean Access Server Does Not Match the CA-Signed Certificate
- Certificate-Related Files

Warning **If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

HA Active-Active Situation Due to Expired SSL Certificates

HA communication for both HA-CAMs and HA-CASs is handled over IPSec tunnels to secure all communications between the two HA pair appliances. This IPSec tunnel is negotiated based on the SSL certificates uploaded to the HA pairs for both CAM and CAS. In case the SSL certificates are not trusted by the two HA peers, have expired, or are no longer valid, the HA heartbeat communication between the two HA pairs breaks down, leading both HA pair appliances to assume the Active HA-Primary) role.

For CASs deployed in VGW mode, this can potentially create a Layer 2 loop that could bring down the network. HA-CAMs with expired or invalid SSL certificates could lead to an Active-Active situation where the database is not synced between the two HA-CAM appliances. Eventually, this situation leads to the CAMs losing all recent configuration changes and/or all recent user login information following an HA-CAM failover event.

As CAM-CAS communication over IPSec tunnels requires valid SSL certificates on both the CAM and CAS, the CAM-CAS communication also breaks down if the SSL certificate expires on either the CAM or CAS. This situation leads to end user authentications failures and the CAS reverting to failback mode per CAS configuration.

Administrators can minimize HA appliance Active-Active situations due to expired SSL certificates by using SSL certificates with longer validity periods and/or using serial port connection (if available and not used to control another CAM or CAS) for HA heartbeat. However, when you configure HA-CAMs to perform heartbeat functions over the serial link and the primary eth1 interface fails because of SSL certificate expiration, the CAM returns a database error indicating that it cannot sync with its HA peer and the administrator receives a “WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!” error message in the CAM web console:

Note Starting with Cisco NAC Appliance Release 4.8, the CAM or CAS generates event log messages to indicate the certificate expiry in addition to the message displayed in the CAM/CAS web console.

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>," 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 11-35)
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.

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, Cisco recommends backing up the existing caCerts file from /usr/java/j2sdk1.4/lib/security/caCerts, overriding it with the file from /perfigo/common/conf/caCerts, then performing "service perfigo restart" on the CAS.

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.

Certificate-Related Files

For troubleshooting purposes, Table 11-1 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 11-1 Clean Access Server Certificate-Related Files

File	Description
/root/.tomcat.key	Private key
/root/.tomcat.crt	Certificate

Table 11-1 Clean Access Server Certificate-Related Files (continued)

File	Description
/root/.tomcat.req	Certificate Signing Request
/root/.chain.crt	Intermediate certificate
/root/.perfigo/caCerts	The root CA bundle

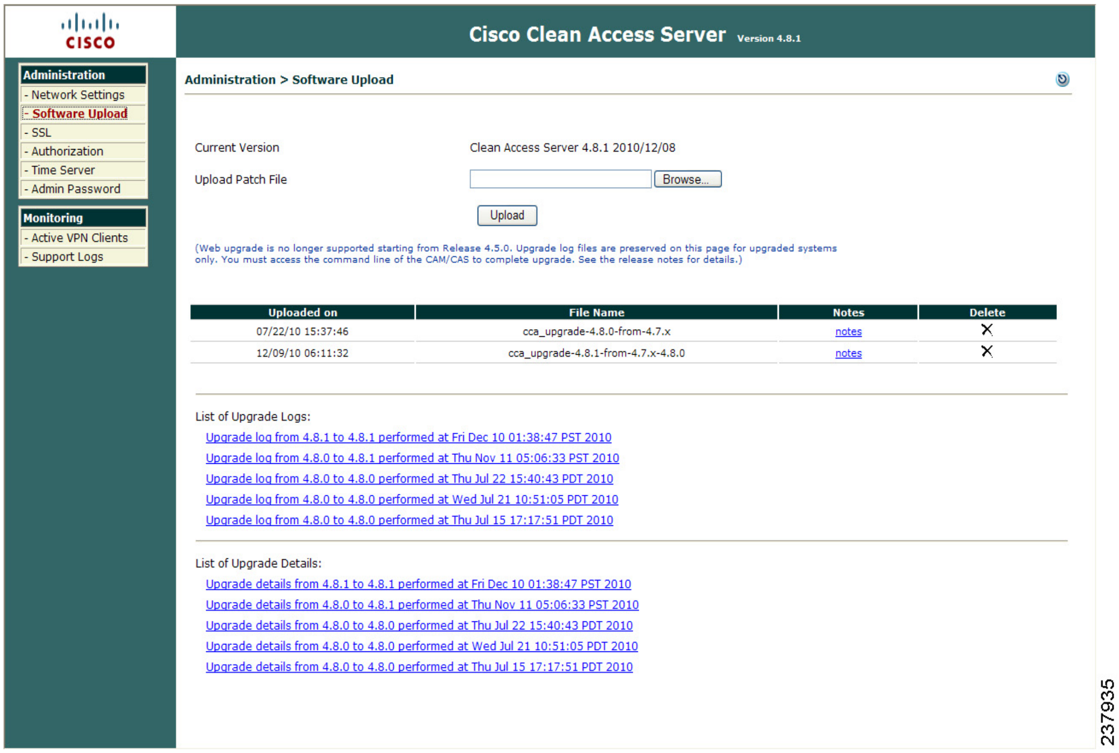
System Upgrade

In Cisco NAC Appliance Release 4.8(1), you can perform system upgrades from Release 4.6(1) and 4.7(x) by uploading a .tar.gz upgrade file to the CAM/CAS and executing an upgrade script using the appliance’s CLI. For complete upgrade details, including instructions for upgrading HA CASs and upgrades via SSH, refer to the “Upgrading” section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*.

You can use the CAS web console to upload Release 4.8(1) .tar.gz upgrade files, and view upgrade logs and upgrade details.

Step 1 Access the CAS software update web console page by navigating to **Administration > Software Upload** (Figure 11-24).

Figure 11-24 CAS Administration > Software Upload



Current Version: Clean Access Server 4.8.1 2010/12/08

Upload Patch File

(Web upgrade is no longer supported starting from Release 4.5.0. Upgrade log files are preserved on this page for upgraded systems only. You must access the command line of the CAM/CAS to complete upgrade. See the release notes for details.)

Uploaded on	File Name	Notes	Delete
07/22/10 15:37:46	cca_upgrade-4.8.0-from-4.7.x	notes	✕
12/09/10 06:11:32	cca_upgrade-4.8.1-from-4.7.x-4.8.0	notes	✕

List of Upgrade Logs:

- Upgrade log from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
- Upgrade log from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010
- Upgrade log from 4.8.0 to 4.8.0 performed at Thu Jul 22 15:40:43 PDT 2010
- Upgrade log from 4.8.0 to 4.8.0 performed at Wed Jul 21 10:51:05 PDT 2010
- Upgrade log from 4.8.0 to 4.8.0 performed at Thu Jul 15 17:17:51 PDT 2010

List of Upgrade Details:

- Upgrade details from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
- Upgrade details from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010
- Upgrade details from 4.8.0 to 4.8.0 performed at Thu Jul 22 15:40:43 PDT 2010
- Upgrade details from 4.8.0 to 4.8.0 performed at Wed Jul 21 10:51:05 PDT 2010
- Upgrade details from 4.8.0 to 4.8.0 performed at Thu Jul 15 17:17:51 PDT 2010

Step 2 If you have downloaded a Release 4.8(1) .tar.gz upgrade image to your local machine from the Cisco Software Download Site as described in the “Upgrading” section of the *Release Notes for Cisco NAC Appliance, Version 4.8(1)*, you can use this web console page to upload that image to the CAS.

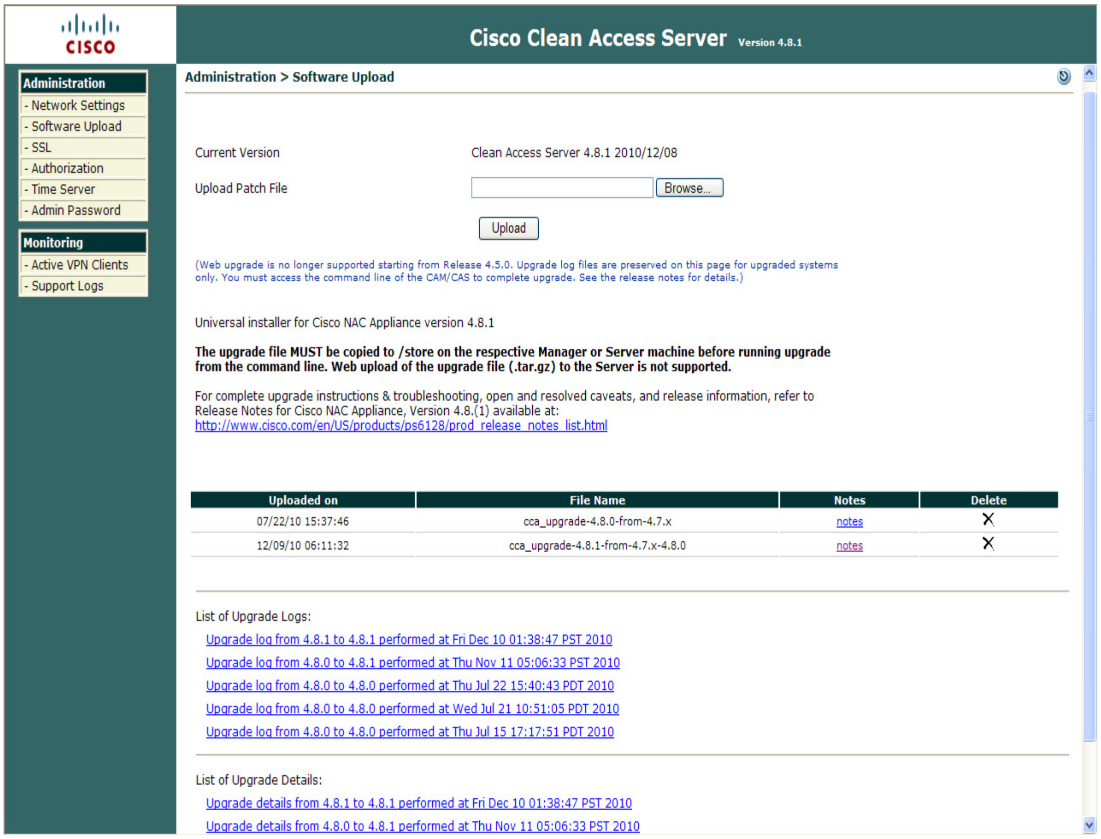
a. Click **Browse** to navigate to the directory on your local machine where you have stored the Release 4.8(1) .tar.gz upgrade file. Depending on the Cisco NAC Appliance release from which you are upgrading, the upgrade image name is one of the following:

- If upgrading from Release 4.6(1)—**cca_upgrade-4.8.1-from-4.6.x.tar.gz**
- If upgrading from Release 4.7(x) or 4.8—**cca_upgrade-4.8.1-from-4.7.x-4.8.0.tar.gz**

b. Click **Upload**. After a brief time, the web console screen automatically refreshes, displaying the newly uploaded Release 4.8(1) upgrade image and the date/time when it was uploaded to the CAS.

Step 3 Once you upload a Release 4.8(1) upgrade image to the CAS, you can also use the **Notes** link that appears after the image file name to view important information about the .tar.gz upgrade image and access a link to the *Release Notes for Cisco NAC Appliance, Version 4.8(1)* (Figure 11-25).

Figure 11-25 CAS Administration > Software Upload > Notes



Administration > Software Upload

Current Version: Clean Access Server 4.8.1 2010/12/08

Upload Patch File

(Web upgrade is no longer supported starting from Release 4.5.0. Upgrade log files are preserved on this page for upgraded systems only. You must access the command line of the CAM/CAS to complete upgrade. See the release notes for details.)

Universal installer for Cisco NAC Appliance version 4.8.1

The upgrade file MUST be copied to /store on the respective Manager or Server machine before running upgrade from the command line. Web upload of the upgrade file (.tar.gz) to the Server is not supported.

For complete upgrade instructions & troubleshooting, open and resolved caveats, and release information, refer to Release Notes for Cisco NAC Appliance, Version 4.8.(1) available at:
http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html

Uploaded on	File Name	Notes	Delete
07/22/10 15:37:46	cca_upgrade-4.8.0-from-4.7.x	notes	✕
12/09/10 06:11:32	cca_upgrade-4.8.1-from-4.7.x-4.8.0	notes	✕

List of Upgrade Logs:

Upgrade log from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
Upgrade log from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010
Upgrade log from 4.8.0 to 4.8.0 performed at Thu Jul 22 15:40:43 PDT 2010
Upgrade log from 4.8.0 to 4.8.0 performed at Wed Jul 21 10:51:05 PDT 2010
Upgrade log from 4.8.0 to 4.8.0 performed at Thu Jul 15 17:17:51 PDT 2010

List of Upgrade Details:

Upgrade details from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
Upgrade details from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010

Step 4 To view upgrade log information, click on the link under **List of Upgrade Logs** to launch a browser window displaying a brief summary of the upgrade process including the date and time the upgrade was performed.

Step 5 To view important upgrade process details, click on the link under **List of Upgrade Details** to launch a browser window displaying the details of the upgrade process, in the following format:

- State before upgrade
- Upgrade process details

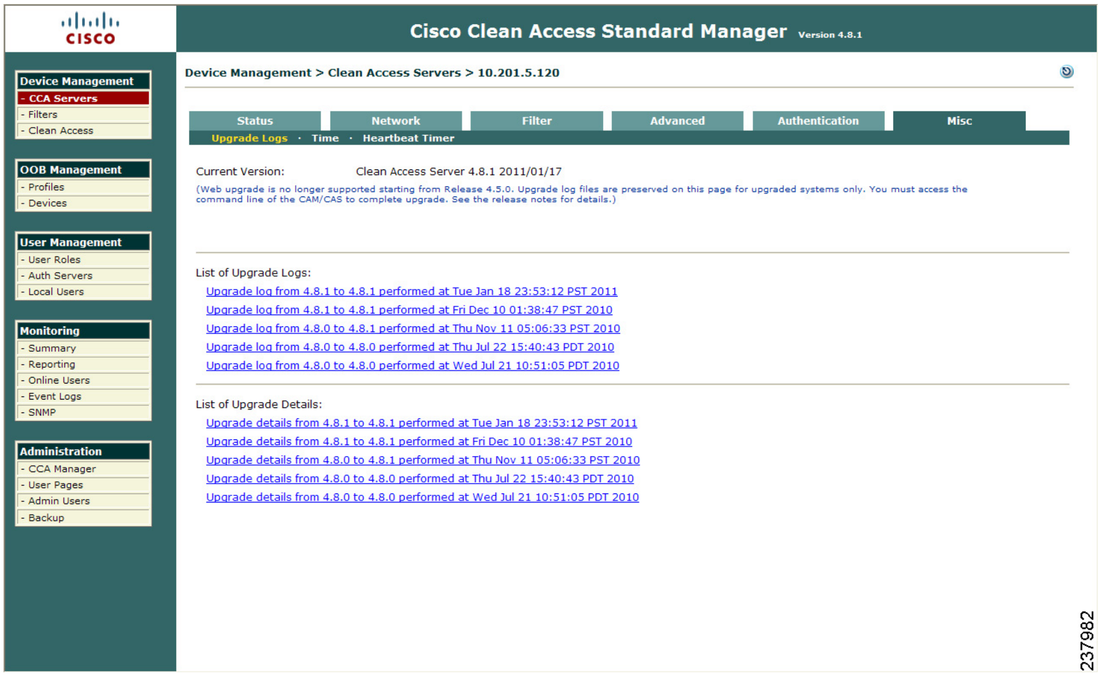
- State after upgrade

It is normal for the “state before upgrade” to contain several warning/error messages (e.g. “INCORRECT”). The “state after upgrade” should be free of any warning or error messages.

You can also use the CAM web console **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Upgrade Logs** page (Figure 11-26) to view the CAS software upgrade notes:

- Click on the link under **List of Upgrade Logs** to display a brief summary of the upgrade process including the date and time it was performed.
- Click on the link under **List of Upgrade Details** to display the details of the upgrade process, in the following format:

Figure 11-26 CAS Upgrade Logs from CAM Web Console



Current Version: Clean Access Server 4.8.1 2011/01/17

(Web upgrade is no longer supported starting from Release 4.5.0. Upgrade log files are preserved on this page for upgraded systems only. You must access the command line of the CAM/CAS to complete upgrade. See the release notes for details.)

List of Upgrade Logs:

Upgrade log from 4.8.1 to 4.8.1 performed at Tue Jan 18 23:53:12 PST 2011
Upgrade log from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
Upgrade log from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010
Upgrade log from 4.8.0 to 4.8.0 performed at Thu Jul 22 15:40:43 PDT 2010
Upgrade log from 4.8.0 to 4.8.0 performed at Wed Jul 21 10:51:05 PDT 2010

List of Upgrade Details:

Upgrade details from 4.8.1 to 4.8.1 performed at Tue Jan 18 23:53:12 PST 2011
Upgrade details from 4.8.1 to 4.8.1 performed at Fri Dec 10 01:38:47 PST 2010
Upgrade details from 4.8.0 to 4.8.1 performed at Thu Nov 11 05:06:33 PST 2010
Upgrade details from 4.8.0 to 4.8.0 performed at Thu Jul 22 15:40:43 PDT 2010
Upgrade details from 4.8.0 to 4.8.0 performed at Wed Jul 21 10:51:05 PDT 2010

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 SSL certificate. The time set on the user machine must fall within the creation date /expiry date range set on the CAS 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 11-2 and the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* for details.

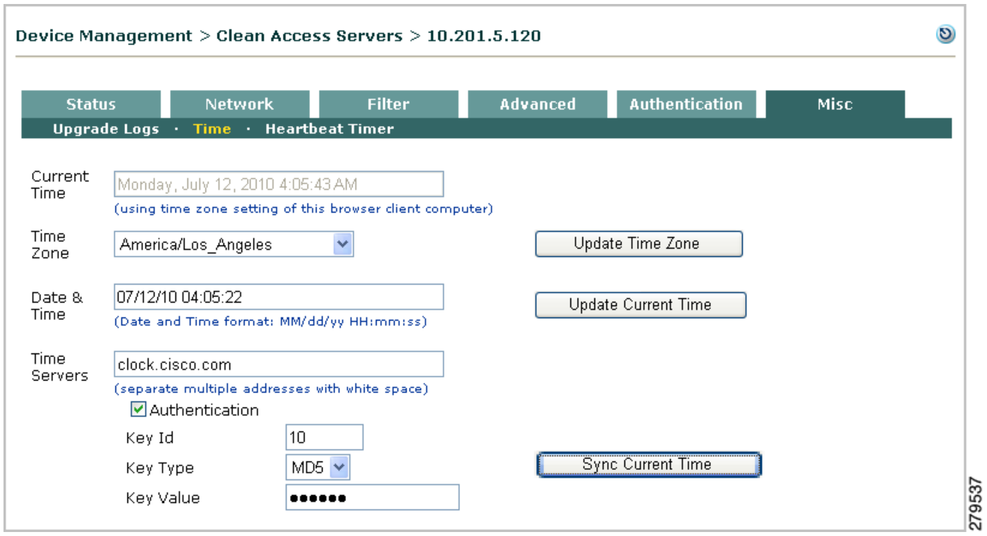
The time can be modified on the CAM under **Administration > CCA Manager > System Time**. See the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(1)* for details.

To view the current time:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time**.

Step 2 The system time for the Clean Access Server appears in the **Current Time** field.

Figure 11-27 Time Form



Current Time: Monday, July 12, 2010 4:05:43 AM
(using time zone setting of this browser client computer)

Time Zone: America/Los_Angeles

Date & Time: 07/12/10 04:05:22
(Date and Time format: MM/dd/yy HH:mm:ss)

Time Servers: clock.cisco.com
(separate multiple addresses with white space)

☑ Authentication

Key Id: 10

Key Type: MD5

Key Value: ●●●●●●

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:

Go to the **Time** form of the **Misc** tab and perform one of the following steps:

- 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.
- 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. If you want to authenticate the server to get the time, check the **Authentication** checkbox to enable NTP authentication. Once this option is enabled, you will be able to enter the following:
   - **Key Id**—Specify a key number.
   - **Key Type**—Currently, only MD5 is supported. The key type **MD5** specifies that message authentication support is provided by using the Message Digest 5 hashing algorithm.
   - **Key Value**—For MD5 authentication, this is a password consisting of a string of one to eight characters. If the string is longer than eight characters, only the first eight will be used.

   Note The NTP Authentication is not available for FIPS-compliant CAMs/CASs.

3. Click **Sync 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.

Note If the NTP Authentication has been enabled, the same Key Id, Key Type, and Key value are used for all the servers.

The CAS then automatically synchronizes the 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 11-28) allow you to configure the level of log detail recorded for troubleshooting purposes in **/perfigo/access/tomcat/logs/nac_server.log**. These web controls are intended as alternatives to using the CLI `loglevel` command to gather system information when troubleshooting.

For normal operation, the log level should always remain at the default setting (**INFO**). 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 **INFO** to **DEBUG** for a specific interval, then reset to **INFO** 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 (**INFO**).

Note Cisco recommends using the **DEBUG** and **TRACE** options only temporarily for very specific issues. Although the CAM records logging information and stores them in a series of nine 20MB files before discarding any old logs, the large amount of logging information can cause the CAM to run out of available log storage space in a relatively short amount of time.

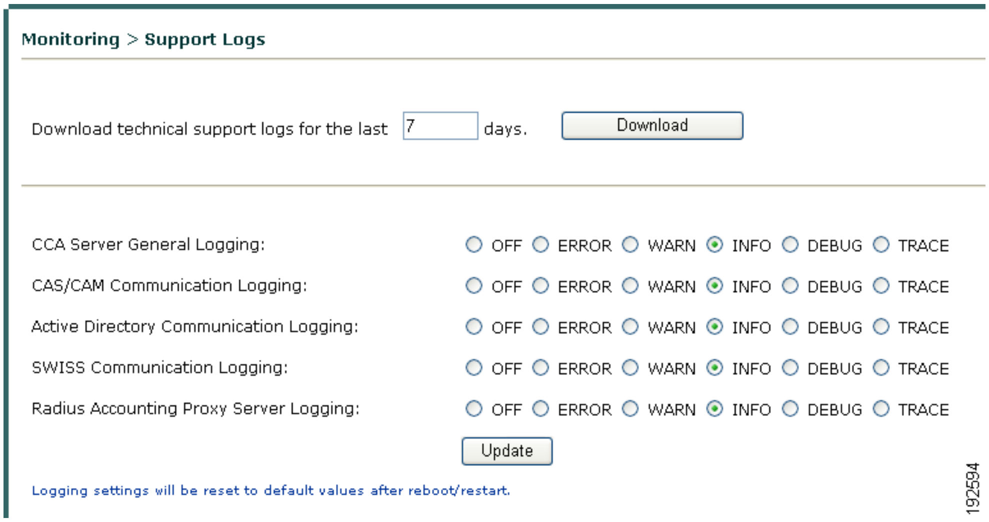
Note To optimize memory usage, CAS support logs page are only available from the CAS direct access console under "Monitoring." (They are not available from the CAS management pages.)

Downloading CAS Support Logs

Step 1 Open the CAS direct access console from a browser using **https://<CAS_eth0_IP_address>/admin** as the URL/Address.

Step 2 Go to **Monitoring > Support Logs** (Figure 11-28).

Figure 11-28 CAS Support Logs



Monitoring > Support Logs

Download technical support logs for the last 7 days. [Download]

CCA Server General Logging: ○ OFF ○ ERROR ○ WARN ● INFO ○ DEBUG ○ TRACE

CAS/CAM Communication Logging: ○ OFF ○ ERROR ○ WARN ● INFO ○ DEBUG ○ TRACE

Active Directory Communication Logging: ○ OFF ○ ERROR ○ WARN ● INFO ○ DEBUG ○ TRACE

SWISS Communication Logging: ○ OFF ○ ERROR ○ WARN ● INFO ○ DEBUG ○ TRACE

Radius Accounting Proxy Server Logging: ○ OFF ○ ERROR ○ WARN ● INFO ○ DEBUG ○ TRACE

[Update]

Logging settings will be reset to default values after reboot/restart.

Step 3 Specify the number of days of debug messages to include in the file you will download for your Cisco customer support request.

Step 4 Click the **Download** button to download the **cas_logs.<CAS_IP_address>.tar.gz** file to your local computer.

Step 5 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 Configuration Guide, Release 4.8(1)* for details.

If requested to do so by the TAC engineer, you can temporarily change the loglevel to obtain more troubleshooting details prior to downloading the support logs.

To changing the LogLevel for CAS logs:

Step 1 Open the CAS direct access console (**https://<CAS_eth0_IP_address>/admin**).

Step 2 Go to **Monitoring > Support Logs**.

Step 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.
- **Active Directory Communication Logging**: This category contains logging information involving Active Directory events to support user Single Sign-On and credential look-up.
- **SWISS Communication Logging**: This category contains log events related to SWISS (proprietary communication protocol) packets sent between this CAS and the Agent.

Note To discover the CAS, the Agent sends SWISS (proprietary CAS-Agent communication protocol) packets on UDP port 8905 for Layer 2 users and port 8906 for Layer 3 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 Layer 3 support is enabled. The Agent performs SWISS discovery every 5 seconds by default.

- **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.

Step 4 Click the LogLevel setting for the category of log:

- **OFF**: No log events are recorded for this category.
- **ERROR**: A log event is written to /perfigo/access/tomcat/logs for the CAS, and /perfigo/control/tomcat/logs for the CAM only if the system encounters a severe error, such as:
  - CAS cannot connect to CAM
  - CAS and CAM cannot communicate
  - CAS cannot communicate with database
- **WARN**: Records only error and warning level messages for the given category.
- **INFO**: Provides more details than the **ERROR** and **WARN** log levels. For example, if a user logs in successfully an Info message is logged. This is the default level of logging for the system.
- **DEBUG**: Records all debug-level logs for the CAS.

- **TRACE**: This is the maximum amount of log information available to help troubleshoot issues with the CAM/CAS.

Note Cisco recommends using the **DEBUG** and **TRACE** options only temporarily for very specific issues. Although the CAM records logging information and stores them in a series of nine 20MB files before discarding any old logs, the large amount of logging information can cause the CAM to run out of available log storage space in a relatively short amount of time.

Change the LogLevel Setting through CLI

The Loglevel setting can be changed using the CLI.

Command Syntax to change loglevel setting on the CAS:

```
[root@cas2 bin]# cd /perfigo/control/bin
[root@cas2 bin]# ./loglevel
Usage: loglevel LOG_NAME (OFF | ERROR | WARN | INFO | DEBUG | TRACE )
[root@cas2 bin]#
```

LOG_NAME is the parameter used to set the CAS log category to be changed.

Example:

```
./loglevel com.perfigo TRACE
```

The above command sets the “CCA Server General Logging” category to the “TRACE” loglevel.

Table 11-2 lists the values used for the “LOG_NAME” parameter and the corresponding GUI setting log categories for CAS.

Table 11-2 Log Names for CAS

Log Name	GUI Setting Log Category
com.perfigo	CCA Server General Logging
com.perfigo.wlan.jmx	CAS/CAM Communication Logging
com.perfigo.wlan.jmx.adsso	Active Directory Communication Logging
com.perfigo.wlan.jmx.swiss	SWISS Communication Logging
com.perfigo.wlan.radius	RADIUS Accounting Proxy Server Logging

Note The log level setting provided in the CLI command is case sensitive.

APPENDIX A

Open Source License Acknowledgements

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

INDEX

A

AD SSO Configuration Steps for CAM, CAS, and AD Server 8-5

AD SSO Overview 8-1

ARP, configuring 4-31

B

Bandwidth

- limiting usage 7-14

bursting 7-14

C

cached ARP, flushing 4-32

calculating subnets (DHCP) 5-10

certificate. See SSL certificate.

Clean Access

- shared devices 10-4

Clean Access Server management pages 1-6

connection checking, user 9-1

CSR, generating 11-14

D

deployment

- operating mode, choosing 2-1

DHCP

- configuring 5-2 to 5-23
- creating pools 5-8
- overview 5-1
- relay 5-3
- relay status 11-2

DNS settings 4-24

F

filter policies 7-1 to 7-16

- IP address 4-43
- MAC address 4-39
- subnet, specifying by 4-43

floating devices 10-4

flushing cached ARP 4-32

fragmentation, IP packet 7-5

G

generating DHCP pools 5-10

global settings 1-7

H

heartbeat timer 9-1

I

interface settings 4-11

IP address

- filtering by 4-43
- reserved 5-22

IP address, configuring the server 4-12, 4-13

IP filter status 11-2

IP fragment packets 7-5

IPSec server status 11-2

L

local settings 1-7
login page 9-3

M

MAC address filter policies 4-39

O

operating modes
- overview 2-1 to 2-8
- Real-IP gateway 2-2
- virtual gateway 2-2

P

passthrough, VLAN ID 4-33

R

real-IP gateway
- overview 2-2

reserved IP addresses 5-22
roles, user
- assignment priority 4-39
- default policies 7-2

routes, static 4-29

S

shared devices 10-4
SSL Certificate
- Certificate-Related Files 11-32
- overview 11-6

SSL certificate
- exporting CSR 11-14

static route, using 4-29
status tab 11-1
subnet, managing access 4-43
subnetting rules 5-6

T

time, system 11-35
timing out users 9-1
transparent Windows login 9-8

U

users
- time-out settings 9-1
- windows login 9-8

V

virtual gateway
- overview 2-2

VLAN settings
- overview 4-32

W

Windows login 9-8